Pure and Applied Mathematics Quarterly
Volume 5, Number 1
(*Special Issue: In honor of
Jean-Pierre Serre, Part 2 of 2*)
81—125, 2009

Serre's Conjecture and Base Change for $GL(2)$

Haruzo Hida

Dedicated to Professor J.-P. Serre on the occasion of his 80th birthday.

Abstract: In this paper, for an odd cyclic totally real extension $F/\mathbb{Q}$, assuming Serre's modularity conjecture of 2-dimension odd mod p Galois representations, we give an elementary proof of the Langlands base change from a space of automorphic forms on the multiplicative group of a definite quaternion algebra $B_{/\mathbb{Q}}$ to the corresponding space on the multiplicative group of $B_F = B \otimes_{\mathbb{Q}} F$ (under some mild assumptions). More generally, for a general totally real Galois extension, we state a conjecture describing the action of $\mathrm{Gal}(F/\mathbb{Q})$ on the 0-dimensional automorphic variety of $B_F^\times$ which implies the existence of base-change relative to $F/\mathbb{Q}$.
Keywords: Serres mod p modularity conjecture, Hecke algebra, base-change, permutation representation

Contents

Received July 3, 2006.
The author is partially supported by the NSF grant: DMS 0244401, DMS 0456252 and DMS 0753991.

1. Introduction

For a totally definite quaternion algebra $B = B_{\mathbb{Q}}$ over $\mathbb{Q}$, we consider the associated algebraic $\mathbb{Q}$-group G defined by $G(A) = (B \otimes_{\mathbb{Q}} A)^\times$ for commutative $\mathbb{Q}$-algebras A. For a totally real finite Galois extension $F/\mathbb{Q}$ with Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, the quotient space $G(F)\backslash G(F_{\mathbb{A}})/U \cdot G(\mathbb{R})$ for an open compact subgroup $U \subset G(F_{\mathbb{A}}^{(\infty)})$ is a finite set of points on which Δ acts through its action on $G(F_{\mathbb{A}})$ if U is stable under Δ. We present in this paper an elementary conjecture (Conjecture 1.2) on this permutation representation which (together with Serre's modularity conjecture) implies the existence of base-change of elliptic modular forms to Hilbert modular forms over F (under certain conditions on level and Nében characters and the cohomological structure of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$). Moreover, we prove the conjecture for any cyclic groups.

We fix a definite quaternion algebra $B = B_{\mathbb{Q}}$ over $\mathbb{Q}$ with a fixed maximal order R. Write Z for the center of G. We have the reduced norm map $N : G_{/\mathbb{Q}} \to \mathbb{G}_{m/\mathbb{Q}}$. We define $G_{1/\mathbb{Q}} = \mathrm{Ker}(N)$, which is the derived group of $G_{/\mathbb{Q}}$. We put $B_F = B \otimes_{\mathbb{Q}} F$. Assuming that $B \otimes_{\mathbb{Q}} F_{\mathfrak{l}}$ is a division algebra at a prime ideal $\mathfrak{l}$ if and only if $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a division algebra at $(\ell) = \mathfrak{l} \cap \mathbb{Z}$, we can take a maximal order R_F stable under the action of Δ with $H^0(\Delta, R_F) = R$ in B. Let Σ_{st} be a set of prime ideals $\mathfrak{q}$ of O for which $B_{\mathfrak{q}} = B \otimes_{\mathbb{Q}} F_{\mathfrak{q}}$ is a division algebra. We identify $R_\ell = R_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ with $M_2(O_\ell)$ for all rational primes ℓ outside Σ_{st} (as rings and as Δ-modules), where $O_{\mathfrak{l}} = \varprojlim_n O/\mathfrak{l}^n$ and $O_\ell = \varprojlim_n O/\ell^n O$. Then for an integral ideal $\mathfrak{N}$ outside Σ_{st}, consider an open compact subgroup

$$U = U_0(\mathfrak{N} \cdot d(B_F)) = \left\{ x \in \widehat{R}_F^\times \middle| x_{\mathfrak{N}} \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \right\} \subset G(F_{\mathbb{A}}^{(\infty)}),$$

where $\widehat{R}_F = \varprojlim_n R_F/nR_F$ with n running through positive integers, $F_{\mathbb{A}}^{(\infty)}$ is the ring of finite adeles of F, $d(B_F) = \prod_{\mathfrak{q}\in\Sigma_{st}} \mathfrak{q}$ and $x_{\mathfrak{N}}$ is the projection of x to $R_{\mathfrak{N}} = \varprojlim_n R/\mathfrak{N}^n$. Write $\widehat{O} = \varprojlim_n O/nO$ for n running through all positive integers. Let $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon^-, \varepsilon_+)$ be a set of four continuous finite order characters $\varepsilon_j : \widehat{O}^\times \to \mathbb{C}^\times$, $\varepsilon^- = \varepsilon_2^{-1}\varepsilon_1$, $\varepsilon_+ : F_{\mathbb{A}}^\times/F^\times \to \mathbb{C}^\times$ with $\varepsilon_+(a) = \varepsilon_1(a)\varepsilon_2(a)$ for $a \in \widehat{O}^\times$. Then if the conductor $\mathfrak{c}(\varepsilon^-)$ of ε^- is a factor of $\mathfrak{N}$, we have a character $\underline{\varepsilon} : U \to \mathbb{C}^\times$ given by $\underline{\varepsilon}(zu) = \varepsilon_+(z)\varepsilon^-(a_{\mathfrak{N}})\varepsilon_2(N(u))$ for $u \in U$ and $z \in Z(F_{\mathbb{A}}^{(\infty)})$. We consider the space $\mathcal{M}_F(\varepsilon)$ of automorphic forms $f : G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}) \to \mathbb{C}$ satisfying $f(xzu) = \varepsilon_+(z)\underline{\varepsilon}(u)f(x)$ for $z \in Z(F_{\mathbb{A}}^{(\infty)})$ and $u \in U_0(\mathfrak{c}(\varepsilon^-)d(B_F))$ (this space was originally introduced in [HMI] Section 3.1 and in some of my earlier papers). For each principal local representation $\pi_v = \pi(\alpha, \beta)$ of $GL_2(F_v)$ for a place v, take $\varepsilon_v = (\alpha|_{O_v^\times}, \beta|_{O_v^\times}, \beta^{-1}\alpha|_{O_v^\times}, \alpha\beta)$. Then there is a unique 1-dimensional subspace $V(\alpha, \beta)$ made up of vectors satisfying $\pi_v(zu)v = \varepsilon_+(z)\underline{\varepsilon}(u)v$. Such a vector is called a minimal vector of π_v. Thus the Hecke eigenforms in $\mathcal{M}_F(\varepsilon)$ is in bijection (up to scalar multiple) with isomorphism classes of locally principal (outside $d(B_F)$) automorphic representations with given Neben types ε, and we expect them to be in bijection with compatible systems of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ with ramification data governed by ε and $d(B_F)$. Indeed, an appropriate p-adic Galois deformation ring with ramification governed by ε and $d(B_F)$ is identified with a local ring of the p-adic Hecke algebra of $\mathcal{M}_F(\varepsilon)$ in the work of Fujiwara ([F1], [F2] and [HMI] Chapter 3). In this sense, $\mathcal{M}_F(\varepsilon_F)$ has a more direct connection to compatible systems than the (slightly undeveloped) space introduced earlier in [H88] (based on the theory of new forms rather than minimal forms).

Let $\varepsilon_{\mathbb{Q}}$ be the character as above for $F = \mathbb{Q}$, and we define ε_F by the pull back of $\varepsilon_{\mathbb{Q}}$ via the norm map $N_{F/\mathbb{Q}}$. We shall prove the following theorem.

Theorem 1.1. *Let $F/\mathbb{Q}$ be a totally real finite simply 2-connected Galois extension. Suppose* Conjecture 1.2 *following this theorem and Serre's conjecture on mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *for all sufficiently large odd primes p outside the level $N = \mathfrak{c}(\varepsilon_{1,\mathbb{Q}})\mathfrak{c}(\varepsilon_{2,\mathbb{Q}})d(B_{\mathbb{Q}})$. In addition to this assumption, we assume*

(R1) *$B_{\mathbb{Q}} \otimes_{\mathbb{Q}} F_{\mathfrak{l}}$ is a division algebra for every prime factor $\mathfrak{l}$ of $d(B_{\mathbb{Q}})$;*
(R2) *$q|d(B_{\mathbb{Q}})$ if a prime q ramifies in $F/\mathbb{Q}$.*

Let π be the infinite dimensional automorphic representation π of $G(\mathbb{A})$ associated to a Hecke eigenform in $\mathcal{M}_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}})$. Write $\rho = \{\rho_{\mathfrak{l}}\}_{\mathfrak{l}}$ for the strictly compatible system (associated to π) of $\mathfrak{l}$-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in the Hecke field T of π. Then, we have a base-change automorphic representation $\widehat{\pi}$ on $G(F_{\mathbb{A}})$ whose strictly compatible system of Galois representations is isomorphic to the restriction of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ and $\widehat{\pi}$ is generated by a Hecke eigenform in $\mathcal{M}_F(\varepsilon_F)$.

Here are some remarks about the theorem:

(1) We call a Galois extension F/E simply 2-connected if $H^j(\mathrm{Gal}(F/E), \mu_2) = 0$ for $j = 1, 2$ (with $\mu_2 = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ on which $\mathrm{Gal}(F/E)$ acts **trivially**). A finite group Γ is called simply 2-connected if $H^j(\Gamma, \mu_2) = 0$ for $j = 1, 2$, where Γ acts **trivially** on μ_2. By a result of Steinberg, for all simply-connected simple Chevalley groups $G_{/\mathbb{Z}}$, the group $G(\mathbb{F}_q)$ for the finite field $\mathbb{F}_q$ of q-elements is simply 2-connected except for the 8 specific exceptional cases ([St1] Theorem 1.1). In particular, if $q > 4$ or q is odd, $G(\mathbb{F}_q)$ is simply 2-connected. See Section 7 for an almost complete list of simply 2-connected simple groups.

(2) C. Khare proved in [Kh] Serre's conjecture in the level 1 case. Since [KW] Theorem 1.2 went farther and announced a proof of Serre's conjecture under a hypothesis in the even conductor case which has been removed by Kisin [Ki] (and Conjecture 1.2 is proven in this paper in the cyclic case; see Proposition 2.5), the theorem will be valid (in due course) under the conditions (R1–2) without assuming any conjectural statements for odd cyclic extensions $F/\mathbb{Q}$, giving a new proof of the base-change theorem of Langlands from $\mathbb{Q}$ to odd cyclic extensions without using much harmonic analysis. By using congruence argument, we can also make base-change to $F/\mathbb{Q}$ of any everywhere principal elliptic cusp form without assuming the division property of $B_{\mathbb{Q}} \otimes_{\mathbb{Q}} F_{\mathfrak{l}}$ for $\mathfrak{l}|d(B_{\mathbb{Q}})$ (see Remark 6.1). We can also prove a similar result for elliptic cusp forms of higher weight as long as π is ordinary for a sufficiently large prime ℓ. These more general results will be discussed in our subsequent paper. We also hope to be able to treat automorphic representations which have supercuspidal local components at some finite places in our future work. Here a Hecke eigenform $f \in \mathcal{M}(\varepsilon_{\mathbb{Q}})$ with $f|T(p) = a_\ell f$ is called ordinary at a prime ℓ

if there exists an embedding $i : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ such that the image $i(a_\ell)$ is an ℓ-adic unit ($\Leftrightarrow |i(a_\ell)|_\ell = 1$). An irreducible automorphic representation π is called ordinary at ℓ if it is generated by a Hecke eigenform ordinary at ℓ.

Now we introduce some more symbols to state the conjecture we mentioned in the theorem. The reduced norm map induces $N : G(F_{\mathbb{A}}^{(\infty)}) \to F_{\mathbb{A}}^{(\infty)\times}$ and $N : G(F) \to F_+^\times$ (for the subgroup $F_+^\times$ of $F^\times$ of totally positive elements), and we consider the pull back image $\mathbb{G} = N^{-1}(F_+^\times (F_{\mathbb{A}}^{(\infty)\times})^2 \widehat{O}^\times)$, which can be written as $\mathbb{G} = G(F)G_1(F_{\mathbb{A}}^{(\infty)})Z(F_{\mathbb{A}}^{(\infty)})U$ for $G_1 = \mathrm{Ker}(N : G \to \mathbb{G}_m)$, where $Z \subset G$ is the center of G. Put $\mathcal{M}_F^{(1)}(\varepsilon) := \{f|_{\mathbb{G}} | f \in \mathcal{M}_F(\varepsilon)\}$. Decomposing $UxU \subset \mathbb{G}$ into $\bigsqcup_{\alpha\in\Omega} \alpha U$, we have a Hecke operator $[UxU]$ acting on $\mathcal{M}_F^{(1)}(\varepsilon)$ by $f|[UxU](g) = \sum_{\alpha\in\Omega} f(g\alpha)$. Let $h_F(\varepsilon) \subset \mathrm{End}_{\mathbb{C}}(\mathcal{M}_F^{(1)}(\varepsilon))$ be the $\mathbb{C}$-subalgebra generated by $[UxU]$ for $x \in \mathbb{G}$ with $x_{\mathfrak{q}} = 1$ for $\mathfrak{q}|d(B_F)\mathfrak{c}(\varepsilon_1)\mathfrak{c}(\varepsilon_2)$. Then $h_F(\varepsilon)$ is a semisimple commutative algebra of finite dimension over $\mathbb{C}$ whose dimension is equal to $\dim_{\mathbb{C}} \mathcal{M}_F^{(1)}(\varepsilon)$. Since $B_F = B \otimes_{\mathbb{Q}} F$, Δ acts on B_F by $(x \otimes \xi)^\sigma = x \otimes \xi^\sigma$ for $\xi \in F$ and $x \in B$, and this action extends to $G(F_{\mathbb{A}}^{(\infty)})$ with the set of Δ-fixed points given by $G(\mathbb{A}^{(\infty)})$. For $U = U_0(\mathfrak{c}(\varepsilon^-)d(B_F))$, the Galois group Δ acts on $S_F(\varepsilon) = G(F)\backslash\mathbb{G}/Z(F_{\mathbb{A}}^{(\infty)})U$, which is a finite set by the approximation theorem. If ε is Δ-invariant (that is, $\varepsilon_j(x^\sigma) = \varepsilon_j(x)$ and $\varepsilon_+(x^\sigma) = \varepsilon_+(x)$ for all x and $\sigma \in \Delta$), we can let $\sigma \in \Delta$ acts on $\mathcal{M}_F^{(1)}(\varepsilon)$ by $\sigma f(x) = f(x^\sigma)$. Then the Galois group Δ acts on $h_F(\varepsilon)$ by $h \mapsto \sigma h \sigma^{-1}$. Thus we have two Δ-sets, $S_F(\varepsilon)$ and $\mathrm{Spec}(h_F(\varepsilon))(\mathbb{C})$. Here is the conjecture assumed in the theorem:

Conjecture 1.2. *We have a Δ-equivariant bijection $S_F(\varepsilon_F) \cong \mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ if $d(B_F)$ is a product of all primes of F above $d(B_{\mathbb{Q}})$ where $\varepsilon_F = \varepsilon_{\mathbb{Q}} \circ N_{F/\mathbb{Q}}$.*

As is well known, for cyclic Δ, this is equivalent to the identity

$$\mathbb{C}[S_F(\varepsilon_F)] \cong \mathbb{C}[\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})] \cong h_F(\varepsilon_F) \quad (\text{as } \Delta\text{-modules})$$

of linearized representations (e.g. [LRG] Exercise 13.5). It is easy to prove the above identity of linearized representations (see Proposition 2.5). Under a mild condition on B, Langlands' theory of soluble base-change proves the conjectural identity as Δ'-sets for all soluble subgroups Δ' of Δ (see Proposition 4.5), which implies $\mathbb{Z}_\ell[S_F(\varepsilon_F)] \cong \mathbb{Z}_\ell[\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})]$ as Δ-modules for all primes ℓ (see [Sc]). The author asked group theorists L. Scott and R. Guralnick if $S_F(\varepsilon_F) \cong \mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ as Δ-sets under the condition that $S_F(\varepsilon_F) \cong \mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$

as Δ'-sets for every proper subgroup $\Delta' \subsetneq \Delta$, hoping to apply an induction on $|\Delta|$ to prove the conjecture. Their answer is negative. First Scott supplied us with a counter example when $\Delta = \mu_2^2$ (see [LRG] Comments after Exercise 13.5). According to Guralnick, the space of functions with values in $\mathbb{Q}$ on conjugacy classes of subgroups (including Δ) is the scalar extension of the Burnside ring (defined over $\mathbb{Z}$) to $\mathbb{Q}$, and the generalized permutation characters θ_X for Δ-sets X assigning to each subgroup $H \subset \Delta$ the number $|X^H|$ of H-fixed points generate the Burnside ring over $\mathbb{Q}$. In particular, writing the characteristic function of Δ (on the set of conjugacy classes of subgroups of Δ) as χ_Δ, we can write $m\chi_\Delta = \theta_X - \theta_Y$ for two Δ-sets X and Y for a sufficiently large positive integer m (to eliminate the denominators), and these two sets X and Y give us a counter example for any group. Thus we really need to study our specific Δ-sets as in the conjecture number-theoretically. We are grateful to Professors Guralnick and Scott for their comments.

By the following result, in theory (but not in practice yet; see the remark following the theorem), one should be able to reduce the (totally real) base-change problem of $GL(2)$ to that of simply 2-connected extensions, because the base-change problem is solved by Langlands for soluble extensions ([BCG]):

Theorem 1.3. *Let $F_0/\mathbb{Q}$ be a totally real finite Galois extension with Galois group Δ_0. If $H^1(\Delta_0, \mu_2) = 0$, there exists a finite abelian totally real 2-extension F/F_0 Galois over $\mathbb{Q}$ with simply 2-connected Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. The extension $\Delta \twoheadrightarrow \Delta_0$ is central.*

Here we mean by an abelian 2-extension an abelian extension with Galois group killed by a 2-power. Suppose that a Galois extension $F/\mathbb{Q}$ is not simply 2-connected (with $H^1(\mathrm{Gal}(F/\mathbb{Q}), \mu_2) = 0$). Take a totally real abelian 2-extension F'/F such that $F'/\mathbb{Q}$ is simply 2-connected whose existence is claimed in Theorem 1.3. Then, we first make base-change from $\mathbb{Q}$ to F' by Theorem 1.1, and then we would like to make a sequence of quadratic descent down to F by Langlands' theory to remove the simple 2-connectedness assumption of Theorem 1.1. By the assumption (R2) of Theorem 1.1, at present stage, without having good control of ramification of F'/F (say, ideally, unramifiedness), we cannot go further this way. In our future work, we hope to remove the assumption (R2), and if successful, we expect to be able to remove the simple 2-connectedness assumption

(replacing G by split $GL(2)$). An outstanding cause why we need to impose (R2) is the following.

(3) Though computation of traces of automorphic representations with a given central character is effective to lift automorphic representation from a field to its prime cyclic extension, it is not as effective for cyclic descent. In particular, quadratic descent is very subtle, because even in the simplest case where F'/F is quadratic, we have two choices π_v and $\pi_v \otimes \left(\frac{F'_v/F_v}{}\right)$ (with the same central character) whose base-change is a given Galois-invariant local representation of $GL_2(F'_v)$ for each place v of F.

Because of non-uniqueness of descent, the comparison of permutation characters of $S_F(\varepsilon_F)$ and $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ becomes technically more demanding if it involves 2-extensions. Some more explanation of this difficulty will be given in Remark 5.1.

Here is a sketch of our idea of proving Theorem 1.1 assuming, for simplicity, the nontriviality of $\varepsilon_{\mathbb{Q}}^-$ and ε_F^-, $d(B_{\mathbb{Q}})$ to contain a sufficiently big prime and ramified primes for $F/\mathbb{Q}$, and the odd class number condition for F. We write π° for the automorphic representation of $GL_2(\mathbb{A})$ associated to π under the Jacquet-Langlands correspondence. Note that $\mathfrak{c}(\varepsilon_{1,\mathbb{Q}})\mathfrak{c}(\varepsilon_{2,\mathbb{Q}})d(B_{\mathbb{Q}})$ gives the conductor $C(\pi)$ of π (and also of π°). Assuming Serre's mod p conjecture of level $C(\pi)$ for a sufficiently large prime p, the modular lifting theorem of Wiles tells us that any 2-dimensional strictly compatible system ρ of conductor $C(\pi)$ is modular. We note that π° is a Steinberg representation at prime factors of $d(B_{\mathbb{Q}})$. Imposing appropriate local conditions on $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})}$ at all $p \in S = \{p|C(\pi)\}$ and unramifiedness outside the finite set S, there are only finitely many such systems up to isomorphisms. Write this finite set of isomorphism classes as $\mathfrak{S}$. By the Steinberg condition at $p|d(B)$, $\rho \in \mathfrak{S}$ cannot be of CM type; so, it is irreducible over $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ for any totally real field F. Thus if we define the analogous set $\mathfrak{S}_F$ of strictly compatible systems of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, the map $\rho \mapsto \rho_F = \rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is an injection of $\mathfrak{S}$ into $\mathfrak{S}_F$ by simple 2-connectedness. The Galois group Δ acts on $\mathfrak{S}_F$ by inner conjugation. By simple 2-connectedness, any system in the Δ-fixed subset $\mathfrak{S}_F^\Delta$ extends uniquely to a strictly compatible system of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathfrak{S}$. Thus $\mathfrak{S}_F^\Delta \hookrightarrow \mathfrak{S}$ by extension; so, $\mathfrak{S}_F^\Delta \cong \mathfrak{S}$. We write $\mathfrak{M}_F$ for the subset of $\mathfrak{S}_F$ made up of systems associated to Hilbert modular automorphic representations.

Thus we need to prove $|\mathfrak{M}_F^\Delta| \geq |\mathfrak{S}|$, which implies that $\mathfrak{M}_F^\Delta = \mathfrak{S}_F^\Delta \cong \mathfrak{S}$. Under the simplifying assumptions, the set $\mathfrak{M}_F$ is in bijection with $\mathrm{Spec}(h_F(\varepsilon))(\mathbb{C})$. Thus $\mathfrak{M}_F^\Delta \cong \mathrm{Spec}(h_F)(\mathbb{C})^\Delta$. Plainly Δ acts on the set $S_F(\varepsilon_F)$; so, we have its fixed point set $S_F(\varepsilon_F)^\Delta$. Then $S_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}})$ gives a subset of $S_F(\varepsilon_F)^\Delta$. By means of the isomorphisms $\mathcal{M}_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}}) \cong h_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}})$ and $\mathcal{M}_F(\varepsilon_F) \cong h_F(\varepsilon_F)$ as Hecke modules and also as Δ-modules (see Lemma 2.3) and by the conjecture, we know that $|\mathfrak{M}_F^\Delta| = |\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})^\Delta| = |S_F(\varepsilon_F)^\Delta| \geq |S_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}})| = |\mathrm{Spec}(h_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}}))(\mathbb{C})| = |\mathfrak{S}|$, because $G(\mathbb{Q}) \subset G(F)$ induces $S_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}}) \subset S_F(\varepsilon_F)^\Delta$.

If base-change/descent can be proven relative to any intermediate field $F/E/\mathbb{Q}$ with $\Delta_E = \mathrm{Gal}(G/E)$, we have the following (hypothetical) "rough" identity:

$$|\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})^\Delta| \doteqdot |\mathfrak{M}_F^{\Delta_E}| \overset{(1)}{=} |\mathfrak{M}_E| \doteqdot |S_E(\varepsilon_E)| \overset{(2)}{=} |S_F(\varepsilon_F)^{\Delta_E}|.$$

The equality (1) follows from the existence of base-change/descent. The equality (2) follows from the argument above Proposition 4.5 under some restrictive assumptions. This identity for all subgroup Δ_E of Δ produces the identity of permutation characters of the two Δ-sets $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ and $S_F(\varepsilon_F)$, which is sufficient to verify $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C}) \cong S_F(\varepsilon_F)$ as Δ-sets (see Lemma 2.4 and [LRG] Exercise 13.5). Thus Conjecture 1.2 is "roughly" equivalent to the existence of base-change. Indeed, we will prove the conjecture in Proposition 4.5 for soluble extensions (under some mild assumptions) using the existence of base-change proven by Langlands.

We will state a more general (relative) version (Theorem 8.4) of Theorem 1.3 in Section 8 where we give a proof of Theorem 8.4. It is a cohomological computation, and the two key ingredients are a theorem of Merkurjev-Suslin telling us that $H^2(\mathrm{Gal}(\overline{K}/K), \mu_2)$ is generated by the classes of quaternion algebras for any subfield $K \subset \mathbb{C}$ and a theorem of Moore–Steinberg of the finiteness of the universal simply 2-connected covering $\mathcal{E}$ of a given finite group Δ with $H^1(\Delta, \mu_2) = 0$.

2. Permutation representations

Let E be a totally real field and F/E be a totally real Galois extension with $\mathrm{Gal}(F/E) = \Delta$ and relative discriminant $d(F/E)$. We consider a quaternion algebra B_E over E with $B_E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^{[E:\mathbb{Q}]}$ for the Hamilton quaternion algebra $\mathbb{H}$; thus, B_E is (totally) definite. We write G for the algebraic group defined over

E such that $G(A) = (B \otimes_E A)^\times$ for E-algebras A. Let G_1 be the algebraic group defined by the kernel of the reduced norm map $N : G_{/E} \to \mathbb{G}_{m/E}$.

Let $B_F = B \otimes_E F$. We assume the following condition corresponding to (R1):

(dd) *every prime factor of $d(B)O$ is a factor of $d(B_F)$.*

and consider the following condition corresponding to (R2):

(df) *every prime factor of $d(F/E)O$ is a factor of $d(B_F)$.*

We are going to show that, under the condition (dd), there exists a maximal order R_F stable under Δ containing a given maximal order R of B. Let $\mathfrak{l}$ be a prime ideal of E. If $B_\mathfrak{l} \cong M_2(E_\mathfrak{l})$, we may identify $B \otimes_E F_\mathfrak{l} = M_2(F_\mathfrak{l})$ so that this identification induces the identification $B_\mathfrak{l} \cong M_2(E_\mathfrak{l})$. Then we have the Δ-stable maximal order $M_2(O_\mathfrak{l})$ of $B \otimes_E F_\mathfrak{l}$. Similarly if $B_\mathfrak{l}$ and $B \otimes_E F_\mathfrak{l}$ both have division simple factors, the maximal orders are unique, which are Galois stable. Take a maximal order R_F of B_F. Then for almost all primes $\mathfrak{l}$ of E, $R_{F,\mathfrak{l}} = R_F \otimes_{O_E} O_{E,\mathfrak{l}}$ coincides with a Δ-stable maximal order of $B \otimes_E F_\mathfrak{l}$. Modifying $R_{F,\mathfrak{l}}$ for a finite set of primes (for which originally $R_{F,\mathfrak{l}}$ is not Galois stable), we may assume that $R_{F,\mathfrak{l}}$ is Galois stable for all $\mathfrak{l}$. Under (dd), only these two cases occur (in other words, $B_{F,\mathfrak{l}} \cong M_2(F_\mathfrak{l})$ but $B_\mathfrak{l} \ncong M_2(E_\mathfrak{l})$ does not happen). Since the Hasse principle holds for maximal orders, we have a maximal order $R_F = B_F \cap (\bigcap_\mathfrak{l} R_{F,\mathfrak{l}})$ stable under Δ.

Let ε_E be a quadruple of characters as in the introduction for E. We consider for a subextension E'/E inside F, and write $\varepsilon_{E'}$ for the pullback of ε_E by the norm map $N_{E'/E}$. Write U for the open compact subgroup $U_0(\mathfrak{c}(\varepsilon_F^-)d(B_F))$ of $G(F_\mathbb{A}^{(\infty)})$. Consider the following finite Δ-set:

$$S_{E'} = G(E')\backslash\mathbb{G}_{E'}/U_{E'}Z(E'^{(\infty)}_\mathbb{A}),$$

where $U_{E'} = U \cap G(E'_\mathbb{A})$ and $\mathbb{G}_{E'} = G(E')G_1(E'^{(\infty)}_\mathbb{A})U_{E'}Z(E'^{(\infty)}_\mathbb{A})$. Thus we have $\mathbb{G}_{E'} = N^{-1}(E'^\times_+(E'^{(\infty)\times}_\mathbb{A})^2\widehat{O}^\times_{E'})$, and $\mathbb{G} = \mathbb{G}_F$. We consider the space $\mathcal{M}^{(1)}_{E'}(\varepsilon_{E'})$ of functions $f : G(E')\backslash\mathbb{G}_{E'} \to \mathbb{C}$ satisfying

$$f(zxu) = \varepsilon_{E'+}(z)\underline{\varepsilon}_{E'}(u)f(x)$$

for $u \in U_{E'}G(E'_\mathbb{R})$ and $z \in Z(E'_\mathbb{A})$. Let $h_{E'}(\varepsilon_{E'})$ be the Hecke algebra over $\mathbb{C}$ acting on $\mathcal{M}^{(1)}_{E'}(\varepsilon_{E'})$ generated by UyU for y with $N(y) = 1$ and $y_\mathfrak{l} = 1$ for $\mathfrak{l}$ ramifying in $B_{E'} = B \otimes_E E'$ or dividing the level of U.

Lemma 2.1. *Suppose* (dd). *Then the automorphic representation of* $\mathbb{G}$ *generated by functions in* $\mathcal{M}_F^{(1)}(\varepsilon_F)$ *is multiplicity-free.*

Proof. Each irreducible automorphic representation Π of $G(F_{\mathbb{A}})$ generated by a Hecke eigenform restricted to $\mathbb{G}$ remains irreducible. The representation Π is either infinite dimensional or one dimensional. If $\dim \Pi = 1$, this is clear. If $\dim \Pi = \infty$, this follows from everywhere non-supercuspidality of Π with a Steinberg place $\mathfrak{q} \in \Sigma_{st}$ (see [LL] Lemmas 2.4–2.8 and Section 6). Let us explain more this point. Start with an irreducible automorphic representation π of $\mathbb{G}$ generated by a function: $S_F \to \mathbb{C}$ in $\mathcal{M}_F^{(1)}(\varepsilon_F)$. We consider the smooth induction $\mathrm{Ind}_{\mathbb{G}}^{G(\mathbb{A}^{(\infty)})}\pi$. Since $G(\mathbb{A}^{(\infty)})/\mathbb{G}$ is a finite abelian group isomorphic to $F^\times_{\mathbb{A}^{(\infty)}}/F^\times_+(F^\times_{\mathbb{A}^{(\infty)}})^2\widehat{O}^\times \cong Cl_F/Cl_F^2$ for the strict ray class group Cl_F of F, the induction can be performed inside the space of automorphic forms on $G(F)\backslash G(\mathbb{A}^{(\infty)})$. Thus by the multiplicity one theorem (cf. [AAG] Chapter 10), $\mathrm{Ind}_{\mathbb{G}}^{G(\mathbb{A}^{(\infty)})}\pi$ is a direct sum of irreducible automorphic representations Π with multiplicity 1. By Frobenius reciprocity (valid for admissible representations), the restriction of Π contains π with multiplicity at most 1. Since Cl_F/Cl_F^2 is a $(2,2,\dots,2)$-group, we have a filtration of normal subgroups $G(\mathbb{A}^{(\infty)}) = \mathbb{G}_0 \triangleright \mathbb{G}_1 \triangleright \mathbb{G}_2 \triangleright \cdots \triangleright \mathbb{G}_e = \mathbb{G}$ so that $\mathbb{G}_i/\mathbb{G}_{i+1} \cong \{\pm 1\}$. We can perform induction at each step. Since $\mathrm{Ind}_{\mathbb{G}}^{G(\mathbb{A}^{(\infty)})}\pi$ is decomposed into a direct sum of nonisomorphic irreducible representations, starting from any irreducible automorphic representation π_i of $\mathbb{G}_i$ appearing in the restriction $\Pi|_{\mathbb{G}_i}$, the smooth induction $\mathrm{Ind}_{\mathbb{G}_i}^{\mathbb{G}_{i-1}}\pi_i$ is again a direct sum of irreducible automorphic representations of $\mathbb{G}_{i-1}$ with multiplicity at most 1. Since $\mathbb{G}_{i-1}/\mathbb{G}_i \cong \{\pm 1\}$, $\mathrm{Ind}_{\mathbb{G}_i}^{\mathbb{G}_{i-1}}\pi_i$ is either irreducible or a direct sum of two nonisomorphic representations of $\mathbb{G}_{i-1}$. If $\mathrm{Ind}_{\mathbb{G}_i}^{\mathbb{G}_{i-1}}\pi_i$ is irreducible, by rearranging the filtration, we may assume that $i = 1$ and $\Pi = \mathrm{Ind}_{\mathbb{G}_1}^{\mathbb{G}_0}\pi_1$. This implies $\Pi \otimes \alpha \cong \Pi$ for the character $\alpha : \mathbb{G}_0/\mathbb{G}_1 \cong \{\pm 1\}$. Since α is quadratic, there is a quadratic extension M/F such that $\alpha = \left(\frac{M/F}{}\right)$ by class field theory. Then by [LL] Proposition 6.5, there exists a Hecke character $\theta : M_{\mathbb{A}}^\times/M^\times \to \mathbb{C}$ such that Π corresponds to the automorphic induction $\pi(\theta)$ from $GL(1)_{/M}$ to $GL(2)_{/F}$ by the Jacquet–Langlands correspondence. However, the automorphic induction $\pi(\theta)$ cannot be Steinberg (see below) at any finite place (in particular at $\mathfrak{l}|d(B_F)$, it has to be Steinberg). This is a contradiction. Thus $\mathrm{Ind}_{\mathbb{G}}^{G(\mathbb{A}^{(\infty)})}\pi$ is isomorphic to $\bigoplus_{\alpha:\mathbb{G}_0/\mathbb{G}\to\{\pm1\}}\Pi\otimes\alpha$ over all characters α of $\mathbb{G}_0/\mathbb{G}$. This implies $\Pi|_{\mathbb{G}} = \pi$

and therefore, any extension Π of π determines π uniquely, and $\Pi|_{\mathbb{G}}$ remains irreducible.

The $\mathfrak{l}$-adic Galois representation for $\mathfrak{l} \nmid N(\mathfrak{q})$ ($\mathfrak{q} \in \Sigma_{st}$) of Π has infinite image over the inertia group $I_{\mathfrak{q}}$, because the corresponding representation Π° of $GL_2(F_{\mathbb{A}})$ under the Jacquet-Langlands correspondence is Steinberg at $\mathfrak{q}$ if $\dim \Pi = \infty$ (see Lemma 4.4). On the other hand, as seen above, any irreducible automorphic representation π on the L^2-space of $G(F)\backslash\mathbb{G}$ which has a nonzero vector in $\mathcal{M}_F^{(1)}(\varepsilon_F)$ extends to an automorphic representation of $G(F_{\mathbb{A}}^{(\infty)})$ generated by an element of $\mathcal{M}_F(\varepsilon_F)$, and if Π extends π, all other extensions are of the form $\Pi \otimes \alpha$ for a quadratic Hecke character $\alpha : F_{\mathbb{A}}^\times/F^\times \to \{\pm 1\}$ trivial on $N(\mathbb{G})$. They never overlap because $\Pi \otimes \alpha \cong \Pi$ happens, by [LL] Proposition 6.5, only when the Galois representation of Π is an induced representation of a Galois character of $\mathrm{Gal}(\overline{F}/M)$ for the quadratic extension M corresponding to α (whose image of $I_{\mathfrak{q}}$ for $\mathfrak{q} \in \Sigma_{st}$ has to be finite). □

Corollary 2.2. *Suppose* (dd). *Then $h_F(\varepsilon_F)$ is commutative semi-simple, and we have $\mathcal{M}_F^{(1)}(\varepsilon_F) \cong h_F(\varepsilon_F)$ as Hecke modules.*

Proof. The action of Hecke operators of $h_F(\varepsilon_F)$ with respect to U is still semi-simple, because π occurs with multiplicity 1 and the action of $h_F(\varepsilon_F)$ determines π (by Lemma 2.1). Thus $h_F(\varepsilon_F)$ is a semi-simple commutative algebra and we have $\mathcal{M}_F^{(1)}(\varepsilon_F) \cong h_F(\varepsilon_F)$ as Hecke modules. □

For any Δ-invariant linear form $\lambda \in \mathrm{Hom}(\mathcal{M}_F^{(1)}(\varepsilon_F), \mathbb{C})^\Delta$, we define a pairing $(\cdot,\cdot) = (\cdot,\cdot)_\lambda : \mathcal{M}_F^{(1)}(\varepsilon_F) \times h_F(\varepsilon_F) \to \mathbb{C}$ by $(f, h) = \lambda(f|h)$. The pairing satisfies $(f|h, h') = (f, hh')$ and $(f \circ \sigma, h) = (f, h^\sigma)$ for $\sigma \in \Delta$, where the action of Δ on $h_F(\varepsilon_F)$ is induced by $UxU \mapsto Ux^{\sigma^{-1}}U$, and this action coincides with the action $h \mapsto \sigma \circ h \circ \sigma^{-1}$.

Lemma 2.3. *Suppose* (dd) *and Δ-invariance of λ. Then the above pairing $(\cdot,\cdot)_F$ is nondegenerate if $\lambda(f) \neq 0$ for all nonzero Hecke eigenforms $f \in \mathcal{M}_F^{(1)}(\varepsilon_F)$ and the set $\Sigma_{st} = \{\mathfrak{p} | d(B_F)\}$ of ramified places of B_F/F is nonempty.*

Proof. Consider the inner product $\langle f, g\rangle = \sum_{x \in S_F} f(x)\overline{g(x)}$ for $f, g \in \mathcal{M}^{(1)}(\varepsilon_F)$. Take $\phi \in \mathcal{M}^{(1)}(\varepsilon_F)$ so that $\langle f, \phi\rangle = \lambda(f)$. Then $\phi^\sigma(x) = \phi(x^\sigma) = \phi(x)$ for all $\sigma \in \Delta$, because λ is Δ-invariant. Since $\lambda(f) \neq 0$ for any Hecke eigenform $f \in \mathcal{M}^{(1)}(\varepsilon_F)$, the automorphic representation generated by all functions in

$\mathcal{M}_F^{(1)}(\varepsilon_F)$ is actually generated by ϕ, because, as we have seen, the automorphic representation generated by ϕ is multiplicity-free (by Lemma 2.1), and each irreducible component π is determined by the eigenvalues on $\pi^U = H^0(U,\pi)$ of the operators in $h_F(\varepsilon_F)$ (by Corollary 2.2). Thus for any given $g \in \mathcal{M}_F^{(1)}(\varepsilon_F)$, we can find Hecke operators h_i such that $g = \sum_i \phi|h_i$. If $(f,h) = 0$ for all $h \in h_F(\varepsilon_F)$, we have $\langle f, g\rangle = \sum_i \langle f, \phi|h_i\rangle = \sum_i \langle f|h_i, \phi\rangle = \sum_i (f, h_i) = 0$, because operators in $h_F(\varepsilon_F)$ is self-adjoint under the inner product $\langle\cdot,\cdot\rangle$ (e.g., [HMI] Lemma 3.5). Since g is arbitrary, we have $f = 0$ by the nondegeneracy of $\langle\cdot,\cdot\rangle$. Let $\mathcal{M}_F^\perp \subset h_F(\varepsilon_F)$ be the orthogonal component of the entire space of $\mathcal{M}_F^{(1)}(\varepsilon_F)$. Then $\dim h_F(\varepsilon_F)/\mathcal{M}_F^\perp = \dim \mathcal{M}_F^{(1)}(\varepsilon_F)$. Since we know by the multiplicity one theorem, $\dim h_F(\varepsilon_F) = \dim \mathcal{M}_F^{(1)}(\varepsilon_F)$, we conclude $\mathcal{M}_F^\perp = 0$, and the pairing is nondegenerate. □

Remark 2.1. Taking a complete representative set Ξ for $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})/\Delta$ and pick a Hecke eigenform $f_\xi \in \mathcal{M}_F^{(1)}(\varepsilon_F)$ with $f_\xi|h = \xi(h)f_\xi$. Then $\phi = \sum_{f\in\widetilde{\Xi}} f$ is Δ-invariant for $\widetilde{\Xi} = \{f_\xi^\sigma | \xi \in \Xi, \sigma \in \Delta\}$, and for $\lambda(f) = \langle f, \phi\rangle$, λ is Δ-invariant and does not vanish on any nonzero Hecke eigenform. We may ask if $\langle f, \delta\rangle \neq 0$ for all nonzero Hecke eigenforms f for the function $\delta \in \mathcal{M}_F^{(1)}(\varepsilon_F)$ supported on $G(F)U_0(\mathfrak{c}(\varepsilon_F^-))$ in $\mathcal{M}_F^{(1)}(\varepsilon_F)$. It is likely that this is true, and ϕ could be a constant multiple of δ.

For a finite set Ω with a left action of Δ, we write $K[\Omega]$ for a field K the vector space of formal linear combination of elements of Ω. Then we let Δ acts on $K[\Omega]$ by $\delta(\sum_{s\in\Omega} a_s s) = \sum_{s\in\Omega} a_s \delta(s)$. We call $\varphi_\Omega = K[\Omega]$ the K-linearized permutation representation of Ω. For any subgroup $\Delta' \subset \Delta$, we define $\theta_\Omega(\Delta') = |\Omega^{\Delta'}|$, where $\Omega^{\Delta'}$ is the set of fixed points of Δ'. The following lemma is a part of Exercise 13.5 of [LRG]:

Lemma 2.4. *Suppose that K is of characteristic 0. Let Ω and Ξ be two finite Δ-sets. Then we have*

(1) *$\varphi_\Omega \cong \varphi_\Xi$ as linear representations of Δ if and only if $\theta_\Omega = \theta_\Xi$ over all cyclic subgroups of Δ;*
(2) *$\Omega \cong \Xi$ as Δ-sets if and only if $\theta_\Omega = \theta_\Xi$.*

Proof. We have $\mathrm{Tr}(\sigma|_{K[\Omega]}) = \theta_\Omega(\langle\sigma\rangle)$. Then from the semi-simplicity of the action of Ω, the identity of trace gives rise to $K[\Omega] \cong K[\Xi]$.

We now prove (2). If all points of Ω are fixed by Δ, the same assertion is true for Ξ; so, we are done. Thus we may assume that one of the Δ-orbits of Ω is nontrivial. Let M be a subgroup maximal among proper subgroups appearing as a stabilizer of a point of Ω. If $MxH = xH$ for a proper subgroup $H \subset \Delta$ appearing as a stabilizer of a point of Ω, we have $x^{-1}Mx \subset H$. Then by the maximality of M, we conclude $H = x^{-1}Mx$. Then $\theta_\Omega(M) = \theta_\Omega(\Delta) + m(M)$, where $m(M)$ is the number of Δ-orbits in Ω isomorphic to Δ/M. Thus if $\theta_\Omega = \theta_\Xi$, there are the same number of orbits isomorphic to Δ/M in Ξ and Ω. Removing these orbits, we get new Δ-sets Ω' and Ξ'. Since we have removed nonempty isomorphic Δ-sets from Ω and Ξ, we have $\theta_{\Omega'} = \theta_{\Xi'}$. Then by induction on $|\Omega|$, we find $\Omega' \cong \Xi'$, which implies $\Omega \cong \Xi$. □

Proposition 2.5. *Suppose* (dd). *Then $h_F(\varepsilon_F)$ is isomorphic to $\mathcal{M}_F^{(1)}(\varepsilon_F)$ as Δ-modules. If further $\Delta = \mathrm{Gal}(F/E)$ is a cyclic group, we have a Δ-equivariant bijection between $S_F(\varepsilon_F)$ and $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$.*

Proof. Since $h_F = h_F(\varepsilon_F)$ is a semi-simple commutative algebra, h_F is isomorphic to $\mathbb{C}[\mathrm{Spec}(h_F)(\mathbb{C})]$ as Δ-modules, and by the trace pairing, $\mathrm{Hom}_{\mathbb{C}}(h_F, \mathbb{C}) \cong h_F$ as Δ-modules. Taking the pairing between h_F and $\mathcal{M}_F^{(1)}(\varepsilon_F)$ as in Remark 2.1, by Lemma 2.3, $\mathcal{M}_F^{(1)}(\varepsilon_F) \cong \mathbb{C}[S_F]$ for $S_F = S_F(\varepsilon_F)$ is isomorphic to $\mathrm{Hom}(h_F, \mathbb{C}) \cong h_F$ as $\mathbb{C}[\Delta]$-modules. This shows the first assertion. Thus we have $\mathbb{C}[S_F] \cong \mathrm{Hom}(h_F, \mathbb{C})$ as Δ-modules, and hence $\mathbb{C}[S_F] \cong \mathbb{C}[\mathrm{Spec}(h_F)(\mathbb{C})]$ as Δ-modules. Then by Lemma 2.4, if Δ is cyclic, we have $S_F \cong \mathrm{Spec}(h_F)(\mathbb{C})$ as Δ-sets. □

Here is a relative version of Conjecture 1.2 which should be true for all totally real finite Galois extensions F/E with Galois group Δ:

Conjecture 2.6. *Assume that $d(B_E) \neq 1$ and that $d(B_F)$ is a product of all primes of F above $d(B_E)$. Then $S_F(\varepsilon_F) \cong \mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ as Δ-sets.*

3. Galois invariants

Let E be a totally real number field of finite degree over $\mathbb{Q}$. We consider a division quaternion algebra $B_{/E}$ such that $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^{[E:\mathbb{Q}]}$. Take a finite totally real Galois extension F/E with Galois group Δ. We consider $B_F = B \otimes_E F$ (but we do not suppose (dd) unless explicitly mentioned). The Galois action on B_F is induced on the right factor F of $B \otimes_E F$. Let G be the algebraic group defined over E such that $G(A) = (B \otimes_E A)^\times$. We consider the space $G(F)\backslash G(F_{\mathbb{A}}^{(\infty)})$.

Lemma 3.1. *The set of Galois invariants*

$$(G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}))^{\Delta} = \{x \in G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}) | \sigma(x) = x \text{ for all } \sigma \in \Delta\}$$

is isomorphic to the image of $G(E)\backslash G(E_{\mathbb{A}}^{(\infty)})$ *in* $G(F)\backslash G(F_{\mathbb{A}}^{(\infty)})$.

Proof. Consider a non-abelian 1-cocycle $\sigma \mapsto a_\sigma \in G(F)$ such that $a_\sigma a_\tau^\sigma = a_{\tau\sigma}$. Then we choose $b = \sum_\tau a_\tau u^\tau \neq 0$ for a suitable $u \in G(F)$ (such a choice of u is possible by Dedekind's theorem). Then we have $a_\sigma b^\sigma = a_\sigma \sum_\tau a_\tau^\sigma u^{\tau\sigma} = \sum_{\tau\sigma} a_{\tau\sigma} u^{\tau\sigma} = b$. In other words, $a_\sigma = bb^{-\sigma}$. Take $x \in G(F_{\mathbb{A}}^{(\infty)})$ representing an element in $(G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}))^{\Delta}$. Then $a_\sigma x^\sigma = x$ so $a_\sigma = xx^{-\sigma} \in G(F)$. By the above argument, we can find $b \in G(F)$ such that $a_\sigma = bb^{-\sigma}$. Then $bb^{-\sigma}x^\sigma = x$ and hence $b^{-1}x \in G(E_{\mathbb{A}}^{(\infty)})$, which represents the class of $x \in (G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}))^{\Delta}$. Thus the natural map $i : G(E)\backslash G(E_{\mathbb{A}}^{(\infty)}) \to (G(F)\backslash G(F_{\mathbb{A}}^{(\infty)}))^{\Delta}$ is surjective. If $i(x) = i(y)$, we have $x = \gamma y$ for $\gamma \in G(F)$. Since we may choose x and y in $G(E_{\mathbb{A}}^{(\infty)})$, we have $\gamma \in G(E) = G(E_{\mathbb{A}}^{(\infty)}) \cap G(F)$. Thus i is a bijection, and this shows the desired result. □

Let U be a closed subgroup of $G(F_{\mathbb{A}}^{(\infty)})$ stable under the action of Δ. Recall that G_1 denotes the derived group of G (that is the kernel of the reduced norm map).

Lemma 3.2. *Let* U *be an open compact subgroup* $U \subset G_1(F_{\mathbb{A}}^{(\infty)})$ *stable under* Δ, *and put* $U_F = U \cap G_1(F)$ *in* $G(F_{\mathbb{A}}^{(\infty)})$. *Suppose one of the following four conditions*

(1) $E[\mu_N]$ *and* F *are linearly disjoint over* E *for each integer* $N > 0$ *with* $\dim_F F[\mu_N] \leq 2$, *and* $H^1(\Delta, \mathbb{Z}/\ell\mathbb{Z}) = 0$ *for each prime* ℓ *with* $\dim_F F[\mu_\ell] \leq 2$;
(2) $U_F \subset G(E)$ *and* $H^1(\Delta, \mathbb{Z}/\ell\mathbb{Z}) = 0$ *for each prime* ℓ *with* $\dim_F F[\mu_\ell] \leq 2$;
(3) $H^1(\Delta, \mu_2) = 0$ *and* ${}^xU_F := {}^xU \cap G_1(F) = \{\pm 1\}$ *for all* $x \in G_1(E_{\mathbb{A}}^{(\infty)})$, *where* ${}^xU = x \cdot Ux^{-1}$;
(4) ${}^xU_F = \{1\}$ *for all* $x \in G_1(E_{\mathbb{A}}^{(\infty)})$.

Then the natural map

$$i : G_1(E)\backslash G_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta} \to G_1(F)\backslash G_1(F_{\mathbb{A}}^{(\infty)})/U$$

is an injection, and if we suppose either (4) *only or* (3) *with* $H^2(\Delta, \mu_2) = 0$*, we have*

$$i : \Big(G_1(F)\backslash G_1(F_{\mathbb{A}}^{(\infty)})/U\Big)^{\Delta} \cong G_1(E)\backslash G_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta}.$$

Write $\varphi(N) = [E[\mu_N] : E]$ for a positive integer N. If either $H^1(\Delta, \mathbb{Z}/\varphi(N)\mathbb{Z}) = 0$ or N is unramified in $F/\mathbb{Q}$ for all integers $N > 1$ with $[F[\mu_N] : F] \leq 2$, the linear-disjointness assumption in (1) of the lemma is satisfied. If U is sufficiently small, the condition (4) is satisfied.

Proof. We use nonabelian group cohomology $H^j(\Delta, ?)$ for $j = 1, 2$ as defined in [GCH] Chapter 3 or the papers by Springer and Kneser in [AGD] Chapter II. Suppose the condition (4). If $i(x) = i(x')$, we have $\gamma x = x'u$ for $\gamma \in G(F)$ and $u \in U$. Then $\gamma^\sigma x = x'u^\sigma$ for $\sigma \in \Delta$, and hence, $\gamma^{\sigma-1} \in {}^xU \cap G(F) = \{1\}$. Thus $\gamma \in G_1(E)$ and hence $u \in U^{\Delta}$, which implies $x = x'$ in $G_1(E)\backslash G_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta}$. By (4), the stabilizer in $G_1(F)$ of each point of $G_1(F_{\mathbb{A}}^{(\infty)})/U$ is trivial. Let $x \in G_1(F_{\mathbb{A}}^{(\infty)})/U$. If $\gamma_\sigma x = x^\sigma$ for $\gamma_\sigma \in G(F)$ with each $\sigma \in \Delta$, we have

$$\gamma_{\sigma\tau} x = x^{\sigma\tau} = (x^\sigma)^\tau = (\gamma_\sigma x)^\tau = \gamma_\sigma^\tau \gamma_\tau x,$$

which implies $\gamma_{\sigma\tau} = \gamma_\sigma^\tau \gamma_\tau$. Therefore $\sigma \mapsto \gamma_\sigma$ is a nonabelian 1-cocycle with values in $G_1(F)$. We have an exact sequence:

$$1 \to G_1(F) \to G(F) \xrightarrow{norm} F_+^\times \to 1.$$

This produces a long exact sequence of sets:

$$1 \to G_1(E) \to G(E) \xrightarrow{norm} E_+^\times \to H^1(\Delta, G_1(F)) \to H^1(\Delta, G(F)) = \{1\}.$$

Since the reduced norm map: $G(E) \xrightarrow{norm} E_+^\times$ is surjective ([BNT] Proposition 3 in page 206), we find $H^1(\Delta, G_1(F)) = \{1\}$. Then as in the proof of Lemma 3.1, we find $b \in G_1(F)$ such that $\gamma_\sigma = b^\sigma b^{-1}$. Thus $b^\sigma b^{-1} x = x^\sigma$ and hence $b^{-1}x \in G_1(E_{\mathbb{A}}^{(\infty)})$. This implies that

$$\Big(G_1(F)\backslash G_1(F_{\mathbb{A}}^{(\infty)})/U\Big)^{\Delta} = G_1(E)\backslash G_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta}.$$

Suppose the condition (3). If $i(x) = i(x')$, we have $\gamma x = x'u$ for $\gamma \in G(F)$ and $u \in U$. Then $\gamma^\sigma x = x'u^\sigma$ for $\sigma \in \Delta$, and hence, $\gamma^{\sigma-1} \in {}^xU \cap G(F) = \{\pm 1\}$. Thus $\sigma \mapsto \gamma^{\sigma-1} \in \mu_2$ is a cocycle, and hence $\gamma^{\sigma-1} = 1$ because $H^1(\Delta, \mu_2) = 0$. Thus $u \in U^{\Delta}$, which implies $x = x'$ in $G_1(E)\backslash G_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta}$, and hence we get the

injectivity of i. To prove the surjectivity of i, we may replace G_1 by $\overline{G}_1 = G_1/\mu_2$ because U contains μ_2. We thus prove

$$\left(\overline{G}_1(F)\backslash\overline{G}_1(F_{\mathbb{A}}^{(\infty)})/U\right)^{\Delta} = \overline{G}_1(E)\backslash\overline{G}_1(E_{\mathbb{A}}^{(\infty)})/U^{\Delta}.$$

By the exact sequence, $\mu_2 \hookrightarrow G_1 \twoheadrightarrow \overline{G}_1$, we get another exact sequence of sets:

$$1 = H^1(\Delta, G_1) \to H^1(\Delta, \overline{G}_1) \to H^2(\Delta, \mu_2) = 1.$$

Thus, we find $H^1(\Delta, \overline{G}_1) = 1$ under $H^2(\Delta, \mu_2) = 1$. By (3), the stabilizer in $G(F)$ of each point of $\overline{G}_1(F_{\mathbb{A}}^{(\infty)})/U$ is trivial. Let $x \in \overline{G}_1(F_{\mathbb{A}}^{(\infty)})/U$. If $\overline{\gamma}_\sigma x = x^\sigma$ for $\overline{\gamma}_\sigma \in \overline{G}_1(F)$ with each $\sigma \in \Delta$, we have

$$\overline{\gamma}_{\sigma\tau} x = x^{\sigma\tau} = (x^\sigma)^\tau = (\overline{\gamma}_\sigma x)^\tau = \overline{\gamma}_\sigma^\tau \overline{\gamma}_\tau x,$$

which implies $\overline{\gamma}_{\sigma\tau} = \overline{\gamma}_\sigma^\tau \overline{\gamma}_\tau$. Therefore $\sigma \mapsto \overline{\gamma}_\sigma$ is a nonabelian 1-cocycle with values in $\overline{G}_1(F)$. As in the proof of Lemma 3.1, we find $b \in \overline{G}_1(F)$ such that $\overline{\gamma}_\sigma = b^\sigma b^{-1}$. Thus $b^\sigma b^{-1} x = x^\sigma$ and hence $b^{-1}x \in \overline{G}_1(E_{\mathbb{A}}^{(\infty)})$ as desired.

We now assume the assumption (1). Since $G_1(F)$ is discrete and U is compact in $G_1(F_{\mathbb{A}}^{(\infty)})$, U_F is discrete compact, and hence is a finite group. Thus for $\zeta \in U_F - Z(F)$, $F[\zeta] \subset D$ is a quadratic extension generated by a root of unity. By our assumption $E[\zeta]$ is linearly disjoint from F over E. Thus $E[\zeta]/E$ is quadratic. Since $[E[\zeta] : E] = 2$, we have $\xi \in E$ such that $E[\zeta] = E[\sqrt{\xi}]$. Regarding $\Delta \subset \mathrm{Gal}(F[\zeta]/E)$, the map $\delta \mapsto (\sqrt{\xi})^{\delta-1} \in \mu_2$ gives a homomorphism from Δ into μ_2, which has to be trivial because of $H^1(\Delta, \mathbb{Z}/2\mathbb{Z}) = 0$. Thus Δ fixes ζ, and hence the assumption (2) is satisfied, and thus the proof in the case under (1) is reduced to the case under (2).

We now suppose the condition (2). Since U is stable under Δ, U_F is stable under Δ. As we remarked already, the action of Δ is trivial on U_F; so, $U_F \subset G(E_{\mathbb{A}}^{(\infty)})$. If $i(x) = i(x')$, that is, $\gamma x = x'u$ for $\gamma \in G(F)$ and $u \in U$ for $x \in G(E_{\mathbb{A}}^{(\infty)})$, we have $\gamma^\sigma x = x' u^\sigma$ for all $\sigma \in \Delta$. In other words, $\gamma^{-\sigma}\gamma = xu^{-\sigma}ux^{-1} \in {}^xU_F$ for ${}^xU = xUx^{-1}$. Thus $\sigma \mapsto \gamma^{-\sigma}\gamma$ is a 1-cocycle of Δ with values in the group ${}^xU_F \subset G(E_{\mathbb{A}}^{(\infty)})$ with trivial Δ-action. Since ${}^xU_F$ is soluble, we have a central sequence ${}^xU_F = U_0 \triangleright U_1 \triangleright \cdots \triangleright U_r = \{1\}$ with prime cyclic U_j/U_{j+1} of order ℓ for primes ℓ as in the assumption of the lemma. Since $H^1(\Delta, \mathbb{Z}/\ell\mathbb{Z}) = 0$ for primes ℓ as above, we have $H^1(\Delta, U_j/U_{j+1}) = 0$ for all j, which implies $H^1(\Delta, {}^xU_F) = 0$ by the long exact sequence of H^1. In other words, we find

$\gamma^{\sigma-1} = 1$ and hence, $\gamma \in G(E)$. Then we have $u \in U^\Delta$, and $x = x'$ in the source of i. □

Recall that the center of G is denoted by Z.

Lemma 3.3. *Let U be a Δ-invariant open subgroup of $G(F_{\mathbb{A}}^{(\infty)})$ such that $g \cdot Ug^{-1} \cap G(F) = Z(F)$ for all $g \in G(F_{\mathbb{A}}^{(\infty)})$. Then the inclusion $G(E_{\mathbb{A}}^{(\infty)}) \ni x \mapsto x \in G(F_{\mathbb{A}}^{(\infty)})$ induces an injection*

$$i : G(E)\backslash \left(G(E)G_1(E_{\mathbb{A}}^{(\infty)})U^\Delta\right)/U^\Delta \hookrightarrow (G(F)\backslash G(F)G_1(F_{\mathbb{A}}^{(\infty)})U/U)^\Delta.$$

If we assume further (dd), (df), *$U \supset Z(F_{\mathbb{A}}^{(\infty)})$ and $N(U) = \widehat{O}^\times(F_{\mathbb{A}}^{(\infty)\times})^2$, the map i is surjective.*

Proof. The map i as above is induced by

$$I : G(E)\backslash G(E_{\mathbb{A}}^{(\infty)})/U^\Delta \to (G(F)\backslash G(F_{\mathbb{A}}^{(\infty)})U/U)^\Delta.$$

Suppose $I(x) = I(y)$ for $x, y \in G(E_{\mathbb{A}}^{(\infty)})$. Then $xs = \gamma y$ for $\gamma \in G(F)$ and $s \in U$. Thus $xs^\sigma = \gamma^\sigma y$ for all $\sigma \in \Delta$. This shows $U \ni s^{-\sigma}s = y^{-1}\gamma^{-\sigma}\gamma y \in y^{-1}G(F)y$. By our assumption, we find $a_\sigma = s^{-\sigma}s \in Z(F)$ is 1-cocycle of Δ with values in $Z(F)$. Since $a_\sigma = s^{-\sigma}s \in Z(F)$, we find $\gamma^{-\sigma}\gamma = ya_\sigma y^{-1} = a_\sigma$. By Hilbert's theorem 90, we find $\delta \in Z(F)$ such that $a_\sigma = \delta^{\sigma-1} = \gamma^{-\sigma}\gamma$. Since $(\delta s)^\sigma = \delta s$ and $(\delta\gamma)^\sigma = \delta\gamma$ for all $\sigma \in \Delta$, we have $\delta s \in U^\Delta$ and $x(\delta s) = \delta\gamma y$ implies $x = y$ in $G(E)\backslash G(E_{\mathbb{A}}^{(\infty)})/U^\Delta$. This shows that I is injective, and hence, i is injective.

To prove the surjectivity of i, we consider the left $\overline{G}(F)$-set $X = G(F_{\mathbb{A}}^{(\infty)})U/U$, where $\overline{G}(F) = G(F)/Z(F)$. If $\overline{x} \in X$ represented by $x \in G_1(F_{\mathbb{A}}^{(\infty)})U$ is fixed by $\gamma \in G(F)$, we have $\gamma x = xu$ for $u \in U$. Thus $\gamma \in G(F) \cap xUx^{-1} = Z(F)$. This shows the stabilizer of $\overline{x}$ in $\overline{G}(F)$ is trivial. If $\overline{x}$ is fixed by Δ, we have $\overline{\gamma}_\sigma\overline{x} = \overline{x}^\sigma$ for $\sigma \in \Delta$. Then as seen above, $\sigma \mapsto \overline{\gamma}_\sigma$ is a 1-cocycle of Δ with values in $\overline{G}(F)$. Write $\overline{\gamma}_\sigma = \gamma_\sigma \mod Z(F)$, and choose $u \in G(F)$ so that $\beta = \sum_\tau u^\tau\gamma_\tau \neq 0$. Then we have

$$\beta^\sigma\gamma_\sigma \equiv \left(\sum_\tau u^{\tau\sigma}\gamma_\tau^\sigma\right)\gamma_\sigma \equiv \sum_{\tau\sigma}\gamma_{\tau\sigma}u^{\tau\sigma} \equiv \beta \mod Z(F),$$

and $\overline{\gamma}_\sigma = \overline{\beta}^{-\sigma}\overline{\beta}$ is a 1-coboundary. This shows that $\overline{\beta}\overline{x} = \overline{\beta}^\sigma\overline{\gamma}_\sigma\overline{x} = \overline{\beta}^\sigma\overline{x}^\sigma$. Replacing $\overline{x}$ by $\overline{\beta}\overline{x}$, we may assume that $\overline{x}$ is fixed by Δ. Then $x^\sigma = \alpha_\sigma x$ for $\alpha \in Z(F)$, because the stabilizer of $\overline{x}$ in $G(F)$ is $Z(F)$. Thus $\sigma \mapsto \alpha_\sigma$ is a

1-cocycle with values in $Z(F)$. By Hilbert's theorem 90, we may assume that $x \in G(E_{\mathbb{A}}^{(\infty)}) = G(F_{\mathbb{A}}^{(\infty)})^{\Delta}$. If we start from $x \in G(F)G_1(F_{\mathbb{A}}^{(\infty)})U$, we modified the original x by multiplication from the left by elements in $G(F)$; so, we may assume $x \in G(E_{\mathbb{A}}^{(\infty)}) \cap G(F)G_1(F_{\mathbb{A}}^{(\infty)})U$. Thus we have $N(x) \in (F_+^\times N(U))^{\Delta}$. Write $N(x) = \xi u$ for $u \in N(U)$ and $\xi \in N(G(F)) = F_+^\times$. Since $x \in G(E_{\mathbb{A}}^{(\infty)})$, ξO is a fractional E-ideal. Since $N(U) = \widehat{O}^\times (F_{\mathbb{A}}^{(\infty)\times})^2$, we have $\xi = z^2 v$ for $v \in \widehat{O}^\times$ and $z \in F_{\mathbb{A}}^\times$. Since the ideal $\xi O = N(x)O$ is an E-ideal, we can ask if $\xi \in (E_{\mathbb{A}}^{(\infty)\times})^2 \widehat{O}^\times$ or not. If it is, by modifying x by an element in U^{Δ} (which contains the center $Z(E_{\mathbb{A}}^{(\infty)})$), we may assume that $\xi = 1$; then, u has to be in U^{Δ}; so, x is in the image of i. If not, there exists a prime ideal $\mathfrak{q}$ of O_E such that ξO is divisible exactly by an odd power of $\mathfrak{q}$, $z = \sqrt{\xi v^{-1}} \in F_{\mathbb{A}}^{(\infty)}$, and F/E has to ramify at $\mathfrak{q}$ with even ramification index; then, $B_{\mathfrak{Q}}$ has to split over $F_{\mathfrak{Q}}$ for a prime $\mathfrak{Q}$ of F over $\mathfrak{q}$, which is impossible under (dd) and (df). □

Let Σ be a set of prime ideals of E with $|\Sigma| \equiv [E : \mathbb{Q}] \mod 2$. Then there exists a quaternion algebra $B = B_{/E}^{\Sigma}$ ramified exactly at primes Σ and all infinite places of E. For a finite set of primes S of F, we put $F_S = \prod_{\mathfrak{l} \in S} F_{\mathfrak{l}}$, $O_S = \prod_{\mathfrak{l} \in S} O_{\mathfrak{l}}$ and $O_{(S)} = F \cap O_S$.

Proposition 3.4. *Let $B_{/E}$ be as above and S be a subset of the set of primes $\mathfrak{l}$ of F above Σ at which $B_{\mathfrak{l}} = B \otimes_E F_{\mathfrak{l}}$ is a division algebra. If $\zeta \in \widehat{R}_F^\times Z(F_{\mathbb{A}}^{(\infty)}) G(F_S) \cap G(F)$ for any given maximal order R_F of B_F is not in $Z(F)$, $F[\zeta] \subset B \otimes_E F$ is isomorphic to a CM quadratic extension M of the following type:*

(1) *M is generated over F by an imaginary root of unity;*
(2) *There exists a totally positive unit $\varepsilon \in O_{(S)}$ such that $M = F[\sqrt{-\varepsilon}]$.*

In particular, if we define $\widetilde{M}_S$ to be the composite of all totally imaginary quadratic extensions of F as listed above, $F[\zeta] \subset B \otimes_E F$ is isomorphic to a CM quadratic extension M of F inside $\widetilde{M}_S$.

Proof. Fix a maximal order R_F of B_F, put $R_{(S)} = R_F \otimes_O O_{(S)}$, and consider $\widehat{R}_S = R_{(S)} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Then we see easily that $\widehat{R}_S^\times = \widehat{R}_F^\times G(F_S)$ for $\widehat{R}_F = \widehat{R}_\emptyset$. If $\zeta \in G(F) \cap \widehat{R}_S^\times Z(F_{\mathbb{A}}^{(\infty)})$, $\zeta = u\xi$ for $\xi \in Z(F_{\mathbb{A}}^{(\infty)})$ and $u \in \widehat{R}_S^\times$. Let $\nu : G_{/E} \to \mathbb{G}_{m/E}$ be the reduced norm map. If $\nu(\zeta) = 1$, we have $\nu(u)\nu(\xi) = \nu(u)\xi^2 = 1$. Thus $\xi \in O_{(S)}^\times$ and hence $\zeta \in R_{(S)}^\times$. Replacing ζ by $\eta = \zeta^2 \nu(\zeta)^{-1}$, we find that $\eta \in R_{(S)}^\times$. We consider the projection $R_S^\times \to G(F_S)$. For $\mathfrak{l} \in S$, $R_{F,\mathfrak{l}}$

is a noncommutative local ring with a unique maximal two-sided ideal $\mathfrak{m}$ with $R_{F,\mathfrak{l}}/\mathfrak{m} = O/\mathfrak{l}$. Thus $B_{\mathfrak{l}}^{\times} = G(F_{\mathfrak{l}}) = \bigcup_{n\in\mathbb{Z}} \mathfrak{m}^n$, and for each $x \in G(F_{\mathfrak{l}})$, we can define $\mathrm{ord}_{\mathfrak{l}}(x) \in \mathbb{Z}$ so that $x \in \mathfrak{m}^{\mathrm{ord}_{\mathfrak{l}}(x)} - \mathfrak{m}^{\mathrm{ord}_{\mathfrak{l}}(x)+1}$. Then we have an extension $1 \to R_{F,\mathfrak{l}}^{\times} \to G(F_{\mathfrak{l}})^{\times} \xrightarrow{\mathrm{ord}_{\mathfrak{l}}} \mathbb{Z} \to 0$, and $G(G_{\mathfrak{l}}) = \mathbb{Z} \ltimes R_{F,\mathfrak{l}}^{\times}$. Then we have an exact sequence $1 \to G_1(F) \cap \widehat{R}_F^{\times} \to G_1(F) \cap \widehat{R}_S^{\times} \xrightarrow{\mathrm{ord}_S} \mathbb{Z}^S$, where $\mathrm{ord}_S = \prod_{\mathfrak{l}\in S} \mathrm{ord}_{\mathfrak{l}}$. It is well known (e.g., [HMI] 2.1.2) that if $\nu(x) \in O_{\mathfrak{l}}$ for $x \in B_{\mathfrak{l}}$ and $\mathfrak{l} \in \Sigma$, we have $x \in R_{F,\mathfrak{l}}$. This shows ord_S is the zero map, and we have $G_1(F)\cap\widehat{R}_S^{\times} = G_1(F)\cap\widehat{R}_F^{\times}$. Since $\eta \in G^1(F) \cap \widehat{R}_F^{\times}$ which is a finite group, we find that η is a primitive nth root of 1 for some positive integer n. Then $\zeta^{2n} = \eta^n\nu(\zeta)^n = \nu(\zeta)^n \in O_{(S)+}^{\times}$, where $O_{(S)+}^{\times}$ is the group of totally positive units in $O_{(S)}$. Thus if $\zeta \notin Z(F)$, $F[\zeta]$ is a quadratic extension of F. If n has an odd prime factor ℓ, $F[\zeta] \supset F[\eta^{n/\ell}]$ and $[F(\zeta) : F] = [F(\eta^{n/\ell}) : F] = 2$, which implies $F[\zeta] = F[\eta] = F[\eta^{n/\ell}]$. Thus in this case, $F[\zeta]$ is a quadratic extension of F generated by a root of unity. Suppose that n is a 2-power. If $n > 2$, $F[\eta] \neq F$, and again we have $F[\zeta] = F[\eta]$, and $F[\zeta]$ is generated by a root of unity. If $n \leq 2$, $\eta = \pm 1$ and $\pm\zeta^2 = \nu(\zeta) \in O_{(S)+}^{\times}$. Since $F[\zeta]$ is totally imaginary, $\eta = -1$ and $\zeta = \sqrt{-\nu(\zeta)}$. □

Corollary 3.5. *Let the notation be as in* Proposition 3.4. *Then the extension $\widetilde{M}_S/F$ is finite, and if $B \otimes_E F$ ramifies at a prime totally splits in $\widetilde{M}_S/F$, we have $(gUg^{-1} \cdot Z(F_{\mathbb{A}}^{(\infty)})) \cap G(F) = Z(F)$ for $U = \widehat{R}_F^{\times} G(F_S) = \widehat{R}_S^{\times}$.*

Proof. There are finitely many CM quadratic extensions over F generated by roots of unity. Since isomorphism classes of CM quadratic extensions of the form $F[\sqrt{-\varepsilon}]/F$ for $\varepsilon \in O_{(S)+}^{\times}$ is in bijection with $O_{(S)+}^{\times}/(O_{(S)}^{\times})^2 - \{1\}$ by $F[\sqrt{-\varepsilon}] \leftrightarrow \varepsilon \in O_{(S)+}^{\times}/(O_{(S)}^{\times})^2 - \{1\}$, there are finitely many such extensions. Thus $\widetilde{M}_S/F$ is a finite $(2, 2, \ldots, 2)$-extension. If B_F/F ramifies at a prime $\mathfrak{q}$ totally splits in $\widetilde{M}_S/F$, $\mathfrak{q}$ splits in any quadratic subfield M/F of $\widetilde{M}_S$. Such an M cannot be embedded into B_F. This shows the last assertion, because $g\widehat{R}_F^{\times}g^{-1} \cap B$ is one of the maximal orders of B_F. □

Instead of imposing ramification for the quaternion algebra B, we can enlarge the level by a square-free ideal outside the given level to assure the condition ${}^xUZ(F_{\mathbb{A}}^{(\infty)}) \cap G_1(F) = Z(F)$.

Lemma 3.6. *Let the notation be as in* Proposition 3.4. *Let Q be a finite set of prime ideals $\mathfrak{q}$ of O unramified over $\mathbb{Q}$ such that*

(1) $\mathfrak{q} \nmid d(B_F)$;
(2) *for any totally imaginary quadratic extension M/F inside $\widetilde{M}_S$, at least one prime $\mathfrak{q} \in Q$ remains prime in M/F.*

Then ${}^xUZ(F_{\mathbb{A}}^{(\infty)}) \cap G_1(F) = Z(F)$ for all $x \in G(F_{\mathbb{A}}^{(\infty)})$, where U is the open compact subgroup $U_0(\mathfrak{Q}d(B_F))$ of $G(F_{\mathbb{A}}^{(\infty)})$ for $\mathfrak{Q} = \prod_{\mathfrak{q}\in Q}\mathfrak{q}$.

Proof. We consider the Eichler order $R_{\mathfrak{q}} \subset M_2(O_{\mathfrak{q}})$ made up of matrices upper triangular modulo $\mathfrak{q}$. Then $R_{\mathfrak{q}}$ is a local ring with residue field isomorphic to $O/\mathfrak{q}$. Take $\zeta \in {}^xUZ(F_{\mathbb{A}}^{(\infty)}) \cap G_1(F)$ outside $Z(F)$. Since $\mathfrak{q}$ is unramified in $F/\mathbb{Q}$, $O_{\mathfrak{q}}[\zeta]$ is the $\mathfrak{q}$-adic integer ring of $F_{\mathfrak{q}}[\zeta]$. If $\mathfrak{q}$ remains prime in $O_{\mathfrak{q}}[\zeta]$, $O_{\mathfrak{q}}[\zeta]/\mathfrak{q}$ is a quadratic extension of $O/\mathfrak{q}$. Thus $O_{\mathfrak{q}}[\zeta]$ cannot be embedded in $R_{\mathfrak{q}}$. This shows $\zeta \notin {}^xUZ(F_{\mathbb{A}}^{(\infty)}) \cap G_1(F)$, a contradiction. This shows the desired result. □

4. Compatible systems

A holomorphic Hilbert modular Hecke eigenform f over a totally real field E is supposed to be associated to a rank 2 motive M defined over E. For each real embedding $\sigma : E \to \mathbb{R}$, $M \otimes_{E,\sigma} \mathbb{R}$ has Hodge weight $(\kappa_{1,\sigma}, \kappa_{2,\sigma})$ and $(\kappa_{2,\sigma}, \kappa_{1,\sigma})$ with $\kappa_{1,\sigma} \le \kappa_{2,\sigma}$. Writing $I_E = \mathrm{Hom}_{\mathrm{field}}(E, \mathbb{R})$, we then define the weight of f to be $\kappa = (\kappa_1, \kappa_2)$, where $\kappa_j = \sum_{\sigma\in I_E} \kappa_{j,\sigma}\sigma$. The existence of the motive is only known if $\kappa_2 - \kappa_1 > I_E$ in general with equality allowed when $[E : \mathbb{Q}]$ is odd (cf. [B]), where $I_E = \sum_{\sigma\in I_E} \sigma$ and the inequality $\kappa_2 - \kappa_1 > I_E$ means that $\kappa_{2,\sigma} - \kappa_{1,\sigma} > 1$ for at least one σ. Put $k_\sigma = \kappa_{2,\sigma} - \kappa_{1,\sigma} + 1$ (which is classically called the weight of the Hilbert modular form).

The weight of f can be also detected via the Galois representation attached to f by the ℓ-adic Hodge-Tate weight if the Galois representation is of Hodge-Tate type. The easiest case of Hodge-Tate type representations is ℓ-ordinary representations. Let us explain this case more. We write $\mathcal{N}_\ell$ for the ℓ-adic cyclotomic character for each prime ℓ. Then $\mathcal{N} = \{\mathcal{N}_\ell\}_\ell$ is a strictly compatible system of ℓ-adic characters with coefficients in $\mathbb{Q}$. Let $\rho = \{\rho_{\mathfrak{l}}\}$ be a two dimensional strictly compatible system of Galois representations with coefficients in a number field T of $\mathrm{Gal}(\overline{E}/E)$ for an algebraic closure $\overline{E}$ of E. Suppose that $\rho_{\mathfrak{l}}$ ramifies only at finitely many places of E and is absolutely irreducible. In other words, $\rho_{\mathfrak{l}}$ ramifies possibly at a finite set S of primes of E (independent of $\mathfrak{l}$) and primes dividing the residual characteristic ℓ of $\mathfrak{l}$. The minimal set S as above is called

the ramification set of primes for ρ. Let ℓ be the rational prime in $\mathfrak{l}$ (the residual characteristic of $\mathfrak{l}$). We call $\rho_{\mathfrak{l}}$ *ℓ-ordinary* if for any prime $\mathfrak{L}|\ell$ of E, $\rho_{\mathfrak{l}}$ restricted to the decomposition group at $\mathfrak{L}$ is isomorphic to an upper triangular representation $\left(\begin{smallmatrix}\varepsilon_{\mathfrak{L}} & * \\ 0 & \delta_{\mathfrak{L}}\end{smallmatrix}\right)$ with $\delta_{\mathfrak{L}}$ unramified. In the ℓ-ordinary case, $\varepsilon_{\mathfrak{L}} = \mathcal{N}_{\ell}^{k-1}$ over an open subgroup of the inertia group $I_{\mathfrak{L}}$ for a positive integer k, and the Hodge–Tate weight of ρ is given by $(0, (k-1)I_E)$.

For $\sigma \in \Delta$, extend σ to an element $\widetilde{\sigma} \in \mathrm{Gal}(\overline{F}/E)$ and define $\rho_{\mathfrak{l}}^{\sigma}(g) = \rho_{\mathfrak{l}}(\widetilde{\sigma} g \widetilde{\sigma}^{-1})$ for $g \in \mathrm{Gal}(\overline{F}/F)$. Then the isomorphism class of $\rho_{\mathfrak{l}}^{\sigma}$ is independent of the choice of the extension $\widetilde{\sigma}$, and $\rho^{\sigma} = \{\rho_{\mathfrak{l}}^{\sigma}\}_{\mathfrak{l}}$ is another strictly compatible system of Galois representations. Writing ℓ for the residual characteristic of $\mathfrak{l}$, we have well defined prime-to–ℓ Artin conductor $C^{(\ell)}(\rho_{\mathfrak{l}})$ of $\rho_{\mathfrak{l}}$ (as we recall the definition in the proof of Lemma 4.4). The p-primary part of $C^{(\ell)}(\rho_{\mathfrak{l}})$ for a prime $p \neq \ell$ is independent of $\mathfrak{l}$. Define $C(\rho)$ by the least common multiple of $\{C^{(\ell)}(\rho_{\mathfrak{l}})\}_{\mathfrak{l}}$. If $\rho^{\sigma} \cong \rho$, $C(\rho)^{\sigma} = C(\rho)$. If $\rho_{\mathfrak{l}}$ extends to a Galois representation $\rho_{E,\mathfrak{l}}$ of $\mathrm{Gal}(\overline{F}/E)$ into $GL_2(T_{E,\mathfrak{l}})$ for a finite extension T_E/T for one prime $\mathfrak{l}$, ρ extends to a strictly compatible system of Galois representations ρ_E (with coefficients in T_E) which has $\rho_{E,\mathfrak{l}}$ as a member (see [Kh1] Section 2 and Lemma 4.2 in the text). The representation $\rho_{\mathfrak{l}}$ extends to a representation $\rho_{E,\mathfrak{l}}$ if and only if the obstruction class $Ob(\rho_{\mathfrak{l}}) \in H^2(\Delta, T_{\mathfrak{l}}^{\times})$ vanishes ([MFG] Theorem 4.35), where Δ acts trivially on $T_{\mathfrak{l}}$.

Here is a conjecture generalizing the one by Shimura–Taniyama:

Conjecture 4.1. *Let ρ be a strictly compatible system of absolutely irreducible representations of the Galois group $\mathrm{Gal}(\overline{F}/E)$ with $\det\rho = \mathcal{N}^{k-1}\chi$ for $k > 0$ and a finite order Hecke character $\chi : E_{\mathbb{A}}^{\times}/E^{\times} \to \overline{\mathbb{Q}}^{\times}$. Suppose that $\rho_{\mathfrak{l}}$ is either ℓ-ordinary for at least one prime $\mathfrak{l}$ or motivic of weight $\kappa_E = (0, (k-1)I_E)$. Then if $\det(\rho)(c) = -1$ for all complex conjugation $c \in \mathrm{Gal}(\overline{F}/E)$, ρ is associated to a cuspidal automorphic representation of $GL_2(E_{\mathbb{A}})$ of conductor $C(\rho)$ and of central character $\chi|\cdot|_{\mathbb{A}}^{2-k}$ whose component at each infinite place is in the holomorphic discrete series of weight k if $k \geq 2$ and is the limit of holomorphic discrete series if $k = 1$.*

The Galois representation of a holomorphic Hecke eigenform is motivic if either $k \geq 3$ or $[F : \mathbb{Q}]$ is odd ([B] and [BR]). If $k = 2$, we always have a prime $\mathfrak{l}$ splits in F/E for which a given f is $\mathfrak{l}$-ordinary. If $k = 1$, a modular Galois representation

is an Artin representation (by a result of Deligne-Serre), it is motivic. Thus the conjecture covers all weight $k \geq 1$. If $\rho_{\mathfrak{l}}$ is ordinary at $\mathfrak{l}$ or motivic, $\rho_{\mathfrak{l}}$ has ℓ-adic Hodge-Tate type with weight $HT = \{0 \leq k-1\}_{\mathfrak{L}}$ for split primes $\mathfrak{L}|\ell$ in E (by our assumption). If we assume that ρ is motivic, the conjecture can be stated without ordinarity condition for the Hodge-Tate weight $\kappa = (\kappa_1, \kappa_2)$ (which is not necessarily of the form $(0, (k-1)I_E)$).

By the potential modularity by Taylor of mod p representations ([T1]; see Lemma 4.2) and by the modular lifting theorem in [W] (see also [DFG]), Serre's mod p modularity conjecture for $k \geq 2$ implies the above conjecture for $E = \mathbb{Q}$ (see [Kh3] Section 6). For $k = 1$, as was pointed out by Serre, Serre's conjecture implies the strong form of Artin's conjecture [Se]; so, the case $k = 1$ is also known for $E = \mathbb{Q}$.

Let F/E be a finite Galois extension with Galois group Δ. Let $\rho_{\mathfrak{l}} : \mathrm{Gal}(\overline{F}/F) \to GL_n(\overline{\mathbb{Q}}_\ell)$ be an absolutely irreducible Galois representation. For $\delta \in \Delta$, extend it to $\widetilde{\delta} \in \mathrm{Gal}(\overline{F}/E)$, and define $\rho_{\mathfrak{l}}^{\delta}(\sigma) = \rho_{\mathfrak{l}}(\widetilde{\delta}\sigma\widetilde{\delta}^{-1})$. The isomorphism class of $\rho_{\mathfrak{l}}^{\delta}$ only depends on δ (e.g., [MFG] 4.3.5).

Lemma 4.2. *Let F/E be a finite totally real Galois extension with simply 2-connected Galois group Δ. Assume $\rho = \{\rho_{\mathfrak{l}}\}_{\mathfrak{l}}$ to be a strictly compatible system as in* Conjecture 4.1 *of 2-dimensional absolutely irreducible $\mathfrak{l}$-adic Galois representations invariant under Δ (that is, $\rho^{\delta} \cong \rho$ for all $\delta \in \Delta$) and that* $\det(\rho) = \{\det(\rho_{\mathfrak{l}})\}_{\mathfrak{l}}$ *extends to a strictly compatible system $\chi\mathcal{N}^{k-1} = \{\chi_{\mathfrak{l}}\mathcal{N}_\ell^{k-1}\}_{\mathfrak{l}}$ (of $\mathfrak{l}$-adic characters) of* $\mathrm{Gal}(\overline{F}/E)$ *for a finite order character χ. If $k \geq 2$, there exists a unique strictly compatible system $\rho_E = \{\rho_{E,\mathfrak{l}}\}_{\mathfrak{l}}$ extending ρ with* $\det(\rho) = \chi\mathcal{N}^{k-1}$.

Proof. More generally, we start with n-dimensional strictly compatible system ρ. If $\rho_{\mathfrak{l}}^{\delta} \cong \delta_{\mathfrak{l}}$ for all $\delta \in \Delta$, as is well known (e.g., [MFG] 4.3.5), we can associate a unique obstruction class $Ob(\rho_{\mathfrak{l}}) \in H^2(\Delta, \overline{\mathbb{Q}}_\ell^\times)$, where Δ acts trivially on $\overline{\mathbb{Q}}_\ell^\times$. Then $Ob(\rho_{\mathfrak{l}}) = 0$ if and only if $\rho_{\mathfrak{l}}$ extends to a continuous representation $\widetilde{\rho}_{\mathfrak{l}} : \mathrm{Gal}(\overline{F}/E) \to GL_n(\overline{\mathbb{Q}}_\ell)$. All other extensions of $\rho_{\mathfrak{l}}$ to $\mathrm{Gal}(\overline{F}/E)$ (if one $\widetilde{\rho}_{\mathfrak{l}}$ exists) are of the form $\widetilde{\rho}_{\mathfrak{l}} \otimes \varphi$ for a character $\varphi : \Delta \to \overline{\mathbb{Q}}_\ell^\times$ (see [MFG] Theorem 4.35). If $\det(\rho_{\mathfrak{l}})$ extends to $\mathrm{Gal}(\overline{F}/E)$, we have $n \cdot Ob(\rho_{\mathfrak{l}}) = 0$ in $H^2(\Delta, \overline{\mathbb{Q}}_\ell^\times)$, because $Ob(\det(\rho_{\mathfrak{l}})) = n \cdot Ob(\rho_{\mathfrak{l}})$ (see [MFG] proof of Lemma 5.32). Thus if $n = 2$, $Ob(\rho_{\mathfrak{l}})$ is in $H^2(\Delta, \overline{\mathbb{Q}}_\ell^\times)[2]$, which is a surjective image of $H^2(\Delta, \mu_2)$ (see Lemma 7.3).

Assume $n = 2$. By the simple 2-connectedness of Δ, we find $Ob(\rho_{\mathfrak{l}}) = 0$ for all $\mathfrak{l}$, and $\rho_{\mathfrak{l}}$ extends to a Galois representation $\widetilde{\rho}_{\mathfrak{l}}$ of $\mathrm{Gal}(\overline{F}/E)$ into $GL_2(\overline{\mathbb{Q}}_\ell)$. Taking the determinant, $\det(\widetilde{\rho}_{\mathfrak{l}})$ is an extension of $\det(\rho_{\mathfrak{l}})$. Thus $\det(\widetilde{\rho}_{\mathfrak{l}}) = \chi_{\mathfrak{l}}\mathcal{N}_\ell^{k-1}\varphi$ for a character $\varphi \in \mathrm{Hom}(\Delta, \overline{\mathbb{Q}}_\ell^\times) = H^1(\Delta, \overline{\mathbb{Q}}_\ell^\times)$. By the simple 2-connectedness, $H^1(\Delta, \mu_2) = 0$, which implies $H^1(\Delta, \overline{\mathbb{Q}}_\ell^\times)[2] = 0$ by Lemma 7.3. Thus the multiplication by 2 is an automorphism of $\mathrm{Hom}(\Delta, \overline{\mathbb{Q}}_\ell^\times)$, and we can find a unique $\psi \in \mathrm{Hom}(\Delta, \overline{\mathbb{Q}}_\ell^\times)$ with $\psi^2 = \varphi$. The $\rho_{E,\mathfrak{l}} = \widetilde{\rho}_{\mathfrak{l}} \otimes \psi^{-1}$ is an extension of $\rho_{\mathfrak{l}}$ with determinant $\chi_{\mathfrak{l}}\mathcal{N}_\ell^{k-1}$. By the uniqueness of ψ as above, the extension $\rho_E = \{\rho_{E,\mathfrak{l}}\}_{\mathfrak{l}}$ with $\det \rho_E = \chi\mathcal{N}^{k-1}$ is unique.

To prove the strict compatibility when $k \geq 2$, we may assume that $\rho_{\mathfrak{l}} \otimes \varphi \ncong \rho_{\mathfrak{l}}$ for any Galois character φ of $\mathrm{Gal}(\overline{F}/E)$, because otherwise, $\rho = \mathrm{Ind}_M^F \phi$ for a compatible system ϕ of characters of a quadratic extension M/F (an in that case, results follows from class field theory). By [T2], if one can find a prime $\mathfrak{l}$ with $\ell \geq \max(k, 5)$ such that $\rho_{\mathfrak{l}} \mod \mathfrak{l}$ has nonsoluble image and a totally real finite extension F'/F inside $\overline{F}$ unramified at ℓ (over $\mathbb{Q}$) such that $\rho_{\mathfrak{l}} \mod \mathfrak{l}$ is associated to a Hilbert Hecke eigenform on $GL_2(F'_{\mathbb{A}})$, then there exists a holomorphic automorphic representation π' of weight k such that the associated strict compatible system $\rho_{\pi'}$ is isomorphic to $\rho|_{\mathrm{Gal}(\overline{F}/F')}$. The existence of such F' was proven in [T1] if $F = \mathbb{Q}$, and it is generalized to general F by C. Virdol assuming that $k \geq 2$, and also it is proven that F' can be chosen to be a Galois extension over $\mathbb{Q}$ in [V] Theorem 2.1. By the independence of weight of the universal nearly ordinary Hecke algebra of level Np^∞ (cf. [H88] and [H89a]), residual modularity of weight 2 forms implies residual modularity of higher weight modular forms. Thus by [T2], we can find an automorphic representation π' on $GL_2(F'_{\mathbb{A}})$ as above. Hereafter we follow [Kh1] Section 2 to prove strict compatibility of ρ_E. By [SBT] Theorem 4.2 (d), for any subfield $L \subset F'$ with soluble Galois group $\mathrm{Gal}(F'/L)$, one can find an automorphic representation π_L on $GL_2(F''_{\mathbb{A}})$ such that $\rho_{\pi_L}|_{\mathrm{Gal}(\overline{F}/F')} \cong \rho$. We can write the trivial character $\mathbf{1}$ of $\mathrm{Gal}(F'/E)$ as $\sum_j m_j \mathrm{Ind}_{L_j}^E \chi_j$ for integers m_j (virtual multiplicity) by an argument of Artin–Brauer for abelian Galois characters χ_j of $\mathrm{Gal}(F'/L_j)$ for intermediate fields $E \subset L_j \subset F'$ with soluble $\mathrm{Gal}(F'/L_j)$. Then we have a virtual identity

$$\rho_{E,\mathfrak{l}} \cong \sum_j m_j \rho \otimes \mathrm{Ind}_{L_j}^E(\chi_j \otimes \rho_{\pi_{L_j},\mathfrak{l}}),$$

which shows the strict compatibility of ρ_E because $\rho_{\pi_{L_j}}$ is strictly compatible. □

Write $\mathfrak{P}$ for a prime factor of rational prime p in O. We put $\mathfrak{p} = \mathfrak{P} \cap O_E$, and we write $D_\mathfrak{p}$ (resp. $D_\mathfrak{P}$) for the decomposition group of $\mathfrak{p}$ (resp. $\mathfrak{P}$) in $\mathrm{Gal}(\overline{F}/E)$ (resp. $\mathrm{Gal}(\overline{F}/F)$). We take $D_\mathfrak{p}$ so that $D_\mathfrak{p} \supset D_\mathfrak{P}$.

Lemma 4.3. *Let the notation and the assumption be as in* Lemma 4.2. *Suppose*

(1) *for a prime* $\mathfrak{P} \nmid \ell$, $\rho_\mathfrak{l}|_{D_\mathfrak{P}} \cong \begin{pmatrix} \eta_{1,\mathfrak{P}} & * \\ 0 & \eta_{2,\mathfrak{P}} \end{pmatrix}$ *for characters* $\eta_{j,\mathfrak{P}} : D_\mathfrak{P} \to \overline{\mathbb{Q}}_\ell$;
(2) $\eta_{j,\mathfrak{P}}$ *extends to a character* $D_\mathfrak{p} \to \overline{\mathbb{Q}}_\ell^\times$;
(3) *if* $\mathfrak{P}$ *ramifies over* $\mathfrak{p}$, *either* $\eta_{1,\mathfrak{P}} \neq \eta_{2,\mathfrak{P}}$ *or* $\rho_\mathfrak{l}|_{D_\mathfrak{P}}$ *is not semi-simple or* $D_\mathfrak{p}/D_\mathfrak{P}$ *does not have dihedral, tetrahedral or octahedral quotient.*

Then $\rho_{E,\mathfrak{l}}|_{D_\mathfrak{p}} \cong \begin{pmatrix} \eta_{1,\mathfrak{p}} & * \\ 0 & \eta_{2,\mathfrak{p}} \end{pmatrix}$ *for one of the extensions* $\eta_{j,\mathfrak{p}}$ *of* $\eta_{j,\mathfrak{P}}$. *If* $\mathfrak{P}$ *is unramified over* $\mathfrak{p}$, *the restriction of* $\eta_{j,\mathfrak{p}}$ *to the inertia group* $I_\mathfrak{p}$ *of* $\mathfrak{p}$ *is determined by* $\eta_{j,\mathfrak{P}}$ *(*$j = 1, 2$*).*

Proof. The last assertion follows from the fact that $I_\mathfrak{P} = I_\mathfrak{p}$ if $\mathfrak{P}$ is unramified over $\mathfrak{p}$.

Since ρ extends to a compatible system of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ with given determinant, $\varphi = \rho_\mathfrak{l}|_{D_\mathfrak{p}}$ extends $\phi = \rho_\mathfrak{l}|_{D_\mathfrak{P}}$. We may assume that ϕ is upper triangular of the form $\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$. Then for $\sigma \in D_\mathfrak{p}$, we have

$$\begin{pmatrix} \phi_1^\sigma(g) & * \\ 0 & \phi_2^\sigma(g)) \end{pmatrix} = \varphi(\sigma g \sigma^{-1}) = \varphi(\sigma) \begin{pmatrix} \phi_1(g) & * \\ 0 & \phi_2(g) \end{pmatrix} \varphi(\sigma)^{-1}$$

for $\phi_j^\sigma(g) = \phi_j(\sigma g \sigma^{-1})$. Thus $D_\mathfrak{p}$ acts on $\{\phi_1, \phi_2\}$. Let D_1 be the stabilizer of ϕ_1 in $D_\mathfrak{p}$. Then there are two possibilities, Case 1: $D_1 = D_\mathfrak{p}$ and Case 2: $[D_\mathfrak{p} : D_1] = 2$. In Case 2, $\varphi = \rho_\mathfrak{l}|_{D_\mathfrak{p}} \cong \mathrm{Ind}_{D_\mathfrak{P}}^{D_\mathfrak{p}} \phi_1$ is irreducible and ϕ_j does not extends to $D_\mathfrak{p}$; so, by our assumption (2), we are in Case 1. If $\phi_1 \neq \phi_2$ or ϕ is not semi-simple, φ has to be upper triangular, and we get the desired result. Thus we may suppose that $\phi_1 = \phi_2$ and ϕ is semi-simple. In this case, φ is either upper triangular or a factor of $\mathrm{Ind}_{D_\mathfrak{P}}^{D_\mathfrak{p}} \phi_1 = \varphi_1 \otimes \mathrm{Ind}_{F_\mathfrak{P}}^{E_\mathfrak{p}} \mathbf{1}$ for an extension φ_1 of ϕ_1. If $\mathfrak{P}$ is unramified over $\mathfrak{p}$, $D_\mathfrak{p}/D_\mathfrak{p}$ is an abelian cyclic group, and $\mathrm{Ind}_{D_\mathfrak{P}}^{D_\mathfrak{p}} \phi_1$ is the sum of characters. Thus φ must be reducible. Suppose that $\mathfrak{P}$ ramifies over $\mathfrak{p}$, $\phi_1 = \phi_2$ with semi-simple ϕ and that φ is irreducible. Then $\mathrm{Ind}_{F_\mathfrak{P}}^{E_\mathfrak{p}} \mathbf{1}$ contains an irreducible factor φ' such that $\varphi \cong \varphi_1 \otimes \varphi'$. The image $\varphi'(D_\mathfrak{p})$ modulo center is either a dihedral, tetrahedral or octahedral group, because $D_\mathfrak{p}$ is soluble. The dihedral, tetrahedral or octahedral image is prohibited by our assumption. □

Lemma 4.4. *Let the notation and the assumption be as in* Lemmas 4.2 *and* 4.3. *For a prime* $\mathfrak{P} \nmid \ell$ *of* O*, suppose* $\rho_{\mathfrak{l}}|_{I_{\mathfrak{P}}}$ *has infinite image. Then we have*

(1) $\rho_{E,\mathfrak{l}}|_{D_{\mathfrak{p}}} \cong \begin{pmatrix} \eta\mathcal{N}_\ell & * \\ 0 & \eta \end{pmatrix}$ *for a character* $\eta : D_{\mathfrak{p}} \to \overline{\mathbb{Q}}_\ell^\times$;
(2) $\eta^2 = (\chi_{\mathfrak{l}}\mathcal{N}_\ell^{k-2})|_{D_{\mathfrak{p}}}$;
(3) $\rho_{E,\mathfrak{l}}|_{D_{\mathfrak{p}}}$ *is not semisimple.*

Proof. We first recall the definition of the conductor ideal $0 < C(\varphi)$ of O of a general strictly compatible system $\varphi = \{\varphi_{\mathfrak{l}}\}_{\mathfrak{l}}$ of two-dimensional Galois representations of $\mathrm{Gal}(\overline{F}/E)$ with coefficients in a number field T. We write the $\mathfrak{p}$–primary part of the ideal $C(\varphi)$ as $c_{\mathfrak{p}}(\varphi)$. Let p be the residual characteristic of $\mathfrak{p}$. This ideal $c_{\mathfrak{p}}(\varphi) = \mathfrak{p}^e$ can be determined by choosing a prime ideal $\mathfrak{l}$ prime to p and looking at the restriction of $\varphi_{\mathfrak{l}}$ to the inertia group of $I_{\mathfrak{p}}$. We take $c_{\mathfrak{p}}(\varphi)$ to be the Artin conductor given in [GME] (5.2) if $\varphi_{\mathfrak{l}}(I_{\mathfrak{p}})$ is finite.

We would like to show that the definition of $c_{\mathfrak{p}}(\varphi)$ is independent of the choice of $\mathfrak{l}$ (assuming the finiteness of $\varphi_{\mathfrak{l}}(I_{\mathfrak{p}})$). Let $\mathfrak{q}$ be another prime of E outside p. Let S be the finite set of ramified primes of φ. Let $\mathfrak{G}_F$ be the Galois group of the maximal extension of F unramified outside S and ℓq for $(\ell) = \mathfrak{l} \cap \mathbb{Z}$ and $(q) = \mathfrak{q} \cap \mathbb{Z}$.

Let I_1 be the wild inertia subgroup of $I_{\mathfrak{p}}$. Since I_1 is p–profinite (see [MFG] 3.2.5), $\varphi_{\mathfrak{l}}(I_1)$ is finite for all $\mathfrak{l}$ prime to p (see [MFG] Lemma 2.19). Take $\sigma \in I_1$. Since $\varphi_{\mathfrak{l}}(\sigma)$ and $\varphi_{\mathfrak{q}}(\sigma)$ are of finite order, these two matrices are semi-simple. Take τ sufficiently close to σ in G so that for a given positive integer N

$$P_1(X) = \det(X - \varphi_{\mathfrak{l}}(\sigma)) \equiv \det(T - \varphi_{\mathfrak{l}}(\tau)) = Q_1(T) \mod \mathfrak{l}^N \text{ and}$$
$$P_2(X) = \det(X - \varphi_{\mathfrak{q}}(\sigma)) \equiv \det(X - \varphi_{\mathfrak{q}}(\tau)) = Q_2(T) \mod \mathfrak{q}^N$$

Since the eigenvalues of $\varphi_{\mathfrak{q}}(\sigma)$ and $\varphi_{\mathfrak{l}}(\sigma)$ are all in μ_M for sufficiently large integer M, if we take N large, the characteristic polynomial of τ determines all eigenvalues of the two polynomials $P_j(T)$. By the Chebotarev density theorem, we can take $\tau = Frob_{\mathfrak{x}}$ for a prime $\mathfrak{x}$ unramified for both $\varphi_{\mathfrak{l}}$ and $\varphi_{\mathfrak{q}}$. Then by compatibility, $Q_1(T) = Q_2(T)$ and hence $P_1(T) = P_2(T)$; so, $\varphi_{\mathfrak{l}}(\sigma)$ and $\varphi_{\mathfrak{q}}(\sigma)$ have the same characteristic polynomial. Since $\varphi_{\mathfrak{l}}(I_1)$ and $\varphi_{\mathfrak{q}}(I_1)$ are both finite, we now know that the two representations factoring through a finite quotient of I_1 are semi-simple and have the same trace. This tells us the two representations of I_1 are equivalent over any algebraically closed field containing $E_{\mathfrak{l}}$ and $E_{\mathfrak{q}}$ (cf.

[MFG] Corollary 2.8), and the conductor defined for $\varphi_\mathfrak{l}|_{I_\mathfrak{p}}$ and $\varphi_\mathfrak{q}|_{I_\mathfrak{p}}$ are equal. Thus $c_\mathfrak{p}(\varphi)$ is well defined independently of $\mathfrak{l} \nmid p$. In particular, if $\varphi_\mathfrak{l}$ is unramified at $\mathfrak{p}$, then $c_\mathfrak{p}(\varphi) = 1$.

We now show that $\varphi_\mathfrak{l}(I_\mathfrak{p})$ is finite if and only if $\varphi_\mathfrak{l}|_{I_\mathfrak{p}}$ is semi-simple. We quote the following facts from [MFG] 3.2.5: $D_\mathfrak{p} = \phi^{\widehat{\mathbb{Z}}} \ltimes I_\mathfrak{p}$; $I_\mathfrak{p} = \widehat{\mathbb{Z}}^{(p)} \ltimes I_1$ for the p–profinite group I_1 (the wild inertia group) and a lift of Frobenius element ϕ; the element ϕ acts on $I_\mathfrak{p}/I_1$ by $\phi\sigma\phi^{-1} = \sigma^P$ for $P = N_{F/\mathbb{Q}}(\mathfrak{p}) = |O/\mathfrak{p}|$.

By the above formulas, we may regard $G/I_\mathfrak{p}$ as a subgroup of G. Then by $\phi\sigma\phi^{-1} = \sigma^P$, the set of eigenvalues $\{\zeta, \xi\}$ of $\varphi_\mathfrak{l}(\sigma)$ for $\sigma \in I_\mathfrak{p}/I_1$ has to satisfy $\{\zeta^P, \xi^P\} = \{\zeta, \xi\}$. Thus they are in μ_{P^2-1}, and hence the abelian group $\varphi_\mathfrak{l}((I_\mathfrak{p}/I_1)^{P^2-1})$ is contained in a unipotent subgroup of $GL_2(E_\mathfrak{l})$. If the restriction of $\varphi_\mathfrak{l}$ to $I_\mathfrak{p}$ is semi-simple, $\varphi_\mathfrak{l}$ has finite image over $I_\mathfrak{p}$. In particular, if $\varphi_\mathfrak{l}(I_1)$ has non-central element, its normalizer is a normalizer of a torus; so, $\varphi_\mathfrak{l}$ is semi-simple, and $\varphi_\mathfrak{l}$ has finite image on $I_\mathfrak{p}$.

Suppose that $\varphi_\mathfrak{l}$ has infinite image on $I_\mathfrak{p}$. Then by the above argument, $\varphi_\mathfrak{l}(I_1)$ is central, and we may assume to have $\sigma \in I_\mathfrak{p}/I_1$ such that $\varphi_\mathfrak{l}(\sigma)$ is non-trivial upper unipotent matrix. Then again by $\phi\sigma\phi^{-1} = \sigma^P$, $\varphi_\mathfrak{l}(\phi)$ is a diagonal matrix having two eigenvalues with ratio P. Since the image under $\varphi_\mathfrak{l}$ of $I_\mathfrak{p}/I_1$ is abelian, we conclude that on G

$$\varphi_\mathfrak{l}(\sigma) \cong \begin{pmatrix} \mathcal{N}_\ell\eta & * \\ 0 & \eta \end{pmatrix}$$

for a character $\eta : D_\mathfrak{p} \to T_\mathfrak{l}^\times$. By local class field theory, we may regard η as a character of $F_\mathfrak{p}^\times$. Then we define the conductor $C(\eta)$ of η by the minimal power $\mathfrak{p}^e$ such that $x \equiv 1 \mod \mathfrak{p}^e \Rightarrow x \in \mathrm{Ker}(\eta)$. Then, we define $c_\mathfrak{p}(\varphi) = C(\eta)^2$ if $C(\eta) \subsetneq O$ and $c_\mathfrak{p}(\varphi) = \mathfrak{p}$ if $C(\eta) = 1$. We can easily check by strict compatibility, this definition does not depend on the choice of $\mathfrak{l}$.

Applying the above argument to the strictly compatible system $\{\rho_{E,\mathfrak{l}}\}_\mathfrak{l}$ of representations of $\mathrm{Gal}(\overline{F}/E)$ extending the given one $\{\rho_\mathfrak{l}\}_\mathfrak{l}$ of $\mathrm{Gal}(\overline{F}/F)$ in the lemma, we get the desired assertion. □

Suppose the conditions (df) and (dd) in Section 2. Thus $\Sigma_{st} \neq \emptyset$ contains all primes ramified in F/E, and Σ_{st} is made up of all primes above $d(B_E)$. In particular, any Δ-invariant automorphic representation of $G(F_\mathbb{A}^{(\infty)})$ is one-dimensional at primes dividing $d(B_E)$. We write $\mathfrak{M}_F^P(\varepsilon_F)$ for the set of isomorphism classes of projective compatible systems of modular Galois representations

associated to irreducible infinite dimensional automorphic representations generated by elements of $\mathcal{M}_F(\varepsilon_F)$. The local representation $\rho_\iota|_{D_\mathfrak{P}}$ is then isomorphic to $\begin{pmatrix}\eta_{2,\mathfrak{P}} & * \\ 0 & \eta_{1,\mathfrak{P}}\end{pmatrix}$, and we can order the two characters $\eta_{j,\mathfrak{P}}$ so that $\eta_{j,\mathfrak{P}} = \varepsilon_{j,\mathfrak{P}}$ on the inertia subgroup $I_\mathfrak{P} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/F)$, where we regard $\varepsilon_{j,\mathfrak{P}}$ as Galois character by local class field theory (see [HMI] Theorem 2.43). Thus $\varepsilon_\mathfrak{p}$ is determined by $\varepsilon_\mathfrak{P}$ for primes $\mathfrak{P}$ unramified in F/E. For primes $\mathfrak{P}$ ramified in F/E, they are in Σ_{st}, and hence $\rho_\iota|_{D_\mathfrak{p}}$ is determined by $\rho_\iota|_{D_\mathfrak{P}}$ up to character twists by Lemma 4.4. In other words, $\rho_f = \rho_{f'}$ as elements of $\mathfrak{M}_F^P(\varepsilon_F)$ for Hecke eigenforms if and only if they are isomorphic each other as representations into $PGL(2)$. Since the (Langlands dual) L-group of $SL(2)$ is $PGL(2)$, by Lemma 2.1 and Corollary 2.2, we know that $\mathrm{Spec}(h_{E'}(\varepsilon_{E'})(\mathbb{C}) \cong \mathfrak{M}_{E'}^P(\varepsilon_{E'})$ as $\mathrm{Gal}(F/E')$-sets for any intermediate extension $F/E'/E$ (cf. [ARL] and [BCG] Chapter 1). Again by Langlands' functoriality (cf. [ARL]), for any soluble subgroup $\Delta' = \mathrm{Gal}(F/E')$ of $\Delta = \mathrm{Gal}(F/E)$, we have $\mathfrak{M}_F^P(\varepsilon_F)^{\Delta'} \cong \mathfrak{M}_{E'}^P(\varepsilon_{E'})$ because any projective representation of $\mathrm{Gal}(\overline{F}/F)$ invariant under $\mathrm{Gal}(F/E')$ extends to a projective representation of $\mathrm{Gal}(\overline{F}/E')$. Since $\mathfrak{M}_{E'}^P(\varepsilon_{E'}) \cong \mathrm{Spec}(h_{E'}(\varepsilon_{E'}))(\mathbb{C})$ and $|\mathrm{Spec}(h_{E'}(\varepsilon_{E'}))(\mathbb{C})| = \dim h_{E'}(\varepsilon_{E'}) = |S_{E'}(\varepsilon_{E'})|$, we get the identity of generalized permutation characters: $\theta_{S_F} = \theta_{\mathrm{Spec}(h_F(\varepsilon_F)(\mathbb{C})}$ from Lemma 3.3 if we have base change relative to F/E' for all intermediate fields E' between F and E and Σ_{st} contains a sufficiently big prime of E which totally splits in $\widetilde{M}_\emptyset/E$ for the number field $\widetilde{M}_\emptyset$ in Proposition 3.4 for $S = \emptyset$ (to make sure the assumptions of Lemma 3.3 are met). Since base-change exists when F/E is soluble (see [BCG]), we get

Proposition 4.5. *Choose a prime* $\mathfrak{q}$ *of* E *which totally splits in* $\widetilde{M}_\emptyset/E$ *for the number field* $\widetilde{M}_\emptyset$ *in* Proposition 3.4 *for* $S = \emptyset$. *Suppose* (dd), (df) *and that* $\mathfrak{q} \in \Sigma_{st}$. *If* F/E *is a soluble Galois extension of totally real fields, then* $S_F(\varepsilon_F) \cong \mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$ *as* $\mathrm{Gal}(F/E)$*-sets.*

5. Base change

Since a proof of Serre's conjecture has been announced by Khare–Wintenberger ([KW] and [KW1]) and Kisin [Ki] for general mod p 2-dimensional odd Galois representations, Conjecture 4.1 will be valid for π as in Theorem 1.1 (once their proofs are confirmed). In any case, Serre's mod p modularity conjecture implies Conjecture 4.1 for $E = \mathbb{Q}$, and to prove Theorem 1.1, we therefore need to deduce

the existence of the base-change $\widehat{\pi}$ assuming Conjecture 4.1 and Conjecture 1.2. We shall do this slightly more generally for the totally real (finite) Galois extension F/E in place of $F/\mathbb{Q}$ in Theorem 1.1. Though Theorem 1.1 is formulated as an existence theorem for base-change, the method employed is actually a descent as sketched in the introduction. This relative setting is important, because we hope to implement a series of descent to remove redundant assumptions of Theorem 1.1. If we have an intermediate Galois extension $F/E/\mathbb{Q}$ and an automorphic representation Π of $G(F_{\mathbb{A}})$ invariant under $\mathrm{Gal}(F/\mathbb{Q})$. Suppose we can make descent of Π to an automorphic representation π_E of $G(E_{\mathbb{A}})$ so that Π is a base-change of π_E to F (in other words, Π descends to π_E). In order to continue this process to descend further π_E to $G(\mathbb{A})$, we need to guarantee the invariance of π_E under $\mathrm{Gal}(E/\mathbb{Q})$. If π_E with a given compatible (Galois invariant) Neben character is uniquely determined by Π, this Galois invariance of π_E follows from that of Π. The importance of simply 2-connectedness of $\mathrm{Gal}(F/E)$ comes from this point. As indicated in the remark (3) following Theorem 1.3, even for quadratic descent (the simplest case of the failure of simply 2-connectedness), this uniqueness of descent often fails; so, we need to impose many conditions including the 2-connectedness in our main result Proposition 5.2 in this section, and this is the main obstacle to removing the restrictive assumptions of Theorem 1.1 even if we have a 2-extension F'/F which is simply 2-connected over $\mathbb{Q}$ (Theorem 1.3). We write $\Delta = \mathrm{Gal}(F/E)$.

We start with the simplest case of base change. We choose a prime $\mathfrak{q}$ of E which totally splits in $\widetilde{M}_\emptyset/E$ for the number field $\widetilde{M}_\emptyset$ in Proposition 3.4 for $S = \emptyset$. Choose a finite set Σ of primes of E such that $|\Sigma| \equiv [E:\mathbb{Q}] \mod 2$ and Σ contains $\mathfrak{q}$. Take the definite quaternion algebra $B_{/E} = B^{\Sigma}$ exactly ramifying at Σ. As in the introduction, we fix a quadruple $\varepsilon_E = (\varepsilon_{1,E}, \varepsilon_{2,E}, \varepsilon_{E+}, \varepsilon_E^-)$ of finite order characters unramified at Σ of $U_0(\mathfrak{c}(\varepsilon_E^-)d(B)) \subset G(E_{\mathbb{A}}^{(\infty)})$. We write ε_F for the pullback of ε_E to groups with coefficients in F. We consider the space $\mathcal{M}_E(\varepsilon_E)$ of automorphic forms on $G(E_{\mathbb{A}})$ as in the introduction, which is the space of functions on $G(E)\backslash G(E_{\mathbb{A}}^{(\infty)})$ with values in $\mathbb{C}$ satisfying $f(xzu) = \varepsilon_{E+}(z)\underline{\varepsilon}_E(u)f(x)$ for $u \in U_0(\mathfrak{c}(\varepsilon_E^-)d(B))$ and $z \in Z(E_{\mathbb{A}}^{(\infty)})$. If ε_E^- is trivial and ε_{E+} is a square, $\mathcal{M}_E(\varepsilon_E)$ has a nontrivial subspace $\mathcal{E}_E(\varepsilon_E)$ made up of functions factoring through the reduced norm map $N : G(E_{\mathbb{A}}^{(\infty)}) \to (E_{\mathbb{A}}^{(\infty)})^\times$. For $f, g \in \mathcal{M}_E(\varepsilon_E)$, $f(x)\overline{g(x)}$ (for complex conjugate $\overline{g(x)}$ of $g(x)$) factors through $Sh_E(\varepsilon) = G(E)\backslash G(E_{\mathbb{A}}^{(\infty)})/U_0(\mathfrak{c}(\varepsilon_E^-)d(B))$, and $\langle f, g\rangle = \sum_{x \in S_E(\varepsilon)} f(x)\overline{g(x)}$ is a

positive definite non-degenerate hermitian form. We write $\mathcal{S}_E(\varepsilon_E)$ for the orthogonal complement of $\mathcal{E}_E(\varepsilon_E)$. We also write $\mathcal{H}_E(\varepsilon_E)$ for the subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathcal{M}_E(\varepsilon_E))$ generated by Hecke operators UxU for $x \in G(E_{\mathbb{A}}^{(\infty)})$ with $x_{\mathfrak{l}} = 1$ if $\mathfrak{l}|\mathfrak{c}(\varepsilon_{E,1})\mathfrak{c}(\varepsilon_{E,2})d(B_E)$. Then $\mathcal{H}_E(\varepsilon_E)$ is a semi-simple commutative algebra and $\mathcal{H}_E(\varepsilon_E) \cong \mathcal{M}_E(\varepsilon_E)$ as $\mathcal{H}_E(\varepsilon_E)$-modules. For any quadratic character $\chi : \widehat{O}_E^{\times} \to \{\pm 1\}$, we can think of $\chi\varepsilon_E$ made up of $\{\chi\varepsilon_{1,E}, \chi\varepsilon_{E,2}, \varepsilon_{E+}, \varepsilon_E^-\}$. As long as ${}^xUZ(E_{\mathbb{A}}^{(\infty)}) \cap G(E) = Z(E)$ ($U = U_0(\mathfrak{c}(\varepsilon_E^-)d(B_E))$) for all $x \in G(E_{\mathbb{A}}^{(\infty)})$, the space $\mathcal{M}_E(\chi\varepsilon_E)$ has dimension equal to $|Sh_E(\varepsilon_E)| = |Sh_E(\chi\varepsilon_E)|$, which is independent of χ (because $Sh_E(\varepsilon_E)$ only depends on ε_E^-). Write D for the relative discriminant of F/E. Thus $O_D = \varprojlim_n O/D^n$ and $O_{E,D} = \varprojlim_n O_E/D^n$.

Remark 5.1. Suppose that F/E is simply 2-connected. We consider the set of compatible systems of Galois representations $\mathfrak{M}_E(\varepsilon_E)$ associated to each point $\mathrm{Spec}(\mathcal{H}_E(\varepsilon_E))(\mathbb{C})$. If the quadratic character χ as above is trivial on $N_{F/E}(\widehat{O}^{\times})$ in $\widehat{O}_E^{\times}$, for $\rho \in \mathfrak{M}_E(\chi\varepsilon)$, the local ramification data of $\rho_F := \rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is described by ε_F. Thus if base-change exists, we have the restriction map $\mathrm{Res} : \mathfrak{M}_E(\chi\varepsilon_E) \sqcup \mathfrak{M}_E(\varepsilon_E) \to \mathfrak{M}_F(\varepsilon_E)$ sending ρ to ρ_F. We now ask

is this map one-to-one?

If χ extends to a global quadratic character $\chi_E : E_{\mathbb{A}}^{\times}/E^{\times} \to \mathbb{C}$, denoting again by χ_E the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$, χ_E remains nontrivial over $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ because $\Delta = \mathrm{Gal}(F/E)$ does not have quadratic characters ($H^1(\Delta, \mu_2) = 0$). Write M/E for the quadratic extension in $\overline{\mathbb{Q}}$ fixed by $\mathrm{Ker}(\chi_E)$. Since χ_E is trivial over $N_{F/E}(\widehat{O}^{\times})$, the Galois character $\chi_F = \chi_E|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is everywhere unramified quadratic. Note here that if $\rho \in \mathfrak{M}_E(\varepsilon_E)$, $\rho \otimes \chi_E$ is in $\mathfrak{M}_E(\chi\varepsilon_E)$. So unless we have $\rho \cong \rho \otimes \chi_E$ (that is, ρ is an induced representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$), we conclude $\rho_F \ncong \rho_F \otimes \chi_F$. In other words, Res is injective on the subset of representations not induced from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$. Anyway $\mathrm{Res} : \mathfrak{M}_E(\varepsilon_E) \to \mathfrak{M}_F(\varepsilon_F)$ is injective. If we cannot extend χ to a global quadratic Hecke character, we expect that $\mathrm{Res} : \mathfrak{M}_E(\chi\varepsilon_E) \sqcup \mathfrak{M}_E(\varepsilon_E) \to \mathfrak{M}_F(\varepsilon_E)^{\Delta}$ is injective; so, $\mathrm{Res} : \mathfrak{M}_E(\varepsilon_E) \to \mathfrak{M}_F(\varepsilon_E)^{\Delta}$ cannot be surjective onto $\mathfrak{M}_F(\varepsilon_F)^{\Delta}$. Note that the condition (df) implies that the index $[\widehat{O}_E^{\times} : N_{F/E}(\widehat{O}^{\times})]$ is odd (see the following lemma); so, under (df), we will not have any quadratic χ factoring through $\widehat{O}_E^{\times}/N_{F/E}(\widehat{O}^{\times})$. Thus this explains the fact that $S_E(\varepsilon_E) \to S_F(\varepsilon_F)$ is injective, but without assuming (df), it may not be surjective onto $S_F(\varepsilon_F)^{\Delta}$ in view of Conjecture 1.2. Anyway, to

remove the assumption (R2) from Theorem 1.1 ((R2) is (df) for $E=\mathbb{Q}$), we need a more careful analysis of the Δ-sets $S_F(\varepsilon_F)$ and $\mathfrak{M}_F(\varepsilon_F)$.

Lemma 5.1. *Suppose a prime $\mathfrak{P}$ of F ramifies over a prime $\mathfrak{p}$ of E. If $\mathfrak{P}$ is a factor of $d(B_F)$ and ρ is associated to a Hecke eigenform in $\mathcal{S}_F(\varepsilon_F)$ invariant under Δ, then $\rho_{\mathfrak{l}}|_{D_{\mathfrak{P}}}$ ($\mathfrak{P}\nmid\ell$) extends to a unique representation $\rho_{\mathfrak{l}}|_{D_{\mathfrak{p}}}$ representation isomorphic to $\begin{pmatrix}\eta\mathcal{N}_\ell & *\\ 0 & \eta\end{pmatrix}$ up to isomorphism for an unramified character η of $D_{\mathfrak{p}}$ with $\eta^2=\chi_{\mathfrak{l}}|_{D_{\mathfrak{p}}}$. If Σ_{st} contains all primes ramified in F/E, $[O_{E,D}^\times : N_{F/E}(O_D^\times)]$ is odd.*

Proof. By Lemma 4.4, we have an extension of $\rho_{\mathfrak{l}}|_{D_{\mathfrak{P}}}$ to $D_{\mathfrak{p}}$ as above, and $\eta^2=\chi_{\mathfrak{l}}|_{D_{\mathfrak{p}}}$. By this equality, if there exists another extension $\rho'_{\mathfrak{l}}|_{D_{\mathfrak{p}}}$ of $\rho_{\mathfrak{l}}|_{D_{\mathfrak{P}}}$, it is isomorphic to $\begin{pmatrix}\eta'\mathcal{N}_\ell & *\\ 0 & \eta'\end{pmatrix}$, and $(\eta/\eta')^2=1$. Since η/η' factors through $\mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$, if it is not trivial, $F_{\mathfrak{P}}$ contains a quadratic extension $M/E_{\mathfrak{p}}$. Then $B\otimes_E M\cong M_2(M)$, and hence $B_{\mathfrak{P}}=B\otimes_E F_{\mathfrak{P}}\cong M_2(F_{\mathfrak{P}})$ contradicting against our assumption that $B_{\mathfrak{P}}$ is a division algebra. Thus $\eta=\eta'$ and the extension is unique.

The group $\frac{O_{E,\mathfrak{p}}^\times}{N_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(O_{\mathfrak{P}}^\times)}$ is isomorphic to the inertia subgroup of $\mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$. As seen above, there is no quadratic extension of $E_{\mathfrak{p}}$ inside $F_{\mathfrak{P}}$, $[O_{E,\mathfrak{p}}^\times : N_{F/E}(O_{\mathfrak{p}}^\times)]$ has to be odd. This shows the last assertion. □

Proposition 5.2. *Let the notation and the assumption be as above. Suppose* Conjectures 2.6 *and* 4.1 *for F/E and the following conditions*

(1) $\kappa=(0,I_E)$;
(2) $\Delta=\mathrm{Gal}(F/E)$ *is simply 2-connected;*
(3) $\mathfrak{q}|d(B_E)$ *for the prime $\mathfrak{q}$ we have chosen above* Remark 5.1;
(4) *if a prime $\mathfrak{l}|d(B_F)$, then $\mathfrak{l}|d(B_E)$ (that is, the condition* (dd)*);*
(5) *if a prime $\mathfrak{l}$ ramifies in F/E, $\mathfrak{l}|d(B_F)$ (that is, the condition* (df)*).*

Let ρ_f be the two dimensional compatible system associated to a Hecke eigenform $f\in\mathcal{S}_E(\varepsilon_E)$. Then we can find a Hecke eigenform $\widehat{f}$ on $\mathcal{S}_F(\varepsilon_F)$ such that the compatible system of Galois representations associated to $\widehat{f}$ is isomorphic to the restriction of ρ_f to $\mathrm{Gal}(\overline{F}/F)$. This correspondence $f\mapsto\widehat{f}$ gives rise to a bijection (up to scalar multiple) between the set of Hecke eigenforms in $\mathcal{S}_E(\varepsilon_E)$ and the set of Δ-invariant Hecke eigenforms in $\mathcal{S}_F(\varepsilon_F)$.

Proof. We first assume that $\varepsilon_F^- \neq 1$. We consider $\mathcal{M}_F(\varepsilon_F)$. By the existence of $\mathfrak{q} \in \Sigma_{st}$, we have ${}^xUZ(F_{\mathbb{A}}^{(\infty)}) \cap G(F) = Z(F)$ for all $x \in G(F_{\mathbb{A}}^{(\infty)})$. Thus by Lemma 3.3, we get $S_E(\varepsilon_E) \hookrightarrow S_F(\varepsilon_F)^{\Delta}$ and

$$|S_E(\varepsilon_E)| \leq |S_F(\varepsilon_F)^{\Delta}|. \tag{5.1}$$

Thus by Conjecture 2.6, we get $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})^{\Delta} \cong S_F(\varepsilon_F)^{\Delta}$. For each compatible system associated to $\lambda \in \mathrm{Spec}(\mathcal{H}_F(\varepsilon_F)(\mathbb{C})^{\Delta}$ extends to a unique strictly compatible system of representations of $\mathrm{Gal}(\overline{F}/E)$ with determinant $\varepsilon_{E+}\mathcal{N}$. Since $\rho_{\mathfrak{l}}|_{D_{\mathfrak{p}}} \cong \begin{pmatrix} \eta_{2,\mathfrak{p}} & * \\ 0 & \eta_{1,\mathfrak{p}} \end{pmatrix}$ and $\eta_{j,\mathfrak{p}}|_{I_{\mathfrak{p}}}$ gives rise to $\varepsilon_{E,j,\mathfrak{p}}$, if $\mathfrak{P}/\mathfrak{p}$ is unramified, $\varepsilon_{E,j,\mathfrak{p}}$ is uniquely determined by $\varepsilon_{F,\mathfrak{P}}$. By the above lemma, even if $\mathfrak{P}$ ramifies in F/E, by the assumption (5), $\varepsilon_{E,j,\mathfrak{p}}$ is determined by $\varepsilon_{F,j,\mathfrak{P}}$. Thus ε_F uniquely determines ε_E. Thus if we write $\mathfrak{M}_F(\varepsilon_F)$ for the set of isomorphism classes of compatible systems associated to each points of $\mathrm{Spec}(\mathcal{H}_F(\varepsilon_F))(\mathbb{C})$, by Conjecture 4.1 and Lemmas 4.3, Lemma 4.4 and 5.1 combined, we have an injection $\mathfrak{M}_F(\varepsilon_F)^{\Delta} \hookrightarrow \mathfrak{M}_E(\varepsilon_E)$. Thus we have

$$|\mathfrak{M}_F(\varepsilon_F)^{\Delta}| \leq |\mathfrak{M}_E(\varepsilon_E)|. \tag{5.2}$$

For each irreducible automorphic representation π of

$$\mathbb{G} = G(F)G_1(F_{\mathbb{A}}^{(\infty)})U_0(\mathfrak{c}(\varepsilon_F^-)d(B_F))Z(F_{\mathbb{A}}^{(\infty)})$$

associated to a point of $\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})$, we may regard π, by $\pi(\sigma, g)\phi(x) = \phi(x^{\sigma}g)$, as a representation of $(\sigma, g) \in \Delta \ltimes \mathbb{G}$ for the semi-direct product $\mathbb{G}' := \Delta \ltimes \mathbb{G}$ under the natural Galois action of Δ on $\mathbb{G}$. Since $\Delta \ltimes \mathbb{G}$ is a normal subgroup of $\mathbb{G}'_0 := \Delta \ltimes G(F_{\mathbb{A}}^{(\infty)})$ with quotient group Cl_F/Cl_F^2, by the same argument as in the proof of Lemma 2.3 studying $\mathrm{Ind}_{\mathbb{G}'}^{\mathbb{G}'_0}\pi$ instead of $\mathrm{Ind}_{\mathbb{G}}^{\mathbb{G}_0}\pi$ in the proof of Lemma 2.3, we can extend π to a Δ-invariant irreducible representation of $\mathbb{G}'_0$, and if one fix its extension Π to $G(F_{\mathbb{A}}^{(\infty)})$ invariant under Δ with central character ε_{F+}, all other extensions invariant under Δ are given by $\Pi \otimes \alpha_F$ for quadratic characters α_F of the strict class group Cl_F of F. By class field theory using the assumption $H^1(\Delta, \mu_2) = 0$, all such characters invariant under Δ are of the form $\alpha_F = \alpha \circ N_{F/E}$ for a character α of $E_{\mathbb{A}}^{\times}/E_+^{\times}$ trivial over $N_{F/E}(\widehat{O}^{\times})$ (and at most quadratic on $\widehat{O}_E^{\times}$). Since $\widehat{O}_E^{\times}/N_{F/E}(\widehat{O}^{\times}) \cong O_{E,D}^{\times}/N_{F/E}(O_D^{\times})$ which has odd order (Lemma 5.1), α has to be unramified everywhere.

Once a compatible central character ε_{F+} is given, any automorphic representation π of $\mathbb{G}$ generated by a Hecke eigenform in $\mathcal{M}_F^{(1)}(\varepsilon_F)$ extends to an automorphic representation Π of $G(F_{\mathbb{A}}^{(\infty)})$ generated by an element of $\mathcal{M}_F(\varepsilon_F)$, and

the set of all extension of π is given by $\{\Pi\otimes\alpha\}_{\alpha:Cl_F/Cl_F^2\to\{\pm1\}}$, where α runs over all characters of Cl_F/Cl_F^2. Therefore $|\{\Pi\otimes\alpha\}^{\Delta}_{\alpha:Cl_F/Cl_F^2\to\{\pm1\}}| = |(Cl_F/Cl_F^2)^{\Delta}| = |Cl_E/Cl_E^2| = 2^e$. Thus we have

$$|\mathfrak{M}_F(\varepsilon_F)^{\Delta}| = 2^e|\mathrm{Spec}(h_F(\varepsilon_F))(\mathbb{C})^{\Delta}| = 2^e|S_F(\varepsilon_F)^{\Delta}|$$

by Conjecture 2.6. Thus we have from (5.1)

$$|\mathfrak{M}_F(\varepsilon_F)^{\Delta}| \ge 2^e|S_F(\varepsilon_F)^{\Delta}| \ge 2^e|S_E(\varepsilon_E)| = |\mathfrak{M}_E(\varepsilon_E)|.$$

Then (5.2) shows that $\mathfrak{M}_F(\varepsilon_F)^{\Delta} \cong \mathfrak{M}_E(\varepsilon_E)$ as desired.

Now assume that $\varepsilon_F^- = 1$. This implies that $\varepsilon_{F+}|_{\widehat{O}^\times} = \varepsilon_1^2$. If ε_F is not a square character on $F_{\mathbb{A}}^{(\infty)}/F_+^\times$, functions in $\mathcal{M}_F(\varepsilon_F)$ (resp. $\mathcal{M}_E(\varepsilon_E)$) cannot factors through the reduced norm map. Then the argument is the same as above. Thus we may assume that ε_{F+} is a square character on $F_{\mathbb{A}}^{(\infty)}/F_+^\times$. Write $\varepsilon_{F+} = \eta_F^2$ for a Hecke character $\eta = \eta_F$. Then $(\eta^{\sigma-1})^2 = \varepsilon_{F+}^{\sigma-1} = 1$ for $\sigma\in\Delta$, and $\sigma\mapsto\eta^{\sigma-1}$ gives a 1-cocycle of Δ with values in the group generated by η (which is isomorphic to μ_2), and by the triviality of $H^1(\Delta,\mu_2)$, η_F has to be Δ-invariant, and hence $\eta_F = \eta_E\circ N_{F/E}$ by the triviality of $H^2(\Delta,\mu_2)$. Thus we have $\mathcal{M}_X(\varepsilon_X)\cong\mathcal{M}_X(\mathbf{1})$ $(X=E,F)$ for the trivial character $\mathbf{1}$ by $f\mapsto f(x)\eta_X^{-1}(N(x))$. Thus we may assume that $\varepsilon_X = \mathbf{1}$. In the same manner as in the case $\varepsilon_F^-\ne 1$, we get

$$\begin{aligned}(5.3)\quad |\mathrm{Spec}(\mathcal{H}_F(\mathbf{1}_F))(\mathbb{C})^{\Delta}| &= 2^e|\mathrm{Spec}(h_F(\mathbf{1}_F))(\mathbb{C})^{\Delta}|\\ &= 2^e|S_F(\mathbf{1}_F)^{\Delta}| \ge 2^e|S_E(\mathbf{1}_E)| = |\mathrm{Spec}(\mathcal{H}_E(\mathbf{1}_E))(\mathbb{C})|.\end{aligned}$$

Let H_F be the Hecke algebra for $\mathcal{S}_F(\mathbf{1}_F)$. Since the Hecke algebra of $\mathcal{E}_F(\mathbf{1}_F)$ is isomorphic to the group algebra $\mathbb{C}[Cl_F/Cl_F^2]$, we have $\mathcal{H}_F\cong H_F\oplus\mathbb{C}[Cl_F/Cl_F^2]$. Note that

$$\mathrm{Spec}(\mathbb{C}[Cl_F/Cl_F^2])(\mathbb{C})^{\Delta} = \mathrm{Hom}(Cl_F/Cl_F^2,\mu_2)^{\Delta} = \mathrm{Spec}(\mathbb{C}[Cl_E/Cl_E^2])(\mathbb{C})^{\Delta},$$

because $(O_{E,D}^\times : N_{F/E}(O_D^\times))$ is odd. This combined with (5.3) shows

$$|\mathfrak{M}_F(\mathbf{1})^{\Delta}| = |\mathrm{Spec}(H_F)(\mathbb{C})^{\Delta}| = |\mathrm{Spec}(H_E)(\mathbb{C})| = |\mathfrak{M}_E(\mathbf{1})|.$$

This finishes the proof. □

6. Proof of Theorem 1.1

By means of p-adic Galois deformation theory ([F]), we remove the assumption: $\mathfrak{q}|d(B_E)$ from Proposition 5.2. This finishes the proof of Theorem 1.1.

Let π be as in Theorem 1.1 with compatible system $\rho = \rho_\pi$. Let Σ_0 be the set of rational primes at which $B_{\mathbb{Q}}$ ramifies. Since $\varepsilon = \varepsilon_{\mathbb{Q}}$ has values in W, we can think of the space $\mathcal{M}^B_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}}; \mathbb{F})$ of functions $f : G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{F}$ satisfying $f(xzu) = \varepsilon_+(z)\underline{\varepsilon}(u)f(x)$ for $z \in Z(\mathbb{A}^{(\infty)})$ and $u \in U_0(\mathfrak{c}(\varepsilon^-)d(B_{\mathbb{Q}}))$. We call such functions mod p automorphic forms. Choosing prime p well, we may assume that the Artin conductor of $\overline{\rho} = \rho \mod \mathfrak{m}_W$ and $\overline{\rho}_F = \overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is equal to the conductor of ρ and ρ_F. Write $C = C(\pi)$ for the Artin conductor of $\overline{\rho}$ (thus $C = \mathfrak{c}(\varepsilon^-)d(B_{\mathbb{Q}})$). We may also assume that $\overline{\rho}_F$ is absolutely irreducible over $\mathrm{Gal}(\overline{\mathbb{Q}}/F[\mu_p])$.

We pick a prime $\mathfrak{p}$ of T with residual characteristic p. We extend $\mathfrak{p}$ to a p-adic place $\overline{\mathfrak{p}}$ of $\overline{\mathbb{Q}}_p$. Then we find a set $\Sigma_1 \supset \Sigma_0$ of primes ℓ for each integer $n > 0$ such that $\ell \in \Sigma_1 - \Sigma_0$ splits totally in the splitting field of $\rho_{\mathfrak{p}} \mod \mathfrak{p}$ over $\widetilde{M}_\emptyset$ and $|\Sigma_1| = |\Sigma_0| + 2$. Let B_1 be the definite quaternion algebra ramified at exactly at the places in Σ_1. Then by the level raising argument of Taylor (cf. [T] and [HMI] 3.1.4) applied to the quaternion algebra B, we can find a Hecke eigenform f_1 in $\mathcal{M}^{B_1}_{\mathbb{Q}}(\varepsilon_{\mathbb{Q}})$ with $\overline{\mathfrak{p}}$-adic Galois representation ρ_1 unramified outside C_1 and Steinberg exactly at Σ_1 such that $\rho_{\mathfrak{p}} \equiv \rho_1 \mod \mathfrak{m}_W$. Indeed, the elliptic cusp form f_1 associated to ρ_1 has level $C_1 = C\prod_{\ell\in\Sigma_1-\Sigma_0}\ell$ and has the same Neben character $\varepsilon_{\mathbb{Q}} \mod \mathfrak{m}_W$. The semi-simplification of $\rho_1|_{I_q}$ for $q|C$ outside Σ_1 is a direct sum of two distinct characters, and f_1 lifts to a mod p Hilbert normalized eigenform $\widehat{f}_1$ on the Shimura variety of $GL_2(F_{\mathbb{A}})$ by Proposition 5.2 combined with the Jacquet-Langlands correspondence over F (see [H05]). Since $\widehat{f}_1$ is Steinberg at $\Sigma_1 \supset \Sigma_0$, choosing further well Σ_1 (and p), we can make level lowering (see [J], [J1] and [F1]; the result of Jarvis is sufficient for our purpose as explained in [F1] Lemma 4.1) and find a Hecke eigenform $\widehat{f}_0$ of level equal to the conductor $C(\rho_F)$ of ρ_F such that $\widehat{f}_1 \equiv \widehat{f}_0 \mod \mathfrak{m}_W$.

By the Galois deformation theory of Taylor-Wiles and Fujiwara ([F]), the Galois representation ρ_F is associated to a Hilbert modular Hecke eigenform $\widehat{f}$ (congruent to $\widehat{f}_0$ modulo $\mathfrak{m}_W$). Indeed, by our choice of p, we are in the minimal case treated in [HMI] 3.2.4 if $[F : \mathbb{Q}]$ is even, and in this case, by [HMI] Theorem 3.28, we find $\widehat{f}$. If $[F : \mathbb{Q}]$ is odd, we can use the quadratic base-change and then quadratic descent to find $\widehat{f}$ as described in [HMI] Section 3.3 (or just by the Galois deformation theory over the odd degree field carried out in [F]).

Again by the Jacquet-Langlands correspondence, we can find $\widehat{f}_B \in \mathcal{M}_F^B(\varepsilon_F)$ associated to the Galois representation ρ_F (as asserted in Theorem 1.1). □

Remark 6.1. The above argument can be also started with empty Σ_0 taking a everywhere principal elliptic Hecke eigenform f of weight 2 using the level optimization of everywhere principal automorphic forms (see [F1]).

7. Simply 2-connected groups

A (finite) group Δ is called simply connected in [Mr] if for every central extension $1 \to A \to \mathcal{E} \xrightarrow{\pi} \Delta \to 1$ of Δ by any abelian group A, there exists a *unique* homomorphism φ of Δ to $\mathcal{E}$ with $\pi \circ \varphi = \mathrm{id}$. The group Δ is simply connected if and only if $H^1(\Delta, \mathbb{Q}/\mathbb{Z}) = H^2(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$ (see [Mr] Lemma 1.1). One of the main results in [Mr] Section 1 is that if $H^1(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$ ($\Leftrightarrow [\Delta, \Delta] = \Delta$), there exists a unique simply connected covering group $\pi : \mathcal{E} \twoheadrightarrow \Delta$ with abelian $\mathrm{Ker}(\pi)$. The group $\mathrm{Ker}(\pi)$ is called the fundamental group of Δ and is written as $\pi_1(\Delta)$. It is known that $H^2(\Delta, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\pi_1(\Delta), \mathbb{Q}/\mathbb{Z})$ canonically ([Mr] Theorem 1.1). Any central covering $\mathcal{F} \twoheadrightarrow \Delta$ with $H^1(\mathcal{F}, \mathbb{Q}/\mathbb{Z}) = 0$ is covered canonically by $\mathcal{E} \twoheadrightarrow \mathcal{F}$ and $\pi_1(\mathcal{F}) \subset \pi_1(\Delta)$ ([Mr] Lemma 1.6), and in this sense, $\mathcal{E} \twoheadrightarrow \Delta$ is universal.

A large class of nonsoluble groups Δ is simply connected. Plainly any finite group of odd order is simply 2-connected (though each odd order group is soluble by Thompson's theorem; so, Langlands' theory in [BCG] applies to such a case). As we mentioned already, for any split simply connected simple linear algebraic groups G_1 (Chevalley groups), $G_1(\mathbb{F}_q)$ satisfies this condition if $q > 3$ (except for $SL_2(\mathbb{F}_9)$; see [St] and [St1] Theorem 1.1). If $H^1(\Delta, \mu_2) = 0$, there is a unique simply 2-connected central extension $\widetilde{\Delta} \twoheadrightarrow \Delta$ with finite kernel $\pi_1(\Delta)_2$. If $H^1(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$, the fundamental 2-group $\pi_1(\Delta)_2$ is the 2-part of the fundamental group of Δ introduced [Mr], and it is a finite abelian 2-group in general. It is a classical result of I. Schur [Sch] that the alternating group $\mathfrak{A}_n$ ($n \geq 5$) is not simply connected with $\pi_1(\mathfrak{A}_n) \cong \mathbb{Z}/2\mathbb{Z}$ except for $n = 6, 7$ (for $n = 6, 7$, $\pi_1(\mathfrak{A}_n) \cong \mathbb{Z}/6\mathbb{Z}$). Thus, by Theorem 1.3, for any totally real $\mathfrak{A}_n$-extension $F_0/\mathbb{Q}$, there exists a totally real quadratic extension F of F_0 with simply 2-connected $\mathrm{Gal}(F/\mathbb{Q})$ (in particular, if $n = 5$ and $\mathrm{Gal}(F_0/\mathbb{Q}) = \mathfrak{A}_5 \cong PSL_2(\mathbb{F}_5)$, we have $\mathrm{Gal}(F/\mathbb{Q}) \cong SL_2(\mathbb{F}_5)$). For simple finite groups Δ, $\pi_1(\Delta)$ is completely determined (see [G1]) and is the Schur multiplier group of Δ in the terminology of

[G1]. For example, the monster is simply connected, but the baby monster has π_1 isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

We would like to localize the theory of [Mr] at the prime 2 (our theory is valid actually at any prime p, but we only need the theory at 2). We call a finite group Δ *simply 2-connected* if for every central extension $1 \to A \to \mathcal{E} \xrightarrow{\pi} \Delta \to 1$ of Δ by an abelian 2-group A, there exists a *unique* homomorphism φ of Δ to $\mathcal{E}$ with $\pi \circ \varphi = \mathrm{id}$. A finite group Δ is simply 2-connected if and only if $H^1(\Delta, \mathbb{T}_2) = H^2(\Delta, \mathbb{T}_2) = 0$ for $\mathbb{T}_2 = \mathbb{Q}_2/\mathbb{Z}_2 = \bigcup_n 2^{-n}\mathbb{Z}/\mathbb{Z}$ (see [Mr] Lemma 1.1).

Proposition 7.1. *Suppose that $H^1(\Delta, \mathbb{Z}/2\mathbb{Z}) = 0$ (so, $H^1(\Delta, \mathbb{T}_2) = 0$). Then there exists a unique central extension $1 \to B \to \mathcal{E} \to \Delta \to 1$ by a finite abelian 2-group B such that $H^j(\mathcal{E}, \mathbb{Z}/2\mathbb{Z}) = H^j(\mathcal{E}, \mathbb{T}_2) = 0$ for $j = 1, 2$ (that is, $\mathcal{E}$ is simply 2-connected).*

We write the group B as $\pi_1(\Delta)_2$ and call it the *fundamental 2-group*. We also call the group $\mathcal{E}$ the *universal 2-covering* of Δ. If $H^1(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$, as in [Mr] Section 1, we have the fundamental group $\pi_1(\Delta)$, and in this case, $\pi_1(\Delta)_2$ is the 2-primary part of $\pi_1(\Delta)$.

Proof. We first show the uniqueness. We follow the proof of a similar fact for "simply connected extensions" in [Mr] Lemma 1.2. Suppose we have two extensions $\pi_i : \mathcal{E}_i \to \Delta$ $(i = 1, 2)$ satisfying the property of the proposition. Let A_i, be the kernel of the projection π_i, and let $\alpha_i \in H^2(\Delta, A_i)$ be the class of the extension. We inflate α_i to a class in $H^2(\mathcal{E}_2, A_1)$ by means of the projection π_2. We then have a central extension

$$1 \to A_1 \to \mathcal{E}_{12} \xrightarrow{p_2} \mathcal{E}_2 \to 1$$

of $\mathcal{E}_2$ by A_1. By hypothesis we can find a unique homomorphism φ of $\mathcal{E}_2$ into $\mathcal{E}_{12}$ with $p_2 \circ \varphi = \mathrm{id}$. Since the class of the extension $\mathcal{E}_{12}$ is the inflation to $\mathcal{E}_2$ of the class of the extension $\mathcal{E}_1$ of Δ, there is a homomorphism β of $\mathcal{E}_{12}$ onto $\mathcal{E}_1$ such that $\pi_1 \circ \beta = \pi_2 \circ p_2$. Now let $\psi = \beta \circ \varphi$, which is a homomorphism of $\mathcal{E}_2$ into $\mathcal{E}_1$; then $\pi_1 \circ \psi = \pi \circ (\beta \circ \varphi) = (\pi_2 \circ p_2) \circ \varphi = \pi_2$ by the above, and so ψ is a homomorphism of group extensions. We reverse the indices and construct a homomorphism ψ' of group extensions from $\mathcal{E}_2$ to $\mathcal{E}_1$. Then $\psi' \circ \psi = \gamma$ is a homomorphism of group extensions from $\mathcal{E}_1$ to itself. Then $\gamma(x)x^{-1}$ is an

element of A_1 and since A_1 is central this is a homomorphism of $\mathcal{E}_1$ into A_1 which is therefore trivial since the commutator subgroup $[\mathcal{E}_1, \mathcal{E}_1]$ and $\mathcal{E}_1^2 = \{x^2 | x \in \mathcal{E}_1\}$ generate $\mathcal{E}_1$. Thus $\gamma(x) = x$. One proves similarly that $(\psi \circ \psi')(y) = y$ for $y \in \mathcal{E}_2$. Thus $\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic as group extensions.

We now construct a simply 2-connected extension. We follow the proof given by [Mr] Lemma 1.3 for simply connected extensions. Let L be the $\mathbb{Z}_2$-free module generated by objects $a(x, y)$, $x, y \in \Delta \times \Delta$. Let R be the subgroup (topologically) generated by the elements $a(st, r)a(s, t)a(s, tr)^{-1}a(t, r)^{-1}$ and $a(1, s)$ and $a(s, 1)$ for all $s, t, r \in \Delta$. Put $B_0 = L/R$, and let $\beta(s, t)$ be the image of $a(s, t)$ in this quotient group. Since Δ is a finite group, L is a $\mathbb{Z}_2$-module of finite type, and hence B_0 is a compact $\mathbb{Z}_2$-module of finite type. Then it is clear that β as a function from $\Delta \times \Delta$ to B_0 is a 2-cocycle of Δ with values in the trivial Δ-module B_0. Let $\mathcal{E}_0$ be the group extension of Δ by B_0 defined by β; $\mathcal{E}_0 = B_0 \times \Delta$ as sets and $(a, g)(b, h) = (ab\beta(g, h), gh)$ is the multiplication. Now suppose that F is any central extension of Δ by an abelian 2-profinite group D. We choose a normalized cocycle γ representing this extension and view F as $D \times \Delta$ with the multiplication defined just as above. Here

$$\text{the normalization means } \gamma(1, *) = \gamma(*, 1) = 1. \tag{7.1}$$

Consider now the mapping ψ_1 from L to D given by $\psi_1(a(s, t)) = \gamma(s, t)$ on the generators. It is clear from the fact that γ is a normalized cocycle that $\psi_1(R) = 1$, and hence ψ_1 defines a homomorphism ψ_0 of B_0 into D with $\psi_0(\beta(s, t)) = \gamma(s, t)$. In view of the definition of the group law in $\mathcal{E}_0$ and F, one sees that ψ_0 extends to a homomorphism of group extensions, again denoted by ψ_0, of $\mathcal{E}_0$ into F. Thus $\mathcal{E}_0$ has the first part of the universal property required for simple 2-connectivity. Now let $\mathcal{E}$ be the subgroup of $\mathcal{E}_0$ generated topologically by the commutator subgroup $[\mathcal{E}_0, \mathcal{E}_0]$ and $\mathcal{E}_0^2 = \{x^2 | x \in \mathcal{E}_0\}$. Since Δ is generated by $[\Delta, \Delta]$ and $\Delta^2 = \{x^2 | x \in \Delta\}$, the projection of $\mathcal{E}$ onto Δ is all of Δ so that $\mathcal{E}$ is a group extension of Δ: $1 \to B \to \mathcal{E} \to \Delta \to 1$ where $B = B_0 \cap \mathcal{E}$. Now $\mathcal{E}_0 = B_0 \cdot \mathcal{E}$ with B_0 central so that $\langle [\mathcal{E}, \mathcal{E}], \mathcal{E}^2 \rangle = \langle [\mathcal{E}_0, \mathcal{E}_0], \mathcal{E}_0^2 \rangle = \mathcal{E}$, and thus $H^1(\mathcal{E}, \mathbb{T}_2) = H^1(\mathcal{E}, \mathbb{Z}/2\mathbb{Z}) = 0$. If F is any central extension of Δ by a 2-profinite abelian group D, we saw that there exists a homomorphism ψ_0 of group extensions of $\mathcal{E}_0$ into F. Thus ψ, the restriction of ψ_0 to $\mathcal{E}$, is also a homomorphism of group extensions. In terms of cohomology, this says exactly that the inflation homomorphism $H^2(\Delta, D) \to H^2(\mathcal{E}, D)$ is the zero map for every trivial 2-profinite Δ-module D. In particular,

$H^2(\Delta, 2^{-n}\mathbb{Z}/\mathbb{Z}) \xrightarrow{\text{Inf}} H^2(\mathcal{E}, 2^{-n}\mathbb{Z}/\mathbb{Z})$ is the zero map. Since the formation of cohomology group commutes with injective limit,

(7.2) the inflation map $H^2(\Delta, \mathbb{T}_2) \to H^2(\mathcal{E}, \mathbb{T}_2)$ is the zero map.

We contend now that $\mathcal{E}$ is simply 2-connected, and to do this, it suffices to show that $H^2(\mathcal{E}, \mathbb{T}_2) = 0$. In view of the Hochschild-Serre spectral sequence for the group extension $\mathcal{E}$ of Δ by B, we have the following commutative diagram with exact rows (cf. [ECH] Appendix B):

$$\begin{array}{ccccc} H^2(\Delta, \mathbb{T}_2) & \xrightarrow{i} & \mathrm{Ker}(H^2(\mathcal{E}, \mathbb{T}_2) \to H^2(B, \mathbb{T}_2)) & \longrightarrow & H^1(\Delta, H^1(B, \mathbb{T}_2)) \\ \| \downarrow & & \| \downarrow & & \downarrow \| \\ E_2^{2,0} & \longrightarrow & E_1^2 & \longrightarrow & E_2^{1,1}. \end{array}$$

We show first that the $E_2^{1,1}$ term, $H^1(\Delta, H^1(B, \mathbb{T}_2))$, is zero. But this group is zero since $H^1(B, \mathbb{T}_2)$ is a trivial Δ-module killed by 2 and Δ is generated by $[\Delta, \Delta]$ and Δ^2. If $\mathrm{Ker}(H^2(\mathcal{E}, \mathbb{T}_2) \to H^2(B, \mathbb{T}_2)) = H^2(\mathcal{E}, \mathbb{T}_2)$, i is the inflation map, which is the zero map as we have already shown in (7.2). Then one must show that the restriction homomorphism $r : H^2(\mathcal{E}, \mathbb{T}_2) \to H^2(B, \mathbb{T}_2)$ is the zero map. This is contained in the following lemma (Lemma 7.2 similar to [Mr] Lemma 1.4), and $H^2(\mathcal{E}, \mathbb{T}_2) = 0$. Since $H^2(\mathcal{E}, \mathbb{T}_2) = 0$, by the long exact sequence associated to the short one: $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{T}_2 \xrightarrow{2\times} \mathbb{T}_2$, we have $0 = H^1(\mathcal{E}, \mathbb{T}_2) \to H^1(\mathcal{E}, \mathbb{Z}/2\mathbb{Z}) \to H^2(\mathcal{E}, \mathbb{T}_2) = 0$ is exact, and hence $H^2(\mathcal{E}, \mathbb{Z}/2\mathbb{Z}) = 0$.

Since $H^2(\mathcal{E}, \mathbb{T}_2) = 0$, by the inflation restriction sequence (and the Hochschild-Serre spectral sequence), we have the following exact sequence:

$$0 = H^1(\mathcal{E}, \mathbb{T}_2) \to H^0(\Delta, H^1(B, \mathbb{T}_2)) \\ \to H^2(\Delta, \mathbb{T}_2) \to \mathrm{Ker}(H^2(\mathcal{E}, \mathbb{T}_2) \to H^2(B, \mathbb{T}_2)) = 0,$$

which shows $H^1(\pi_1(\Delta)_2, \mathbb{T}_2) = H^0(\Delta, H^1(B, \mathbb{T}_2)) \cong H^2(\Delta, \mathbb{T}_2)$ canonically by the transgression map. Since $H^2(\Delta, \mathbb{T}_2)$ is the Pontryagin dual group of $H_2(\Delta, \mathbb{Z}_2)$, $\pi_1(\Delta)_2 = B$ is a finite group, and hence $\mathcal{E}$ is a finite group. □

Lemma 7.2. *If a profinite group $\mathcal{E}$ is topologically generated by $[\mathcal{E}, \mathcal{E}]$ and $\mathcal{E}^2$ and $B \subset \mathcal{E}$ is any central 2-subgroup, then the restriction homomorphism $H^2(\mathcal{E}, \mathbb{T}_2) \to H^2(B, \mathbb{T}_2)$ is the zero map.*

Proof. Let $\alpha \in H^2(\mathcal{E}, \mathbb{T}_2)$ and $\mathcal{F}$ be the corresponding extension of $\mathcal{E}$ by $\mathbb{T}_2$. If $s \in \mathcal{E}$ and $t \in B$, let s' and t' be representatives of s and t in $\mathcal{F}$. Then the commutator $[s', t']$ depends only on s and t, and we denote it by $\varphi(s, t)$. We note that φ is a bilinear map from $\mathcal{E} \times B$ into $\mathbb{T}_2$, and since $\mathcal{E}$ is generated by $[\mathcal{E}, \mathcal{E}]$ and $\mathcal{E}^2$, $\varphi(s, t) = 1$.

Now let $\mathcal{F}'$ be the inverse image of B in $\mathcal{F}$. Since $\varphi = 1$, $\mathcal{F}'$ is an abelian 2-group. Then $\mathcal{F}'$ is an extension of B by $\mathbb{T}_2$. Since $\mathbb{T}_2$ is $\mathbb{Z}_2$-injective, this extension splits, and this says that the restriction of α to B is the trivial class as desired. □

We add one more cohomological lemma. Let Δ be a finite group. We study $H^2(\Delta, k^\times)$ for an algebraically closed field k of characteristic 0. Here Δ acts trivially on $k^\times$.

Lemma 7.3. *Let k be an algebraically closed field of characteristic 0. Then we have $H^j(\Delta, \mathbb{Q}/\mathbb{Z}) \cong H^j(\Delta, k^\times)$ for $j > 0$. If $H^j(\Delta, \mathbb{Z}/2\mathbb{Z}) = 0$ for $j > 0$, we have*

$$H^j(\Delta, \mathbb{Q}/\mathbb{Z})[2] = H^j(\Delta, k^\times)[2] = 0,$$

where Δ acts trivially on the modules appearing in the above statements.

Proof. We consider the exact sequence of the trivial Δ-modules: $0 \to \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{2\times} \mathbb{Q}/\mathbb{Z} \to 0$ and the corresponding cohomology exact sequence:

$$0 \to H^{j-1}(\Delta, \mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to H^j(\Delta, \mathbb{Z}/2\mathbb{Z}) \to H^j(\Delta, \mathbb{Q}/\mathbb{Z})[2] \to 0.$$

From this, we conclude that $H^j(\Delta, \mathbb{Z}/2\mathbb{Z}) = 0 \Rightarrow H^j(\Delta, \mathbb{Q}/\mathbb{Z})[2] = 0$.

We now consider the following exact sequence of trivial Δ-modules:

$$0 \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\exp} k^\times \to U \to 1.$$

By definition, U is uniquely divisible; so, $H^j(\Delta, U) = 0$ for all $j > 0$. In particular, we have $H^j(\Delta, \mathbb{Q}/\mathbb{Z}) \cong H^j(\Delta, k^\times)$. □

8. Embedding problems of a universal 2-covering group

Let E be a totally real number field of finite degree. Let F_0/E be a finite totally real Galois extension with Galois group Δ_0. Suppose that $H^1(\Delta_0, \mathbb{Z}/2\mathbb{Z}) = 0$. We shall show that there exists a totally real Galois extension F/E containing F_0 such that $\mathrm{Gal}(F/E) \to \Delta_0$ is the 2-universal covering.

We define F'/F_0 to be the maximal totally real 2-extension of F_0. The Galois group $\mathrm{Gal}(F'/F_0)$ is a 2-profinite group. We pick a Galois extension E'/E inside F' containing F_0. Write $\Delta' = \mathrm{Gal}(E'/E)$, $\mathfrak{G}' = \mathrm{Gal}(F'/E')$ and $\mathfrak{G} = \mathrm{Gal}(F'/E)$. Thus we get an exact sequence $1 \to \mathfrak{G}' \to \mathfrak{G} \to \Delta' \to 1$. Then by Hochschild–Serre spectral sequence, we get the following exact sequence:

$$0 \to H^1(\Delta', \mu_2) \to H^1(\mathfrak{G}, \mu_2) \to H^0(\Delta', H^1(\mathfrak{G}', \mu_2)) \to H^2(\Delta', \mu_2) \xrightarrow{\mathrm{Inf}} \mathrm{Ker}(H^2(\mathfrak{G}, \mu_2) \to H^2(\mathfrak{G}', \mu_2)).$$

For each normalized 2-cocycle $c : \Delta_0 \to \mu_2$ (see (7.1) for normalization), define the algebra structure on $D = F_0[\Delta_0]$ by $\delta a \delta^{-1} = \delta(a)$ for $a \in F_0$ and $\delta \cdot \delta' = c(\delta, \delta')\delta\delta'$. In this way, we get a central simple algebra over E whose class in the Brauer group $Br(E)[2] = H^2(\mathrm{Gal}(\overline{F}_0/E), \mu_2)$ is the inflated image of c. By Merkurjev's theorem, elements in $H^2(\mathrm{Gal}(\overline{F}_0/E), \mathbb{Z}/2\mathbb{Z}) \cong H^2(\mathrm{Gal}(\overline{F}_0/E), \mu_2) = Br(E)[2]$ is generated by the classes of quaternion algebras. Thus inflated image is trivialized over a $(2, \dots, 2)$-extension M of E. Since there are infinitely many choices of splitting field of a given quaternion algebra, there are infinitely many choices of M. Indeed, for a quaternion algebra $B_{/E}$, any field M embeddable into B splits B. Since M is embeddable into B if and only if M_v/E_v is a quadratic extension for all places v of E ramified in B, we can impose ramification condition of M/E freely for any given finite set of places of E unramified in B. Since c get trivialized over $\mathrm{Gal}(\overline{F}_0/F_0)$ and F_0 is totally real, it is trivialized over a totally real $(2, \dots, 2)$-extension of E. Thus we have proven

Lemma 8.1. *We can choose finitely many quaternion algebras $B_{1/E}, \dots, B_{j/E}$ such that*

(1) *Brauer classes of $B_{1/E}, \dots, B_{j/E}$ in $Br(E)[2] \cong H^2(\mathrm{Gal}(\overline{F}_0/E), \mu_2)$ generate a subgroup containing the inflated image* $\mathrm{Im}(\mathrm{Inf})$ *of $H^2(\Delta_0, \mu_2)$;*
(2) *B_j splits at all real places of E.*

Lemma 8.2. *Let L be a Galois extension of E in F' containing F_0. Then we have $H^j(\mathrm{Gal}(L/E), L_+^\times) = H^j(\mathrm{Gal}(L/E), L^\times)$ if $j \geq 1$. Here Galois cohomology group is a continuous cohomology with respect to the Krull topology on* $\mathrm{Gal}(L/E)$ *and discrete topology on the Galois modules.*

Proof. We first assume that L/E is a finite extension. We have the following exact sequence:

$$1 \to L_+^\times \to L^\times \xrightarrow{\pi} \mathbb{F}_2[\mathrm{Gal}(L/E)]^{[E:\mathbb{Q}]} \to 0$$

of $\mathrm{Gal}(L/E)$-modules, where $L_+^\times$ is the subgroup of totally positive elements in $L^\times$. Indeed, the set ∞_L of infinite places of L is isomorphic to $\mathrm{Gal}(L/E)^{[E:\mathbb{Q}]}$ as $\mathrm{Gal}(L/E)$-set, and $\pi(\xi) = \sum_{v\in\infty_L} \frac{1-\sigma_v(\xi)/|\sigma_v(\xi)|}{2} v$ for the field embedding $\sigma_v : L \hookrightarrow \mathbb{R}$ associated to each real place v. The long exact sequence associated to the above short one tells us $H^j(\mathrm{Gal}(L/E), L_+^\times) = H^j(\mathrm{Gal}(L/E), L^\times)$ if $j \geq 2$, since $H^j(\mathrm{Gal}(L/E), \mathbb{F}_2[\mathrm{Gal}(L/E)]) = 0$ for $j > 0$.

If $j = 1$, we find

$$1 \to E_+^\times \to E^\times \xrightarrow{\pi} \mathbb{F}_2^{[E:\mathbb{Q}]} \to H^1(\mathrm{Gal}(L/E), L_+^\times) \to H^1(\mathrm{Gal}(L/E), L^\times) \to 0$$

is exact, and π is surjective. Thus again we conclude

$$H^1(\mathrm{Gal}(L/E), L_+^\times) = H^1(\mathrm{Gal}(L/E), L^\times) = 0.$$

The general result follows taking the injective limit, because

$$H^j(\mathrm{Gal}(L/E), X) = \varinjlim_{L'/E} H^j(\mathrm{Gal}(L'/E), X)$$

for finite Galois extensions L'/E inside L for discrete Galois modules X (see [MFG] Corollary 4.26). □

Lemma 8.3. *We have* $H^2(\mathrm{Gal}(F'/E), \mu_2) = H^2(\mathrm{Gal}(F'/E), \mathbb{T}_2) = 0$*, and the cohomology group* $H^2(\mathrm{Gal}(F'/E), F'^\times)$ *is uniquely* 2*-divisible.*

Proof. Let $L = F'$ and $\Delta' = \mathrm{Gal}(L/E)$. Since $H^j(\Delta', L_+^\times) \cong H^j(\Delta', L^\times)$ by the morphism induced by the inclusion and $L_+^\times = (L^\times)^2$, $H^j(\Delta', L^\times)$ is 2-divisible. Indeed, $L^\times \xrightarrow{2\times} L_+^\times \hookrightarrow L^\times$ induces a surjection $H^2(\Delta', L^\times) \xrightarrow{2\times} H^2(\Delta', L^\times)$ by the above lemma, and at the same time, we get $H^2(\Delta', \mu_2) = H^2(\Delta', L^\times)[2]$. Thus $H^2(\Delta', L^\times)[2] = Br(L/E)[2]$ is generated by quaternion algebras by a result of Merkurjev and Suslin (see [MeS] and [Me]). These quaternion algebras are splits over the totally real field L, and therefore they are split in a totally real quadratic extension of L, but L does not have any totally real quadratic extension. Thus we find $Br(L/E)[2] = 0$, which show $H^2(\Delta', \mu_2) = H^2(\Delta', \mathbb{F}_2) = 0$. Since the formation of the Galois cohomology commutes with injective limit, $H^2(\Delta', \mathbb{T}_2) = \varinjlim_n H^2(\Delta', 2^{-n}\mathbb{Z}/\mathbb{Z})$ which is 2-torsion module. We have an exact sequence

$0 = H^2(\Delta', \mathbb{F}_2) \to H^2(\Delta', \mathbb{T}_2) \xrightarrow{2\times} H^2(\Delta', \mathbb{T}_2)$. Thus the multiplication by 2 is injective. This combined with 2-power torsion property of $H^2(\Delta', \mathbb{T}_2)$ implies its vanishing. □

Theorem 8.4. *Let F_0/E be a totally real Galois extension with $\Delta_0 = \mathrm{Gal}(F_0/E)$. Suppose that $H^1(\Delta_0, \mathbb{Z}/2\mathbb{Z}) = 0$. If $\mathcal{E}$ is the 2-universal covering of Δ_0, then there exists a totally real Galois extension F/E containing F_0 such that $\mathrm{Gal}(F/E) \cong \mathcal{E}$, and in particular, $H^j(\mathrm{Gal}(F/E), \mu_2) = 0$ for $j = 1, 2$ and F/F_0 is a finite abelian 2-extension with $\mathrm{Gal}(F/F_0) \cong \pi_1(\Delta_0)_2$.*

Proof. We proceed by induction on $|\pi_1(\Delta_0)_2|$. If $\pi_1(\Delta_0)_2$ is trivial, $F_0 = F$ and there is nothing to prove.

We suppose that $H^2(\Delta_0, \mu_2) \neq 0$. By the above lemma, we can find a Galois extension L_0/E containing F_0 inside F' such that $H^2(\mathcal{E}_0', \mu_2) = H^2(\mathcal{E}_0', \mathbb{T}_2) = 0$ for $\mathcal{E}_0' = \mathrm{Gal}(L_0/E)$. Let $T = \mathbb{T}_2$ or μ_2. We thus have an exact sequence $1 \to B_0 \to \mathcal{E}_0' \to \Delta_0 \to 1$. Let $\overline{[B_0, B_0]}$ be the closure in B_0 of its commutator subgroup, and put $B_0^{ab} = B_0/\overline{[B_0, B_0]}$. Since B_0^{ab} is a compact $\mathbb{Z}_2[\Delta_0]$-module, we may consider $DB_0^{ab} = \sum_{\sigma \in \Delta_0} (\sigma - 1) B_0^{ab}$ and $B_{0,\Delta_0} = B_0^{ab}/DB_0^{ab} = H_1(\Delta_0, B_0^{ab})$. We define $\mathcal{E}_1 = \mathcal{E}_0/DB_0^{ab}$ and $B_1 = B_{0,\Delta_0}$. We have a central extension

$$1 \to B_1 \to \mathcal{E}_1 \to \Delta_0 \to 1.$$

By the Hochschild-Serre spectral sequence applied to the extension: $1 \to B_0 \to \mathcal{E}_0 \to \Delta_0 \to 1$, we have the following exact sequence

$$H^0(\Delta_0, H^1(B_0, T)) \xrightarrow{d_2^{0,1}} H^2(\Delta_0, T) \xrightarrow{\mathrm{Inf}} \mathrm{Ker}(H^2(\mathcal{E}_0, T) \to H^0(\Delta_0, H^2(B_0, T))).$$

Since $H^2(\mathcal{E}_0, T) = 0$, the map: $H^0(\Delta_0, H^1(B_0, T)) \xrightarrow{d_2^{0,1}} H^2(\Delta_0, T)$ is surjective. Note that $H^0(\Delta_0, H^1(B_0, T)) = H^1(B_{0,\Delta_0}, T) = H^1(B_1, T)$, and the map

$$H^0(\Delta_0, H^1(B_1, T)) \xrightarrow{d_2^{0,1}} H^2(\Delta_0, T)$$

is surjective. By the Hochschild-Serre spectral sequence applied to the extension: $1 \to B_1 \to \mathcal{E}_1 \to \Delta_0 \to 1$, we have the following exact sequence

$$H^0(\Delta_0, H^1(B_1, T)) \xrightarrow{d_2^{0,1}} H^2(\Delta_0, T) \xrightarrow{\mathrm{Inf}} \mathrm{Ker}(H^2(\mathcal{E}_1, T) \to H^0(\Delta_0, H^2(B_1, T))),$$

and $H^2(\Delta_0, T) \xrightarrow{\mathrm{Inf}} H^2(\mathcal{E}_1, T)$ is the zero map. Then again by Hochschild-Serre, $\mathrm{Ker}(H^2(\mathcal{E}_1, T) \to H^0(\Delta_0, H^2(B_1, T))) \hookrightarrow H^1(\Delta_0, H^1(B_1, T))$ is injective. Since

Δ_0 acts trivially on B_1 and hence on $H^1(B_1,T)=\mathrm{Hom}(B_1,T)$, we have the vanishing $H^1(\Delta_0,H^1(B_1,T))=0$ because $H^1(\Delta_0,\mathbb{Z}/2\mathbb{Z})=0$. Thus the restriction map $H^2(\mathcal{E}_1,T)\xrightarrow{\mathrm{Res}}H^2(B_1,T)$ is injective because

$$\mathrm{Ker}(H^2(\mathcal{E}_1,T)\to H^0(\Delta_0,H^2(B_1,T)))\hookrightarrow H^1(\Delta_0,H^1(B_1,T))=0.$$

Now assume that $T=\mu_2$. Let $\mathcal{E}_2=\mathcal{E}_1/B_1^2$ and $B_2=B_1/B_1^2$. Since

$$H^0(\Delta_0,H^1(B_1,\mu_2))=H^0(\Delta_0,H^1(B_1/B_1^2,\mu_2)),$$

$H^2(\Delta_0,\mu_2)\xrightarrow{\mathrm{Inf}}H^2(\mathcal{E}_2,\mu_2)$ is the zero map, and $H^2(\mathcal{E}_2,\mu_2)\xrightarrow{\mathrm{Res}}H^2(B_2,\mu_2)$ is injective. Let $\mathcal{E}_3$ be the subgroup of $\mathcal{E}_2$ topologically generated by $[\mathcal{E}_2,\mathcal{E}_2]$ and $\mathcal{E}_2^2$. Then for $B_3=B_2\cap\mathcal{E}_3$, we have an extension

$$1\to B_3\to\mathcal{E}_3\to\Delta_0\to 1.$$

By construction, $\mathcal{E}_3$ is topologically generated by $[\mathcal{E}_3,\mathcal{E}_3]$ and $\mathcal{E}_3^2$, $\mathcal{E}_3\twoheadrightarrow\Delta_0$ is a 2-covering. In particular, B_3 is a finite dimensional $\mathbb{F}_2$-vector subspace of B_2, and it has complementary direct summand $B_3^\perp$ in B_2 with $B_2=B_3\oplus B_3^\perp$. Then $\mathcal{E}_2\cong\mathcal{E}_3\times B_3^\perp$. By Künneth formula (cf. [CGP] 0.8 and 5.8), we have

$$H_2(\mathcal{E}_2,\mathbb{F}_2)\cong\bigoplus_{p+q=2,p\ge0,q\ge0}H_p(\mathcal{E}_3,\mathbb{F}_2)\otimes H_q(B_3^\perp,\mathbb{F}_2).$$

Via Pontryagin dual, we have

$$H^2(\mathcal{E}_2,\mathbb{F}_2)\cong\bigoplus_{p+q=2}H^p(\mathcal{E}_3,\mathbb{F}_2)\otimes H^q(B_3^\perp,\mathbb{F}_2)\cong H^2(B_3^\perp,\mathbb{F}_2)\oplus H^2(\mathcal{E}_3,\mathbb{F}_2).$$

Since this decomposition is compatible with the inflation map and the restriction map, $H^2(\Delta_0,\mu_2)\xrightarrow{\mathrm{Inf}}H^2(\mathcal{E}_3,\mu_2)$ is the zero map, and the restriction map $H^2(\mathcal{E}_3,\mu_2)\xrightarrow{\mathrm{Res}}H^2(B_3,\mu_2)$ is injective. Thus $\mathcal{E}_3\to\Delta_0$ is a nontrivial covering (in the sense of [Mr] Section 1) because $H^2(\Delta_0,\mu_2)$ is nontrivial. Thus $B_3\neq\{1\}$. In other words, if $\mathcal{E}\twoheadrightarrow\Delta_0$ is the 2-universal covering group, we have a surjective homomorphism $\mathcal{E}\to\mathcal{E}_3$ making the following diagram commutative ([Mr] Lemma 1.6):

$$\begin{array}{ccc}\mathcal{E} & \xrightarrow{\text{onto}} & \mathcal{E}_3\\ \downarrow & & \downarrow\\ \Delta_0 & = & \Delta_0.\end{array}$$

Now $\mathcal{E}_3$ and Δ_0 share the same 2-universal covering group $\mathcal{E}$ and $\mathcal{E}$ is a finite group. Thus $|\pi_1(\mathcal{E}_3)_2|=|\pi_1(\Delta_0)_2|/|B_3|<|\pi_1(\Delta_0)_2|$. Replacing F_0/E by the

Galois extension F_1/E with $\mathrm{Gal}(F_1/E) = \mathcal{E}_3$, by the induction hypothesis, we find a Galois extension F/E containing F_1 such that $\mathrm{Gal}(F/E) = \mathcal{E}$. □

References

Books

[AAG] S. S. Gelbart, *Automorphic Forms on Adele Groups*, Annals of Math. Studies **83**, Princeton University Press, Princeton, NJ, 1975.

[AFG] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Mathematics, Vol. **114**. Springer, 1970.

[AGD] A. Borel and G. D. Mostow edited, *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math. **9**, 1966, AMS

[ARL] A. Borel and W. Casselman edited, *Automorphic forms, representations, and L-functions*. Part 1–2. Proc. Symp. in Pure Math., XXXIII. American Mathematical Society, Providence, R.I., 1979

[BCG] R. P. Langlands, *Base change for $GL(2)$*, Annals of Math. Studies **96**, Princeton University Press, 1980.

[BNT] A. Weil, *Basic Number Theory*, Springer, New York, 1974.

[CGP] K. S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer, New York, 1982.

[ECH] J. S. Milne, Étale Cohomology, Princeton University Press, Princeton, NJ, 1980.

[GCH] J.-P. Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Springer, 2002

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.

[HMI] H. Hida, *Hilbert modular forms and Iwasawa theory*, Oxford University Press, 2006

[LRG] J.-P. Serre, *Linear Representations of Finite Groups*, GTM **42**, Springer, 1977

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.

[SBT] J. Arthur and L. Clozel, *Simple algebras, Base change and the advanced theory of the trace formula*, Ann. of Math. Studies, **120**, Princeton University Press, 1989

Articles

[B] D. Blasius, Elliptic curves, Hilbert modular forms, and the Hodge conjecture, in *Contributions to Automorphic Forms, Geometry, and Number Theory*, pp.83–103, Johns Hopkins University Press, Baltimore, MD, 2004.

[BR] D. Blasius and J. D. Rogawski, Motives for Hilbert modular forms, Inventiones Math. **114** (1993), 55–87.

[D] F. Diamond, The refined conjecture of Serre, in "Elliptic Curves, Modular Forms & Fermat's Last Theorem," International Press, 1995, pages 22–37.

[DFG] F. Diamond, M. Flach and L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms. Ann. Sci. École Norm. Sup. (4) **37** (2004), 663–727.

[F] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 1999 arXiv.math/NT0602606

[F1] K. Fujiwara, Level optimization in the totally real case, preprint 2000, arXiv.math/NT062586

[F2] K. Fujiwara, Galois deformations and arithmetic geometry of Shimura varieties. International Congress of Mathematicians. Vol. II, 347–371, Eur. Math. Soc., Zürich, 2006.

[G] R. L. Griess, Jr., Schur multipliers of the known finite simple groups. Bull. Amer. Math. Soc. **78** (1972), 68–71

[G1] R. L. Griess, Jr., Schur multipliers of the known finite simple groups. III. Proceedings of the Rutgers group theory year, 1983–1984, 69–80, Cambridge Univ. Press, Cambridge, 1985

[H88] H. Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. of Math. **128** (1988), 295–384.

[H89a] H. Hida, On nearly ordinary Hecke algebras for $GL(2)$ over totally real fields, Adv. Studies in Pure Math. **17** (1989), 139–169.

[H89b] H. Hida, Nearly ordinary Hecke algebras and Galois representations of several variables, Proc. JAMI Inaugural Conference, Supplement to Amer. J. Math. (1989), 115–134.

[H05] H. Hida, The integral basis problem of Eichler, IMRN **2005** no.34, 2101–2122

[HM] H. Hida and Y. Maeda, Non-abelian base-change for totally real fields, Special Issue of Pacific J. Math. in memory of Olga Taussky Todd, 189–217, 1997.

[J] F. Jarvis, Level lowering for modular mod l representations over totally real fields. Math. Ann. **313** (1999), 141–160

[J1] F. Jarvis, Mazur's principle for totally real fields of odd degree. Compositio Math. **116** (1999), 39–79.

[Kh] C. Khare, Serre's modularity conjecture : The level one case. Duke Mathematical Journal, **134** (2006), 557–589

[Kh1] C. Khare, On Serre's modularity conjecture: a survey of the level one case, LMS lecture notes series 320, 270–299

[Kh3] C. Khare, Modularity of Galois representations and motives with good reduction properties, J. Ramanujan Math. Soc. **22**, (2007) 1-26

[Ki] M. Kisin, Modularity of 2-adic Barsotti-Tate representations, preprint, 2007 (available at `http://www.math.uchicago.edu/~kisin/preprints.html`)

[KW] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (I), preprint, 2006 (available at `http://www.math.utah.edu/~shekhar/papers.html`)

[KW1] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (II), preprint, 2006 (available at `http://www.math.utah.edu/~shekhar/papers.html`)

[LL] J.-P. Labesse and R. P. Langlands, L-indistinguishability for SL(2). Canad. J. Math. **31** (1979), 726–785

[Me] A. S. Merkurjev, Brauer groups of fields. Comm. Algebra **11** (1983), 2611–2624

[MeS] A. S. Merkurjev and A. A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), 1011–1046 and 1135–1136

[Mr] C. Moore, Group extensions of p-adic and adelic groups, Publ. IHES **35** (1968), 157–222

[Sc] L. L. Scott, Integral equivalence of permutation representations, In "Group theory" (Granville, OH, 1992), 262–274, World Sci. Publishing, River Edge, NJ, 1993

[Sch] I. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. Reine Angew. Math. **139** (1911), 155-250

[Se] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230 (Œuvres IV, 107–158, No. 143).

[St] R. Steinberg, Générateurs, relations et revêtements de groupes algébriques, 1962 Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962) pp. 113–127 Librairie Universitaire, Louvain; Gauthier-Villars, Paris

[St1] R. Steinberg, Generators, relations and coverings of algebraic groups, J. Algebra, **71** (1981), 527–543

[T] R. Taylor, On Galois representations associated to Hilbert modular forms, Inventiones Math. **98** (1989), 265–280.

[T1] R. Taylor, Remarks on a conjecture of Fontaine and Mazur, Journal of the Inst. of Math. Jussieu **1** (2002), 125–143.

[T2] R. Taylor, On the meromorphic continuation of degree two L-functions, preprint

[V] C. Virdol, Non-solvable base change for Hilbert modular forms and zeta functions of twisted quaternionic Shimura varieties, preprint, 2008 (available at `http://www.math.columbia.edu/~virdol/research.html`)

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551.

Haruzo Hida
Department of Mathematics, UCLA, Los Angeles CA 90095-1555, U.S.A.
E-mail: hida@math.ucla.edu