Invent. math. 98, 265–280 (1989)

*Inventiones mathematicae*


# On Galois representations associated to Hilbert modular forms

Richard Taylor*
Department of Mathematics, Princeton University, Princeton, NJ 08544, USA

## Introduction

Let $F$ be a totally real number field and let $I$ denote the set of embeddings $\tau$: $F \hookrightarrow \mathbf{R}$. Let $k=(k_\tau)\in \mathbf{Z}^I_{>0}$ and suppose all the $k_\tau$ have the same parity. Then there is a notion of Hilbert cusp form of weight $k$ and level $n$ (an ideal of $\mathcal{O}_F$). There are also certain Hecke operators $T_q$ for $q$ a prime of $F$ and $S_a$ for $a$ an ideal of $F$ prime to $n$. We give precise definitions at the start of section one. Suppose that $f$ is such a form and that $f|T=\theta(T)f$ for $T$ any of the above Hecke operators. Then it is known that the field $L_f$ generated over $\mathbf{Q}$ by the $\theta(T)$ is a number field. We shall denote its ring of integers by $\mathcal{O}_f$. The following conjecture is familiar:

**Conjecture 1.** *Let $f$ be as described above and let $\wp$ be a prime of $\mathcal{O}_f$ (above a rational prime $p$), then there is a continuous representation:*

$$\rho\colon \operatorname{Gal}(F^{ac}/F)\to GL_2(\mathcal{O}_{f,\wp})$$

*which is unramified outside $np$ and such that if $q$ is a prime of $F$ not dividing $np$ then:*

$$\operatorname{tr}\rho(\operatorname{Frob} q)=\theta(T_q),$$
$$\det\rho(\operatorname{Frob} q)=\theta(S_q)\,\mathbf{N}\,q.$$

In the case that each $k_\tau \geqq 2$ the conjecture has been proved whenever:

1. $[F:\mathbf{Q}]$ odd.
2. $[F:\mathbf{Q}]$ even and $f$ corresponding to an automorphic representation $\pi_f = \otimes\, \pi_{f,v}$ such that for some finite place $v$, $\pi_{f,v}$ is special or supercuspidal.
3. $p$ is an ordinary prime for $f$ (i.e. $p$ is prime to $\theta(T_q)$ for each prime $q$ of $F$ above $p$).

---

* Supported by a Sloan Foundation Doctoral Dissertation Fellowship

*Current address:* D.P.M.M.S., Cambridge University, 16 Mill Lane, Cambridge CB2 ISB, U.K.

Cases 1 and 2 were established in successively greater generality by Eichler, Shimura, Deligne, Ohta and Rogawski and Tunnell. Case 3 was established by Wiles by different methods, working from the results for cases 1 and 2. Although for a given eigenform $f$, infinitely many primes $p$ seem to be ordinary for $f$, one can not at present show that a general $f$ will be ordinary at any prime $p$. The purpose of this article is to prove the conjecture in the case of $[F:\mathbf{Q}]$ even and each $k_\tau \geqq 2$.

The conjecture can be strengthened to describe the restriction of $\rho$ to the decomposition group $D_q$ for $q|n$ but $q \not| p$. In the Cases 1, 2 and 3 above such a result has been proved by Deligne, Langlands, Carayol and Wiles. We shall prove such a strengthened result in the cases we treat. In fact our main theorem will be:

**Theorem 2.** *Let $[F:\mathbf{Q}]$ be even, $f$ as described above and $\mathfrak{p}$ a prime of $\mathcal{O}_f$ (lying above a rational prime $p$) then there is a continuous representation:*

$$\rho\colon \operatorname{Gal}(F^{ac}/F) \to GL_2(\mathcal{O}_{f,\mathfrak{p}})$$

*which is unramified outside $np$ and such that if $q$ is a prime of $F$ not dividing $np$ then:*

$$\operatorname{tr} \rho(\operatorname{Frob} q) = \theta(T_q),$$
$$\det \rho(\operatorname{Frob} q) = \theta(S_q)\,\mathbf{N}\,q.$$

*Moreover if $q|n$, $q \not| p$ and $\theta(T_q) \neq 0$ and if $\sigma \in D_q$ lies above* $\operatorname{Frob}_q$ *then:*

$$\operatorname{tr} \rho(\sigma) = \theta(T_q) + \chi(\sigma)(\mathbf{N}\,q)\,\theta(T_q)^{-1},$$
$$\det \rho(\sigma) = \chi(\sigma)\,\mathbf{N}\,q.$$

*Here $\chi$ is the continuous Galois character extending the map* $\operatorname{Frob} q \mapsto \theta(S_q)$ *for $q$ a prime not dividing $np$.*

If $f$ is a newform and $q \not| p$ this describes $\rho|D_q$ unless $f$ is associated to an automorphic representation $\otimes \pi_v$ with $\pi_q$ either supercuspidal, special, or principal series coming from two ramified characters. In the first two cases $\rho|D_q$ is described by the work of Carayol [C] and in the third we may twist $f$ by a finite character to reduce it to a case we can treat ($\pi_q$ principal series, coming from a pair of characters at least one of which is unramified).

It should be mentioned that in Case 3 above Wiles has described the restriction of $\rho$ to the decomposition group $D_q$ for $q|p$. Also the case $k_\tau = 1$ for all $\tau$ has been treated by Deligne-Serre, Rogawski-Tunnell and Wiles.

Our method of proof follows the method Wiles used for the "$\Lambda$-adic" case, see [W]. The idea is to find congruences between the form $f$ and forms of level $n\lambda$ for suitable primes $\lambda$ which are "new at $\lambda$" and fall into Case 2. We can then build the desired representation from those already constructed using Wiles' method of "pseudo-representations" (see [W]).

The congruences we need are generalisations of those first studied by Ribet in [R]. Here we establish their existence by first using the correspondence of Jacquet and Langlands to switch to modular forms on a totally definite quaternion algebra and then essentially following the original method of Ribet. We learnt the idea of switching to a totally definite quaternion algebra to establish congruences between modular forms from Hida's paper [H]. To show that we have found sufficient congruences we use a result of Brylinski and Labesse ([BL]).

After this article was written, Blasius and Rogawski [BR] found a completely different proof of conjecture one, which relies on the fact that $U(2)$ is an endoscopic group of $U(2,1)$. In the Cases 1–3 above this gives no new information. In the cases considered in this paper their method has the advantage that it shows the representation obtained is of Hodge-Tate type. However they are unable to describe the restriction of $\rho$ to the decomposition group at bad primes.

It is a pleasure to acknowledge the debt this work owes to that of Wiles [W] and that of Ribet [R]. The author has also benefited from many discussions with Fred Diamond. Finally I would like to thank Andrew Wiles for his constant help and encouragement.

## 1. Congruences

We shall let $F$ denote a totally real field of even degree, say $d$. We shall let $I$ denote the set of embeddings $F \hookrightarrow \mathbf{R}$. We shall let $A$ denote $M_2(F)$ and $D$ denote the unique quaternion algebra over $F$ ramified at exactly all the infinite places. We shall fix a maximal order $\mathcal{O}_D$ of $D$. Choose a subfield $K$ of $\mathbf{C}$ which is Galois over $\mathbf{Q}$, which splits $D$ and such that there is an isomorphism $j\colon \mathcal{O}_D \otimes_{\mathbf{Z}} \mathcal{O}_K \xrightarrow{\sim} M_2(\mathcal{O}_K)^I$. There are algebraic groups $G^A$ and $G^D$ over $F$ with $G^A(F)=A^\times$ and $G^D(F)=D^\times$ along with the reduced norm morphisms $\nu_A\colon G^A \to \mathbf{G}_m$ and $\nu_D\colon G^D \to \mathbf{G}_m$.

If $L$ is a number field we shall let $\mathbf{A}_L$ denote its ring of adeles which we decompose into its finite and infinite parts as $\mathbf{A}_L = L_f \times L_\infty$. If $G$ is an algebraic group over $F$ we shall write $G_f$ and $G_\infty$ for $G(F_f)$ and $G(F_\infty)$ respectively. We fix isomorphisms $M_2(\mathcal{O}_{F,v}) \cong \mathcal{O}_D \otimes_{\mathcal{O}_F} \mathcal{O}_{F,v}$. This gives an isomorphism $G_f^D \cong G_f^A$ which we shall use to identify these groups, which we shall denote simply as $G_f$.

Fix $k=(k_\tau)\in \mathbf{Z}^I$ such that each component $k_\tau$ is $\geqq 2$ and such that all components have the same parity. Set $t=(1, \ldots, 1)\in \mathbf{Z}^I$ and set $m=k-2t$. Also choose $v\in \mathbf{Z}^I$ such that each $v_\tau \geqq 0$, some $v_\tau=0$ and $m+2v=\mu t$ for some $\mu \in \mathbf{Z}_{\geqq 0}$.

Now if $f\colon G^A(\mathbf{A}_F) \to \mathbf{C}$ and $u=u_f u_\infty \in G_f^A \times G_\infty^A$ then we define:

$$(f|_k u)(x) = j(u_\infty, z_0)^{-k} \nu(u_\infty)^{v+k-t} f(x u^{-1})$$

where:

- $z_0=(\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathscr{H}^I$, with $\mathscr{H}$ denoting the upper half complex plane
- $j\colon G_\infty^A \times \mathscr{H}^I \to \mathbf{C}^I$ by $\begin{pmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{pmatrix} \times z_\tau \mapsto (c_\tau z_\tau + d_\tau)$.

If $U \subset G_f$ is an open compact subgroup we define $S_k^A(U)$ to be the set of functions from $GL_2(F)\backslash G^A(\mathbf{A}_F)$ to $\mathbf{C}$ satisfying the following conditions:

1. $f|_k u = f$ for all $u \in U C_\infty$ where $C_\infty = (\mathbf{R}^\times \cdot SO_2(\mathbf{R}))^I \subset G_\infty^A$.

2. For all $x \in G_f$ the function $f_x\colon \mathscr{X}^I \to \mathbf{C}$ defined by:

$$u\, z_o \mapsto j(u, z_0)^k\, v(u)^{t-k-v} f(x\,u)$$

for $u \in G_\infty^A$ is holomorphic (it is easily checked to be well defined).

3. $\int\limits_{\mathbf{A}_F/F} f\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} x\right) da = 0$ for all $x \in G^A(\mathbf{A}_F)$ and $da$ an additive Haar measure on $\mathbf{A}_F/F$.

If $U$ and $U'$ are open compact subgroups in $G_f$ and if $x \in G_f$ we define a Hecke operator:

$$[U\,x\,U'] : S_k^A(U) \to S_k^A(U')$$

by:

$$f \mapsto \sum f|_k\, x_i$$

where $U\,x\,U' = \coprod U\,x_i$.

We shall introduce the following notation, where $n$ denotes an ideal of $\mathcal{O}_F$ and $\lambda$ denotes a prime of $F$ not dividing $n$:

- $U_0 = \prod\limits_q GL_2(\mathcal{O}_{F,q})$ where $q$ runs over finite primes of $F$.
- $U(n) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_0 \,|\, c \in n,\ a - 1 \in n\right\}$.
- $U(n, \lambda) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_0 \,|\, c \in n\,\lambda,\ a - 1 \in n\right\}$.
- $S_k^A(n) = S^A(U(n))$ and $S^A(n, \lambda) = S_k^A(U(n, \lambda))$.
- $T_q$, for $q$ a prime of $F$, will denote the Hecke operator $\left[U\begin{pmatrix} 1 & 0 \\ 0 & \pi_q \end{pmatrix} U\right]$ where $\pi_q$ is an element of $F_f$ which is 1 everywhere except at $q$ where it is a uniformiser.
- $S_a$, for a fractional ideal of $F$, will denote the Hecke operator $\left[U\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} U\right]$ where $\alpha = \prod\limits_q \pi_q^{v_q(a)}$ (note that although $\pi_q$ is not uniquely determined by $q$, $T_q$ is well defined if $U = U(n)$ or $U(n, \lambda)$, and that $S_a$ is well defined if $U = U(n)$ or $U(n, \lambda)$ with $(a, n) = 1$).
- $\mathbf{T}_k(n)$ will denote the $\mathbf{Z}$-algebra in $\operatorname{End}(S^A(n))$ generated by all the $T_q$ for $q$ a prime of $F$ and the $S_a$ for $a$ an integral ideal of $F$ prime to $n$.
- $\mathbf{T}_k(n, \lambda)$ will denote the $\mathbf{Z}$-algebra in $\operatorname{End}(S^A(n, \lambda))$ generated by all the $T_q$ for $q \neq \lambda$ a prime of $F$ and the $S_a$ for $a$ an integral ideal of $F$ prime to $n\,\lambda$.
- if $f \in S_k^A(n)$ is an eigenform of the Hecke algebra $\mathbf{T}_k(n)$ we shall let $\theta_f\colon \mathbf{T}_k(n) \to \mathbf{C}$ denote the morphism determined by $f|_k T = \theta_f(T) f$ for all $T \in \mathbf{T}_k(n)$. Also $L_f$ will denote the number field generated by the image of $\theta_f$ and $\mathcal{O}_f$ its integers. (It is a theorem of Shimura that $L_f$ is a number field (see for example [Sa]).)

We also have an embedding:

$$S_k^A(n)^2 \hookrightarrow S_k^A(n, \lambda),$$
$$(f_1, f_2) \mapsto f_1 + f_2|_k \begin{pmatrix} \pi_\lambda & 0 \\ 0 & 1 \end{pmatrix}$$

which is compatible with the action of the Hecke operators $T_q$ for $q \neq \lambda$ and $S_a$ for $a$ prime to $n\lambda$. It is well known that there is a unique $\mathbf{T}_k(n, \lambda)$ submodule of $S_k^A(n, \lambda)$, which we shall denote $S_k^A(n, \lambda)^{\text{new}}$, such that we have a direct sum of $\mathbf{T}_k(n, \lambda)$ modules:

$$S_k^A(n, \lambda) = S_k^A(n)^2 \oplus S_k^A(n, \lambda)^{\text{new}}.$$

We shall let $\mathbf{T}_k(n, \lambda)^{\text{old}}$ and $\mathbf{T}_k(n, \lambda)^{\text{new}}$ denote the image of $\mathbf{T}_k(n, \lambda)$ in $\operatorname{End}(S_k^A(n)^2)$ and $\operatorname{End}(S_k^A(n, \lambda)^{\text{new}})$, respectively.

We can now state the main result of this section:

**Theorem 1.** *Let $f \in S_k^A(n)$ be an eigenform of the Hecke algebra $\mathbf{T}_k(n)$. Then there is a non-zero ideal $E_f$ of $\mathcal{O}_f$ such that for all primes $\lambda \nmid n$ of $F$ there is an ideal $\mathcal{I}_\lambda$ of $\mathcal{O}_f$ and a map:*

$$\mathbf{T}_k(n, \lambda)^{\text{new}} \otimes \mathcal{O}_f \longrightarrow \mathcal{O}_f / \mathcal{I}_\lambda,$$
$$T_q \mapsto \theta_f(T_q),$$
$$S_a \mapsto \theta_f(S_a)$$

*where for all primes $\wp$ of $\mathcal{O}_f$ not dividing $\mathbf{N}\lambda$:*

$$v_\wp(\mathcal{I}_\lambda) \geqq v_\wp(\theta_f(T_\lambda^2 - S_\lambda(\mathbf{N}\lambda + 1)^2)) - v_\wp(E_f(\mathbf{N}\lambda + 1)).$$

*Remarks.* Roughly speaking the point of this theorem is that the morphism $\theta_f$: $\mathbf{T}_k(n, \lambda) \to \mathcal{O}_f$, which a priori factors through $\mathbf{T}_k(n, \lambda)^{\text{old}}$, also factors through $\mathbf{T}_k(n, \lambda)^{\text{new}}$ when it $(\theta_f)$ is considered modulo an ideal $\mathcal{I}_\lambda$ which is essentially given as $\theta_f(T_\lambda^2 - S_\lambda(1 + \mathbf{N}\lambda)^2)$, at least up to an error term $E_f(\mathbf{N}\lambda + 1)$ which will be easily controlable. Alternatively one could understand this theorem as saying there exists $f' \in S_k^A(n, \lambda)^{\text{new}}$ with $f \equiv f' \bmod \mathcal{I}_\lambda$ with an appropriate notion of congruence. For a discussion of these two ways of interpreting congruences between modular forms the reader might like to consult [R] (this treats the case $F = \mathbf{Q}$, but conceptually this makes no difference).

We have contented ourselves with a statement which is sufficient for our purpose of constructing Galois representations and whose proof is as uncomplicated as possible. In fact in the case $k = 2t$ we can choose $E_f$ such that $E_f | (\theta_f(T_q)^{h_F} - (\mathbf{N}q + 1)^{h_F})$ for all primes $q \nmid n$ and $(E_f | \theta_f(T_q)^{h_F} - (\mathbf{N}q)^{h_F})$ for all primes $q | n$, where $h_F$ denotes the strict class number of $F$. The proof just requires slightly more care (see the end of this section for more details).

To prove this theorem we introduce modular forms for the algebra $D$. Our exposition follows that of Hida [H], as indeed did our exposition of Hilbert modular forms above.

We must first define some modules. For any ring $R$ and for $a, b \in \mathbf{Z}_{\geqq 0}$ we let $S_{a,b}(R)$ denote the right $M_2(R)$ module $S^a(R^2)$ (the $a^{\text{th}}$ symmetric power, i.e., the maximal symmetric quotient of the $a^{\text{th}}$ tensor power) with $M_2(R)$ action:

$$x\alpha = (\det \alpha)^b x S^a(\alpha).$$

If $R^2$ has natural basis $e_1, e_2$ then $S_{a,b}(R)$ has a basis $f_0, \ldots, f_a$ where $f_i = e_1^{\otimes i} \otimes e_2^{\otimes (a-i)}$. With respect to this basis we define a duality:

$$\begin{aligned} \langle\ ,\ \rangle \colon S_{a,b}(R)^2 &\to R, \\ (x, y) &\mapsto (x w)^t y \end{aligned}$$

where $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(R)$. Note that:

$$\langle x\alpha, y\alpha\rangle = x w (w^{-1} \alpha w^t\alpha)^t y = (\det \alpha)^{a+2b} \langle x, y\rangle$$

as $w^{-1} \alpha w = (\det \alpha)^t\alpha^{-1}$.

Now for $k \in \mathbf{Z}^I$, $m$, $v$, $\mu$ as before set:

$$L_k = \bigotimes_I S_{m_\tau, v_\tau}(\mathbf{C}).$$

This has a $G_\infty^D$ action via the map $j \colon G_\infty^D \to GL_2(\mathbf{C})^I$ which we chose. We define a duality on $L_k$ by:

$$\langle \otimes x_\tau, \otimes y_\tau\rangle = \prod \langle x_\tau, y_\tau\rangle,$$

and then:

$$\langle x\alpha, y\alpha\rangle = (\mathbf{N} v\alpha)^\mu \langle x, y\rangle.$$

Finally if $\mathcal{O}_K \subset R \subset \mathbf{C}$ then we define $L_k(R)$ to be:

$$\bigotimes_I S_{m_\tau, v_\tau}(R)$$

which is an $R$ lattice in $L_k$ and inherits an action of $\mathcal{O}_D^\times$ (via $j$). Then $\langle\ ,\ \rangle$ gives a duality $L_k(R)^2 \to R$.

If $f \colon G^D(\mathbf{A}) \to L_k$ and $u = u_f u_\infty \in G^D(\mathbf{A})$ we set:

$$(f|_k u)(x) = f(x u^{-1}) \cdot u_\infty.$$

For $U \subset G_f$ an open compact subgroup, set:

$$\begin{aligned} S_k^D(U) &= \{f \colon D^\times \backslash G^D(\mathbf{A}_F) \to L_k \mid f|_k u = f \ \ \forall u \in U G_\infty^D\} \\ &= \{f \colon G_f/U \to L_k \mid f(\alpha x) = f(x) \cdot \alpha^{-1} \ \ \forall x \in G_f,\ \alpha \in D^\times\} \end{aligned}$$

(where the action of $D^\times$ is via $j \colon D^\times \to GL_2(K)^I$). We also define $I_k(U)$ to be zero unless $k = 2t$ in which case it consists of those elements of $S_{2t}^D$ which factor through $\nu$: $G_f/U \to F_f^\times/\nu U$. For $U, U'$ open compact subgroups in $G_f$ and $x \in G_f$ we define a Hecke operator:

$$[U x U'] : S_k^D(U) \to S_k^D(U'),$$
$$f \mapsto \sum f|_k x_i$$

where $U x U' = \coprod U x_i$. It is easy to check that $[U x U'] : I_k(U) \to I_k(U')$.

It is a theorem of Jacquet and Langlands [JL] (as completed by Arthur [A]) and of Shimizu [Su] that there are compatible isomorphisms:

$$i_U\colon\ S_k^D(U)/I_k(U) \xrightarrow{\sim} S_k^D(U)$$

for each $U$, which commute with the action of all the Hecke operators $[U x U']$ (see Theorem 2.1 of [H] for the theorem in this form).

We also set $X(U)$ to be the finite set:

$$D^\times \backslash G_f/U$$

and define a duality on $S_k^D(U)$ by setting:

$$\langle f, g \rangle = \sum_{[x] \in X(U)} \langle f(x), g(x) \rangle (\mathbf{N}\,\nu\, x)^\mu.$$

Here $\mathbf{N}\,\nu$ is the composite of $\mathbf{N}\,\nu$: $G_f \to \mathbf{Q}_f^\times$ with the natural map $\mathbf{Q}_f^\times \to \mathbf{Q}_{>0}^\times$ (which is the identity on the diagonally embedded copy of $\mathbf{Q}_{>0}^\times$), and the definition is easily checked to be good (note $\mathbf{N}\,\nu\, U = \{1\}$). One can also show that:

$$\langle f|_k [U x U'], g \rangle = (\mathbf{N}\,\nu\, x)^\mu \langle f, g|_k [U' x^{-1} U] \rangle.$$

Although the computation is easy, we give it here as we shall have to make several more like it. Let $U x U' = \coprod U x u_i$ so that $U' = \coprod u_i^{-1}(U' \cap x^{-1} U x)$, then:

$$\begin{aligned}
\langle f|_k [U x U'], g \rangle &= \sum_i \sum_{[y] \in X(U')} \langle f(y u_i^{-1} x^{-1}), g(y) \rangle (\mathbf{N}\,\nu\, y)^\mu \\
&= \sum_{[y] \in X(U' \cap x^{-1} U x)} \langle f(y x^{-1}), g(y) \rangle (\mathbf{N}\,\nu\, y)^\mu \\
&= \sum_{[y] \in X(x U' x^{-1} \cap U)} \langle f(y), g(y x) \rangle (\mathbf{N}\,\nu\, y)^\mu (\mathbf{N}\,\nu\, x)^\mu \\
&= \langle f, g|_k [U' x^{-1} U] \rangle (\mathbf{N}\,\nu\, x)^\mu
\end{aligned}$$

where the last line follows by a similar reasoning to that used in the first three lines. Note that in particular $[U x U']$: $I_k(U)^\perp \to I_k(U')^\perp$.

We define $S_k^D(n)$, $S_k^D(n, \lambda)$, $\mathbf{T}_k^D(n)$ and $\mathbf{T}_k^D(n, \lambda)$ by analogy with the case of $S^A$. Again we get a map:

$$i\colon\ S_k^D(n)^2 \to S_k^D(n, \lambda),$$
$$(f_1, f_2) \to f_1 + f_2|_k \eta$$

where we set for the rest of this section $\eta=\begin{pmatrix}\pi_\lambda & 0\\ 0 & 1\end{pmatrix}$. In fact we have a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & I_k(n) \arrow[r, equal] \arrow[d] & I_k(n) \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & I_k(n)^2 \arrow[r] \arrow[d] & S_k^D(n)^2 \arrow[r] \arrow[d] & S_k^A(n)^2 \arrow[r] \arrow[d] & 0\\
0 \arrow[r] & I_k(n,\lambda) \arrow[r] \arrow[d] & S_k^D(n,\lambda) \arrow[r] & S_k^A(n,\lambda) \arrow[r] & 0\\
 & 0 & & &
\end{tikzcd}$$

where the map $I_k(n)\to I_k(n)^2$ is given by $f\mapsto(f,-f)$. The commutativity follows from the compatibility of the maps $i_U$ with the Hecke operators, because the map $S_k^D(n)^2\to S_k^D(n,\lambda)$ may be written:

$$(f_1,f_2)\mapsto f_1|_k[U(n)\,1\,U(n,\lambda)]+f_2|_k[U(n)\,\eta\,U(n,\lambda)].$$

Note that in particular $I_k(n,\lambda)\subset i\,S_k^D(n)^2$.

We define $S_k^D(n,\lambda)^{\mathrm{new}}$ to be $(i\,S_k^D(n)^2)^\perp$. Then we have:

**Lemma 1.** 1. $S_k^D(U)=I_k(U)\oplus I_k(U)^\perp$.

2. $S_k^D(n,\lambda)=i\,S_k^D(n)^2\oplus S_k^D(n,\lambda)^{\mathrm{new}}$ *and* $S_k^D(n,\lambda)^{\mathrm{new}}\cong S_k^A(n,\lambda)^{\mathrm{new}}$ *as modules over the Hecke algebra. (Thus* $\mathbf{T}_k^D(n,\lambda)^{\mathrm{new}}\cong\mathbf{T}_k(n,\lambda)^{\mathrm{new}}$ *with the obvious notation.)*

*Proof.* First assume that $k=2t$. Then $S_k^D(U)=\mathbf{C}^{X(U)}$. We can give this space an $\mathbf{R}$ structure by considering $\mathbf{R}^{X(U)}\subset\mathbf{C}^{X(U)}$, and the assertions of the lemma depend only on the $\mathbf{R}$ structure. However working with $\mathbf{R}^{X(U)}$ the lemma is easy to prove as $\langle\ ,\ \rangle$ is an inner product on $\mathbf{R}^{X(U)}$.

Now assume $k\neq 2t$. There is nothing to prove for the first assertion. For the second, note that $S_k^D(n,\lambda)\cong S_k^A(n,\lambda)$ and redefine (for the moment) $S_k^D(n,\lambda)^{\mathrm{new}}$ to be the submodule corresponding to $S_k^A(n,\lambda)^{\mathrm{new}}$ under this isomorphism. Then $S_k^D(n,\lambda)=i\,S_k^D(n)^2\oplus S_k^D(n,\lambda)^{\mathrm{new}}$ and, because $\langle\ ,\ \rangle$ is a duality, we need only show that $\langle i\,S_k^D(n)^2, S_k^D(n,\lambda)^{\mathrm{new}}\rangle=0$ to conclude that our two definitions of $S_k^D(n,\lambda)^{\mathrm{new}}$ coincide and hence that the lemma holds.

However if $\mathbf{T}$ denotes the abstract Hecke algebra generated by the operators $T_q$ and $S_q$ for $q\nmid n\lambda$ then it is known that $\mathbf{T}$ is diagonalisable on $i\,S_k^D(n)^2$ and $S_k^D(n,\lambda)^{\mathrm{new}}$. Thus it will do to show that if $f\in i\,S_k^D(n)^2$ and $g\in S_k^D(n,\lambda)^{\mathrm{new}}$ are eigenforms of $\mathbf{T}$ then $\langle f,g\rangle=0$. But, if not, the usual calculation shows that $\theta_g(T_q)=\theta_f(T_q)\,\chi(q)$ where $\chi$ is the finite character defined by $\chi(q)=\theta_f(S_q)^{-1}(\mathbf{N}\,q)^\mu$ for $q\nmid n\lambda$. Thus if $\pi_f$ and $\pi_g$ are the corresponding automorphic representations the strong multiplicity one theorem implies that $\pi_f\otimes(\chi\circ\det)=\pi_g$. However $\lambda$ divides the conductor of $\pi_g$, but neither that of $\pi_f$ nor that of $\chi$ which is a contradiction.

Later we shall require the following:

**Lemma 2.** *Let $i^\dagger\colon S_k^D(n,\lambda)\to S_k^D(n)^2$ be the adjoint of the map $i\colon S_k^D(n)^2\to S_k^D(n,\lambda)$ defined with respect to the natural pairings on $S_k^D(n,\lambda)$ and $S_k^D(n)\oplus S_k^D(n)$ (an orthogonal direct sum). Then $i^\dagger\circ i\colon S_k^D(n)^2\to S_k^D(n)^2$ is given by the following matrix:*

$$\begin{pmatrix} \mathbf{N}\lambda+1 & (\mathbf{N}\lambda)^\mu S_{\lambda^{-1}} T_\lambda \\ T_\lambda & (\mathbf{N}\lambda)^\mu(\mathbf{N}\lambda+1)\end{pmatrix}.$$

*Proof.* If $i^\dagger\circ i=\begin{pmatrix} A & B\\ C & D\end{pmatrix}$ then $A$, $B$, $C$ and $D$ are determined by the equations:

$$\begin{aligned}
\langle f, g|_k A\rangle_{U(n)} &= \langle f, g\rangle_{U(n,\lambda)},\\
\langle f, g|_k B\rangle_{U(n)} &= \langle f|_k \eta, g\rangle_{U(n,\lambda)},\\
\langle f, g|_k C\rangle_{U(n)} &= \langle f, g|_k \eta\rangle_{U(n,\lambda)},\\
\langle f, g|_k D\rangle_{U(n)} &= \langle f|_k \eta, g|_k \eta\rangle_{U(n,\lambda)}.
\end{aligned}$$

Easy computations like the one given above now prove the lemma. (Recall that $[U(n)\colon U(n,\lambda)]=\mathbf{N}\lambda+1$.)

We shall now give $S_k^D(U)$ an integral structure if $U\subset U_0$. We have two maps $D\otimes_{\mathbf{Q}} K_f \xrightarrow{\sim} M_2(K_f)^I$. The first, which we shall write as the identity, comes from our identification of $G^D(F_f)$ with $G^A(F_f)$. The second, which we shall denote as $j$, comes from the map $j\colon D\otimes_{\mathbf{Q}} K\to M_2(K)^I$. Then $j(g)=\delta g\delta^{-1}$ for some $\delta\in(\prod G^A(\mathcal{O}_{K,v}))^I$. We let $G_f$ act on $\mathcal{O}_K$ lattices in $L_k(K)$ through the map:

$$G_f \xrightarrow{j} M_2(K_f)^I \to \mathrm{End}(L_k(K))\otimes_K K_f.$$

We shall write $L\mapsto Lg$. Note that if $g\in(\prod M_2(\mathcal{O}_{F,v}))\cap G_f$ then $L_k(R)g\subset L_k(R)$. If $R$ is a ring such that $\mathbf{C}\supset R\supset \mathcal{O}_K$ and if $g\in G_f$ we define $L_k(R)g$ to be $L_k(\mathcal{O}_K)g\otimes R$. We now define the module of $R$ integral modular forms $S_k^D(U;R)$ to be the module consisting of those $f\in S_k^D(U)$ such that $f(g)\in L_k(R)g^{-1}$ for all $g\in G_f$. Alternatively we can think of $S_k^D(U;R)$ as:

$$\bigoplus_{[g]\in X(U)} (L_k(R)\,g^{-1})^{D^\times\cap gUg^{-1}}.$$

Thus we see that $S_k^D(U;R)$ is an $R$ lattice in $S_k^D(U)$. Also it is easily verified that if $x\in G_f\cap\prod M_2(\mathcal{O}_{F,q})$ and if $U, U'\subset U_0$ then $[UxU']\colon S_k^D(U;R)\to S_k^D(U';R)$ because:

$$\begin{aligned}
(f|_k[UxU'])(g) &= \textstyle\sum f(g u_i^{-1} x^{-1})\\
&\in \textstyle\sum L_k(R)\, x\, u_i\, g^{-1}\subset L_k(R)\, g^{-1}
\end{aligned}$$

where $UxU'=\coprod Uxu_i$.

We now want to examine the effect of our pairing on the integral structure.

**Lemma 3.** *There are non-zero integers $C_1$ and $C_2$ such that for any open $U\subset U_0$:*

$$C_1\langle S_k^D(U;R), S_k^D(U;R)\rangle\subset R$$

*and:*

$$\langle f, S_k^D(U;R)\rangle\subset R \Rightarrow C_2 f\in S_k^D(U;R).$$

*Proof.* Fix a decomposition $G_f = \coprod_{j\in J} D^\times t_j U_0$. Then if $U \subset U_0$ we have $G_f = \coprod_{j\in J}\coprod_l D^\times t_j u_l U$ with each $u_l \in U_0$. Then:

$$S_k^D(U; R) = \perp_{j\in J} \perp_l (L_k(R)\, t_j^{-1})^{D^\times \cap t_j u_l U u_l^{-1} t_j^{-1}}.$$

The lemma is true for each of the orthogonal summands separately, so it will do to show that there are only finitely many possibilities for $L_k(R)^{D^\times \cap W}$ as $W$ varies over open subgroups of $t_j U_0 t_j^{-1}$.

However if $X = \bigcup L_k(R)^{D^\times \cap U}$ as $U$ varies over open compact subgroups then $X$ is a submodule of $L_k(R)$ and in fact $X = L_k(R)^{D^\times \cap W_0}$ for some open compact subgroup $W_0$. Without loss of generality we may suppose that $W_0 \lhd t_j U_0 t_j^{-1}$. Then if $W \subset t_j U t_j^{-1}$:

$$L_k(R)^{D^\times \cap W} = X^{(D^\times \cap W)(D^\times \cap W_0)/(D^\times \cap W_0)}$$

but $(D^\times \cap W)(D^\times \cap W_0)/(D^\times \cap W_0)$ is constrained to be one of the finite number of subgroups of the finite group $(D^\times \cap t_j U_0 t_j^{-1})/(D^\times \cap W_0)$.

Before finally proving Theorem 1 we need one more result (the analogue of a theorem of Ihara in Ribet's proof):

**Lemma 4.** *Let $R \supset \mathcal{O}_K[1/N\lambda]$. There is a non-zero integer $C_3$ independent of $\lambda$ such that for $\lambda$ not dividing $n$:*

$$C_3^{-1}\, i(S_k^D(n; R)^2) \supset S_k^D(n, \lambda; R) \cap i(S_k^D(n)^2) \supset i(S_k^D(n; R)^2).$$

*Proof.* The second inclusion is easy. We divide the proof of the first into two cases.

*Case 1* ($k = 2t$). In this case $S_k^D(U; R) = R^{X(U)}$ which is how we shall think about these spaces for the moment. We consider two maps:

$$\begin{aligned} \pi_1, \pi_2 &: X(n, \lambda) \to X(n),\\ \pi_1 &: \quad [g] \mapsto [g],\\ \pi_2 &: \quad [g] \mapsto [g\eta^{-1}]. \end{aligned}$$

We define an equivalence relation $\sim$ on $X(n, \lambda)$ by $x \sim y$ if there is a chain $x = x_0, x_1, \ldots, x_m = y$ such that, for each $i$, $x_i$ and $x_{i+1}$ have the same image in $X(n)$ under either $\pi_1$ or $\pi_2$. Let $y_1, \ldots, y_s$ be representatives for the $\sim$ equivalence classes $c_1, \ldots, c_s$. Also define a "radius" function $d$ on $X(n, \lambda)$ by setting $d(x)$ to be the length of the smallest chain $x = x_0, \ldots, x_d = y_j$ exhibiting $x \sim y_j$ for some $j$.

Let $f = i(f_1, f_2) \in S_k^D(n, \lambda) \cap i\, S_k^D(N)^2$. We first claim that we may assume that $f_1(y_i) = 0$ for all $i$. In fact define:

$$\begin{aligned} f_1' &: X(n) \to R,\\ &\quad \pi_1 c_i \to \{f(y_i)\} \end{aligned}$$

and:

$$\begin{aligned} f_2' &: X(n) \to R,\\ &\quad \pi_2 c_i \to \{f(y_i)\}. \end{aligned}$$

Then $f=i(f_1-f_1', f_2+f_2')$ and $(f_1-f_1')(y_i)=0$ for all $i$.

Now assuming this we shall show by induction on $d(x)$ that $f_1(\pi_1 x)$ and $f_2(\pi_2 x)$ are in $R$ for all $x$. First note that $f_1(\pi_1 x)+f_2(\pi_2 x)\in R$ so that if one is in $R$ so is the other. If $d(x)=0$ then $f_1(\pi_1 x)\in R$ as required. Assume $d(x)=m$ and that the result is true for all $x'$ with $d(x')<m$. Then we can find an $x'$ with $d(x')=m-1$ and $\pi_i(x)=\pi_i(x')$ for $i=1$ or 2. Then either $f_1(\pi_1 x)$ or $f_2(\pi_2 x)$ lies in $R$ as required.

*Case 2* ($k\neq 2t$). Let $f=i(f_1, f_2)\in S_k^D(n, \lambda; R)\cap i\, S_k^D(n)^2$. Note that $L_k(R)\eta=L_k(R)$ and hence for $g\in G_f$:

$$f_1(g)+f_2(g\eta^{-1})\in L_k(R)\, g^{-1}=L_k(R)\,\eta\, g^{-1}.$$

Thus it will do to show that $C_3 f_1\in S_k^D(n; R)$. But if $g\in G_f$ and $u\in U(n)$ then:

- $f_1(gu)=f_1(g)$,
- $f_1(g\eta^{-1}u\eta)\in L_k(R)\, g^{-1}-f_2(g\eta^{-1}u)=L_k(R)\, g^{-1}-f_2(g\eta^{-1})$
  $=L_k(R)\, g^{-1}+f_1(g)$,
- and so $f_1(g\eta^{-1}u\eta)\equiv f_1(g) \bmod L_k(R)\, g^{-1}$.

Thus if $V_\lambda$ is the subgroup of $G_f$ generated by $U(n)$ and $\eta^{-1}U(n)\eta$ and if $\alpha\in D^\times\cap g V_\lambda g^{-1}$ we see that:

$$f_1(g)\equiv f_1(g)\,\alpha \bmod L_k(R)\, g^{-1}.$$

Let $g_1, \ldots, g_r\in G_f$ represent the points of $X(n)$. Then it will do to show that there are non-zero integers $C(g_i)$ independent of $\lambda$ such that if $x\in L_k$ satisfies:

$$x\equiv x\,\alpha \bmod L_k(R)\, g_i^{-1}$$

for all $\alpha\in D^\times\cap g_i V_\lambda g_i^{-1}$, then $C(g_i)\,x\in L_k(R)\, g_i^{-1}$. However we can find an ideal $m$ and a non-zero integer $C$ independent of $\lambda$ and of $i$ such that:

$$C L_k(R)\, g_i^{-1}\subset L_k(R)\subset C^{-1} L_k(R)\, g_i^{-1}$$

and $g_i V g_i^{-1}\supset W_\lambda\times W^\lambda$ where:

$$W_\lambda=\{u\in GL_2(F_\lambda)\,|\,\det u\in \mathcal{O}_{F,\lambda}^\times\},$$
$$W^\lambda=\{u\in \prod_{q\neq\lambda} GL_2(\mathcal{O}_{F,q})\,|\,u\equiv 1 \bmod m\}.$$

(It is well known that $GL_2(\mathcal{O}_{F,\lambda})$ and $\eta^{-1}GL_2(\mathcal{O}_{F,\lambda})\eta$ generate $W_\lambda$.) Let $\Gamma_m$ be the principal congruence subgroup of level $m$ in $SL_2(\mathcal{O}_F)$. Then for $x$ as above and $\alpha\in D^\times\cap(W_\lambda\times W^\lambda)$, $Cx\equiv Cx\alpha \bmod L_k(R)$. But if $\beta\in\Gamma_m$ then by the strong approximation theorem we can find $\alpha\in D^\times\cap(W^\lambda\times W_\lambda)$ arbitarily congruent to $\delta^{-1}\beta\delta$ outside $\lambda$; and hence:

$$Cx\equiv Cx\beta \bmod L_k(R)$$

where now the action of $\beta$ is via $SL_2(F)\hookrightarrow GL_2(K)^I$ diagonally and not via $j$. Now considering elements $\begin{pmatrix}1 & m'\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ m' & 1\end{pmatrix}$ in $\Gamma_m$ for $0\neq m'\in m$ produces a constant $C'$ depending only on $m$ and $k$ such that $C'Cx\in L_k(R)$ and so $C'C^2x\in L_k(R)g_i^{-1}$, as desired.

We are now in a position to prove Theorem 1. We may assume that $K\supset L_f$ and set $R=\mathcal{O}_K[1/\mathbf{N}\lambda]$. Then we can find $f'\in S_k^D(n;R)$ such that:

$$f'\in I_k(n)^\perp,$$
$$f'|_k T=\theta_f(T)f' \qquad \forall T\in\mathbf{T}_k(n),$$
$$C_4(Kf'\cap(S_k^D(n;R)+I_k(n)))\subset Rf'$$

for some non-zero ideal $C_4$ of $R$ depending only on $K$, $k$ and $n$. Let $a=\theta_f(T_\lambda^2-S_\lambda(\mathbf{N}\lambda+1)^2)$ and let $g=((1+\mathbf{N}\lambda)S_\lambda f', -T_\lambda f')$ so that $a^{-1}i^\dagger\circ i(g)=(-f',0)$. Then:

$$\begin{aligned}\langle C_1C_3a^{-1}i(g), iS_k^D(n)^2\cap S_k^D(n,\lambda;R)\rangle &\subset C_1\langle a^{-1}i(g), i(S_k^D(n;R)^2)\rangle\\ &=C_1\langle a^{-1}i^\dagger\circ i(g), S_k^D(n;R)^2\rangle\\ &\subset R.\end{aligned}$$

We may extend $\langle C_1C_3a^{-1}i(g),-\rangle$ to a linear map $S_k^D(n,\lambda;R)\to R$ and thus there is an $h\in S_k^D(n,\lambda)^{\text{new}}$ with $h+C_1C_2C_3a^{-1}i(g)\in S_k^D(n,\lambda;R)$. Then for each $T\in\mathbf{T}_k^D(n,\lambda)$:

$$h|_kT-\theta_f(T)h\in a^{-1}C_1C_2C_3\,i(g|_kT-\theta_f(T)g)+S_k^D(n,\lambda;R)=S_k^D(n,\lambda;R).$$

Thus we get a map:

$$\begin{aligned}\mathbf{T}_k(n,\lambda)^{\text{new}}\otimes R &\twoheadrightarrow R/\mathcal{I}_\lambda,\\ T_q &\mapsto \theta_f(T_q),\\ S_a &\mapsto \theta_f(S_a)\end{aligned}$$

where:

$$\begin{aligned}\mathcal{I}_\lambda &=\{x\in R\mid xh\in S_k^D(n,\lambda;R)\}\\ &\subset\{x\in R\mid xC_1C_2C_3^2a^{-1}g\in S_k^D(n;R)^2+\ker i\}\\ &\subset a(1+\mathbf{N}\lambda)^{-1}\{x\in R\mid xC_1C_2C_3^2f'\in S_k^D(n;R)+I_k(n)\}\\ &\subset a(1+\mathbf{N}\lambda)^{-1}C_1^{-1}C_2^{-1}C_3^{-2}C_4^{-1}\end{aligned}$$

as desired.

Finally we indicate how we can control the error term as we claimed after the statement of theorem one. In the case $k=2t$ the constants $C_1$, $C_2$ and $C_3$ may all be chosen to be one as we see easily from the proofs of lemmas three and four. We claim that there are infinitely many prime ideals $\mu$ such that we may choose $C_4$ to be any one of:

- $(\theta_f(T_q)^{h_F}-(1+\mathbf{N}q)^{h_F})\,\mu$ for $q\nmid n$,
- $(\theta_f(T_q)^{h_F}-(\mathbf{N}q)^{h_F})\,\mu$ for $q\mid n$.

This would be enough to establish the remark. To prove the claim note that for infinitely many $\mu$ we may choose $f'_\mu \in S_k^D(n; R)$ such that:

$$\mu(K f'_\mu \cap S_k^D(n; R)) \subset R f'_\mu .$$

Then take:

$$f' = f'_\mu | (T_q^{h_F} - (1 + \mathbf{N}\, q)^{h_F})$$

for any $q \nmid n$ or:

$$f' = f'_\mu | (T_q^{h_F} - (\mathbf{N}\, q)^{h_F})$$

for any $q | n$. Then $f'$ will satisfy the requirements at the start of the last paragraph because $(T_q^{h_F} - (1 + \mathbf{N}\, q)^{h_F})$ for $q \nmid n$ and $(T_q^{h_F} - (\mathbf{N}\, q)^{h_F})$ for $q | n$ kill $I_k(n)$ and preserve $I_k(n)^\perp$.

## 2. Galois representations

We first recall Wiles' notion of a pseudo-representation (see [W]). Let $R$ be a ring and $G$ a group with a distinguished element $c$ of order two. By a pseudo-representation $r$ of $G$ into $R$ we mean a collection of maps:

$$\begin{aligned} A&: \quad G \to R, \\ D&: \quad G \to R, \\ T&: \quad G \to R, \\ X&: G \times G \to R \end{aligned}$$

satisfying the following conditions:

- $2A_{\sigma\tau} = A_\sigma A_\tau + X_{\sigma,\tau}$,
- $2D_{\sigma\tau} = D_\sigma D_\tau + X_{\tau,\sigma}$,
- $A_\sigma = T_\sigma + T_{c\sigma}$,
- $D_\sigma = T_\sigma - T_{c\sigma}$,
- $T_1 = 2$ and $T_c = 0$,
- $X_{c,\sigma} = X_{\sigma,c} = 0$,
- $X_{\sigma,\tau} X_{\rho,\eta} = X_{\sigma,\eta} X_{\rho,\tau}$,
- $4X_{\sigma\tau,\rho\eta} = A_\sigma A_\eta X_{\tau,\rho} + A_\eta D_\tau X_{\sigma,\rho} + A_\sigma D_\rho X_{\tau,\eta} + D_\tau D_\rho X_{\sigma,\eta}$.

We define the trace of $r$ to be $\mathrm{Tr}(r) = T$ and the "determinant" to be $\mathrm{Det}(r)$: $\sigma \mapsto A_\sigma D_\sigma - X_{\sigma,\sigma}$. Note that a pseudo-representation is determined by its trace (as follows at once from the first four properties). Also if $\rho$: $G \to GL_2(R)$ is a representation with $\rho(c)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ then $\rho$ determines a unique pseudo-representation $r$ with the same trace. In fact if $\rho(\sigma)=\begin{pmatrix}a_\sigma & b_\sigma\\ c_\sigma & d_\sigma\end{pmatrix}$ then $r$ is given by:

$$\begin{aligned} A&: \quad \sigma\mapsto 2a_\sigma,\\ D&: \quad \sigma\mapsto 2d_\sigma,\\ T&: \quad \sigma\mapsto a_\sigma+d_\sigma,\\ X&: (\sigma,\ \tau)\mapsto 4b_\sigma d_\tau. \end{aligned}$$

Finally if $R$ is a principal ideal domain whose field of fractions $F_R$ does not have characteristic two and if $r$ is a pseudo-representation valued in $R$ then there is a representation

$$\rho\colon G\to GL_2(F_R)$$

with $\rho(c)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $\operatorname{tr}\rho=\operatorname{Tr} r$ and $4\det\rho=\operatorname{Det} r$. If 2 is invertible in $R$ or if $R$ is the integers in a finite extension of $\mathbf{Q}_2$ and $r$ is continuous from a compact group then we can take $\rho\colon G\to GL_2(R)$. For a proof we refer the reader to Wiles' article [W].

We now give a version of the results of Ohta [O], Rogawski-Tunnell [RT] and Carayol [C]:

**Proposition 1.** *Let $p$ be a rational prime, $n$ an ideal of $F$ and $\lambda$ a prime of $F$ not dividing $n$. Then there is a continuous pseudo-representation of* $\mathrm{Gal}(F^{ac}/F)$ *valued in $\mathbf{T}_k(n,\lambda)^{\mathrm{new}}\otimes\mathbf{Z}_p$ which is unramified outside $n\lambda p$ and such that:*

$$(\operatorname{Tr} r)(\operatorname{Frob} q)=T_q,$$

$$(\operatorname{Det} r)(\operatorname{Frob} q)=4S_q\,\mathbf{N}q$$

*for $q\nmid n\lambda p$. Moreover there is a unique continuous Galois character $\chi$ extending* $\operatorname{Frob} q\mapsto S_q$ *for $q\nmid n\lambda p$; and for $q\mid n\lambda$ but $q\nmid p$ and $\sigma$ in the decomposition group of $q$ lying above* $\operatorname{Frob} q$ *we have that:*

$$(\operatorname{Det} r)(\sigma)=4\chi(\sigma)\,\mathbf{N}q$$

*and either $T_q^{s_q}=0$ (where $s_q$ is the highest power of $q$ dividing $n\lambda$) or:*

$$(T_q^2-T_q(\operatorname{Tr} r)(\sigma)-\chi(\sigma)\,\mathbf{N}q)^2=0.$$

*Proof.* We can replace $\mathbf{T}_k(n,\lambda)^{\mathrm{new}}\otimes\mathbf{Z}_p$ by $\mathbf{T}_k(n,\lambda)^{\mathrm{new}}\otimes\mathbf{Q}_p^{ac}=\bigoplus\mathcal{R}_i$ where each $\mathcal{R}_i$ is local with a unique map $\theta_i\colon\mathcal{R}_i\twoheadrightarrow\mathbf{Q}_p^{ac}$. In fact we shall show for $\mathcal{R}$ any $\mathcal{R}_i$ there is a representation into $GL_2(\mathcal{R})$ with the desired properties. Now it is known that there is a genuine continuous representation:

$$\rho\colon \mathrm{Gal}(F^{ac}/F)\to GL_2(\mathbf{Q}_p^{ac})$$

such that for $q \nmid n\lambda p$:

$$\operatorname{tr}\rho(\operatorname{Frob} q)=\theta(T_q),$$
$$\det\rho(\operatorname{Frob} q)=\theta(S_q)\,\mathbf{N}\,q.$$

Giving $\operatorname{Gal}(F^{ac}/F)$ a trivial action on $\mathscr{R}$ we can think of $\rho\colon \operatorname{Gal}(F^{ac}/F)\to GL_2(\mathscr{R})$; and, because for $q\nmid n\lambda$ $T_q=\theta(T_q)$ and $S_q=\theta(S_q)$ in $\mathscr{R}$, $\rho(\operatorname{Frob} q)$ will satisfy the required relations for $q\nmid n\lambda p$. In particular we see that $\chi$ is well defined and $\det\rho=\chi\mathbf{N}$.

For $q|n\lambda$ but $q\nmid p$ there are two possibilities either $\theta(T_q)=0$ in which case $T_q^{s_q}=0$ in $\mathscr{R}$; or $(T_q-\theta(T_q))^2=0$ in $\mathscr{R}$ and if $\pi=\bigotimes\pi_v$ is the automorphic representation corresponding to $\mathscr{R}$ then $\pi_q$ is principal series or special with at least one defining character unramified. In the second case, if $\sigma$ is as in the theorem then $\theta(T_q)^2-\theta(T_q)\operatorname{tr}\rho(\sigma)-\chi(\sigma)\mathbf{N}\,q=0$ (see Carayol [C]), and hence:

$$(T_q^2-T_q(\operatorname{Tr} r)(\sigma)-\chi(\sigma)\,\mathbf{N}\,q)^2=0$$

in $\mathscr{R}$, as desired.

We can now prove our main theorem:

**Theorem 2.** *Let p be a rational prime, n an ideal of F and $f\in S_k^A(n)$ an eigenform for $\mathbf{T}_k(n)$, where each $k_\tau\geqq 2$. Let $\theta\colon \mathbf{T}_k(n)\to\mathcal{O}_f$ be the corresponding morphism* (i.e. *$f|_k T=\theta(T)f$ for all $T\in\mathbf{T}_k(n)$*) *where $\mathcal{O}_f$ denotes the integers of the number field generated by the image of $\theta$. Let $\wp$ be a prime of $\mathcal{O}_f$ above p, then there is a continuous representation:*

$$\rho\colon \operatorname{Gal}(F^{ac}/F)\to GL_2(\mathcal{O}_{f,\wp})$$

*which is unramified outside $np$ and such that if q is a prime of F not dividing $np$ then:*

$$\operatorname{tr}\rho(\operatorname{Frob} q)=\theta(T_q),$$
$$\det\rho(\operatorname{Frob} q)=\theta(S_q)\,\mathbf{N}\,q.$$

*Moreover if $q|n$ but $q\nmid p$ then either $\theta(T_q)=0$ or if $\sigma\in D_q$ lies above* $\operatorname{Frob}_q$ *then:*

$$\operatorname{tr}\rho(\sigma)=\theta(T_q)+\chi(\sigma)(\mathbf{N}\,q)\,\theta(T_q)^{-1},$$
$$\det\rho(\sigma)=\chi(\sigma)\,\mathbf{N}\,q$$

*where $\chi$ is the continuous Galois character extending* $\operatorname{Frob} q\mapsto\theta(S_q)$ *for q a prime not dividing $np$.*

*Proof.* It will do to find a pseudo-representation with the desired properties with the condition "$\operatorname{tr}\rho(\sigma)=\theta(T_q)+\chi(\sigma)(\mathbf{N}\,q)\,\theta(T_q)^{-1}$ for $\theta(T_q)\neq 0$" replaced by:

$$\theta(T_q^{s_q})\,(\theta(T_q^2)-\theta(T_q)\,(\operatorname{Tr} r)(\sigma)-\chi(\sigma)\,\mathbf{N}\,q)^2=0.$$

In fact it will do to show that for each $m>0$ there is such a pseudo-representation $r_m$ valued in $\mathcal{O}_f/\wp^m$, for then $r_m\equiv r_{m+1}\bmod\wp^m$ (because a continuous pseudo-representation is determined by its trace on a dense set of elements) and so we can put them together to construct $r$.

Assume for the moment that for each positive integer $m$ we can find infinitely many primes $\lambda$ of $F$ such that $\mathbf{N}\,\lambda\equiv\alpha_\lambda/\beta_\lambda\equiv 1 \bmod \wp^{t(m)}$ where $t(m)=m+v_\wp(E_f)$

$+[\mathcal{O}_f:\mathbf{Z}]$, $E_f$ is as in Theorem 1 and $\alpha_\lambda$ and $\beta_\lambda$ are the roots of $X^2-\theta(T_\lambda)+\theta(S_\lambda)\mathbf{N}\lambda=0$. Then for such a $\lambda$, $v_p(1+\mathbf{N}\lambda)\leqq[\mathcal{O}_f:\mathbf{Z}]$ and:

$$\begin{aligned}\theta(T_\lambda^2-S_\lambda(1+\mathbf{N}\lambda)^2)&=\theta(S_\lambda)\left((1+\alpha_\lambda/\beta_\lambda)(1+\beta_\lambda/\alpha_\lambda)\mathbf{N}\lambda-(1+\mathbf{N}\lambda)^2\right)\\&\equiv 0 \bmod \wp^{t(m)}.\end{aligned}$$

Thus combining Theorem 1 with the above proposition we would obtain the desired pseudo-representation, except that we may lose information about Frob $\lambda$. However two such $\lambda$ determine the same pseudo-representation and between them determine the desired information about Frob $q$ for all $q$.

Thus it just remains to prove that we can find infinitely many such $\lambda$. However Brylinski and Labesse [BL] have shown the existence of a continuous representation:

$$\beta\colon \mathrm{Gal}(F^{ac}/F)\to GL_{2^d}(\mathcal{O}_{f,\wp})$$

unramified outside some finite set of primes; and such that, for almost all primes $q$ of $F$, which lie above a prime $\bar{q}$ of $\mathbf{Q}$ which splits completely in the normal closure of $F$, the characteristic polynomial of $\beta(\mathrm{Frob}\, q)$ has roots:

$$\prod_{q'\in I_1}\alpha_{q'}\prod_{q'\in I_2}\beta_{q'}$$

as $I_1, I_2$ run over partitions of the primes of $F$ above $\bar{q}$ into two sets. Let $M/\mathbf{Q}$ be the composite of the normal closure of $F$, the cyclotomic field of conductor $p^{t(m)}$ and the fixed field of $\{\sigma\in\mathrm{Gal}(F^{ac}/F)\,|\,\beta(\sigma)\equiv 1 \bmod \wp^{t(m)}\}$. Then all but finitely many of the (infinite number) of primes that split completely in $M$ will satisfy our requirements.

## References


[A] Arthur, J.: The Selberg Trace Formula for Groups of $F$-rank One. Ann. Math. **100**, 326–385 (1974)

[BR] Blasius, D., Rogawski, J.: Galois Representations for Hilbert Modular Forms (Preprint)

[BL] Brylinski, J.L.: Labesse, J.P.: Cohomologies d'Intersection et Fonctions $L$ de Certaines Variétés de Shimura. Ann. Sci. Ec. Norm. Super. (4) **17**, 361–412 (1984)

[C] Carayol, H.: Sur les Représentations $p$-adiques Associées aux Formes Modulaires de Hilbert. Ann. Sci. Ec. Norm. Super. (4) **19**, 409–468 (1986)

[H] Hida, H.: On $p$-adic Hecke Algebras for $GL_2$ over Totally Real Fields. Ann. Math. **128**, 295–384 (1988)

[JL] Jacquet, H., Langlands, R.P.: Automorphic Forms on $GL_2$. Lect. Notes Math., vol. 114, Berlin Heidelberg New York: Springer 1970

[O] Ohta, M.: On the Zeta Function of an Abelian Scheme over the Shimura Curve. Jpn. J. Math. **9**, 1–26 (1983)

[R] Ribet, K.: Congruence Relations between Modular Forms. Proc. I.C.M. 1983, pp. 503–514

[RT] Rogawski, J.D., Tunnell, J.B.: On Artin $L$-functions Associated to Hilbert Modular Forms of Weight One. Invent. Math. **74**, 1–42 (1983)

[Sa] Shimura, G.: The Special Values of the Zeta Functions associated with Hilbert Modular Forms. Duke Math. J. **45**, 637–679 (1978)

[Su] Shimitzu, H.: Theta Series and Modular Forms on $GL_2$. J. Math. Soc. Jpn **24**, 638–683 (1973)

[W] Wiles, A.: On Ordinary $\lambda$-adic Representations Associated to Modular Forms. Invent. Math. **94**, 529–573 (1988)


Oblatum 4-X-1988 & 18-IV-1989