Title
The integral basis problem of Eichler

Journal
International Mathematics Research Notices, 2005(34)

ISSN
1073-7928

Author
Hida, H

Publication Date
2005-07-01

Peer reviewed

THE INTEGRAL BASIS PROBLEM OF EICHLER

HARUZO HIDA

ABSTRACT. For a quaternion algebra B over a totally real field F unramified at every finite place and most ramified at infinite places of F, we prove that the space of $\mathbb{Z}[\frac{1}{E}]$-integral Hilbert modular forms of weight 2 and of level 1 is spanned over $\mathbb{Z}[\frac{1}{E}]$ by the theta series of the norm form of B. Here $E = 6d(F)\prod_{\psi}$ (the numerator of $L(-1,\psi^2)$) where $d(F)$ is the discriminant $d(F)$ of F and ψ runs over all unramified characters of $\mathrm{Gal}(\overline{F}/F)$.

The basis problem of Eichler is to find an explicit basis (over $\mathbb{C}$) of an appropriate space of elliptic modular forms by means of theta series of the norm forms of definite quaternion algebras. He achieved this in the 1950s by comparing the traces of Hecke operators acting on the space of automorphic forms on such quaternion algebras and on elliptic modular forms (see [Ei]).

This basis problem has its origin in Jacobi's celebrated formula (in "Fundamenta Nova" Sections 40-42) of the number $S_4(n)$ of ways of expressing a given integer n as a sum of four squares:

$$S_4(n) = 8\sigma_1(n) \ \text{ with } \ \sigma_1(n) = \sum_{0<d|n} d \ \text{ for odd positive integers } n.$$

This formula has the following heuristic meaning: We take the quaternion algebra $H = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$ and $ki = -j = ik$. Then the norm form on the order $R_2 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ is given by $N(x) = \overline{x}x = x_1^2+x_2^2+x_3^2+x_4^2$ for $x = x_1+x_2i+x_3j+x_4k$ and $\overline{x} = x_1-x_2i-x_3j-x_4k$ (quaternion conjugation). This order R_2 is not maximal, and as Hurwitz proved in [Hu], $R = R_2[\frac{1+i+j+k}{2}]$ is a maximal order of H. Since all right ideals of R are principal (R is a non-commutative Euclidean domain) and $[R : R_2] = 2$, as long as n is odd, $N(x) = n$ (for $x \in R_2$) if and only if $R_2\overline{x}xR_2 = nR_2$ up to units in $R_2^\times = \{\pm 1, \pm i, \pm j, \pm k\}$. The number of ways of making prime decomposition as above of the two sided ideals pR for a prime p into a product of left and right ideal factors is given therefore by the sum $\sigma_1(p) = 1 + p$ of divisors of p for odd p.

We can think of the same problem for $M_2(\mathbb{Q})$ in place of H. Then the norm on $M_2(\mathbb{Z})$ is the determinant map:

$$\det(x) = x_1x_4 - x_2x_3 \ \text{ for } x = \left(\begin{smallmatrix} x_1 & x_2 \\ x_3 & x_4 \end{smallmatrix}\right),$$

which is an indefinite quadratic form. The number of integer matrices x with $p = \det(x)$ for a prime p up to units in $GL_2(\mathbb{Z})$ is the number of left cosets of $GL_2(\mathbb{Z})$ in the double coset $GL_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)GL_2(\mathbb{Z})$:

$$\begin{aligned} &GL_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)GL_2(\mathbb{Z}) \\ &\quad = GL_2(\mathbb{Z})\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\bigsqcup GL_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\bigsqcup GL_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)\bigsqcup\cdots\bigsqcup GL_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & p-1 \\ 0 & p \end{smallmatrix}\right) \end{aligned}$$

The author is partially supported by an NSF grant. DMS 0244401.

by the theory of elementary divisors; so, it is given again by $\sigma_1(p)$. Basically, we get the same formula for H and $M_2(F)$. Define for a subring A of $\mathbb{C}$

$$G_2(p;A)=\left\{f\in G_2(\Gamma_0(p))\middle| f=\sum_{n=0}^{\infty}a(n,f)q^n \text{ with } a(n,f)\in A \text{ if } n\geq 0\right\}$$

for $\Gamma_0(p)=\left\{\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\middle| c\equiv 0 \mod p\right\}$ for a prime p, where $G_2(\Gamma_0(p))$ is the space of holomorphic modular forms on $\Gamma_0(p)$ of weight 2. The space $G_2(2;\mathbb{Z})$ of $\mathbb{Z}$-integral modular forms of weight 2 on $\Gamma_0(2)$ is spanned by an Eisenstein series

$$E(z)=\frac{1}{24}+\sum_{n=1}^{\infty}\sigma_1^{(2)}(n)q^n \ (q=\exp(2\pi iz)),$$

where $\sigma_1^{(2)}(n)$ is the sum of odd positive divisors of n. At the same time, by the theta series of the maximal order $R\supset R_2$ of H:

$$\theta(z)=\sum_{\alpha\in R}q^{\alpha\overline{\alpha}}\in G_2(2;\mathbb{Z}),$$

and what Jacobi (basically) proved is $\theta(z)=24\cdot E(z)$ (because $R^\times=R_2^\times\sqcup\{\frac{\pm 1\pm i\pm j\pm k}{2}\}$ with $|R^\times|=24$; see [Hu] (5)). Thus $G_2(2;\mathbb{Z})$ is spanned by $\theta(z)$. This shows that the integral structures on $G_2(\Gamma_0(2))$ coming from the q-expansion and $\theta(z)$ are equal.

This type of identity of elliptic modular forms and quaternionic automorphic forms are vastly generalized by Jacquet-Langlands, in terms of the identity of automorphic representations. The character (or trace) identity makes sense, because $H\otimes_{\mathbb{Q}}\mathbb{Q}_p=M_2(\mathbb{Q}_p)$ for all odd primes p; so, for such primes, local factors of automorphic representations of $GL(2)$ and $H^\times$ can be identified. However the computation of traces only yields a noncanonical identity of representations.

What we would like to do is to normalize the Jacquet-Langlands correspondence and explore when we have a canonical identity of the two integral structures coming from theta series and q-expansions (comparing automorphic forms and modular forms defined over smaller rings). Though Jacobi's example gives the identity of the two integral structures over $\mathbb{Z}$ (because of the nonexistence of cusp forms on $\Gamma_0(2)$), to achieve this for cusp forms, it would be necessary to invert the Eisenstein ideal (and possibly the prime 2). So far, the integral basis problem has been studied geometrically by using the fact that the definite quaternion algebra B different from $M_2(\mathbb{Q}_p)$ only at a single prime p appears as endomorphism algebra of super-singular elliptic curves over $\overline{\mathbb{F}}_p$. This type of research was carried out by Ohta and Oesterle in the 1980s and yielded good $\mathbb{Z}_{(p)}$–basis of $G_2(p;\mathbb{Z}_{(p)})$ ($\mathbb{Z}_{(p)}=\mathbb{Q}\cap\mathbb{Z}_p$) by means of the theta series of maximal orders (and ideals) of B, and more recently, M. Emerton determined the $\mathbb{Z}[\frac{1}{2}]$-span in $G_2(p;\mathbb{Z})$ of the theta series of the definite quaternion algebra B by refining further the geometric means ([Em]). Since the method is a bit too geometric, it might be difficult to carry it out for Hilbert modular forms and for indefinite quaternion algebras, and the geometric proof for more general quaternion algebras could be lengthy. We would like to present first a short proof of a result (Theorem 3.1) slightly weaker than Emerton's theorem ([Em] Theorem 0.3), reducing the result to the original Eichler's theorem and the method of Taylor-Wiles (see [TW] and [D]), and then we will generalize the result to quaternion algebras (unramified at all finite places) over totally real fields (Theorem 4.3), reducing it to the Jacquet-Langlands correspondence and the generalization of the work of

Taylor-Wiles by Fujiwara [F] to totally real fields. The solution of the integral basis problem has an application towards a solution of the anticyclotomic main conjecture for CM fields (see [H04]).

1. Duality and Hecke Algebras

Although our method works well over any totally real fields F (taking care of holomorphic Hilbert modular forms of any weight $k \geq 2$ and definite or indefinite quaternion algebras over F), all of the essential ideas show up in the elliptic modular case; so, for simplicity, we assume, in the following three sections, that B is definite ramified only at p and ∞, $F = \mathbb{Q}$ and $k = 2$. We describe the results in more general cases at the end of the paper.

Let N be a square free integer. Then a cusp form of weight 2 on $\Gamma_0(N)$ is a holomorphic function $f : \mathfrak{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\} \to \mathbb{C}$ rapidly decreasing towards cusps of $\Gamma_0(N)$ which satisfies the functional equation

$$f(\gamma(z)) = f(z)J(\gamma, z) \ (\gamma(z) = \frac{az+b}{cz+d} \ \text{ and } \ J(\gamma, z) = \det(\gamma)^{-1}(cz+d)^2)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. For a prime ℓ, decomposing

$$\Gamma_0(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right) \Gamma_0(N) = \bigsqcup_{\alpha} \Gamma_0(N)\alpha,$$

we take average $f|T(\ell)(z) = \sum_\alpha f(\alpha(z))J(\alpha, z)^{-1}$ which is again a cusp form on $\Gamma_0(N)$. Thus we get the linear operator $T(\ell)$ acting on the space $S_2(N; \mathbb{C}) := S_2(\Gamma_0(N))$ of cusp forms on $\Gamma_0(N)$. We can extend the definition of $T(\ell)$ for commuting operators $T(n)$ indexed by integers n. By the explicit decomposition: $\alpha = \left(\begin{smallmatrix} 1 & u \\ 0 & \ell \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$, for $f = \sum_{n=1}^{\infty} a(n, f)q^n$, we find a celebrated formula of Hecke:

$$a(m, f|T(n)) = \sum_{0<d|m, d|n} d \cdot a(\frac{mn}{d^2}, f) \ (\Rightarrow a(1, f|T(n)) = a(n, f)). \tag{1.1}$$

Thus, for any subring $A \subset \mathbb{C}$, defining

$$S_2(N; A) = \{f \in S_2(N; \mathbb{C}) | a(n, f) \in A\},$$

the operator $T(n)$ preserves the A-module $S_2(N; A)$. It is a theorem of Shimura that $S_2(N; A) = S_2(N; \mathbb{Z}) \otimes_{\mathbb{Z}} A$; so, $T(n)$ is an integral operator. Define $\mathcal{H}_2(N; A) \subset \operatorname{End}_A(S_2(N; A))$ by the A–subalgebra generated by $T(n)$ for all $n = 1, 2, \ldots$.

Theorem 1.1 (Duality)**.** *Define an A–bilinear pairing*

$$(\ ,\ ) : \mathcal{H}_2(N; A) \times S_2(N; A) \to A \quad \textit{by} \quad (h, f) = a(1, f|h).$$

Then $(\ ,\ )$ induces isomorphisms

$$\operatorname{Hom}_A(S_2(N; A), A) \cong \mathcal{H}_2(N; A) \quad \textit{and} \quad \operatorname{Hom}_A(\mathcal{H}_2(N; A), A) \cong S_2(N; A),$$

and the latter isomorphism is given by $\phi \mapsto \sum_{n=1}^{\infty} \phi(T(n))q^n$.

Proof. Since $S_2(N; A) = S_2(N; \mathbb{Z}) \otimes_{\mathbb{Z}} A$, we may assume that $A = \mathbb{Z}$. Actually we need to treat $A = \mathbb{Q}$ first. The space $S_2(N; \mathbb{Q})$ is finite dimensional over $\mathbb{Q}$; so, we need to prove non-degeneracy of the pairing. By (1.1), $a(1, f|T(n)) = a(n, f)$; so, if $(h, f) = 0$ for all h, $a(n, f) = (T(n), f) = 0$ for all n, and hence $f = 0$. If $(h, f) = 0$ for all f, then $0 = (h, f|T(n)) = a(1, f|T(n)h) = (T(n), f|h) = a(n, f|h)$; so, $f|h = 0$ for all f, which implies $h = 0$. If $\phi \in \operatorname{Hom}_{\mathbb{Z}}(\mathcal{H}_2(N; \mathbb{Z}), \mathbb{Z})$, then we find $f \in S_2(N; \mathbb{Q})$ with $(h, f) = \phi(h)$, and $a(n, f) = (T(n), f) = \phi(T(n)) \in \mathbb{Z}$; so,

$f \in S_2(N;\mathbb{Z})$. This shows $S_2(N;\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{H}_2(N;\mathbb{Z}),\mathbb{Z})$. Since $\mathbb{Z}$ is a PID, we also have $\mathrm{Hom}_{\mathbb{Z}}(S_2(N;\mathbb{Z}),\mathbb{Z}) \cong \mathcal{H}_2(N;\mathbb{Z})$. □

This tells us

Corollary 1.2. *Let $H = \mathcal{H}_2(N;A)$. Let V and V' be H–modules free of finite rank over A with an A–bilinear pairing $\langle\ ,\ \rangle : V \times V' \to A$. Define a formal q–expansion $\Theta(v \otimes v') = \sum_{n=1}^{\infty}\langle v|T(n), v'\rangle q^n$. Then Θ gives an H–linear map of $V \otimes_A V'$ into $S_2(N;A)$ regarding $V \otimes_A V'$ as an H–module through V. If V is H–free of rank 1, $\mathrm{Hom}_A(V,A) \cong V'$ by $\langle\ ,\ \rangle$ and $\langle hv, v'\rangle = \langle v, hv'\rangle$ for $h \in H$, Θ induces an isomorphism $V \otimes_H V' \cong S_2(N;A)$.*

Proof. Just apply the theorem to $\Theta(v \otimes v') \in \mathrm{Hom}_A(H,A) = S_2(N;A)$ given by $\Theta(v \otimes v')(h) = \langle hv, v'\rangle$. □

2. Jacquet-Langlands Correspondence

We take the definite quaternion algebra $B_{/\mathbb{Q}}$ as above and fix a maximal order $R \subset B$ (an order of B is a subring which is a $\mathbb{Z}$–lattice of B). We consider the set $\mathcal{I}$ of all fractional right R–ideals of B

(that is a $\mathbb{Z}$–lattice $\mathfrak{a}$ of B with $\mathfrak{a}R \subset \mathfrak{a}$). We say two such ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if $\mathfrak{a} = \alpha\mathfrak{b}$ for $\alpha \in B^\times$. Then $\mathcal{I}/\sim = Cl$ is the ideal classes of B, which are finite. Take a complete representative set $\{\mathfrak{a}_i | i = 1,\dots,h\}$ for Cl. Then $R_i = \mathfrak{a}_i R \mathfrak{a}_i^{-1}$ is another maximal order of B. We put $e_i = |R_i^\times|$. Then e_i is divisible only by two primes 2 and 3. If one introduces the adele ring $\mathbb{A}$, then $Cl \cong B^\times \backslash B_{\mathbb{A}}^\times / \widehat{R}^\times B_\infty^\times$ for $B_{\mathbb{A}} = B \otimes_{\mathbb{Q}} \mathbb{A}$, $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R}$ and $\widehat{R} = \prod_p R_p$ for $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Suppose that 6 is invertible in A (so, $e_i^{-1} \in A$). We consider the space of functions

$$S(A) = \left\{ \phi : Cl \to A \,\middle|\, \sum_i e_i^{-1}\phi(\mathfrak{a}_i) = 0 \right\}.$$

Thus $f \in S(A)$ can be considered as a function $f : B^\times \backslash B_{\mathbb{A}}^\times \to A$; similarly, a modular form can be considered as a function on $GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A})$. Thus $S(A)$ is a space of automorphic forms on the algebraic group $B^\times$. Assuming that 6 is invertible in A (so, $e_i^{-1} \in A$), we define a pairing $\langle\ ,\ \rangle : S(A) \times S(A) \to A$ by $\langle f, g\rangle = \sum_i e_i^{-1} f(\mathfrak{a}_i) g(\mathfrak{a}_i)$. Then $\langle\cdot,\cdot\rangle$ is a perfect pairing.

We can define an operator $T(n)$ acting on $S(A)$ for integer $n > 0$ as follows. If $\mathfrak{a} \subset R$ is a right integral ideal, we define $N(\mathfrak{a})$ by the index $[R : \mathfrak{a}]$. For any right fractional ideal $\mathfrak{a}$ and a right integral ideal $\mathfrak{b}$ of norm n, we can define the product $\mathfrak{a}\mathfrak{b} = \{\sum_j a_j b_j | a_j \in \mathfrak{a}, b_j \in \mathfrak{b}\}$, which is a right fractional ideal. Thus $\mathfrak{a}_i\mathfrak{b} \sim \mathfrak{a}_{j(i;\mathfrak{b})}$ for a unique $j(i;\mathfrak{b})$, and we may define

$$f|T(n)(\mathfrak{a}_i) = \sum_{\mathfrak{b}:N(\mathfrak{b})=n} f(\mathfrak{a}_{j(i;\mathfrak{b})})$$

for $\mathfrak{b}$ running over all integral right R–ideals with norm n. By definition, we have $\langle f|T(n), g\rangle = \langle f, g|T(n)\rangle$. For simplicity, we assume that $R_\ell \cong M_2(\mathbb{Z}_\ell)$ except for one prime $\ell = p$ and write $H(A)$ for $\mathcal{H}_2(p;A)$.

Theorem 2.1 (Eichler, Jacquet-Langlands)**.** *We have $S(\mathbb{C}) \cong S_2(p;\mathbb{C})$ as modules over $H(\mathbb{C})$, where the action of $T(n)$ is specified above.*

From this, by a descent argument, we find

Corollary 2.2. *For any subring A of $\mathbb{C}$, $S(A)$ is a faithful $H(A)$–module, and if A is a $\mathbb{Q}$–algebra, $S(A)$ is free of rank 1 over $H(A)$.*

It is easy to verify that $\Theta(f\otimes g)=\sum_{i,j}\frac{1}{e_ie_j}f(\mathfrak{a}_i)g(\mathfrak{a}_j)\theta(\mathfrak{a}_i\mathfrak{a}_j^{-1})$ for $f,g\in S(A)$ (see [Ei] II.6), where $\theta(\mathfrak{a}_i\mathfrak{a}_j^{-1})=\sum_{\xi\in\mathfrak{a}_i\mathfrak{a}_j^{-1}}q^{N(\xi)/N(\mathfrak{a}_i\mathfrak{a}_j^{-1})}$. In [Ei] II.6, left ideals are studied instead of right ideals here; so, all the formulas there are valid after applying the involution $\mathfrak{a}\mapsto\mathfrak{a}^{-1}$ to left ideals $\mathfrak{a}$.

Let us describe the Jacquet-Langlands correspondence in a more general setting. Take an open compact subgroup U in $B_{\mathbb{A}}^{\times}$ of the form $U=U^{(p)}\times R_p^{\times}$, and consider the finite set $Y(U)=B^{\times}\backslash B_{\mathbb{A}}^{\times}/UB_{\infty}^{\times}$. The reduced norm map $N:B\to\mathbb{Q}$ induces $N:Y(U)\to Cl_U=\mathbb{A}^{\times}/\mathbb{Q}^{\times}N(U)\mathbb{R}_+^{\times}$. Taking a complete representative set $\{a_i\}$ for $Y(U)$, we define $e_i=|a_iUa_i^{-1}\cap B^{\times}|$. Then e_i is only divisible by primes 2 and 3, and if 6 is invertible in A, we have a pairing $\langle\phi,\phi'\rangle=\sum_i e_i^{-1}\phi(a_i)\phi'(a_i)$ on the space of functions on $Y(U)$. Define $S(U;A)\subset\{f:Y(U)\to A\}$ by the orthogonal complement of functions factoring through $N:Y(U)\to Cl_U$. Then decomposing a double coset $UxU=\bigsqcup_y yU$ for $x\in B_{\mathbb{A}}^{\times}$ with $x_\infty=1$, we can define the Hecke operator $[UxU]:S(U;A)\to S(U;A)$ by $f|[UxU](a)=\sum_y f(ay)$. Identifying $\widehat{R}^{(p)}$ with $M_2(\widehat{\mathbb{Z}}^{(p)})$ for $\widehat{R}^{(p)}=\prod_{\ell\neq p}R_\ell$ and $\widehat{\mathbb{Z}}^{(p)}=\prod_{\ell\neq p}\mathbb{Z}_\ell$, we may regard $U^{(p)}$ as a subgroup of $GL_2(\mathbb{A}^{(p\infty)})$. We put

$$U_0(p)=U^{(p)}\times\left\{x\in GL_2(\mathbb{Z}_p)\middle|x\equiv\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\mod pM_2(\mathbb{Z}_p)\right\}.$$

Then write $X(U_0(p))$ for the compactified modular curve

$$GL_2(\mathbb{Q})_+\backslash GL_2(\mathbb{A})_+/U_0(p)Z(\mathbb{R})SO_2(\mathbb{R})\cup\{\text{cusps}\},$$

where $GL_2(\mathbb{R})^+$ is the identity connected component of $GL_2(\mathbb{R})$ and $GL_2(\mathbb{A})_+=\{x\in GL_2(\mathbb{A})|x_\infty\in GL_2(\mathbb{R})^+\}$ and $GL_2(\mathbb{Q})_+=\mathrm{GL}_2(\mathbb{Q})\cap GL_2(\mathbb{A})_+$ in $GL_2(\mathbb{A})$. We then define $S_2(U_0(p);\mathbb{C})=H^0(X(U_0(p)),\Omega_{X(U_0(p))/\mathbb{C}})$. For any double coset $U_0(p)xU_0(p)$ can be considered as an algebraic correspondence of $X(U_0(p))$, we have a natural action of Hecke operators $[U_0(p)xU_0(p)]$ acting on $S_2(U_0(p);\mathbb{C})$. Then we have the following result (e.g., [AAG] Theorem 10.5 or [PAF] Theorem 4.34):

Theorem 2.3 (Jacquet-Langlands)**.** *Let the notation and the assumption be as above. Then we have a $\mathbb{C}$-linear isomorphism $i:S(U;\mathbb{C})\cong S_2(U_0(p);\mathbb{C})$ satisfying $i\circ[UxU]=[U_0(p)xU_0(p)]\circ i$ for all $x\in GL_2(\mathbb{A}^{(p\infty)})=(B_{\mathbb{A}}^{(p\infty)})^{\times}$ and $i\circ[U\varpi U]=[U_0(p)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)U_0(p)]\circ i$ for $\varpi\in R_p$ with $N(\varpi)=p$.*

3. Integral Correspondence

Take a sufficiently large valuation ring W finite flat over $\mathbb{Z}_\ell$ as a base ring. Wiles proved the identify of a non-Eisenstein local ring $\mathbb{T}$ of $H(W)=H(\mathbb{Z})\otimes_{\mathbb{Z}}W$ with an appropriate universal Galois deformation ring, using a limiting argument due to Wiles and R. Taylor ([TW], see also [MFG] Theorem 3.35). To describe briefly the limiting argument, fix a local ring $\mathbb{T}$ with maximal ideal $\mathfrak{m}$, and write $t(q)$ for the image of $T(q)$ in $\mathbb{T}$. The local ring $\mathbb{T}$ is called "Eisenstein" if there exists a pair of Galois characters $\phi,\varphi:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathbb{T}^{\times}$ unramified outside $p\ell$ such that $t(q)\equiv\phi(Frob_q)+\varphi(Frob_q)\mod\mathfrak{m}$ for almost all primes q outside $p\ell$. Here $Frob_q$ indicates the Frobenius element at q. We assume that $\mathbb{T}$ is not Eisenstein. The

local ring $\mathbb{T}$ carries the associated Galois representation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{T})$ with $\mathrm{Tr}(\rho_{\mathbb{T}}(Frob_q)) = t(q)$ for all primes q outside $p\ell$. The residual representation $\overline{\rho}_{\mathbb{T}} = \rho_{\mathbb{T}} \mod \mathfrak{m}$ is absolutely irreducible (because $\mathbb{T}$ is not Eisenstein), and hence the isomorphism class of $\rho_{\mathbb{T}}$ is unique by a result of Carayol-Serre (e.g., [MFG] Proposition 2.13). Take a finite set Q of primes q outside $p\ell$ with $q \equiv 1 \mod \ell$ so that $\overline{\rho}_{\mathbb{T}}(Frob_q)$ has two distinct eigenvalues. Fixing a choice of an eigenvalue α_q of $\overline{\rho}_{\mathbb{T}}(Frob_q)$ for $q \in Q$, we have a unique local component $\mathbb{T}_Q$ (with maximal ideal $\mathfrak{m}_Q$) of the Hecke algebra (with coefficients in W) on $\Gamma(Q) = \Gamma_0(p) \cap \bigcap_{q\in Q} \Gamma_1(q)$ covering $\mathbb{T}$ with $u(q) \equiv \alpha_q \mod \mathfrak{m}_Q$ for the image $u(q)$ of the Hecke operator $U(q)$. This ring $\mathbb{T}_Q$ is written as h_Q in the middle of page 127 of [MFG]. The limiting argument is done using faithful W-free modules M_Q over $\mathbb{T}_Q$ of level $\Gamma(Q)$ and taking a limit as $|Q| \to \infty$. In particular, $\mathbb{T}$ is proven to be a local complete intersection over W. As later pointed out by F. Diamond and K. Fujiwara (see for example, [MFG] Theorem 3.35), their argument yields freeness over $\mathbb{T}_Q$ of the module M_Q (including the starting module $M_\emptyset$). Wiles took $\mathbb{T}(H^1(X_0(p), W))$ as his starting module $M_\emptyset$ over $\mathbb{T}$ and $M_Q = \mathbb{T}_Q(H^1(X(Q), W))$ for each Q, where $X(Q) = X(U_0(p))$ for $U = \widehat{\Gamma}(Q) \subset B_{\mathbb{A}}^\times$ defined by

$$\begin{aligned} \widehat{\Gamma}_0(Q) &= \left\{(x_\ell) \in \widehat{R}^\times \middle| x_q \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod qR_\ell \text{ for all } q \in Q\right\} \\ \widehat{\Gamma}(Q) &= \left\{(x_\ell) \in \widehat{R}^\times \middle| x_q \equiv \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \mod qR_\ell \text{ for all } q \in Q\right\} \end{aligned} \tag{3.1}$$

in $B_{\mathbb{A}}^\times$. In [MFG] 3.2.7, the local ring itself $\mathbb{T}_Q$ is taken to be M_Q (using the fact that $\mathbb{T}_Q \cong \mathbb{T}_Q(H^1(X(Q), \mathcal{O}_{X(Q)})) \cong \mathrm{Hom}_W(\mathbb{T}_Q(H^0(X(Q), \Omega_{X(Q)/W}), W)$ by the Grothendieck-Serre duality). We can instead take $\mathbb{T}(S(W))$ as $M_\emptyset$ and take M_Q to be the space $\mathbb{T}_Q(S(\widehat{\Gamma}(Q); W))$ for $\widehat{\Gamma}(Q)$ in (3.1), because the Hecke algebra on $\Gamma(Q) \subset SL_2(\mathbb{Z})$ over W acts on quaternionic automorphic forms in $S(\widehat{\Gamma}(Q); W)$ by the Jacquet-Langlands correspondence. The result is

Theorem 3.1. *Assume that p is an odd prime. Let ℓ be an odd prime outside $3(p-1)$. Then $S(\mathbb{Z}_{(\ell)})$ is free of rank 1 over $H(\mathbb{Z}_{(\ell)})$, and Θ induces an isomorphism of $H(\mathbb{Z}_{(\ell)})$–modules:*

$$S(\mathbb{Z}_{(\ell)}) \otimes_{H(\mathbb{Z}_{(\ell)})} S(\mathbb{Z}_{(\ell)}) \cong S_2(p; \mathbb{Z}_{(\ell)}),$$

and $H(\mathbb{Z}_{(\ell)})$ is a local complete intersection, where $\mathbb{Z}_{(\ell)} = \left\{\frac{a}{b} \middle| \ell \nmid b\right\}$.

Since the linear map $\Theta : S(\mathbb{Z}[\frac{1}{3(p-1)}]) \otimes_{H(\mathbb{Z}[\frac{1}{3(p-1)}])} S(\mathbb{Z}[\frac{1}{3(p-1)}]) \to S_2(p; \mathbb{Z}[\frac{1}{3(p-1)}])$ is an isomorphism after localization at each maximal ideal of $\mathbb{Z}[\frac{1}{3(p-1)}]$, it is an isomorphism over $\mathbb{Z}[\frac{1}{3(p-1)}]$. In other words, this solves Eichler's basis problem integrally over $\mathbb{Z}[\frac{1}{3(p-1)}]$, and $S_2(p; \mathbb{Z}[\frac{1}{3(p-1)}])$ is contained in the subspace generated by the theta series $\theta(\mathfrak{a}_i\mathfrak{a}_j^{-1})$ over $\mathbb{Z}[\frac{1}{3(p-1)}]$.

Proof. By Corollary 1.2, we need to prove that $S(\mathbb{Z}_{(\ell)})$ is free of rank 1 over $H(\mathbb{Z}_{(\ell)})$. Since the pairing $\langle \cdot, \cdot \rangle$ is well defined only over the ring A in which 6 is invertible, we are forced to assume that $\ell \nmid 6$. Since freeness over $H(\mathbb{Z}_{(\ell)})$ is unaffected by scalar extension from $\mathbb{Z}_{(\ell)}$ to a valuation ring W finite flat over $\mathbb{Z}_\ell$, we only need to prove the freeness of $M_\emptyset$ over the given local ring $\mathbb{T}$ of the Hecke algebra $H(W)$ for sufficiently large valuation ring W. Thus we may assume that $\mathbb{T}$ and W share

the same residue field. Then we show that $S(W)$ is free of rank 1 over $H(W)$ for all ℓ prime to $p-1$. Since $S_2(\Gamma_0(p))=0$ if $p\le 7$, we may assume that $p\ge 11$.

We consider the space of automorphic forms $S_Q(A)=S(\widehat{\Gamma}(Q);A)$. A prime ℓ is called Eisenstein if there exists an Eisenstein local component of $H(W)$. If ℓ is Eisenstein, we can find a normalized Hecke eigenform in $S_2(\Gamma_0(p))$ congruent modulo a prime above ℓ to the unique Eisenstein series on $\Gamma_0(p)$ and $\ell|p-1$ (see [M]). Thus by our assumption $\ell\nmid p-1$, there is no Eisenstein component. Thus we apply the method of Taylor-Wiles component-by-component. Fix one such local component $\mathbb{T}$ with associated Galois representation $\rho_{\mathbb{T}}$ and residual representation $\overline{\rho}$. We put $M_Q=\mathbb{T}_Q(S(\widehat{\Gamma}(Q);W))$ on which the group $\Gamma_0(Q)/\widehat{\Gamma}(Q)\cong\prod_{q\in Q}(\mathbb{Z}/q\mathbb{Z})^\times$ acts naturally. We write Δ_Q for the ℓ-Sylow subgroup of $\Gamma_0(Q)/\widehat{\Gamma}(Q)$. We therefore need to verify

(1) The deformation problem attached to $\mathbb{T}$ is minimal (that is, either "Selmer," "strict" or "flat" at ℓ in the terminology of [Wi1] page 457 and in Cases (A) or (B) at p in the terminology of [Wi1] page 458; see below);
(2) M_Q is free of finite rank over $W[\Delta_Q]$ and $M_Q/\mathfrak{a}_Q M_Q\cong M_\emptyset$ as $\mathbb{T}_Q$-modules, where $\mathfrak{a}_Q$ is the augmentation ideal of $W[\Delta_Q]$ (the condition (tw5) in Theorem 3.35 of [MFG]).
(3) $\overline{\rho}$ is irreducible over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[\sqrt{\ell^*}])$ for $\ell^*=(-1)^{(\ell-1)/2}\ell$.

The condition (2) follows from a horizontal control theorem and is easier to verify in our case than the cases dealt with in [TW] and [MFG] 3.2.7 because $S_Q(W)=H^0(Y(Q),W)$ for the finite set $Y(Q)=B^\times\backslash B_{\mathbb{A}}^\times/\widehat{\Gamma}(Q)B_\infty^\times$ while the choice in [TW] is $\mathbb{T}_Q(H^1(X(Q),W))$ and the choice in [MFG] 3.2.7 is $\mathbb{T}_Q$ itself. Since the proof for our choice now is anyway similar to the argument in [MFG] proving Corollary 3.19 there, we only point out that the assertion (2) follows from the discussion of control (or congruence) of automorphic forms on $B_{\mathbb{A}}^\times$ in [T] Section 1 (particularly Lemma 4) and leave the verification of (2) to the reader (in any case, the work has been done in [F] in the more general Hilbert modular case). Since the first three conditions (tw1-3) of [MFG] Theorem 3.35 are independent of the choice of the modules M_Q, they are verified in [TW] (or in 3.2.8 of [MFG]) under the condition (3). The condition (tw4) follows from the condition (tw5) which is the condition (2) above.

We now verify the condition (1). First suppose $p\neq\ell$. Locally at p, since the abelian variety associated to each Hecke eigenform $f\in S(\Gamma_0(p))$ is of multiplicative type, the Galois representation $\overline{\rho}$ restricted to the decomposition group D_p at p is isomorphic to $\left(\begin{smallmatrix}\chi_\ell & *\\ 0 & 1\end{smallmatrix}\right)$ up to twists by unramified characters. Here χ_ℓ is the ℓ-adic cyclotomic character. By the level-lowering argument of [Wi1] Chapters 2 and 3, we have to have a Hecke eigenform of level 1 which gives rise to $\overline{\rho}$. Since $S_2(SL_2(\mathbb{Z}))=0$, this is impossible, and $\overline{\rho}$ has to be ramified, and hence we are in Case (A) at p.

Now we study the structure at $\ell\neq p$. Since $\ell\neq p$, the Galois representation $\overline{\rho}$ is associated to a finite flat group scheme, which is in the Selmer case if it is ordinary (nonconnected) and in the flat case if it is connected.

Suppose $\ell=p$. If $\overline{\rho}$ is not wildly ramified, it is flat, and again by level lowering combined with $S_2(SL_2(\mathbb{Z}))=0$, this does not happen. We are in the "strict" case.

In the above argument dealing with the local behaviour of $\overline{\rho}$, we have found a nontrivial unipotent element in the image of the inertia group at p under $\overline{\rho}$, which

prohibits $\overline{\rho}$ to be an induced representation from a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ of a quadratic field $M/\mathbb{Q}$. In particular, we conclude (3). □

4. Hilbert Modular Case

In this section, we study the integral basis problem for Hilbert modular forms. We fix a totally real finite extension $F \neq \mathbb{Q}$ of $\mathbb{Q}$ of degree d. We write $d(F)$ for the discriminant of $F/\mathbb{Q}$ and O for the integer ring of F.

Let us recall the definition of the adelic Hilbert modular forms of level 1 and of weight 2. We write I for the set of all real embedding of F (identifying it with the set of archimedean places of F). We thus identify $F \otimes_{F,\sigma} \mathbb{R}$ with $\mathbb{R}$ for $\sigma \in I$; so, $F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^I$ via $\xi \otimes x \mapsto (\sigma(\xi)x)_{\sigma\in I} \in \mathbb{R}^I$. We consider the upper half complex plane $\mathfrak{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$ and let $g = (g_\sigma) \in GL_2(F_\infty) = GL_2(\mathbb{R})^I_+$ act on $\mathfrak{H}^I$ by component-wise linear fractional transformation. Here $GL_2(\mathbb{R})_+$ is the identity connected component of the Lie group $GL_2(\mathbb{R})$. We write Z for the center of the algebraic group $GL(2)_{/F}$.

The automorphy factor $J(g,z)$ of the weight 2 is given by

$$J(g,z) = \prod_{\sigma\in I} \left(\det(g_\sigma)^{-1} j(g_\sigma, z_\sigma)^2\right) \tag{4.1}$$

for $g = (g_\sigma) \in GL_2(F_\infty) = GL_2(\mathbb{R})^I$ and $z = (z_\sigma) \in \mathfrak{H}^I$. Here we put $j\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\right) = cz+d$ for $z \in \mathbb{C}$. Then we define $S_2(\mathbb{C})$ to be the space of functions $f : GL_2(F_\mathbb{A}) \to \mathbb{C}$ satisfying the following conditions (cf., [PAF] 4.3.1):

(A1) We have the following automorphy

$$f(\alpha x u z) = f(x) J(u_\infty, \mathbf{i})^{-1}$$

for all $\alpha \in GL_2(F)$, $z \in Z(F_\mathbb{A})$, and $u \in GL_2(\widehat{O})C_\mathbf{i}$ for the stabilizer $C_\mathbf{i}$ in $GL_2(\mathbb{R})^I_+$ of $\mathbf{i} = (\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathfrak{Z} = \mathfrak{H}^I$;

(A2) Choosing $u \in GL_2(\mathbb{R})^I_+$ with $u(\mathbf{i}) = z$ for each $z \in \mathfrak{H}^I$, define a function $f_g : \mathfrak{H}^I \to \mathbb{C}$ by $f_g(z) = f(gu_\infty)J(u_\infty, \mathbf{i})$ for each $g \in GL_2(F_\mathbb{A}^{(\infty)})$. Then f_g is a holomorphic function on $\mathfrak{H}^I$ for all g;

(A3) $f_g(z)$ is exponentially decreasing as $\mathrm{Im}(z) \to \infty$ for each $g \in GL_2(F_\mathbb{A}^{(\infty)})$.

Let $\mathbf{e}_\mathbb{A} : F\backslash F_\mathbb{A} \to \mathbb{C}^\times$ be the standard continuous additive character with $\mathbf{e}_\mathbb{A}(x_\infty) = \exp(2\pi i \sum_{\sigma\in I} x_\sigma)$. Each member f of $S_2(\mathbb{C})$ has a Fourier expansion of the following form ([MFG] Theorem 3.10 and [H96] Sections 2.3–4),

$$f\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) = |y|_\mathbb{A} \sum_{0\ll\xi\in F} \mathbf{a}_\infty(\xi y, f)\mathbf{e}_\mathbb{A}(i\xi y_\infty)\mathbf{e}_\mathbb{A}(\xi x). \tag{4.2}$$

Here $y \mapsto \mathbf{a}_\infty(y,f)$ is a function defined on $y \in F_\mathbb{A}^\times$ only depending on its finite part $y^{(\infty)}$, and $\left(\begin{smallmatrix} y_\infty & 0 \\ 0 & 1 \end{smallmatrix}\right) \mapsto \mathbf{e}_\mathbb{A}(iy_\infty)$ is the restriction of the canonical Whittaker function of $GL_2^+(\mathbb{R})$ to matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (whose Mellin transform gives the optimal Γ-factor of the standard L-function of f). The function $\mathbf{a}_\infty(y,f)$ is supported by the set $(\widehat{O} \times F_\infty) \cap F_\mathbb{A}^\times$ of integral ideles. By (A1), $f \in S_2(\mathbb{C})$ is invariant under $f(x) \mapsto f(xu)$ for a diagonal element $u \in GL_2(\widehat{O})$, and therefore, $\mathbf{a}_\infty(y,f)$ only depends on the ideal $yO = y\widehat{O} \cap F$. In this sense, for a fractional ideal $\mathfrak{n}$, we take $y \in F_\mathbb{A}^\times$ with $\mathfrak{n} = yO$ and put $\mathbf{a}_\infty(\mathfrak{n}, f) = \mathbf{a}_\infty(y,f)$. Then we have the following

formula for the standard Hecke operator $T(\mathfrak{n})$ analogous to (1.1) (e.g., [PAF] (4.65) and (4.77)):

$$(4.3)\quad \mathbf{a}_\infty(\mathfrak{m}, f|T(\mathfrak{n})) = \sum_{\mathfrak{d}\supset\mathfrak{m}+\mathfrak{n}} N(\mathfrak{d})\cdot \mathbf{a}_\infty(\frac{\mathfrak{m}\mathfrak{n}}{\mathfrak{d}^2}, f)\ (\Rightarrow \mathbf{a}_\infty(O, f|T(n)) = \mathbf{a}_\infty(\mathfrak{n}, f)),$$

where $\mathfrak{d}$ runs over common divisors of the ideals $\mathfrak{m}$ and $\mathfrak{n}$.

By the q-expansion principle due to Rapoport valid over $\mathbb{Z}$ (e.g., [Ch]), for any subalgebra $A \subset \mathbb{C}$, the association $A \mapsto S_2(A) = \{f \in S_2(\mathbb{C})|\mathbf{a}_\infty(y, f) \in A\}$ gives rise to a well-defined integral structure of $S_2(\mathbb{C})$. For any ring (or even any module) A (not necessarily in $\mathbb{C}$), $S_2(A) = S_2(\mathbb{Z})\otimes_{\mathbb{Z}} A$ is therefore well-defined. Each element $f \in S_2(A)$ has its q-expansion coefficients $\mathbf{a}_\infty(y, f) \in A$. By (4.3), the Hecke operators $T(\mathfrak{n})$ acts on $S_2(A)$ preserving the integral structure.

We write $\mathcal{H}_2(A) \subset \mathrm{End}_A(S_2(A))$ for the A–subalgebra generated by $T(\mathfrak{n})$ for all integral ideals $\mathfrak{n}$.

Theorem 4.1 (Duality)**.** *For a commutative ring A with identity, define an A–bilinear pairing*

$$(\ ,\ ) : \mathcal{H}_2(A)\times S_2(A) \to A \quad by \quad (h, f) = \mathbf{a}_\infty(O, f|h).$$

Then $(\ ,\ )$ induces isomorphisms

$$\mathrm{Hom}_A(S_2(A), A) \cong \mathcal{H}_2(A) \quad and \quad \mathrm{Hom}_A(\mathcal{H}_2(A), A) \cong S_2(A),$$

and the latter isomorphism is given by $\phi \mapsto f(\phi)$ with $\mathbf{a}_\infty(y, f(\phi)) = \phi(T(yO))$ for all idele $y \in F_{\mathbb{A}}^\times$.

The proof of this theorem is the same as the one for Theorem 1.1. We thus have

Corollary 4.2. *Let $H = \mathcal{H}_2(A)$. Let V and V' be H–modules free of finite rank over A with an A–bilinear pairing $\langle\ ,\ \rangle : V\times V' \to A$. Define a formal q–expansion $\Theta(v\otimes v')$ by $\mathbf{a}_\infty(y, \Theta(v\otimes v')) = \langle v|T(yO), v'\rangle$ for integral ideles y. Then Θ gives an H–linear map of $V\otimes_A V'$ into $S_2(A)$ regarding $V\otimes_A V'$ as an H–module through V. If V is H–free of rank 1, $\mathrm{Hom}_A(V, A) \cong V'$ by $\langle\ ,\ \rangle$ and $\langle hv, v'\rangle = \langle v, hv'\rangle$ for $h \in H$, Θ induces an isomorphism $V\otimes_H V' \cong S_2(A)$.*

We take a division quaternion algebra B over F unramified at every finite place. We fix a maximal order R of B and identify $\widehat{R}$ with $M_2(\widehat{O})$. Let $\mathbb{H} = H\otimes_{\mathbb{Q}}\mathbb{R}$ (the Hamilton quaternion algebra). Then $B_\infty = B\otimes_{\mathbb{Q}}\mathbb{R}$ is isomorphic to the product of r copies of $M_2(\mathbb{R})$ and $d-r$ copies of $\mathbb{H}$. Then $r \equiv d \mod 2$. For an open compact subgroup $U \subset B_{\mathbb{A}}^\times$ (for $B_{\mathbb{A}} = B\otimes_{\mathbb{Q}}\mathbb{A}$), we consider the automorphic manifold $Y(U) = B^\times\backslash B_{\mathbb{A}}^\times/UF_{\mathbb{A}}^\times C$ and the class set $Cl(U) = B^\times\backslash B_{\mathbb{A}}^\times/UF_{\mathbb{A}}^\times B_{\infty+}^\times$, where C is a maximal compact subgroup of $B_\infty^\times$ and $B_{\infty+}^\times$ is the identity connected component of $B_\infty^\times$. Note that $Cl(U) = Y(U)$ if $r = 0$. We write simply Cl for $Cl(\widehat{R}^\times)$. Then by the approximation theorem, $Cl(U)$ is a finite set. As is well known, $Y(U)$ is a compact complex analytic space of dimension r, and if U is sufficiently small, $Y(U)$ is a smooth compact complex manifold. To guarantee the W-freeness of $H^r(Y(U), W)$, we assume

(dm) $r \le 1$,

though our argument works well as long as we have W-freeness of the cohomology groups $H^r(Y(U), W)$ for all U appearing in this situation (which has been verified for Hilbert modular varieties by [G] for quadratic F and by Dimitrov [Dm] for more general Hilbert modular varieties under some restrictive assumptions).

First suppose $r = 1$. Choosing a complete representative set inside finite ideles of B for $Cl(U)$ (and writing it again as $Cl(U)$ by abusing notation), we have

$$H^1(Y(U), A) = \bigoplus_{a \in Cl(U)} H^1(\Gamma_a(U), A)$$

for $\Gamma_a(U) = (aUa^{-1}B_\infty^\times) \cap B_+^\times$. Here $H^1(\Gamma_a(U), A)$ is the group cohomology for the $\Gamma_a(U)$-module A with trivial action.

Take a sufficiently small U so that $Y(U)$ is smooth, we define

$$S(A) = H_0(\widehat{R}^\times, H^1(Y(U), A)) \text{ (the coinvariant under the action of } \widehat{R}^\times),$$

$$S^*(A) = H^0(\widehat{R}^\times, H^1(Y(U), A)) \text{ (the invariant under the action of } \widehat{R}^\times).$$

The module $S(A)$ has Poincaré duality pairing

$$\langle \cdot, \cdot \rangle : S(A) \times S^*(A) \to A,$$

which is a perfect alternating A-duality pairing (as long as $S(A)$ is A-free and is canonically isomorphic to $S^*(A)$; see below). If $A = \widehat{\mathbb{Z}}$ and W, writing A^* for the Pontryagin dual module of A, the above pairing $\langle \cdot, \cdot \rangle$ induces a perfect Pontryagin duality between $S^*(A^*)$ and $S(A)$ (here as before W is a valuation ring finite flat over $\mathbb{Z}_\ell$). Let $\overline{\Gamma}_a(U) = \Gamma_a(U)/(\Gamma_a(U) \cap Z(F))$. By the Hochschild-Serre spectral sequence applied to $H^1(\overline{\Gamma}_a(U), A^*)$ (for $A = W$ and $\widehat{\mathbb{Z}}$) combined with the Poincaré duality as above, if ℓ is prime to $6d(F)$, we have

$$S(W) \cong \bigoplus_a H^1(\overline{\Gamma}_a(\widehat{R}^\times), W) \cong \bigoplus_a H_1(\overline{\Gamma}_a(\widehat{R}^\times), W) \cong S^*(W), \tag{4.4}$$

which is independent of the choice of U and is W-free of finite rank. Indeed, if $H^1(\Gamma_a(U), W)$ is W-selfdual under the cup product pairing, we have $S(W) \cong S^*(W)$ canonically. The self duality follows from the W-freeness of $H^m(\overline{\Gamma}_a(U), W)$ if $m \geq 2$ ($\Leftrightarrow H^2(\overline{\Gamma}_a(U), W) \cong W$ and $H^m(\Gamma_a(U), W) = 0$ if $m > 2$), which in turn follows if $\overline{\Gamma}_a(U)$ is ℓ-torsionfree. By [H88] Lemma 7.1, $\overline{\Gamma}_a(\widehat{R}^\times)$ is ℓ-torsionfree if ℓ is prime to $6d(F)$. Similarly, the order of the torsion part of $S^*(\mathbb{Q}/\mathbb{Z}) = S^*(\widehat{\mathbb{Z}}^*)$ is supported by primes q which gives the torsion of $\overline{\Gamma}_a(\widehat{R}^\times)$; so, $S(W)$ is W-free if ℓ is prime to $6d(F)$. Hereafter, assuming $\ell \nmid 6d(F)$, we identify $S(W)$ and $S^*(W)$.

By the Hilbert modular version of the Jacquet-Langlands correspondence (e.g., [PAF] Theorem 4.34 or [H88] Theorem 2.1) combined with the Eichler-Shimura isomorphism (e.g., [PAF] Theorem 4.36), $S(A)$ is naturally a module over $\mathcal{H}_2(A)$ and have $\langle f|h, g\rangle = \langle f, g|h\rangle$ for $f, g \in S(A)$ and $h \in \mathcal{H}_2(A)$.

Identifying B_∞ with $M_2(\mathbb{R}) \times \mathbb{H}^{d-1}$, we can let $B_{\infty+}^\times$ act on $\mathfrak{H}$ by linear fractional transformation through the component $M_2(\mathbb{R})$. Under this identification, we have $B_{\infty+}^\times / C_+ F_\infty^\times \cong \mathfrak{H}$ for the maximal compact subgroup C_+ of $B_{\infty+}^\times$ fixing $\sqrt{-1} \in \mathfrak{H}$. On the other hand, for the maximal compact subgroup C of $B_\infty^\times$ containing C_+, C_+ is a normal subgroup of index 2 inside C, and $B_\infty^\times / C F_\infty^\times \cong B_{\infty+}^\times / C_+ F_\infty^\times \cong \mathfrak{H}$. Thus C/C_+ acts on $\mathfrak{H}$, and its action is basically the complex conjugation (given by $z \mapsto -\overline{z}$ if we choose the embedding $B \hookrightarrow M_2(\mathbb{R})$ suitably). Then C/C_+ acts on $Y(\widehat{R}^\times)$ and hence on $S(A)$. Hereafter suppose that 2 is invertible in A. Thus we have $S(A) = S^+(A) \oplus S^-(A)$ for the $\pm$ eigenspace $S^\pm(A)$ of C/C_+, and the Poincare duality induces a perfect pairing $\langle \cdot, \cdot \rangle : S^+(A) \times S^-(A) \to A$. Since the action of C/C_+ commutes with Hecke operators (e.g., [H88] Theorem 2.2), $S^\pm(A)$ is a module over $\mathcal{H}_2(A)$.

Now suppose $r = 0$. Decompose $B_{\mathbb{A}}^\times = \bigsqcup_i B^\times a_i \widehat{R}^\times F_{\mathbb{A}}^\times B_\infty^\times$, and write $R_i = B \cap a_i \widehat{R} a_i^{-1}$ and $e_i = |R_i^\times / O^\times|$ (which is a finite number). If $6d(F)$ is invertible in A, e_i for all i is invertible in A. If we take a Haar measure dx on $B_{\mathbb{A}}^\times / F_{\mathbb{A}}^\times$ so that $\int_{\widehat{R}^\times/\widehat{O}^\times} dx = 1$ and the standard Haar measure on the discrete subgroup $B^\times/F^\times \subset B_{\mathbb{A}}^\times$, we have the quotient measure on Cl still denoted by dx. Define a pairing $\langle \cdot, \cdot \rangle : H^0(Cl, A) \times H^0(Cl, A) \to A$ by $\langle f, g \rangle = \int_{Cl} f(x)g(x)dx = \sum_j \frac{1}{e_i} f(a_i)g(a_i)$ for $f, g \in H^0(Cl, A)$. This pairing is the Poincaré duality on Cl and is perfect as long as $6d(F)$ is invertible in A.

Let Cl_F for the strict class group of F. Then the reduced norm map induces a map $N : Cl \to Cl_F/Cl_F^2$, which is surjective. The space $H^0(Cl_F/Cl_F^2, A)$ of functions on Cl_F can be embedded into $H^0(Cl_F/Cl_F^2, A)$ by the pull-back of N. We then define $S(A) \subset H^0(Cl, A)$ by the orthogonal complement of $H^0(Cl_F/Cl_F^2, A) \subset H^0(Cl, A)$. The pairing $\langle \cdot, \cdot \rangle$ on $S(A)$ remains perfect. Again, by Jacquet-Langlands correspondence, $S(A)$ has a natural right action of $\mathcal{H}_2(A)$ written as $f \mapsto f|h$ for $f \in S(A)$ and $h \in \mathcal{H}_2(A)$, and we have $\langle f|h, g \rangle = \langle f, g|h \rangle$ for all $f, g \in S(A)$ and $h \in \mathcal{H}_2(A)$.

We then define $\Theta(v \otimes v') \in S_2(A)$ by $\mathbf{a}_\infty(y, \Theta(v \otimes v')) = \langle v | T(yO), v' \rangle$ for $v \otimes v'$ in $S(A) \otimes_{\mathcal{H}_2(A)} S(A)$ when $r = 0$ and in $S^+(A) \otimes_{\mathcal{H}_2(A)} S^-(A)$ when $r = 1$. As shown in [H04] (7.9) when $r = 0$, $\Theta(f \otimes g)$ is the classical theta series of the definite quaternion algebra $B_{/F}$. In the indefinite case, by the analytic computation in [Sh] II, Theorem 3.1, $\Theta(f \otimes g)$ is the integral against Siegel's indefinite theta series (over the Shimura variety of the orthogonal group of the indefinite norm form of $B_{/F}$) of $f \otimes g$ regarded as an automorphic form on the orthogonal similitude group (isogenous to $B^\times \times B^\times$).

Theorem 4.3. *Let the notation and the assumption be as above, and define a positive integer E by $E = 6d(F) \prod_\psi$(the numerator of $L(-1, \psi^2)$), where $d(F)$ is the discriminant $d(F)$ of F and ψ runs over all unramified characters of $\mathrm{Gal}(\overline{F}/F)$ with values in $\mathbb{C}^\times$. Then, for any $\mathbb{Z}[\frac{1}{E}]$-algebra A, $S(A)$ when $r = 0$ and $S^\pm(A)$ when $r = 1$ are free of rank 1 over $\mathcal{H}_2(A)$, and Θ induces an isomorphism of $\mathcal{H}_2(A)$–modules:*

$$S_2(A) \cong \begin{cases} S(A) \otimes_{\mathcal{H}_2(A)} S(A) & \text{if } r = 0, \\ S^+(A) \otimes_{\mathcal{H}_2(A)} S^-(A) & \text{if } r = 1, \end{cases}$$

and $\mathcal{H}_2(\mathbb{Z}[\frac{1}{E}])$ is a local complete intersection.

This theorem solves the integral basis problem over $\mathbb{Z}[\frac{1}{E}]$ for $S_2(\mathbb{Z}[\frac{1}{E}])$.

Proof. The proof is the same as the one given for Theorem 3.1, following [F] instead of [Wi1]. We shall give a sketch of the proof giving the key points of the arguments (since going through all the details of the Taylor-Wiles system argument as in [MFG] Sections 3.2.6-8 for Hilbert modular forms would requires us to spend many pages). A detailed proof of the result in [F] will be described in my forthcoming book [HMI].

Let W be a sufficiently large valuation ring finite flat over $\mathbb{Z}_\ell$ for primes $\ell \nmid E$. We take a local component $\mathbb{T}$ of $\mathcal{H}_2(W)$. Then we have a Galois representation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{F}/F) \to GL_2(\mathbb{T})$ for an algebraic closure $\overline{F}$ of F, which is unramified outside primes of F over ℓ (e.g. [T]) and characterized by the fact $\rho_{\mathbb{T}}(Frob_{\mathfrak{q}})$ for

primes of $\mathfrak{q}$ outside ℓ is given by $t(\mathfrak{q})$ (the image of $T(\mathfrak{q})$ in $\mathbb{T}$). The determinant character $\det(\rho_{\mathbb{T}})$ is given by the ℓ-adic cyclotomic character χ_ℓ.

For the maximal ideal $\mathfrak{m}$ of $\mathbb{T}$, we put $\overline{\rho} = \rho_{\mathbb{T}} \mod \mathfrak{m}$, and call $\mathbb{T}$ Eisenstein if $\overline{\rho}$ is not absolutely irreducible. By the solution of Iwasawa's conjecture by Wiles [Wi], if we have an Eisenstein component $\mathbb{T}$, we claim that ℓ is irregular (with respect to F) if $\ell \nmid 2d(F)$. Thus if $\ell \nmid E$, $\mathbb{T}$ is not Eisenstein. Here is the proof of the claim. Write $\overline{\rho}^{ss}$ for the semi-simplification of $\overline{\rho}$. Then $\overline{\rho}^{ss} = \overline{\psi} \oplus \overline{\varphi}$ for two characters $\overline{\psi}, \overline{\varphi} : \mathrm{Gal}(\overline{F}/F) \to k^\times$ for $k = \mathbb{F}_{\ell^s}$ unramified outside ℓ. Write ψ (resp. φ) for the Teichimüller lift of $\overline{\psi}$ (resp. $\overline{\varphi}$). If $[F : \mathbb{Q}]$ is odd, we can find an abelian variety factor $A_{/F}$ of the Jacobian of the level 1 Shimura curve $Y(\widehat{R}^\times)$ associated to B with real multiplication by the integer ring O_E of a totally real field E such that the semi-simplification of $A[\mathfrak{L}]$ is isomorphic to $\overline{\rho}^{ss}$ for a prime ideal $\mathfrak{L}|\ell$ of O_E (by the Jacquet-Langlands correspondence and [H81] Theorems 4.12). If $[F : \mathbb{Q}]$ is even, by the level raising argument in [T], we can find a quaternion algebra B' with a maximal order R' such that B' ramifies only at one finite place $\mathfrak{q} \nmid \ell$ and at all but one infinite place whose Shimura curve of the level group $\widehat{R'}^\times$ has Jacobian containing a factor $A_{/F}$ as above. By Carayol [Ca], the abelian variety A has good reduction at all places $\mathfrak{l}$ of F dividing ℓ. Thus $\overline{\psi}$ (resp. $\overline{\varphi}$) is associated to a finite locally free commutative group scheme $G_{\overline{\psi}}$ (resp. $G_{\overline{\varphi}}$) of rank ℓ^s over $O_\mathfrak{l}$ whose generic fiber is a k-vector spaces of dimension 1 (this fact also follows from Corollary 2.13 in [Dm]). Then assuming that ℓ is prime to $2d(F)$ and writing κ for the composite of $O/\mathfrak{l} = \mathbb{F}_{\ell^n}$ and $k = \mathbb{F}_{\ell^s}$, by Proposition 4.4 (following this proof), $\overline{\psi}([u, F_\mathfrak{l}]) = N_{\kappa/k}(\overline{u})^{-\nu}$ for $\nu = 0, 1$, where $[u, F_\mathfrak{l}]$ is the local Artin symbol of $u \in O_\mathfrak{l}^\times$ and $\overline{u} = u \mod \mathfrak{l}$. Since $\psi\varphi$ is the ℓ-adic Teichmüller character ω, we may assume $G_{\overline{\psi}} \cong \mathbb{Z}/\ell\mathbb{Z}$ and $G_{\overline{\varphi}} \cong \mu_\ell$. In particular, the component $\mathbb{T}$ is ℓ-ordinary. Thus ψ is unramified everywhere, and $\psi\varphi = \omega$ (see [Dm] 3.1 for an alternative argument showing the unramifiedness without using Proposition 4.4). This is exactly the case which Wiles studied in [Wi], and the order of the $\psi\varphi^{-1}$-part of the class group of $H(\mu_\ell)$ for the (strict) Hilbert class field H/F is divisible by ℓ. Since $\psi\varphi = \omega$, we have $\psi\varphi^{-1} = \psi^2\omega^{-1}$, and by the F-version of the Kummer's criterion (which follows from [Wi]), ℓ then divides the numerator of $L(-1, \psi^2)$. Thus $\ell|E$, and ℓ is irregular if ℓ is prime to $2d(F)$ and $\mathbb{T}$ is Eisenstein. As pointed out by Dimitrov, there is an alternative geometric argument to show $\ell|$the numerator of $L(-1, \psi^2)$ (for Eisenstein primes ℓ) without recourse to Wiles' theorem. Here is a sketch of the argument of Dimitrov. The representation $\overline{\rho}^{ss}$ is unramified outside ℓ and crystalline at primes dividing ℓ of weights 0 and 1 (by Breuil and Fontaine-Laffaille; [Dm] Proposition 2.12). Therefore one of the two characters ψ and φ, say ψ as before, is unramified (Corollary 2.13 in [Dm]). Then the Eisenstein series associated to ψ and φ is congruent modulo $\mathfrak{m}$ to a cusp form (on which $\mathbb{T}$ acts non-trivially) in the sense that they have congruent Hecke eigenvalues. By the q-expansion principle and Andreatta-Goren's computation (see [AG]) of the kernel of the q-expansion on the graded ring of all Hilbert Modular forms, one deduces that ℓ divides also the constant term of the Eisenstein series (which implies $\ell|$the numerator of $L(-1, \psi^2)$).

Hereafter we assume that $\mathbb{T}$ is not Eisenstein. Let $\overline{\rho}_\mathfrak{q}$ be the restriction of $\overline{\rho}$ to the decomposition group $D_\mathfrak{q}$ in $\mathrm{Gal}(\overline{F}/F)$ at a prime $\mathfrak{q}$. As in [Wi1], we can classify the local behaviour of $\overline{\rho}$ in the following cases: Let $\mathfrak{l}$ be a prime factor of ℓ in O.

(Selmer) $\overline{\rho}_{\mathfrak{l}} \cong \left(\begin{smallmatrix} \overline{\varepsilon}_{\mathfrak{l}} & * \\ 0 & \overline{\delta}_{\mathfrak{l}} \end{smallmatrix}\right)$ for characters ε and unramified δ of $D_{\mathfrak{l}}$ and $\overline{\rho}_{\mathfrak{l}}$ is associated to a finite flat group scheme over $O_{\mathfrak{l}}$;
(Flat) $\overline{\rho}_{\mathfrak{l}}$ is irreducible and is associated to a finite flat group scheme over $O_{\mathfrak{l}}$.

Under the assumption $\ell \nmid d(F)$, $\overline{\varepsilon}_{\mathfrak{l}}$ is ramified at $\mathfrak{l}$; so, $\overline{\delta}_{\mathfrak{l}} \neq \overline{\varepsilon}_{\mathfrak{l}}$.

By the result of [T1] Theorem 1.6, for non-Eisenstein $\mathbb{T}$, $\overline{\rho}_{\mathfrak{l}}$ falls either in the Selmer case or in the flat case. A Galois representation $\rho : \mathrm{Gal}(\overline{F}/F) \to GL_2(A)$ for an artinian local W-algebra A with maximal ideal $\mathfrak{m}_A$ is called a minimal deformation of $\overline{\rho}$ if the following conditions are satisfied:

- $\rho \mod \mathfrak{m}_A$ is isomorphic to $\overline{\rho}$;
- ρ is unramified outside ℓ;
- $\det(\rho) = \iota \circ \chi_\ell$ for the W-algebra structure morphism $\iota : W \to A$.

We call ρ flat at $\mathfrak{l}$ if ρ is associated to a finite flat group scheme over $O_{\mathfrak{l}}$. We call ρ Selmer at $\mathfrak{l}$ if $\rho_{\mathfrak{l}} = \rho|_{D_{\mathfrak{l}}} \cong \left(\begin{smallmatrix} \varepsilon_{\mathfrak{l}} & * \\ 0 & \delta_{\mathfrak{l}} \end{smallmatrix}\right)$ in $GL_2(A)$ for characters $\varepsilon_{\mathfrak{l}} \equiv \overline{\varepsilon}_{\mathfrak{l}} \mod \mathfrak{m}_A$ and unramified $\delta_{\mathfrak{l}} \equiv \overline{\delta}_{\mathfrak{l}} \mod \mathfrak{m}_A$. Imposing the unramifiedness outside ℓ and the flatness or the Selmer condition at each prime factor $\mathfrak{l}$ of $\mathfrak{l}$ accordingly as $\overline{\rho}$ is flat at $\mathfrak{l}$ or Selmer at $\mathfrak{l}$, we have the universal p-profinite local ring $\mathcal{R}$ and a universal minimal deformation $\boldsymbol{\rho} : \mathrm{Gal}(\overline{F}/F) \to GL_2(\mathcal{R})$. Fujiwara proved the identity $\mathcal{R} \cong \mathbb{T}$ by refining Wiles' limiting method (taking the starting module $M_\emptyset$ to be $\mathbb{T}(S(W))$ if $r = 0$ and $\mathbb{T}(S^{\pm}(W))$ when $r = 1$). His proof yields the freeness of $M_\emptyset$ over $\mathbb{T}$. Since $S(\mathbb{C})$ when $r = 0$ and $S^{\pm}(\mathbb{C})$ when $r = 1$ are free of rank 1 over $\mathcal{H}_2(\mathbb{C})$ by the Jacquet-Langlands correspondence (e.g. [PAF] Theorem 4.34 or [H88] Theorem 2.1) combined with the strong multiplicity one theorem for $GL(2)$, the rank of $M_\emptyset$ over $\mathbb{T}$ is equal to 1. Take a finite set Q of prime ideals $\mathfrak{q}$ outside ℓ with $N(\mathfrak{q}) \equiv 1 \mod \ell$ such that $\overline{\rho}(Frob_{\mathfrak{q}})$ has two distinct eigenvalues. Fixing a choice of eigenvalues of $\overline{\rho}(Frob_{\mathfrak{q}})$ for each $\mathfrak{q} \in Q$, we can define the local ring $\mathbb{T}_Q$ of the Hecke algebra of level $\widehat{\Gamma}(Q)$ covering $\mathbb{T}$. Here, as before, identifying $\widehat{R}$ with $M_2(\widehat{O})$,

$$
\begin{aligned}
&\widehat{\Gamma}_0(Q) = \left\{ x \in GL_2(\widehat{O}) \middle| x_{\mathfrak{q}} \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod \mathfrak{q}R_{\mathfrak{q}} \text{ for all } \mathfrak{q} \in Q \right\} \\
&\widehat{\Gamma}(Q) = \widehat{O}^{\times} \cdot \left\{ x \in GL_2(\widehat{O}) \middle| x_{\mathfrak{q}} \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \mod \mathfrak{q}R_{\mathfrak{q}} \text{ for all } \mathfrak{q} \in Q \right\}.
\end{aligned} \tag{4.5}
$$

Then we choose M_Q by $\mathbb{T}_Q(H^0(Y(\widehat{\Gamma}(Q)), W))$ if $r = 0$ and $\mathbb{T}_Q(H^1(Y(\widehat{\Gamma}(Q)), W)^{\pm})$ if $r = 1$, where $H^1(Y(\widehat{\Gamma}(Q)), W)^{\pm}$ is the $\pm$-eigenspace in $H^1(Y(\widehat{\Gamma}(Q)), W)$ under the action of C/C_+.

As in the case of the proof of Theorem 3.1, we need to check the following three points

(1) The deformation problem attached to $\mathbb{T}$ is minimal (that is, either "Selmer" or "flat" at $\mathfrak{l}|\ell$);
(2) M_Q is free of finite rank over $W[\Delta_Q]$ and $M_Q/\mathfrak{a}_Q M_Q \cong M_\emptyset$ as $\mathbb{T}_Q$-modules, where $\mathfrak{a}_Q$ is the augmentation ideal of $W[\Delta_Q]$ (the condition (tw5) in Theorem 3.35 of[MFG]), where Δ_Q is the ℓ-Sylow subgroup of $\widehat{\Gamma}_0(Q)/\widehat{\Gamma}(Q) \cong \prod_{\mathfrak{q} \in Q}(O/\mathfrak{q})^{\times}$.
(3) $\overline{\rho}$ is irreducible over $\mathrm{Gal}(\overline{F}/F[\sqrt{\ell^*}])$. This condition is necessary to find an infinite sequence of finite sets Q satisfying the properties fitting well into the Taylor-Wiles system in [F] (see also [MFG] 3.2.6).

In [F], Fujiwara actually assumes that $\overline{\rho}$ is irreducible over $\mathrm{Gal}(\overline{F}/F[\mu_\ell])$. Since $\mathrm{Gal}(F[\mu_\ell]/F)$ is cyclic for $\ell \geq 3$, by the Frobenius reciprocity, this condition is equivalent to the irreduciblity of $\overline{\rho}$ over $\mathrm{Gal}(\overline{F}/F[\sqrt{\ell^*}])$ if ℓ is unramified in $F/\mathbb{Q}$.

The condition (1) is already checked. The verification of (2) if $r = 1$ is the same as in the case of $F = \mathbb{Q}$ (e.g. [TW]) resorting to the Hochschild-Serre spectral sequence of $H_1(\overline{\Gamma}_a(U), W)$ (identifying, as in (4.4), M_Q with the $\pm$-eigenspace under the action of C/C_+ in $\mathbb{T}_Q(\bigoplus_a H_1(\overline{\Gamma}_a(U), W))$ for $U = \widehat{\Gamma}(Q)$), and the case where $r = 0$ is much easier. In any case, the work has been done in [F]. Thus we verify (3) for primes $\ell \nmid 6d(F)$. Suppose $\overline{\rho} \cong \mathrm{Ind}_M^F \lambda$ for a Galois character $\lambda : \mathrm{Gal}(\overline{F}/M) \to \mathbb{F}_{\ell^s}^\times$ for the quadratic extension $M = \mathbb{Q}[\sqrt{\ell^*}]$. Here we take ℓ^s with s as small as possible. Fix a prime factor $\mathfrak{l}$ of ℓ in F. We write V for the $\mathfrak{l}$-adic integer ring of the $\mathfrak{l}$-adic completion $M_\mathfrak{l}$. Since $\overline{\rho}$ is flat or Selmer at $\mathfrak{l}$, λ gives the action of $\mathrm{Gal}(\overline{M}_\mathfrak{l}/M_\mathfrak{l})$ on a finite flat group scheme $G_{/V_\mathfrak{l}}$ which is an $\mathbb{F}_{\ell^s}$ vector space of dimension 1. Write ℓ^n for the order of $O/\mathfrak{l}$. Again by the proposition following this proof, if $\ell > 2$ is unramified in $F/\mathbb{Q}$, writing m for the GCD of s and n and k for the subfield of κ of order ℓ^m, $\lambda([u, M_\mathfrak{l}]) = N_{\kappa/k}(\overline{u})^{-\nu}$ for $\nu = 0, 1, 2$ and $\overline{u} = u \mod \mathfrak{m}_V$, where $[u, M_\mathfrak{l}]$ is the local Artin symbol. We have

$$N_{\kappa/k}(\overline{u})^{-2\nu} = \lambda([u, M_\mathfrak{l}])\lambda([u^\sigma, M_\mathfrak{l}]) \\ = \det(\overline{\rho})([u, M_\mathfrak{l}]) = \chi_\ell([u, M_\mathfrak{l}]) = N_{\mathbb{F}_{\ell^n}/\mathbb{F}_\ell}(\overline{u})^{-1}$$

for the generator $\sigma \in \mathrm{Gal}(M/F)$. Writing $\kappa_0 = \mathbb{F}_{\ell^n} \cap k$, we have $N_{\kappa/k}(\overline{u}) = N_{\mathbb{F}_{\ell^n}/\kappa_0}(\overline{u})$ for all $\overline{u} \in \mathbb{F}_{\ell^n}$, because $\mathbb{F}_{\ell^n} = V/\mathfrak{m}_V$ and k is linearly disjoint over κ_0. Then the above identity implies that for all $\overline{u} \in \mathbb{F}_{\ell^n}^\times$,

$$N_{\mathbb{F}_{\ell^n}/\kappa_0}(\overline{u})^{-2\nu} = N_{\mathbb{F}_{\ell^n}/\mathbb{F}_\ell}(\overline{u})^{-1} = N_{\kappa_0/\mathbb{F}_\ell}(N_{\mathbb{F}_{\ell^n}/\kappa_0}(\overline{u}))^{-1}.$$

Since $N_{\mathbb{F}_{\ell^n}/\kappa_0} : \mathbb{F}_{\ell^n}^\times \to \kappa_0^\times$ is surjective, rewriting $x \in \kappa_0^\times$ for $N_{\mathbb{F}_{\ell^n}/\kappa_0}(\overline{u})$, we have $x^{-2\nu} = N_{\kappa_0/\mathbb{F}_\ell}(x)^{-1}$ for all $x \in \kappa_0^\times$. Let $\ell^t = |\kappa_0|$. Since $N_{\kappa_0/\mathbb{F}_\ell}(x) = x^{1+\ell+\cdots+\ell^{t-1}}$, we thus find $2\nu \equiv 1 + \ell + \cdots + \ell^{t-1} \mod \ell^t - 1$. Since $0 \leq \nu \leq 2$, if $\ell \geq 4 \geq 2\nu$, this is impossible. When $\nu = 2$, we could have $2\nu = 4 = 1 + 3$ for $\ell = 3$ and $t = 2$. Thus we have verified (3) for $\ell \geq 4$. See [Dm] Lemma 3.4 for an alternative argument proving (3) for primes ℓ different from $2k - 1$ for the weight k (so in our case, $k = 2$ and therefore for $\ell \geq 4$). □

The following proposition is based on the classification theory of commutative finite flat group schemes due to Oort-Tate and Raynaud whose proof can be found in [O] Proposition 1:

Proposition 4.4. *Let V be a discrete valuation ring finite flat over $\mathbb{Z}_\ell$ with residue field $\mathbb{F}_{\ell^n}$ and quotient field K. Let G be a finite locally free group scheme of rank ℓ^s over V on which $k = \mathbb{F}_{\ell^s}$ acts by V-endomorphisms. Let m be the GCD of n and s, and regard k as the finite subfield of κ with ℓ^m elements. Then the action of $\mathrm{Gal}(K^{ab}/K)$ for the maximal abelian extension K^{ab}/K on the generic fiber of G is given by the character $\varphi : \mathrm{Gal}(K^{ab}/K) \to k^\times$ satisfying $\varphi([u, K]) = N_{\kappa/k}(\overline{u})^{-\nu} \in k^\times$ ($\overline{u} = u \mod \mathfrak{m}_V$) for the local Artin symbol $[u, K]$ for $u \in V^\times$, where $\nu \geq 0$ is an integer satisfying $\nu \frac{\ell^s - 1}{\ell^m - 1} = \sum_{i=0}^{s-1} c_i \ell^i$ for integers c_i with $0 \leq c_i \leq e$ for the ramification index e of $V/\mathbb{Z}_\ell$.*

In the circumstances of the proof of Theorem 4.3, this proposition is used in the following two cases: (1) $K = F_\mathfrak{l}$ with $e = 1$ and (2) $K = M_\mathfrak{l}$ with $e = 2$. In Case

(1), the only possibility of $\nu = 0, 1$, and in Case (2), if $\ell \geq 3$, the only possibility of ν is $0, 1, 2$.

For the reader's convenience, we recall (a sketch of) the proof by Ohta of this proposition.

Proof. Let $v : V \to \mathbb{Z} \cup \{\infty\}$ be the valuation normalized so that $v(\varpi) = 1$ if ϖ generates the maximal ideal $\mathfrak{m}$ of V. First we deal with the case where $s|n$. We consider the Teichmüller lift $\chi : k^\times = \mathbb{F}_q^\times \to V^\times$ of the fixed field inclusion $k \hookrightarrow \kappa$. Then by [R] Corollary 1.5.1, G is isomorphic to $\mathrm{Spec}(V[X_1, \ldots, X_s]/\mathfrak{a})$, where $\mathfrak{a}$ is the ideal generated by $X_i^\ell - \delta_i X_{i+1}$ ($i \in \mathbb{Z}/\ell\mathbb{Z}$, $\delta_i \in V$ and $v(\delta_i) \leq e$ for all i). The action of $\lambda \in k^\times$ on the bialgebra is given by $[\lambda]X_i = \chi(\lambda)^{\ell^i} X_i$. Writing $\varphi_G = \varphi$ for the character of $\mathrm{Gal}(\overline{K}/K)$ giving the Galois action on the generic fiber of G, the splitting field of φ_G is the splitting field of the equations $X_i^q - a_i X_i = 0$ for $a_i = \delta_i^{\ell^{s-1}} \delta_{i+1}^{\ell^{s-2}} \cdots \delta_{i+s-1}$. By the explicit formula of the tame norm residue symbol, we find that

$$\varphi_G(t) = N_{\kappa/k}((-1)^{v(a_0)v(t)} a_0^{v(t)} t^{-v(a_0)} \mod \mathfrak{m})$$

for all $t \in K^\times$. This shows the assertion if $s|n$.

In general, we put $N = ns/m$, and take the (unique) unramified extension K' inducing the residual extension κ'/κ for $\kappa' = \mathbb{F}_{\ell^N}$. Taking the valuation ring V' of K' with normalized valuation v' and maximal ideal $\mathfrak{m}'$, we apply the above argument to $G' = G \otimes_V V'$ over V'. We write $a_0' \in V'$ for the number a_0 corresponding to $G'_{/V'}$. By local class field theory, $\varphi_G(u) = \varphi_{G'}(t)$ if $u = N_{K'/K}(t)$. Thus by the first step of the proof, we get $\varphi_G(u) = N_{\kappa'/k}(t \mod \mathfrak{m}')^{-v'(a_0')}$. Since $\varphi_G([u, K]) \in k = \mathbb{F}_{\ell^m}$ for all $u \in V^\times$, we find that $v(a_0')$ is divisible by $\frac{\ell^s - 1}{\ell^m - 1}$. Write $\nu = \frac{v(a_0)(\ell^m - 1)}{\ell^s - 1} \in \mathbb{Z}$. Since K'/K is unramified, we have

$$\varphi_G(u) = N_{\kappa'/k}(t \mod \mathfrak{m}')^{-\nu} = N_{\kappa/k}(\overline{u})^{-\nu}$$

as desired. □

When we deal with a higher parallel weight $k \geq 2$, we need to consider the "crystalline" condition in place of the "flat" condition. Here we note that k is an even integer. To have the universal crystalline deformation ring, we need to invert also the primes less than the weight. Thus primes we have to avoid to get a result similar to Theorem 4.3 for weight $k \geq 2$ are

- prime factors of 6;
- primes less than k;
- prime factors of the numerator of $L(1 - k, \psi^2)$ for an unramified character ψ of $\mathrm{Gal}(\overline{F}/F)$ into $\mathbb{C}^\times$;
- $2k - 1$ if $2k - 1$ is a prime, $\ell = 2k - 1$ is the prime for which the condition (3) in the above proof could fail (for example, $\ell = 23$ for $k = 12$ and $F = \mathbb{Q}$; see [Dm] Lemma 3.4).

For a general quaternion algebra B over a totally real field F satisfying (dm) but ramifying at some finite places, we can define $S(A)$ and $S^\pm(A)$ in the same manner as above. Writing D for the product of ramified primes in B/F, we consider the space of Hilbert modular new forms $S_2^{new}(\widehat{\Gamma}_0(D); A)$ on $\widehat{\Gamma}_0(D)$ with q-expansion coefficients in A and with trivial central character. Let $H(A) = \mathcal{H}_2(D; A)$ be the A-subalgebra generated by Hecke operators $T(\mathfrak{n})$ in $\mathrm{End}_A(S_2^{new}(\widehat{\Gamma}_0(D); A))$. Then

we have $\Theta : S(A) \otimes_{H(A)} S(A) \to S_2^{new}(\widehat{\Gamma}_0(D); A)$. In this general case, assuming to have the exact level lowering result (Mazur's principle) for $\overline{\rho}$ (which is not yet known in full generality), we need to avoid the primes satisfying the following condition in addition to the ones excluded already:

- prime factors outside ℓ of D for which $\overline{\rho}$ is unramified;
- prime factors $\ell > k$ of D for which $\overline{\rho}$ is crystalline;
- prime factors of $\prod_{\mathfrak{l}|D}(\psi^2(\mathfrak{l})N(\mathfrak{l})^{k-1} - 1)$ for an everywhere unramified character ψ of $\mathrm{Gal}(\overline{F}/F)$ into $\mathbb{C}^\times$; (strictly speaking, we need to remove prime factors of the numerator of $L^{(D)}(1-k, \psi^2) = \prod_{\mathfrak{l}|D}(1 - \psi(\mathfrak{l})N(\mathfrak{l})^{k-1})L(1-k, \psi^2)$).

This point would be clear from our proof given above, because $\overline{\rho}$ in such a case is associated to a primitive form of lower level than D.

References

Books

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

[BCM] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961–83

[HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, forthcoming

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

[PAF] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, 2004, Springer

Articles

[AG] F. Andreatta and E. Z. Goren, Hilbert modular forms: mod p and p-adic aspects, preprint, to appear in the Memoirs of the AMS (downloadable at http://www.math.mcgill.ca/goren/publications.html)

[Ca] H. Carayol, Sur la mauvaise réduction des courbes de Shimura, Compositio Math. **59** (1986), 151–230

[Ch] C.-L. Chai, Arithmetic minimal compactification of the Hilbert-Blumenthal moduli spaces, Appendix to [Wi1], Ann. of Math. **131** (1990), 541–554.

[D] F. Diamond, The Taylor-Wiles construction and multiplicity one. Invent. Math. **128** (1997), 379–391

[Dm] M. Dimitrov, Galois representations modulo p and cohomology of Hilbert modular varieties, preprint, 2004 (downloadable at http://www.math.jussieu.fr/~dimitrov/)

[Ei] M. Eichler, The basis problem for modular forms and the traces of the Hecke operators, in "Modular functions of one variable, I" Lecture Notes in Math., **320** (1973), 75–151

[Em] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms, J. Amer. Math. Soc. **15** (2002), 671–714

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

[G] E. Ghate, On the freeness of the integral cohomology groups of Hilbert-Blumenthal varieties as Hecke modules, preprint, 2004 (downloadable at http://www.math.tifr.res.in/~eghate)

[H81] H. Hida, On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves, Amer. J. Math. **103** (1981), 727–776.

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

[H96] H. Hida, On the search of genuine p–adic modular L–functions for $GL(n)$, Mémoire SMF **67**, 1996

[H04] H. Hida, Anticyclotomic main conjectures, preprint, 2004 (downloadable at www.math.ucla.edu/~hida)

[Hu] A. Hurwitz, Über die Zhalentheorie der Quaternionen, Göttingen Nachr. Akad. Wiss. 1896, 313–340 (Werke No. LXIV)

[M] B. Mazur, Modular curves and the Eisenstein ideal, Publ. IHES **47** (1977), 33–186

[O] M. Ohta, The representation of Galois group attached to certain finite group schemes, and its application to Shimura's theory, in"Algebraic Number Theory," papers contributed for the Int. Symp. Kyoto 1976, pp.149–156

[R] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$. Bull. Soc. Math. France **102** (1974), 241–280

[Sh] G. Shimura, On certain zeta functions attached to two Hilbert modular forms: II. The case of automorphic forms on a quaternion algebra, Ann. of Math. **114** (1981), 569–607

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

[T1] R. Taylor, On Galois representations associated to Hilbert modular forms II, in Series in Number Theory **1** (1995): "Elliptic curves, Modular forms, & Fermat's last theorem", pp.185–191

[TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke modules, Ann. of Math. **141** (1995), 553–572

[Wi] A. Wiles, The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493–540

[Wi1] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555
E-mail address: hida@math.ucla.edu