Special Values of Hilbert Modular Functions

Martin L. Karel

Introduction

Recently, Baily has established new foundations for complex multiplication in the context of Hilbert modular functions; see [1]-[4]. However, in his treatment there is a restriction on the class of CM-points treated. Namely, the order of complex multiplications associated to the point must be the maximal order in its quotient field. The purpose of this paper is two-fold: (1) to remove the restriction just mentioned; (2) to recover a result of Tate on the conjugates of CM-points by arbitrary Galois automorphisms of $\bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$). This is done without the use of moduli.

An important feature of our approach is that, at the outset, we introduce a projective system of disconnected arithmetic quotients (Hilbert modular varieties) and a $\mathbb{Q}$-structure compatible with certain automorphisms of the system; see [10]. On each connected component, projective co-ordinates are given by Hilbert modular forms with cyclotomic Fourier coefficients. Affine co-ordinates are weight zero quotients of these and are called «arithmetic Hilbert modular functions».

The CM-points are naturally grouped into orbits of certain idele class groups. Our main result describes how these orbits are permuted by Galois conjugation. It follows quickly that the value of any arithmetic Hilbert modular function at a CM-point z is abelian over the reflex field K' attached to z. Combined with recent, deeper work of Baily, which provides congruence relations among such values, our results lead to a complete description of the conjugate $\sigma(z)$ for every CM-point z and every $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}/K')$. On the other

hand, if σ is a Galois automorphism that does not fix K', then the complete description of $\sigma(z)$ involves a connected component c in a group of finite idele classes; our results lead to Tate's description of c^2; see Chap. 7 of [11].

Notations

$\mathfrak{f}$:   a totally real number field of degree $n \geqslant 1$ with distinct embeddings

$$\varphi_j^0 \colon \mathfrak{f} \to \mathbb{R} \quad \text{for} \quad j = 1, 2, \ldots, n; \qquad \Phi^0 = (\varphi_1^0, \ldots, \varphi_n^0).$$

$\mathfrak{o}$:   the ring of integers in $\mathfrak{f}$; $\hat{\mathfrak{o}} = \mathfrak{o} \otimes \hat{\mathbb{Z}}$, where $\hat{\mathbb{Z}} = \operatorname{inv} \lim \mathbb{Z}/m\mathbb{Z}$.

$\mathbb{A}^f$: $\mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$, and for any number field L, $L(\mathbb{A}^f) = L \otimes_{\mathbb{Q}} \mathbb{A}^f$.

G: Weil's ground field restriction of GL_2 from $\mathfrak{f}$ to $\mathbb{Q}$, i.e., the group scheme

$$A \longmapsto GL_2(A \otimes_{\mathbb{Z}} \mathfrak{o})$$

for every commutative ring A with 1.

Z: the center of G; $\bar{Z} =$ the closure of $Z(\mathbb{Q})$ in $G(\mathbb{A}^f)$.

$\mathfrak{H}$:   the complex upper half plane.

X: $X = (\mathbb{C} - \mathbb{R})^n$ has 2^n connected components, one of which is $\mathfrak{H}^n = X_+$.

$G(\mathbb{R})^+$:   the connected component of 1 in $G(\mathbb{R})$; $G(\mathbb{Q})_+ = G(\mathbb{Q}) \cap G(\mathbb{R})^+$. Via Φ^0, $G(\mathbb{R})$ is isomorphic to $GL_2(\mathbb{R})^n$, which acts transitively on X by linear fractional transformations in the components.

$U(o)$:   stabilizer in $GL_2(\mathbb{R})^n$ of a point o in $\mathfrak{H}^n$.

$\mathbb{K}$:   a (varying) compact open subgroup of $G(\mathbb{A}^f)$ such as

$$\mathbb{K}(\nu) = \{ g \in G(\hat{\mathbb{Z}}) \colon g - 1 \in \nu \cdot M_2(\hat{\mathfrak{o}}) \},$$

where ν is a finite idele.

$V_{\mathbb{K}} =$ $G(\mathbb{Q})_+ \backslash (X_+ \times G(\mathbb{A}^f)/\mathbb{K}) = G(\mathbb{Q}) \backslash (X \times G(\mathbb{A}^f)/\mathbb{K})$; see 2.1.2 in [8].

$V =$ $G(\mathbb{Q})_+ \backslash (X_+ \times G(\mathbb{A}^f)/\bar{Z})$ is the limit of the projective system of $V_{\mathbb{K}}$'s. Given $\mathfrak{z}$ in X and x in $G(\mathbb{A}^f)$ we let $[\mathfrak{z}, x]$ denote the corresponding point of V and let $[\mathfrak{z}, x]_{\mathbb{K}}$ denote its image in V_K.

$W_{\mathbb{K}} =$ $G(\mathbb{Q})_+ \backslash (GL_2^+(\mathbb{R})^n \times G(\mathbb{A}^f)/\mathbb{K}) = G(\mathbb{Q}) \backslash (GL_2(\mathbb{R})^n \times G(\mathbb{A}^f)/\mathbb{K})$.

1. Galois Action

The idea used in [10] to introduce $\mathbb{Q}$-structure on $V_{\mathbb{K}}$ in case $\mathfrak{f} = \mathbb{Q}$ has been extended by Baily to an arbitrary totally real field $\mathfrak{f}$ and to the subgroups $\mathbb{K} = \mathbb{K}(\nu)$; see [3, §5]. We wish to treat arbitrary open compact subgroups $\mathbb{K}$ of $G(\mathbb{A}^f)$.

Define the automorphy factor $j(g, \mathfrak{z})$ to be the functional determinant: if

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})^n, \qquad \mathfrak{z} \in X,$$

then

$$j(g, \mathfrak{z}) = \prod_{j=1}^{N} (c_j \mathfrak{z}_j + d_j)^{-2}(a_j d_j - b_j c_j).$$

For arbitrary open compact subgroups $\mathbb{K}$ of $G(\mathbb{A}^f)$, one defines as in [2, §5.1] the graded algebra $\mathcal{C}(\mathbb{K})$ whose components $\mathcal{C}(\mathbb{K}, w)$ are the spaces of functions f on $W_\mathbb{K}$ with values in $\mathbb{C}$ such that, if $g \in GL_2(\mathbb{R})$, $x \in G(\mathbb{A}^f)$:

(i) $f(gu, x) = f(g, x)j(u, o)^w$ for all u in $U(o)$;

(ii) the functions $\lambda_x f: g(o) \mapsto f(g, x)j(g, o)^{-w}$ are holomorphic in $\mathfrak{H}^n$ and have Fourier expansions of the form

$$\lambda_x f(\mathfrak{z}) = \sum_{\ell} a_x(\ell) e^{2\pi i(\ell, \mathfrak{z})},$$

where ℓ runs over a lattice in $\Phi^0(\mathfrak{f}^n) \subset \mathbb{R}^n$ intersected with the cone of squares in $\mathbb{R}^n$, and $(\ell, \mathfrak{z})$ is the scalar product in $\mathbb{C}^n$.

By $\mathcal{C}(\mathbb{K}; \mathbb{Q}_{ab})$ we denote the subalgebra of forms with Fourier coefficients $a_x(\ell) \in \mathbb{Q}_{ab}$, the maximal abelian extension of $\mathbb{Q}$, for every $x \in G(\mathbb{A}^f)$. Among the arithmetic forms are certain Eisenstein series; namely, those forms f on $W_\mathbb{K}$ such that each $\lambda_x f$ is a $\mathbb{Q}_{ab}$-linear combination of the classical Eisenstein series introduced by Kloosterman; see [1, 5.2] and [2, 4.3].

1.1 Lemma. *If $m \in G(\mathbb{A}^f)$, then $R(m)$ gives an isomorphism from $\mathcal{C}(\mathbb{K})$ to $\mathcal{C}(m\mathbb{K}m^{-1})$ and maps $\mathcal{C}(\mathbb{K}; \mathbb{Q}_{ab})$ onto $\mathcal{C}(m\mathbb{K}m^{-1}; \mathbb{Q}_{ab})$.*

This follows at once from the following identity for x in $G(\mathbb{A}^f)$ and f in $\mathcal{C}(\mathbb{K})$:

$$(1) \qquad\qquad \lambda_x R(m)f = \lambda_{xm} f.$$

1.2. We define $\mathbb{Q}$-structure in two steps: (1) $\mathcal{C}(\mathbb{K}; \mathbb{Q}_{ab})$ spans $\mathcal{C}(\mathbb{K})$ over $\mathbb{C}$, so there is a natural $\mathbb{Q}_{ab}$-structure on V (and the action of $G(\mathbb{A}^f)$ on V by right translation is defined over $\mathbb{Q}_{ab}$ according to Lemma 1.1); (2) there is a semi-linear action of $\mathrm{Aut}(\mathbb{Q}_{ab})$ on $\mathcal{C}(\mathbb{K}; \mathbb{Q}_{ab})$ that commutes with the action of $G(\mathbb{A}^f)$ and with the natural inclusion maps. This has already been done in case $\mathbb{K} = \mathbb{K}(\nu)$; see [3, §5] and [10, §2]. Therefore, it will suffice to show for $\mathbb{K}$ containing $\mathbb{K}(N)$ that (1) holds and that the action of $\mathrm{Aut}(\mathbb{Q}_{ab})$ on $\mathcal{C}(\mathbb{K}; \mathbb{Q}_{ab})$

preserves $\mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$. The latter is obvious: since the action of $\sigma \in \mathrm{Aut}\,(\mathbb{Q}_{ab})$ on $\mathcal{Q}(\mathbb{K}(N); \mathbb{Q}_{ab})$ commutes with the action of $G(\mathbb{A}^f)$, the stabilizers of f and of σf in $G(\mathbb{A}^f)$ are the same.

To show that $\mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$ spans $\mathcal{Q}(\mathbb{K})$ over $\mathbb{C}$, first define a projection

$$\pi: \mathcal{Q}(\mathbb{K}(N)) \longrightarrow \mathcal{Q}(\mathbb{K})$$

by averaging the finite set of operators $R(m)$, $m \in \mathbb{K}/\mathbb{K}(N)$. Then, by Lemma 1.1, π maps $\mathcal{Q}(\mathbb{K}(N); \mathbb{Q}_{ab})$ onto $\mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$ so

$$\mathcal{Q}(\mathbb{K}) = \pi(\mathcal{Q}(\mathbb{K}(N); \mathbb{Q}_{ab})) \otimes \mathbb{C} = \mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab}) \otimes \mathbb{C}.$$

Since the Galois action is semi-linear, i.e., $\sigma(af) = \sigma(a)\sigma(f)$ for $a \in \mathbb{Q}_{ab}$ and $f \in \mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$, the algebra of invariants, call it $\mathcal{Q}(\mathbb{K})^{\mathbb{Q}}$, spans $\mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$ as a vector space over $\mathbb{Q}_{ab}$; see [5], AG, §14. By the Fundamental Theorem of Invariant Theory, $\mathcal{Q}(\mathbb{K})^{\mathbb{Q}}$ is finitely generated, so $\mathcal{Q}(\mathbb{K})^{\mathbb{Q}}$ is a $\mathbb{Q}$-structure on $\mathcal{Q}(\mathbb{K})$ and determines a $\mathbb{Q}$-structure on $V_{\mathbb{K}}$. For every nested pair of open compact subgroups $\mathbb{K} \subsetneq \mathbb{K}'$, the covering map $V_{\mathbb{K}} \to V_{\mathbb{K}'}$ is defined over $\mathbb{Q}$, and for every m in $G(\mathbb{A}^f)$, the maps $R(m): V_{\mathbb{K}} \to V_{m^{-1}\mathbb{K}m}$ are defined over $\mathbb{Q}$. Thus, the projective system of $V_{\mathbb{K}}$'s along with all the automorphisms $R(m)$, $m \in G(\mathbb{A}^f)$, has a $\mathbb{Q}$-structure.

1.3. Originally, the action of $\mathrm{Aut}\,(\mathbb{Q}_{ab})$ on $\mathcal{Q}(\mathbb{K}(\nu); \mathbb{Q}_{ab})$ was defined with the help of Eisenstein series. Having established its existence, we can give a natural description of this Galois action. Define the cyclotomic character

$$\chi: \mathrm{Aut}\,(\mathbb{Q}_{ab}) \to \hat{\mathbb{Z}}^{\times}$$

by $\zeta^{\chi(\sigma)} = \zeta^{\sigma}$ for every root of unity $\zeta \in \mathbb{C}$. Let

$$u = u(\sigma): = \begin{bmatrix} \chi(\sigma) & 0 \\ 0 & 1 \end{bmatrix}^{-1} \quad \text{in} \quad G(\mathbb{A}^f).$$

Then, for every x in $G(\mathbb{A}^f)$ and every f in $\mathcal{Q}(\mathbb{K}; \mathbb{Q}_{ab})$

(1) $$\lambda_x(\sigma f) = (\lambda_{ux}f)^{\sigma},$$

where the superscript σ replaces each Fourier coefficient $a_{ux}(\ell)$ of $\lambda_{ux}(f)$ (at the cusp ∞) by its image $a_{ux}(\ell)^{\sigma}$ under σ. To prove (1), it suffices to treat the special case where f is an Eisenstein series $\tilde{\mathcal{E}}_{\mathbb{G}}$, in the notation of [3, §5.1], because every automorphic form is a quotient of isobaric polynomials in the Eisenstein series attached to sufficiently small subgroups $\mathbb{K}$. In view of 1.1(1), since $R(x)$ commutes with the action of σ, we may take $x = 1$. When $f = \tilde{\mathcal{E}}_{\mathbb{G}}$ and $x = 1$, then (1) results from a routine calculation using, in the notation of [3, §5.2] (where $\chi(\sigma)$ is written $\hat{\sigma}$), the transformation laws:

(i) $\lambda_1(\tilde{\mathcal{E}}_{\mathbb{G}})^\sigma = \lambda_1(\tilde{\mathcal{E}}_{\hat{\sigma}\mathbb{G}})$;

(ii) $R(u)\tilde{\mathcal{E}}_{\mathbb{G}} = \tilde{\mathcal{E}}_{u(\mathbb{G})}$.

The main point of the calculation is that $u(\hat{\sigma} \cdot \mathbb{G}) = \hat{\sigma} \cdot u(\mathbb{G})$.

2. CM-Points

Recall that $h \in X$ is called a «CM-point (= special point) of X» if there is a totally imaginary quadratic extension K of $\mathfrak{f}$ and a $\mathfrak{f}$-algebra embedding q of K into $M_2(\mathfrak{f})$, the algebra of 2-by-2 matrices over $\mathfrak{f}$, such that h is an isolated fixed point of $q(K^\times) \subset GL_2(\mathfrak{f}) \hookrightarrow GL_2(\mathbb{R})^n$. Then q is the regular embedding with respect to a basis $(\tau, 1)$ of K over $\mathfrak{f}$; call it q_τ. View $q = q_\tau$ as a map of algebra varieties over $\mathfrak{f}$, so it also embeds $K(\mathbb{A}^f)$: $= K \otimes \hat{\mathbb{Z}}$, the finite adele ring of K, into $M_2(\mathfrak{f}(\mathbb{A}^f))$. Let T be the maximal $\mathbb{Q}$-torus of G containing $q(K^\times)$, so $q(K^\times) = T(\mathbb{Q})$. Note that $T(\mathbb{R})$ is the isotropy group of h in $G(\mathbb{R})$.

A «lifting to K» of Φ^0: $\mathfrak{f}^n \to \mathbb{R}^n$ is an embedding Φ: $K^n \to \mathbb{C}^n$, of algebras over K, that restricts to Φ^0 on $\mathfrak{f}^n$. View K as embedded in K^n diagonally. To $h \in X$ fixed by $q_\tau(K^\times)$ associate the pair of complex conjugate liftings $\{\Phi, \bar{\Phi}\}$ such that $h = \Phi(\tau) = \bar{\Phi}(\bar{\tau})$ for some $\tau \in K - \mathfrak{f}$. Write $K_h = K$ and $\Phi_h = \Phi$. Observe that if $[\Phi(\tau), x] = [\Phi'(\tau'), 1]$, then for some $\gamma \in G(\mathbb{Q})$, $\Phi'(\gamma \cdot \tau') = \Phi(\tau)$, so either $\gamma \cdot \tau' = \tau$ or $\gamma \cdot \tau' = \bar{\tau}$, but not both; thus $\Phi' = \Phi$ or $\Phi' = \bar{\Phi}$, so the pair $\{\Phi_h, \bar{\Phi}_h\}$ depends only on $[h, x]$.

By «CM-point (= special point) of V» we mean a point $z = [h, x]$ in V with $x \in G(\mathbb{A}^f)$ and h a CM-point of X. To such a point $[h, x]$ with $h = \Phi(\tau)$, assign the «CM-type» $\langle K_h, \Phi_h \rangle = \langle K_h, \bar{\Phi}_h \rangle$ and the embedding q_τ^x: $K(\mathbb{A}^f) \to M_2(\mathfrak{f}(\mathbb{A}^f))$ defined by $b \mapsto x^{-1}q_\tau(b)x$. Since $\gamma q_\tau \gamma^{-1} = q_{\gamma(\tau)}$ for all $\gamma \in GL_2(\mathfrak{f})$, it follows that q_τ^x depends only on $z = [\Phi(\tau), x]$, so we write r_z: $= q_\tau^x$.

Suppose that $\sigma \in \mathrm{Aut}\,(\mathbb{C})$. Then there is a unique map π_σ permuting coordinates so that $\sigma \circ \pi_\sigma \Phi^0 = \Phi^0$. The map $\Phi \mapsto \sigma\Phi$: $= \sigma \circ \pi_\sigma \Phi$ permutes the liftings Φ of Φ^0 to K.

Main Theorem. *Let $h = \Phi_h(\tau)$ be a CM-point of X of type $\langle K, \Phi_h \rangle$. For each $\sigma \in \mathrm{Aut}\,(\mathbb{C})$ there exists $b \in K(\mathbb{A}^f)$ such that*

$$\sigma[h, x] = [\sigma\Phi_h(\tau), q_\tau(b)x]$$

for every $x \in G(\mathbb{A}^f)$.

3. Proof of the Main Theorem

3.1. The Main Theorem will be proved using two technical lemmas. Since the action of $\sigma \in \mathrm{Aut}\,(\mathbb{C})$ on V commutes with right translations by elements

of $G(\mathbb{A}^f)$, we can suppose $x = 1$. Also, since $[h, 1]$ is right-invariant under $q(K^\times) = T(\mathbb{Q}) \subset G(\mathbb{A}^f)$, so is $\sigma[h, 1]$. In fact, every element $[\Phi(\tau), u] \in V$, with Φ lifting Φ^0 to K and u in $T(\mathbb{A}^f)$, is right-invariant under $T(\mathbb{Q})$ because if $\lambda \in T(\mathbb{Q})$, then $[\Phi(\tau), u] = [\lambda\Phi(\tau), \lambda u] = [\Phi(\tau), u\lambda]$. Our first lemma is a converse to this.

3.2. Lemma. *If $z \in V$ is right-invariant under every $t \in T(\mathbb{Q}) \subset G(\mathbb{A}^f)$, then $z = [\Phi(\tau), u]$ for some lifting Φ of Φ^0 to K and some $u \in T(\mathbb{A}^f)$.*

PROOF. It is well known and easy to check that z is a CM-point, say of type $\langle K', \Phi' \rangle = \langle K', \bar{\Phi}' \rangle$. Write $z = [\Phi'(\tau'), u']$ with τ' in $K' - \mathfrak{f}$, u' in $G(\mathbb{A}^f)$. Let $q' = q_{\tau'} : K' \to M_2(\mathfrak{f})$, and let $h' = \Phi'(\tau')$. The proof involves three steps:

(i) $K' = K$;

(ii) one can choose $\tau' = \tau$;

(iii) if $\tau' = \tau$, then $u' \in \mathfrak{N}(T)(\mathbb{Q}) \cdot T(\mathbb{A}^f)$, where $\mathfrak{N}(T)$ is the normalizer of T in G, so one can choose $u \in T(\mathbb{A}^f)$.

Step (i).   The conjugation $\text{Int}(u') : x \mapsto u'x(u')^{-1}$ takes $q(K^\times)$ into $q'((K')^\times)\bar{Z} \subset q'(K'\mathfrak{f}(\mathbb{A}^f)) \subset q'(K'(\mathbb{A}^f))$ because if $t \in q(K^\times)$, which is embedded in $G(\mathbb{A}^f)$, then $[h', u't] = [h', u']$ only if $\text{Int}(u')t \in \gamma\bar{Z}$ with $\gamma \in G(\mathbb{Q})$ such that $\gamma h' = h'$. Since $\text{Int}(u')$ acts trivially on $q(\mathfrak{f}(\mathbb{A}^f)^\times) = Z(\mathbb{A}^f) = q'(\mathfrak{f}(\mathbb{A}^f)^\times)$,

$$\text{Int}(u') : q(K \otimes \mathbb{A}^f) \to q'(K' \otimes \mathbb{A}^f)$$

induces an isomorphism m of $\mathfrak{f}(\mathbb{A}^f)$-algebras from $K(\mathbb{A}^f)$ to $K'(\mathbb{A}^f)$. In particular, for each finite place v of k, then

$$K \otimes \mathfrak{f}_v \cong K' \otimes \mathfrak{f}_v,$$

Since $K \otimes \mathfrak{f}_v = \oplus K_w$, ($w$ ranges over the places of K over v), and similarly for K', a prime of $\mathfrak{f}$ is totally decomposed in K iff it is totally decomposed in K'. An easy application of Čebotarev's Density Theorem shows that $K' \cong K$; see Ex. 6.1 on p. 362 of [6]; since K and K' are quadratic extensions of $\mathfrak{f}$, they coincide. For the case at hand, the result is Satz 18 of Hilbert's paper [9]; cf. [2, pp. 86-87].

Step (ii).   Since $G(\mathbb{Q})$ acts transitively on $K - \mathfrak{f}$, one gets

$$[\Phi'(\tau'), u'] = [\Phi'(\tau), \gamma u']$$

for some $\gamma \in G(\mathbb{Q})$. Therefore, we can choose $\tau' = \tau$.

Step (iii).   Suppose that $\tau' = \tau$, so $q' = q$. Fix $\lambda \in K - \mathfrak{f}$ with $\lambda^2 \in \mathfrak{f}^\times$. Then $m(\lambda)$ and $m(\lambda + 1)$ both lie in $K^\times c\ell(\mathfrak{f}^\times)$, where «$c\ell(\mathfrak{f}^\times)$» is the closure of $\mathfrak{f}^\times$

in $\mathfrak{f}(\mathbb{A}^f)^\times$. Write $m(\lambda) = \lambda'\zeta$ with $\lambda' \in K$, $\zeta \in \mathcal{O}(\mathfrak{f}^\times)$ and similarly $m(\lambda + 1) = \lambda_1\zeta_1$. Then $\lambda' = a\lambda + b$ for some a, b in $\mathfrak{f}$ with $a \neq 0$; however, $(\lambda')^2 = \lambda^2/\zeta^2$ lies in $K \cap \mathfrak{f}(\mathbb{A}^f) = \mathfrak{f}$, so $2ab\lambda = 0$; hence $\lambda' = a\lambda$, $\zeta^2 = 1/a^2$, and we may assume $a = 1$, i.e., $\lambda' = \lambda$, $\zeta^2 = 1$. Write $\lambda_1 = a_1\lambda + b_1$ with a_1, b_1 in $\mathfrak{f}$. Since $m(\lambda + 1) = = m(\lambda) + 1$, it follows that $b_1\zeta_1 = 1$, and $\zeta = a_1\zeta_1$ must lie in $\mathfrak{f}$. Therefore, $m(\lambda) = \pm\lambda$ and m must be either $b \mapsto b$ or $b \mapsto \bar{b}$. Since $T(\mathbb{A}^f)$ is its own centralizer in $G(\mathbb{A}^f)$, it follows that u' must lie either in $T(\mathbb{A}^f)$ or in $q(\eta)T(\mathbb{A}^f)$, where

$$q(\eta) := \begin{bmatrix} -1 & \tau + \bar{\tau} \\ 0 & 1 \end{bmatrix}$$

represents the non-trivial coset of $T(\mathbb{Q})$ in $\mathfrak{N}(T)(\mathbb{Q})$.

If $u' = q(\eta)u$ with u in $T(\mathbb{A}^f)$, then $[\Phi'(\tau), u'] = [\bar{\Phi}'(\tau), u]$ and we set $\Phi = \bar{\Phi}'$, otherwise we set $\Phi = \Phi'$, $u = u'$.

Note. Lemma 1 of [4, §2.3.1] implies a stronger version of Lemma 3.2 above. Namely, one can weaken the hypothesis of Lemma 3.2 by assuming only that z is right-invariant under a single non-central element of $T(\mathbb{Q})$.

3.3. Henceforth, the variable Φ will denote a lifting of Φ^0 to K. If

$$\Phi = (\varphi_1, \ldots, \varphi_n),$$

then one defines the «type-norm» $N_\Phi : K \to \mathbb{C}$ to be the product of coordinates, so

$$N_\Phi : b \mapsto \varphi_1(b) \cdots \varphi_n(b).$$

Let $B_{\tau,\Phi}$ be the projection of $\Phi(\tau) \times T(\mathbb{A}^f)$ into V, and let B_τ be the union of all the orbits $B_{\tau,\Phi}$. Thus far, we have shown that σ preserves B_τ: in fact, $\sigma B_{\tau,\Phi_h} = B_{\tau,\Phi}$ for some Φ. We must show that $\Phi = \sigma\Phi_h$.

Let $\mathbb{K}$ be any open compact subgroup of $G(\mathbb{A}^f)$. One sees easily that there exists a $\mathbb{Q}$-rational holomorphic modular form ψ for $\mathbb{K}$, of non-zero weight w, such that the zeros of ψ, viewed as a subset of $V_\mathbb{R}$, are disjoint from $pr_\mathbb{K}(B_\tau)$. Fix ψ, w. As in [4, §3.4], one defines for m in $G(\mathbb{A}^f)$:

$$\mathfrak{A} := gcd_\mathfrak{f}(m)^{-2}\langle\det(m)\rangle,$$

where $\langle b \rangle$ denotes the ideal associated with $b \in \mathfrak{f}(\mathbb{A}^f)^\times$,

$$gcd_\mathfrak{f}(m)^{-1} := \{b \in \mathfrak{f} : mb \in M_2(\mathfrak{d})\}$$

is an ideal of $\mathfrak{f}$, and one defines a modular function ψ_m by:

$$\psi_m([g(o), u]) := N(\mathfrak{A})^w \psi(g, um)/\psi(g, u), \qquad (g \in GL_2(\mathbb{R})^n, u \in G(\mathbb{A}^f)).$$

Suppose that $z \in B_{\tau, \Phi}$. Let

$$M = r_z(b) = q(b) \quad \text{with} \quad b \in K^\times.$$

Then

(1) $$\psi_M(z) = r^w \cdot N_\Phi(b)^w$$

for some rational number r independent of $z \in B_\tau$; see [4, §3.4].

To show that $\Phi = \sigma\Phi_h$ we construct a coordinate function f that is constant on each orbit $B_{\tau, \Phi}$ and has value there $N_\Phi(b)^w$. It is necessary first to choose b such that $N_\Phi(b)^w \neq N_{\Phi'}(b)^w$ unless $\Phi = \Phi'$. According to [3, §6.3], for some b_0 in K, the $2n$ images of b_0 under the embeddings of K into $\mathbb{C}$ are pairwise relatively prime. One can take $b = b_0$.

With $M = q_\tau(b)$, let $\mathbb{K}' := \mathbb{K} \cap M \cdot \mathbb{K} \cdot M^{-1}$, and let $f := r^{-w}\psi_M$. Then f is defined over $\mathbb{Q}$ on $V_{\mathbb{K}'}$ and restricts to the constant $N_\Phi(b)^w$ on $pr_{\mathbb{K}'}(B_{\tau, \Phi})$, so the orbits $pr_{\mathbb{K}'}(B_{\tau, \Phi})$ for distinct Φ must be disjoint, and therefore the orbits $B_{\tau, \Phi}$ must also be disjoint.

3.4. Lemma. *If* $\sigma[\Phi_h(\tau), 1] = [\Phi'(\tau), u]$ *for some* $u \in T(\mathbb{A}^f)$, *then* $\Phi' = \sigma\Phi_h$.

PROOF. Choose b and f as in section 3.3 and write $\mathbb{K}$ in place of $\mathbb{K}'$, so that $f([\Phi(\tau), s]_\mathbb{K}) = N_\Phi(b)^w$ for every s in $T(\mathbb{A}^f)$ and every lifting Φ. We claim that if $\Phi = \sigma\Phi_h$ then

(1) $$N_\Phi(b)^w = N_{\Phi'}(b)^w.$$

Indeed, the left side is

$$\sigma(N_{\Phi_h}(b)^w) = \sigma f([\Phi_h(\tau), 1]_\mathbb{K}),$$

while the right side is

$$f([\Phi'(\tau), u]_\mathbb{K}) = f\sigma([\Phi_h(\tau), 1]_\mathbb{K}),$$

but $\sigma f = f\sigma$. Since $\Phi \mapsto N_\Phi(b)^w$ separates liftings Φ of Φ^0 to K, it follows that $\Phi' = \sigma\Phi_h$.

3.5. Summary. Since $G(\mathbb{A}^f)$, acting on the right, commutes with σ, we may suppose by section 1 that $z = [\Phi_h(\tau), 1]$, so that z is invariant under $T(\mathbb{Q})$ acting to the right. Then $\sigma(z)$ is also invariant under $T(\mathbb{Q})$. Thus, by Lemma 3.2, $\sigma(z) = [\Phi'(\tau), u]$ for some Φ' lifting Φ^0 to K and some u in $T(\mathbb{A}^f)$. Then Lemma 3.4 shows that $\Phi' = \sigma\Phi_h$, which proves the Main Theorem:

$$\sigma[\Phi_h(\tau), x] = [\sigma\Phi_h(\tau), q_\tau(b)x]$$

for some b in $K(\mathbb{A}^f)$. In other words, $\sigma(B_{\tau, \Phi}) = B_{\tau, \sigma\Phi}$.

4. Conclusions

We now derive some consequences of the Main Theorem.

4.1. Let $\Gamma = \text{Aut}(\bar{\mathbb{Q}})$, and let $z \in V$ be a CM-point of CM-type, say, $\langle K, \Phi \rangle$. From the Main Theorem, since the $B_{\tau, \Phi}$ are distinct, the isotropy group of z in Γ, call it Γ_z, is contained in the isotropy group of Φ,

$$\Gamma_\Phi := \{\sigma \in \Gamma : \sigma\Phi = \Phi\}.$$

Thus, the field L_z generated over $\mathbb{Q}$ by the co-ordinates of z must contain the field K_Φ of all algebraic numbers fixed by Γ_Φ. The field K_Φ is the *reflex field* for the CM-type $\langle K, \Phi \rangle$ i.e., the subfield of $\bar{\mathbb{Q}}$ corresponding to the isotropy group of tr_Φ, the linear form given by the sum of the co-ordinates of Φ; see [11, p. 23]. We can now show that L_z/K_Φ is abelian. Let

$$I(K) := K(\mathbb{A}^f)^\times / c\ell(K^\times).$$

4.1.1. Theorem. *The field extension L_z/K_Φ is abelian. Moreover, its Galois group is embedded naturally into $I(K)$.*

PROOF. Note that $I(K) = K(\mathbb{A}^f)^\times / K^\times c\ell(\mathfrak{f}^\times)$ and define $b_\Phi : \Gamma \to I(K)$ as follows: for $\sigma \in \Gamma$, let $b_\Phi(\sigma)$ be the unique element b of $I(K)$ that satisfies

$$(1) \qquad \sigma[\Phi(\tau), x] = [\sigma\Phi(\tau), q_\tau(b)x] = [\sigma\Phi(\tau), xr_z(b)].$$

Using the transitivity of $G(\mathbb{Q})$ on $K - \mathfrak{f} \subset X$, one checks easily that $b_\Phi(\sigma)$ is independent of τ. Moreover, by straightforward calculation,

$$(2) \qquad b_\Phi(\sigma\sigma') = b_{\sigma'\Phi}(\sigma)b_\Phi(\sigma').$$

Thus, b_Φ restricts to a homomorphism on Γ_Φ, and one sees at once that the kernel of $b_\Phi|\Gamma_\Phi$ is Γ_z. Thus, L_z is abelian over K_Φ, and b_Φ embeds the Galois group Γ_Φ/Γ_z into $I(K)$. For a more classical argument, see [4, §4]. Note that Γ_z and hence L_z depend only on the CM-type of z.

4.2. The Reciprocity Law. For any number field F let NR_F be the norm residue symbol relative to F. Suppose that z is a CM-point in V of type $\langle K, \Phi \rangle$ and let $\langle K', \Phi' \rangle$ be the *reflex type*, so $K' = K_\Phi$; see [11, p. 23]. Let $N_{\Phi'}$ be the reflex type norm (= product of the components of Φ'). Then the image lies in K. Since Φ' extends trivially to $K'(\mathbb{A}^f) = K' \otimes \mathbb{A}^f$ by linearity in $\mathbb{A}^f$, $N_{\Phi'}$ also extends. Take $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/K')$ and a finite idele s of K' such that $NR_{K'}(s) = \sigma \,|\, K'_{ab}$. Recent work of Baily shows that, *if L_z/K' is an abelian extension, then*

$$(1) \qquad N_{\Phi'}(s)c\ell(K^\times) = b_\Phi(\sigma).$$

In view of 4.1, however, L_z is always abelian over K', so (1) holds without restriction on the CM-point z. This is essentially Shimura's reciprocity law restricted to the Hilbert modular case.

4.3. *The Type Transfer.* Let ρ denote complex conjugation, and let $[\Phi]$ be the set of components of any lifting Φ. Following [11, p. 164], one defines Tate's «type transfer» on Γ: $= \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$t_\Phi \colon \Gamma \to \mathrm{Gal}\,(K_{ab}/K).$$

Choose for each $\varphi \in [\Phi]$ an element $w_\varphi \in \Gamma$ such that $\varphi = w_\varphi \,|\, K$, and let $w_{\rho\varphi} := \rho w_\varphi$. Then, for $\sigma \in \Gamma$,

$$t_\Phi(\sigma) := \Pi_\varphi w_{\sigma\varphi}^{-1}\, \sigma w_\varphi \cdot \mathrm{Gal}\,(\overline{\mathbb{Q}}/K_{ab}), \qquad (\varphi \in [\Phi]).$$

By Theorem 1.1 of [11, Chap. 7, §1], if $x \in K'(\mathbb{A}^f)$ and if $\sigma \in \mathrm{Gal}\,(\overline{\mathbb{Q}})$ restricts to $NR_{K'}(x^{-1})$ on K'_{ab}, then

(1) $$NR_K \circ N_{\Phi'}(x) = t_\Phi(\sigma).$$

If σ fixes Φ, then $t_\Phi(\sigma) = NR_K(b_\Phi(\sigma)^{-1})$ according to 4.2(1). In general, let $f_\Phi(\sigma)$ denote the class in $K(\mathbb{A}^f)^\times/c\ell(K^\times)$ such that $t_\Phi(\sigma) = NR_K(f_\Phi(\sigma)^{-1})$, and let $c_\Phi(\sigma) := b_\Phi(\sigma)/f_\Phi(\sigma)$.

4.4. The rest of the paper is devoted to a proof of Tate's result: $c_\Phi(\sigma)^2 = 1$. We begin by collecting properties of u_Φ with $u = b, f$ or c. Permissible values of u are marked parenthetically. Recall that χ is the cyclotomic character, defined in 1.3.

In case $u = f$, the properties below are proved in [11, Chap. 7]; the case $u = c$ follows from the other two cases.

4.4.1$_u$. $u_\Phi(\sigma\sigma') = u_{\sigma'\Phi}(\sigma)u_\Phi(\sigma')$, $\qquad (u = b, f, c)$.

Proof. For $u = b$, this is 4.1 (2).

4.4.2$_u$. $u_\Phi(\rho) = 1$, $\qquad (u = b, f, c)$.

Proof. For $u = b$. Choose g, g' in $G(\mathbb{R})$ such that

$$g(o) = \Phi(\tau) \quad \text{and} \quad g'(o) = \rho\Phi(\tau).$$

It suffices to show that $\rho[\Phi(\tau), 1] = [\rho\Phi(\tau), 1]$, i.e., if f_1 and f_2 are $\mathbb{Q}$-rational modular forms of weight w for some $\mathbb{K}$, and if $f_2(g, 1) \neq 0$, then

(1) $$\rho(f_1(g, 1)/f_2(g, 1)) = f_1(g', 1)/f_2(g', 1).$$

By definition of $\mathfrak{A}(\mathbb{K}, w)$,

(2) $$j(g, o)^{-w}f_i(g, 1) = F_i(g(o))$$

for a holomorphic Hilbert modular form $F_i = \lambda_1 f_i$ for $G(\mathbb{Q}) \cap \mathbb{K}$ acting on $\mathfrak{H}^n$, $i = 1, 2$.

For any Hilbert modular form F with Fourier expansion

$$F(\mathfrak{z}) = \Sigma_\lambda a(\lambda)e^{2\pi i(\lambda, \mathfrak{z})},$$

the function $F^\rho(\mathfrak{z}): = \overline{F(-\bar{\mathfrak{z}})}$ has complex conjugate Fourier coefficients to those of $F(\mathfrak{z})$, i.e., $\overline{a(\lambda)} = a(\lambda)^\rho$ in place of $a(\lambda)$. Therefore,

(3) $$\rho(F(\Phi(\tau))) = F^\rho(-\rho\Phi(\tau)).$$

Let $f = f_i (= \rho f)$, $F = \lambda_1(f)$ and $u = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} (= u(\rho)$, cf. 1.3). By 1.3(1) with $\sigma = \rho$, $x = u$, then $\lambda_1(f)^\rho = \lambda_u(f)$, so (cf. (2))

(4) $$j(h, o)^w F^\rho(h(o)) = f(h, u).$$

Since $u \in G(\mathbb{Q})$, one has $f(g', 1) = f(ug', u)$; hence,

(5) $$f(g', 1) = j(ug', o)^w F^\rho(-\rho\Phi(\tau)).$$

Combining (2), (3) and (5) gives (1), as required.

4.4.3$_u$. *If* $\sigma K = K$, *then* $u_{\Phi_{\sigma-1}}(\sigma') = (u_\Phi(\sigma'))^\sigma$.

PROOF FOR $u = b$.   This results from transport of structure. Our construction of V as $G(\mathbb{Q})\backslash(X \times G(\mathbb{A}^f)/\bar{Z})$ depends on the action of $G(\mathbb{Q}) = GL_2(\mathfrak{f})$ on X, which is determined by $\Phi^0: \mathfrak{f} \to \mathbb{R}^n$, so write $V = V(\Phi^0)$. Similarly, write

$$W(\Phi^0) = G(\mathbb{Q})\backslash(GL_2(\mathbb{R})^n \times G(\mathbb{A}^f)/\bar{Z}).$$

Note that $\sigma\mathfrak{f} = \mathfrak{f}$. Identifying $G(\mathbb{A}^f)$ with $GL_2(\mathfrak{f}(\mathbb{A}^f))$ we see that σ induces an automorphism of $G(\mathbb{A}^f)$ and that $1 \times \sigma$ induces isomorphisms

$$t_V: V(\Phi^0) \to V(\Phi^0\sigma^{-1}) \quad \text{and} \quad t_W: W(\Phi^0) \to W(\Phi^0\sigma^{-1}).$$

We claim that t_V commutes with Galois action on V, i.e., t_W commutes with Galois action on $\mathfrak{A}(\mathbb{K}; \mathbb{Q}_{ab})$. In the notation of §1, if $f \in \mathfrak{A}(\mathbb{K})$,

(1) $$\lambda_x(f \circ t_W)) = \lambda_{\sigma(x)}f.$$

Thus, the pullback vía t_W preserves $\mathbb{Q}_{ab}$-arithmeticity of forms. Suppose that $\sigma' \in \text{Aut}(\mathbb{C})$. Our claim amounts to

(2) $$\sigma'(f \circ t_W) = (\sigma'f) \circ t_W.$$

To check this, take any $x \in G(\mathbb{A}^f)$; recall that with $u = u(\sigma')$, 1.3(1) gives $\lambda_x(\sigma'f) = (\lambda_{ux}f)^{\sigma'}$; apply λ_x to (2), transform the result by 1.3(1), and by (1), and observe that the equivalent holds because Aut ($\mathbb{C}$) fixes u.

Apply $t_V\sigma' = \sigma't_V$ to $[\Phi(\tau), 1]$ to get, for $\sigma' \in$ Aut ($\mathbb{C}$),

$$(3) \qquad [\sigma'\Phi(\tau), \sigma(q_\tau(b_\Phi(\sigma')))] = [\sigma'\Phi\sigma^{-1}(\sigma(\tau)), q_{\sigma(\tau)}(b_{\Phi\sigma^{-1}}(\sigma'))].$$

From $\sigma(q_\tau(b)) = q_{\sigma(\tau)}(\sigma(b))$ it follows that $b_{\Phi\sigma^{-1}}(\sigma') = \sigma(b_\Phi(\sigma'))$, as required.

4.4.4. $c_\Phi(\sigma)c_\Phi(\sigma)^\rho = 1.$

PROOF. For $u = f$, the following is proved in [11]; see Chapter 7, Theorem 2.2:

$$(1)_u \qquad\qquad u_\Phi(\sigma)u_\Phi(\sigma)^\rho \in \chi(\sigma)c\ell(K^\times).$$

Therefore, it will suffice to check $(1)_b$.

Let $\pi_0(V)$ be the set of connected components of V. We identify $\pi_0(V)$ with

$$\pi_0(f(\mathbb{A})^\times/f^\times)/\pi_0(Z(\mathbb{R})) \cong \pi_0(f(\mathbb{A}^f)^\times/f_+^\times)$$

via the determinant, as in (2.7.1) of [7]. By our definition of $\mathbb{Q}$-structure on V, each connected component is defined over $\mathbb{Q}_{ab}$. Thus, the effect of $\sigma \in$ Aut ($\mathbb{C}$) on $\pi_0(V)$ is determined by $\sigma|\mathbb{Q}_{ab}$, namely, to multiply by $\chi(\sigma)$. Thus, if $\sigma[\Phi(\tau), 1] = [\sigma\Phi(\tau), q_\tau(a)]$, then

$$(2) \qquad\qquad aa^\rho = \det(q_\tau(a)) \in \chi(\sigma)c\ell(K^\times).$$

Since $b_\Phi(\sigma) = a \cdot c\ell(K^\times)$, $(1)_b$ follows.

4.4.5. *If $\sigma\Phi = \sigma'\Phi$, then $c_\Phi(\sigma) = c_\Phi(\sigma')$.*

PROOF. In case $\sigma' = 1$, the required identity, $c_\Phi(\sigma) = 1$ is equivalent to the reciprocity law 4.2 (1); see 4.3. In general,

$$(1) \qquad\qquad c_\Phi(\sigma^{-1}\sigma') = c_\Phi(\sigma^{-1}\sigma),$$

since both sides equal 1. Apply $4.4.1_c$ to conclude.

4.5. Theorem. *The map b_Φ: Aut ($\mathbb{C}$) $\to K(\mathbb{A}^f)^\times/c\ell(K^\times)$ defined by*

$$\sigma[\Phi(\tau), 1] = [\sigma\Phi(\tau), q_\tau(b_\Phi(\sigma))], \qquad (\tau \in K - f),$$

satisfies

$$NR_K(b_\Phi(\sigma)^{-1})^2 = t_\Phi(\sigma)^2.$$

PROOF. Having now verified the necessary properties of $b_\Phi(\sigma)$, etc., we can proceed as in Chapter 7 of [11]. It suffices to show that $c_\Phi(\sigma)^2 = 1$. Thus, in view of 4.4.4, one requires $c_\Phi(\sigma)^\rho = c_\Phi(\sigma)$. By 4.4.5, $c_\Phi(\sigma\rho) = c_\Phi(\rho\sigma)$; hence, by 4.4.1$_c$ and 4.4.2$_c$ it follows that $c_\Phi(\sigma) = c_{\rho\Phi}(\sigma)$. Since $\rho\Phi = \Phi\rho$, one can use 4.4.3$_c$ to get $c_\Phi(\sigma)^\rho = c_\Phi(\sigma)$, as required.

Notes. (i) We used 4.4.3. only with $\sigma = \rho$, and this case is easy: apply σ' to the identity $[\Phi(\tau), 1] = [\bar\Phi(\bar\tau), 1]$, and use the Main Theorem along with $q_{\bar\tau}(a) = q_\tau(\bar a)$ to get

$$b_\Phi(\sigma')^\rho = b_{\rho\Phi}(\sigma').$$

(ii) In [2], the restriction to CM-points with maximal associated order arose from difficulty in proving that a CM-point and its conjugates have the same associated order. We have circumvented the problem; however, it is easy to recover this result. The order associated to a CM-point $z = [\Phi(\tau), x]$ is

$$R(z): = K \cap r_z^{-1}(M_2(\hat{\mathfrak{o}})),$$

where $r_z(b) = x^{-1}q_\tau(b)x$. By our Main Theorem, for every $\sigma \in \text{Aut}(\mathbb{C})$, $r_{\sigma(z)} = r_z$, so $R(\sigma(z)) = R(z)$.

References

[1] Baily, W. L., Jr. On the theory of Hilbert modular functions. I. Arithmetic groups and Eisenstein series, *J. of Alg.*, **90** (1984), 567-605.

[2] —, Arithmetic Hilbert modular forms, in *Automorphic Forms of Several Variables*, Taniguchi Symposium, Katata, 1983, Birkhäuser, Boston, 1984.

[3] —, Arithmetic Hilbert modular functions II, *Revista Matemática Iberoamericana*, **1** (1985), 85-119.

[4] —, Arithmetic Hilbert modular functions. III, in *Contributions to several complex variables*, 1-40, Aspects of Math., Vieweg, Braunschweig, 1986.

[5] Borel, A. *Linear Algebraic Groups*, W. A. Benjamin, New York and Amsterdam, 1969.

[6] Cassels, J. W. S. and Fröhlich, A. *Algebraic Number Theory*, Academic, London, 1967.

[7] Deligne, P. Travaux de Shimura, in *Séminaire Bourbaki*, 1970/71, no. 389, *Lecture Notes in Math.*, vol. 244, Springer-Verlag.

[8] —, Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques, in *Proc. of Symp. in Pure Math.*, **33** (1979), part. 2, pp. 247-290, Am. Math. Soc., Providence, 1979.

[9] Hilbert, D. Über die Theorie der relativquadratischen Zahlkörpers, *Math. Ann.* **51** (1899), 1-127.

[10] Karel, M.   Special values of elliptic modular forms, in *Automorphic Forms of Several Variables*, Taniguchi Symposium, Katata, 1983, Birkhäuser, Boston, 1984.

[11] Lang, S.   *Complex Multiplication*, Springer-Verlag, New York, 1983.

Martin L. Karel*
Department of Mathematical Sciences
Camden College of Arts and Sciences
Rutgers University, Camden, NJ 08102