Abelian Varieties with Complex Multiplication (for Pedestrians)

J. S. Milne

The main theorem of Shimura and Taniyama (see [73, Thm. 5.15]) describes the action of an automorphism \( \tau \) of \( \mathbb{C} \) on an abelian variety of CM-type and its torsion points in the case that \( \tau \) fixes the reflex field of the variety. In his Cornell's article [56], Taniyama made a conjecture concerning conjugates of Shimura varieties that (see [58]) leads to a conjectural description of the action of \( \tau \) on the variety and its torsion points for all \( \tau \). Recently (July 1981) Deligne proved this conjecture (see [33]). Deligne expresses his result as an identity between two Frobenius reductive groups, the Taniyama group of Taniyama and his own motivic Galois group associated with the Tannakian category of motives of abelian varieties over \( \mathbb{Q} \) of potential CM-type. Earlier (April 1981) Tate (see [15-3]) gave a more down-to-earth conjecture than that stated in [83] and partially proved his conjecture.

The purpose of these notes is to use Deligne's ideas to given as direct a proof as possible of the conjecture.
in the form stated by Tate. It is also shown that the three forms of the conjecture, those in 533, 573, and 5153, are equivalent.

Also, Tate's ideas are used to simplify the construction of the Manin-Mumford group. In the first three sections I have followed Tate's manuscript [15] very closely, sometimes word-for-word.

These notes are a rough outline of two of my lectures at the conference on Shimura Varieties, Vancouver, 21-25 Aug 1981. The remaining lectures I described how the result on abelian varieties of CM-type could be applied to give a proof of Langlands's conjecture on congruences of Shimura varieties for most (perhaps all) Shimura varieties.

**Notation:** $\text{rec}_E: \mathbb{A}^x_E \to \text{Gal}(E^{ab}/E)$ is normalized so that a uniformizing parameter corresponds to the inverse of the usual (arithmetic) $A$-function. When $E$ is totally complex, $\text{rec}_E$ factors into $\mathbb{A}^x_E \to \mathbb{A}^x_F/E \xrightarrow{E} \text{Gal}(E^{ab}/E)$.

\begin{align*}
\mathbb{Z} &= \mathbb{Z}/m\mathbb{Z}, \quad \mathbb{A}^x = \mathbb{Z} \otimes \mathbb{Q}, \quad \mathbb{A}^c = \mathbb{R} \mathbb{A}^c \otimes E, \quad A_F = \mathbb{A}^c \times (E \otimes \mathbb{R}).
\end{align*}

$\text{Inv}(\cdot)$ = complex conjugation.

\[2 \text{ Be wary of the signs!}\]

If $E \subset \mathbb{C}$, then $E^{ab}$ and $\overline{E}$ are also in $\mathbb{C}$.

If $T$ is a torus $/E$, then $X_s(T) = \text{Hom}_E(G_m, T)$. 
§1 Statement of the theorem

Let $A$ be an abelian variety over $\mathbb{C}$, and let $K$ be a subfield of $\text{End}(A) \otimes \mathbb{Q}$ of degree $2 \dim(A)$ over $\mathbb{Q}$; such an abelian variety is said to have complex multiplication by $K$. (More generally, one can allow $K$ to be a product of fields such $H_1(A, \mathbb{Q})$ is free of rank over $K$.) The representation of $K$ on the tangent space to $A$ at zero is of the form $\bigoplus_{\phi \in \mathcal{F}} \phi$ with $\mathcal{F}$ a subset of $\text{Hom}(K, \mathbb{C})$. The pair $(K, \mathcal{F})$ is a CM-type, i.e., $K$ is a CM-field and $\text{Hom}(K, \mathbb{C}) = \mathcal{F} \cup \bar{\mathcal{F}}$.

A Hecke form for $A$ is a $\mathbb{Q}$-bilinear skew-symmetric form $\psi$ on $H_1(A, \mathbb{Q})$ such that

$$(x, y) \mapsto \psi(x, iy) : H_1(A, \mathbb{Q}) \times H_1(A, \mathbb{Q}) \to \mathbb{C}$$

is symmetric and positive definite. We shall always assume that $\psi$ is compatible with the complex multiplication in the sense that

$$\psi(ax, y) = \psi(x, (a)y), \quad a \in K, \quad x, y \in H_1(A, \mathbb{Q}).$$

A Hecke form with this property always exists.

Let $C^\mathcal{F}$ be the set of complex-valued functions on $\mathcal{F}$ and embed $K$ into $C^\mathcal{F}$ through the natural map $a \mapsto (\phi(a), \ldots)_{\phi \in \mathcal{F}}$; let $\mathcal{K} = K \cap \text{End}(A)$. There then exist a $\mathbb{Z}$-lattice $\Omega$ in $K$ stable under $K$, an element $t \in K^\times$, and an $\mathcal{K}$-linear analytic isomorphism $\Theta : C^\mathcal{F}/\mathcal{O} \cong A$ such that $\psi(x,y) = Tr_{K/\mathbb{Q}}(t x \cdot y)$ where, in the last equation, we have used $\Theta$ to identify $H_1(A, \mathbb{Q}) \cong \mathcal{K}$ with $\mathcal{O} \otimes \mathbb{Q} = K$. The variety is said to be of type $(K, \mathcal{F}; \mathcal{O}, t)$ relative to $\Theta$. The type determines the triple $(A, K \hookrightarrow \text{End}(A) \otimes \mathbb{Q}, \psi)$ up to isomorphism. Conversely, the triple
determines the type up to a change of the following form: if \( \Theta \) is replaced by \( \Theta \circ \alpha^{-1}, \alpha \in K^\times \), then the type becomes \((K, \overline{\phi}; \alpha \sigma, t / \alpha \sigma)\).

Let \( \tau \in \text{Aut}(C) \). Then \( K \rightarrow \text{End}(A) \otimes \mathbb{Q} \) induces a map \( K \rightarrow \text{End}(\tau A) \otimes \mathbb{Q} \), so that \( \tau A \) also has complex multiplication by \( K \). The form \( \psi \) is associated with a divisor \( D \) on \( A \), and we let \( \tau \psi \) be the Riemann form for \( \tau A \) associated with \( \tau D \). It has the following characterization: after multiplying \( \psi \) with a nonzero rational number, we can assume that it takes integral values on \( H_1(A, \mathbb{Z}) \); define \( \psi_m \) to be the pairing \( A_m \times A_m \rightarrow \mathbb{Z} \), \( (x, y) \mapsto \exp(2\pi i \psi(x, y)/m) \); then \( (\tau \psi)_m(\tau x, \tau y) = \tau(\psi_m(x, y)) \).

In the next section we shall define (following Tate) for each CM-type \((K, \phi)\) a map \( f_\phi: \text{Aut}(C) \rightarrow \mathbb{A}^1_k \) such that \( f_\phi(\tau), f_\phi(\overline{\tau}) = \mathbb{A}(\tau, K^\times) \), all \( \tau \in \text{Aut}(C) \). We can now state the new main theorem of complex multiplication in the form first appearing (as a conjecture) in Tate [15].

**Theorem 1.1** (Shimura, Taniyama, Langlands, Deligne). Suppose \( A \) has type \((K, \phi; \alpha, t)\) relative to \( \Theta : C^1 / \alpha \cong A \). Let \( \tau \in \text{Aut}(C) \) and let \( f \in \mathbb{A}^1_k \) lie in \( f_\phi(\tau) \).

(a) The variety \( \tau A \) has type \((K, \tau \phi; f \sigma, \mathbb{k}(\tau)/f, \tau f)\) relative to \( \Theta', \) say.

(b) It is possible to choose \( \Theta' \) so that
\[
\begin{align*}
\mathbb{A}^1_K &\rightarrow \mathbb{A}^1_K / \alpha \otimes \mathbb{Z} = K / \alpha \\
\downarrow f &\downarrow f
\end{align*}
\]
\[
\begin{align*}
\mathbb{A}^1_K &\rightarrow \mathbb{A}^1_K / f \sigma \otimes \mathbb{Z} = K / f \sigma \\
\downarrow f &\downarrow f
\end{align*}
\]
\[
\begin{align*}
\Theta &\rightarrow \Theta' \\
\tau A &\rightarrow \tau A_{\text{tors}}
\end{align*}
\]
commutes, where $A_{\text{tors}}$ denotes the torsion subgroup of $A$.

**Remark 1.2** Prior to its complete proof, the theorem was known in three important cases.

(a) If $\tau$ fixes the reflex field $(K, \Phi)$ then the theorem becomes the old main theorem of complex multiplication, proved by Shimura and Taniyama (see (1.8) below). This case is used in the proof of the general result.

(b) Tate [15] proved first part (a) of the theorem, and he showed that (b) holds when $\tau$ is replaced by $f e$, $e \in A_{K_0}^f$, $e^2 = 1$, $K_0$ the maximal real subfield of $K$. We include Tate’s proof of this result, although it is not necessary for the general case.

(c) Shih [12] proved the theorem under the assumption that there exists an automorphism $\sigma$ of $K$ of order 2 such that $\tau(\Phi \cap \Phi \sigma) = \Phi \cap \Phi \sigma$ and $\tau(\Phi \cap \Phi \sigma) = \Phi \cap \Phi \sigma$. As we shall see, the proof is a special case of the general proof.

We now rewrite the theorem in more invariant form. Let

$$TA = \varinjlim A_m = \varinjlim \left( \frac{H_i(A, \mathbb{Z})}{H_i(A, \mathbb{Z})} \right) = H_i(A, \hat{\mathbb{Z}}),$$

and let $V^fA = TA \otimes \varphi = H_i(A, \varphi) \otimes A^f$. Then $\varphi$ gives rise to a pairing

$$\psi^f = \varprojlim \varphi_m : V^fA \times V^fA \longrightarrow \Omega^1(\mathcal{O})$$

where $\Omega^1(\mathcal{O}) = \varprojlim \mu_m(\mathcal{O}) \otimes \varphi$.

**Theorem 1.3.** Let $A$ have type $(K, \Phi)$; let $\tau \in \text{Aut}(\mathbb{C})$, and let $f \in f_{\text{reg}}(\tau)$. 

(a) $\tau$ is a $K$-linear isomorphism $\tau : H_{1}(\Lambda, \mathcal{O}) \rightarrow H_{1}(\tau \Lambda, \mathcal{O})$ such that:

(i) $\psi(\frac{x_{1}x_{2}}{x_{1}f}, x, y) = \tau \psi(dx, dy)$, $x, y \in H_{1}(\Lambda, \mathcal{O})$;

(ii) \[
\begin{array}{ccc}
V^{f}(A) & \xrightarrow{f} & V^{f}(A) \\
\downarrow \tau & & \downarrow \tau \circ \delta \circ \iota \\
V^{f}(\tau A) & & 
\end{array}
\]

commutes.

Lemma 1.4. The statements (1.1) and (1.3) are equivalent.

Proof. Let $\Theta$ and $\Theta'$ be as in (1.1), and let $\Theta_{1} : K \xrightarrow{\sim} H_{1}(\Lambda, \mathcal{O})$ and $\Theta'_{1} : K \xrightarrow{\sim} H_{1}(\tau \Lambda, \mathcal{O})$ be the maps induced by $\Theta$ and $\Theta'$. Then

$\psi(\Theta_{1}(x), \Theta(1y)) = \text{Tr}(tx, ty)$

and

$\psi(\Theta'_{1}(x), \Theta'(1y)) = \text{Tr}(t\tau x, ty)$

where $\tau = \chi(z)/x_{1}f$

and

\[
\begin{array}{ccc}
A_{K}^{f} & \xrightarrow{\Theta_{1}} & V^{f}(A) \\
\downarrow \delta & & \downarrow \tau \\
A_{K}^{f} & \xrightarrow{\Theta'_{1}} & V^{f}(\tau A)
\end{array}
\]

commutes. Let $\chi = \Theta'_{1} \circ \Theta_{1}^{-1}$; then

$\tau \psi(dx, dy) = \text{Tr}(t\chi \Theta_{1}(x), (\Theta_{1}^{-1}(y))) = \psi(\chi x, y)$

and

$\tau = \Theta'_{1} \circ \Theta_{1}^{-1} = \Theta'_{1} \circ \Theta_{1}^{-1} \circ f = \Theta_{1} \circ f$.

Conversely, let $\lambda$ be as in (1.3) and choose $\Theta_{1}'$ so that $\lambda = \Theta'_{1} \circ \Theta_{1}^{-1}$. It is then easy to check (1.1).
§2 Definition of $f_{\bar{\phi}}(\tau)$

Let $(K, \Phi)$ be a CM-type. Consider an embedding $K \hookrightarrow \mathbb{C}$, and extend it to an embedding $i : K^{ab} \hookrightarrow \mathbb{C}$. Choose elements $W_\rho \in \text{Aut}(\mathbb{C})$, one for each $\rho \in \text{Hom}(K, \mathbb{C})$, such that

$$W_\rho \circ i \mid K = \rho, \quad W_\rho = \iota W_\rho.$$ 

For example, choose $W_\rho$ for $\rho \in \Phi$ (or any other CM-type) to satisfy the first equation, and define $W_\rho$ for the remaining $\rho$ by the second equation. For any $\tau \in \text{Aut}(\mathbb{C})$, $W_{\tau \rho} \circ W_\rho \circ i \mid K = W_{\tau \rho}^{-1} \circ \tau \rho \mid K = i$. Thus $i^{-1} \circ W_{\tau \rho}^{-1} \circ W_\rho \circ i \in \text{Gal}(K^{ab}/K)$, and we can define $F_{\bar{\phi}} : \text{Aut}(\mathbb{C}) \to \text{Gal}(K^{ab}/K)$ by

$$F_{\bar{\phi}}(\tau) = \prod_{\phi \in \Phi} i^{-1} \circ W_{\tau \phi}^{-1} \circ W_\phi \circ i.$$ 

Lemma 2.1. $F_{\bar{\phi}}$ is independent of the choice of $\{W_\rho\}$.

Proof. Any other choice is of the form $W_\rho' = W_\rho h_\rho$, $h_\rho \in \text{Aut}(\mathbb{C}/K)$. Thus $F_{\bar{\phi}}(\tau)$ is changed by $i^{-1} \circ (\prod_{\phi \in \Phi} W_{\tau \phi}^{-1} h_\phi) \circ i$. The conditions on $w$ and $w'$ imply that $h_\rho = h_\rho$, and it follows that the inside product is $1$ because $\tau$ permutes the unordered pairs $\{\phi, \bar{\phi}\}$.

Lemma 2.2. $F_{\bar{\phi}}$ is independent of the choice of $i$ (and $K \hookrightarrow \mathbb{C}$).

Proof. Any other choice is of the form $i' = \sigma \circ i$, $\sigma \in \text{Aut}(\mathbb{C})$. Take $W_\rho' = W_\rho \circ \sigma^{-1}$, and then

$$F_{\bar{\phi}}'(\tau) = \prod_{\phi \in \Phi} i'^{-1} \circ (\sigma^{-1} W_{\tau \phi}^{-1} \circ W_\phi \circ \sigma^{-1}) \circ i' = F_{\bar{\phi}}(\tau).$$

Thus we can suppose $K \hookrightarrow \mathbb{C}$ and ignore $i$; then
\[ F_\Phi(\tau) = \prod_{\phi \in \Phi} w_{\phi}^{-1} \cdot \tau \cdot w_{\phi} \mod \text{Aut}(C/K^{ab}). \]

Proposition 2.3. For any \( \tau \in \text{Aut}(C) \), there is a unique \( f_\Phi(\tau) \in \mathbb{A}_K^{fx}/K^x \) such that

(a) \( r_K(f_\Phi(\tau)) = F_\Phi(\tau) \)

(b) \( f_\Phi(\tau) \cdot i f_\Phi(\tau) = \chi(\tau) K^x \).

Proof. Since \( r_K \) is surjective, there is an \( f \in \mathbb{A}_K^{fx}/K^x \) such that \( r_K(f) = F_\Phi(\tau) \). We have

\[
 r_K(f \cdot i f) = r_K(f) \cdot r_K(i f) = r_K(f) \cdot i r_K(f) \cdot i^{-1} = F_\Phi(\tau) \cdot F_\Phi(\tau)
\]

\[
 = V_{K/Q}(\tau),
\]

where \( V_{K/Q} : \text{Gal}(\bar{Q}/Q)^{ab} \rightarrow \text{Gal}(\bar{Q}/K)^{ab} \) is the transfer (Verlagerung) map. As \( V_{K/Q} = r_K \cdot \chi \) it follows that \( f \cdot i f = \chi(\tau) K^x \mod (\ker r_K) \). The next lemma shows that \( i \cdot i \) acts bijectively on \( \ker r_K \), and so there is a unique \( a \in \ker r_K \) such that \( a \cdot i a = (f \cdot i f)/\chi(\tau) K^x \); we must take \( f_\Phi(\tau) = f/a \).

Lemma 2.4. \( \ker (r_K : \mathbb{A}_K^{fx}/K^x \rightarrow \text{Gal}(K^{ab}/K)) \) is uniquely divisible by all integers, and its elements are fixed by \( i \).

Proof. The kernel of \( r_K \) is \( \bar{K}^x/K^x \) where \( \bar{K}^x \) is the closure of \( K^x \) in \( \mathbb{A}_K^{fx} \). It is also equal to \( \bar{U}/U \) for any subgroup \( U \) of \( O_K^x \), of finite index. A theorem of Chevalley (see [Ek, 3.5])
shows that $\mathbb{A}_K^{\infty}$ induces the pro-finite topology on $U$. If we take $U$ to be contained in the real subfield of $K$ and $\text{torsion-free}$, then it is clear that $\overline{U}/U$ is fixed by $\tau$ and (being isomorphic to $(\widehat{\mathbb{Z}}/\mathbb{Z})^{\dim(A)}$) uniquely divisible.

Remark 2.6. A more direct definition of $f_{\Phi}(\tau)$, but one involving the Weil group, can be found in (7.2).

Proposition 2.7. The maps $f_{\Phi} : \text{Aut}(C) \rightarrow \mathbb{A}_K^{\infty}/K^{x}$ have the following properties:

(a) $f_{\Phi}(\sigma \tau) = f_{\tau \Phi}(\sigma) f_{\Phi}(\tau)$;
(b) $f_{\Phi}(\tau|K)(\sigma) = \tau f_{\Phi}(\sigma)$ if $\tau K = K$;
(c) $f_{\Phi}(1) = 1$.

Proof: Let $f = f_{\tau \Phi}(\sigma) f_{\Phi}(\tau)$. Then

$$v_K(f) = F_{\tau \Phi}(\sigma) F_{\Phi}(\tau) = \prod_{\phi \in \Phi} w_{\sigma \tau \phi} \sigma w_{\tau \phi} w_{\tau 0} \tau w_{\tau} = f_{\Phi}(\sigma \tau)$$

and $f, f = \chi(\sigma) \chi(\tau) K^{x} = \chi(\sigma \tau) K^{x}$. Thus $f$ satisfies the conditions that determine $f_{\Phi}(\sigma \tau)$. This proves (a), and (b) and (c) can be proved similarly.

Let $E$ be the reflex field for $(K, \Phi)$, so that

$\text{Aut}(C/E) = \{ \tau \in \text{Aut}(C) | \tau \Phi = \Phi \}$. Then $E \text{Aut}(C/K)$ is stable under the left action of $\text{Aut}(C/E)$, and we write

$$\text{Aut}(C/K) \Phi^{-1} = \bigcup_f \text{Aut}(C/E) \text{ (disjoint union)};$$

the set $f = \{ \psi | E \}$ is a CM-type for $E$, and $(E, \Phi)$ is the
The map \( a \mapsto \Phi^x(a) : E \to \mathcal{A}_E \) factors through \( \mathcal{A}_E \) and defines a morphism of algebraic tori \( \Phi^x : E^* \to \mathcal{A}_E^* \).

The (old) main theorem of complex multiplication states the following: let \( \pi \in \text{Aut}(\mathcal{C}/E) \), and let \( a \in \mathcal{A}_E^{cx}/E^* \) be such that \( r_E(a) = \pi \); then (1.1) is true after \( \pi \) has been replaced by \( \Phi^x(a) \) (see [13, Thm 5.15]; the sign differences result from different conventions for the reciprocity law and the action of Galois groups.) The rest result shows that this is in agreement with (1.1).

**Proposition 2.8.** For any \( \pi \in \text{Aut}(\mathcal{C}/E) \), and \( a \in \mathcal{A}_E^{cx}/E^* \) such that \( r_E(a) = \pi \), \( \Phi^x(a) \in F_\pi \).

**Proof:** Partition \( \Phi \) into orbits, \( \Phi = \bigcup_j \Phi_j \), for the left action of \( \text{Aut}(\mathcal{C}/E) \). Then \( \text{Aut}(\mathcal{C}/K) \Phi_j = \bigcup_j \text{Aut}(\mathcal{C}/K) \Phi_j \), and

\[
\text{Aut}(\mathcal{C}/K) \Phi_j = \text{Aut}(\mathcal{C}/K)(\sigma_j^{-1} \text{Aut}(\mathcal{C}/E)) = (\text{Hom}_K(L_j, E) \sigma_j^{-1}) \text{Aut}(\mathcal{C}/E)
\]

where \( \sigma_j \) is any element of \( \text{Aut}(\mathcal{C}) \) such that \( \sigma_j \mid K \in \Phi_j \) and \( L_j = (\sigma_j^{-1} E) K \). Thus \( \Phi^x(a) = \prod b_j \), with \( b_j = N_{L_j/K}(\sigma_j^{-1}(a)) \). Let \( F_j(\pi) = \prod_{x \in \Phi_j} \pi \Phi^x(\pi \Phi^x(b_j)) \) (mod \( \text{Aut}(\mathcal{C}/K^{ab}) \)). We begin by showing that

\[
F_j(\pi) = r_K(b_j).
\]

The basic properties of Artin's reciprocity law show that

\[
\begin{align*}
\mathcal{A}_E^{cx} & \longrightarrow \mathcal{A}_{\sigma_j L_j}^{cx} \quad \sigma_j^{-1} \quad \mathcal{A}_{L_j}^{cx} \quad N_{L_j/K} \quad \mathcal{A}_E^{cx} \\
\downarrow r_E & \quad \downarrow \sigma_j L_j \quad \downarrow r_{L_j} \quad \downarrow r_K \\
\text{Galm}(E^{ab}/E) & \quad \sigma_j \text{Galm}(L_j^{ab}/L_j) \quad \sigma_j^{-1} \quad \text{Galm}(L_j^{ab}/L_j) \quad \text{rest.} \quad \text{Galm}(K^{ab}/K)
\end{align*}
\]

commutes. Therefore \( r_K(b_j) \) is the image of \( r_E(a) \) by the three
makes in the bottom row of the diagram. Consider \( \{ ty | t \phi \in \mathcal{X} \}, \phi \in \mathcal{S}_j \); this is a set of coset representatives for \( \sigma_j \mathcal{A} \text{ut}(C/L_j) \sigma_j^{-1} \quad \mathcal{A} \text{ut}(C/E) \) in \( \mathcal{A} \text{ut}(C/E) \), and so \( F_j(r) = \prod_{\phi \in \mathcal{S}_j} t_\phi^{-1} t_\phi \sigma_j = \mathcal{F}_j^{\sigma_j^{-1}} \mathcal{V}(r) \sigma_j \mod \mathcal{A} \text{ut}(C/K^m) \).

Thus \( F_j(r) = F_j^{\sigma_j^{-1}} \mathcal{V}(r) \sigma_j \).

Thus \( r_k(F_j^{\sigma_j^{-1}} \mathcal{V}(r) \sigma_j) = \prod r_k(b_j) = \prod F_j(r) = F_k(r) \). Clearly \( \mathcal{F}^*(a) \) is \( \mathcal{F}^*(a) \in \mathcal{X}(r) K^* \) and so this shows that \( a \in \mathcal{F}_k(r) \).
§ 3 Start of the proof; Tate's result

We shall work with the statement (1.2) rather than (1.1). The variety \( r \mathcal{A} \) has type \((K, r\mathcal{F})\) because \( r\mathcal{F} \) describes the action of \( K \) on the tangent space to \( r \mathcal{A} \) at zero. Choose any \( K \)-linear isomorphism \( \omega : H_1(\mathcal{A}, \mathcal{O}) \cong H_1(r \mathcal{A}, \mathcal{O}) \). Then

\[
V^f(A) \xrightarrow{\tau} V^f(r \mathcal{A}) \xrightarrow{(\omega \otimes 1)^{-1}} V^f(A)
\]

is an \( A_K^f \)-linear isomorphism, and hence is multiplication by some \( g \in A_K^f \); thus \( (\omega \otimes 1)_g = \tau \).

**Lemma 3.1.** For this \( g \), we have

\[
(\omega \psi)(g \cdot x, y) = (\omega \psi)(x, y), \quad \text{all } x, y \in V^f(A).
\]

**Proof:** By definition,

\[
(\omega \psi)(r x, r y) = \tau(\psi(x, y)) \quad \text{and} \quad x, y \in V^f(A).
\]

\[
(\omega \psi)(g x, g y) = \psi(g, g) = \psi(g, g) x, y \quad \text{and} \quad x, y \in V^f(A).
\]

On replacing \( x \) and \( y \) by \( g x \) and \( g y \) in the second equality, we find

\[
(\omega \psi)(r x, r y) = \psi(g x, g y) = \psi(\psi(x, y), y)
\]

As \( \tau(\psi(x, y)) = X(\tau) \psi(x, y) = \psi(X(\tau) x, y) \), the lemma is now obvious.

**Remark 3.2.** On taking \( x, y \in H_1(\mathcal{A}, \mathcal{O}) \) in (3.1), we can deduce that

\[
X(\tau)/g \cdot g \in K^x, \quad \text{therefore} \quad \{ X(\tau)/g \cdot g \} \equiv X(\tau) \mod K^x.
\]

The only choice involved in the definition of \( g \) is that of \( \tau \).
and \( \sigma \) is determined up to multiplication by an element of \( K^* \). Thus the class of \( g \) in \( \mathbb{A}^F_K / K^* \) depends only on \( A \) and \( \sigma \). In fact it depends only on \( (K, \mathcal{F}) \) and \( \sigma \), because any other abelian variety of type \( (K, \mathcal{F}) \) is isogenous to \( A \) and leads to the same class \( g K^* \). We define \( \mathcal{G}_K^F (\sigma) = g K^* \in \mathbb{A}^F_K / K^* \).

**Proposition 3.3.** The maps \( \mathcal{G}_K^F : \text{Aut}(C) \rightarrow \mathbb{A}^F_K / K^* \) have the following properties:

(a) \( \mathcal{G}_K^F (\sigma \tau) = \mathcal{G}_K^F (\tau) \mathcal{G}_K^F (\sigma) \);

(b) \( \mathcal{G}_K^F (\tau^{-1} \sigma) = \tau \mathcal{G}_K^F (\sigma) \) if \( \tau K = K \);

(c) \( \mathcal{G}_K^F (1) = 1 \);

(d) \( \mathcal{G}_K^F (\tau), \mathcal{G}_K^F (\sigma) = \chi(\tau) K^* \).

**Proof.** (a) Choose isomorphisms \( \alpha : H_1(A, \Omega) \rightarrow H_1(\tau A, \Omega) \) and \( \beta : H_1(\tau A, \Omega) \rightarrow H_1(\sigma \tau A, \Omega) \), and let \( g = (\alpha \circ 1) \circ \tau \) and \( g_\tau = (\beta \circ 1) \circ \tau \) so that \( g \) and \( g_\tau \) represent \( \mathcal{G}_K^F (\tau) \) and \( \mathcal{G}_K^F (\sigma) \) respectively. Then

\[
(\beta \circ 1) \circ (g_\tau \circ g) = (\beta \circ 1) \circ g_\tau \circ (\alpha \circ 1) \circ g = \tau \cdot \beta,
\]

which shows that \( g_\tau \circ g \) represents \( \mathcal{G}_K^F (\tau \cdot \beta) \).

(b) If \( (A, K \rightarrow \text{End}(A) \otimes Q) \) has type \( (K, \mathcal{F}) \), then \( (A, K \rightarrow \text{End}(\tau A) \otimes Q) \) has type \( (K, \mathcal{F} \otimes \tau^{-1}) \). The formula in (b) can be proved by transport of structure.

(c) Complex conjugation \( i : A \rightarrow \bar{A} \) is a homeomorphism (relative to the complex topology) and so induces a \( K \)-linear isomorphism \( i : H_1(A, \Omega) \rightarrow H_1(A, \bar{Q}) \).

The map \( i : V^F(A) \rightarrow V^F(\bar{A}) \) is \( i \) again, and so on taking \( \tau = i \), we find \( g = 1 \).

(d) This is proved in (3.2).
Theorem 1.2 (hence also 1.1) becomes true if \( f^\circ \) is replaced by \( g^\circ \). Our task is to show that \( f^\circ = g^\circ \). To this end we set \( e^{\circ}_n(\tau) = g^\circ(\tau)/f^\circ(\tau) \in A^nx/K^n \).

Proposition 3.4. The maps \( e^{\circ}_n : \text{Aut}(\mathcal{O}) \to A^nx/K^n \) have the following properties:

(a) \( e^{\circ}_n(\sigma \tau) = e^{\circ}_n(\sigma) e^{\circ}_n(\tau) \);
(b) \( e^{\circ}_n(\tau^{-1}) = \tau e^{\circ}_n(\tau) \) \( \mathcal{O} \tau K = K \);
(c) \( e^{\circ}_n(1) = 1 \);
(d) \( e^{\circ}_n(\tau). e^{\circ}_n(\overline{\tau}) = 1 \);
(e) \( e^{\circ}_n(\tau) = 1 \) \( \tau \equiv \overline{\tau} \).

Proof: (a), (b), and (c) follow from (a), (b), and (c) of (2.7) and (3.3), and (d) follows from (3.3d) and (2.3b). The condition \( \tau e^{\circ}_n = e^{\circ}_n \) in (e) means that \( \tau \) fixes the reflex field of \((K, \bar{\phi})\) and, as we observed in §2, the theorems are known to hold in that case, which means that \( f^\circ(\tau) = g^\circ(\tau) \).

Proposition 3.5. Let \( K_0 \) be the maximal real subfield of \( K \); then \( e^{\circ}_n(\tau) \in A^nx/K^n_0 \) and \( e^{\circ}_n(\tau)^- = 1 \); moreover \( e^{\circ}_n(\tau) \) depends only on the effect of \( \tau \) on \( K_0 \), and is 1 if \( \tau K_0 = 1 \).

Proof: Replacing \( \tau \) by \( \sigma^{-1} \tau \) in (a), we find using (e) that \( e^{\circ}_n(\tau) = e^{\circ}_n(\sigma) \) \( \mathcal{O} \sigma \tau = \sigma \bar{\tau} \), i.e., \( e^{\circ}_n(\tau) \) depends only on the restriction of \( \tau \) to the reflex field of \((K, \bar{\phi})\). From (b) with \( \tau = 1 \), we find using \( \bar{\phi} = \bar{\phi} \) that \( e^{\circ}_n(\sigma) = e^{\circ}_n(\sigma) \). Putting \( \tau = 1 \), then \( \theta, \overline{\theta} = 1 \).
in (a), we find that \( e_{\bar{E}}(\sigma) = 1 e_{\bar{E}}(\tau) \) and \( e_{\bar{E}}(\tau) = e_{\bar{E}}(\tau) \). Denote \( \mathfrak{a} \) and \( \mathfrak{b} \) have the same effect on \( E \) we conclude \( e_{\bar{E}}(\tau) = 1 e_{\bar{E}}(\tau) \).

Thus \( e_{\bar{E}}(\tau) \in (A^{\times}_k / K^{\times})^{<\mathfrak{a}>} = A^{\times}_K / K^{\times} \), where \( <\mathfrak{a}> = \text{gal}(K/K_0) \), and (1) shows that \( e(\tau)^2 = 1 \).

**Corollary 3.6.** Part (a) of (1.1) is true; part (b) of (1.1) becomes true when \( \mathfrak{a} \) is replaced by \( \mathfrak{e} \), with \( e \in A^{\times}_K \), \( e^2 = 1 \).

**Proof:** Let \( e \in E_{\bar{E}}(\tau) \). Then \( e^2 \in K^{\times} \) and, since an element of \( K^{\times} \) that is a square locally at all finite primes is a square, we can correct \( e \) to achieve \( e^2 = 1 \). Now (1.1) is true with \( \mathfrak{a} \) replaced by \( \mathfrak{e} \), but \( e \) (being a unit) does not affect part (a) of (1.1).

We can now sketch the proof of the theorem. It seems to be essential to prove it simultaneously for all abelian varieties. To do this, one needs to define a universal \( e \), giving rise to all \( E_{\bar{E}}(\tau) \). The universal \( e \) is a map into the homomorphism. In §4 we review some of the theory concerning the homomorphism, and in (5.1) we state the existence of \( e \). The proof of (5.1), which requires Deligne's result [48] on Hodge cycles on abelian varieties, is carried out in §7 and §8. The remaining step, proving that \( e = 1 \), is less difficult, and is carried out in §6.
§4 The torus group

Let $E$ be a CM-field. The torus group corresponding to $E$ is a pair $(S^E, \mu^E)$ consisting of a $Q$-rational torus $S^E$ and a cocharacter $\mu^E \in X_*(S^E)$ defined over $E$ whose weight $w^E \equiv -(1+1) \mu^E$ is defined over $Q$. It is characterized by having the following universal property: for any $Q$-rational torus $T$ and $\mu \in X_*(T)$ defined over $E$ whose weight is $Q$-rational, there is a unique $Q$-rational homomorphism $\rho : S^E \to T$ such that $\rho \circ \mu^E = \mu$.

For $\rho \in \text{Hom}(E, Q)$, let $[\rho]$ be the character of the torus $E^* \to E^*$ defined by $\rho$. Then $\{[\rho] \mid \rho \in \text{Hom}(E, Q)\}$ is a basis for $X^*(E^*)$, and it is clear that

$$X^*(S^E) = \{x \in X^*(E^*) \mid \sum (2-1)(1+1)x = 0, \text{all } x \in \text{Aut}(C)\}$$

$$X^*(\mu^E) = \sum \eta_{\rho} [\rho] \mapsto \eta_{\rho} : X^*(S^E) \to \mathbb{Z}$$

because this has a universal property dual to that of $(S^E, \mu^E)$. In particular, there is a canonical map

$$E^* \to S^E \quad \text{(equal to } N_{E/Q} \cdot \text{Res}_{E/Q}(\mu^E))$$

and it is known (cf. [11, 3]) that the kernel of this map is the Zariski closure of any sufficiently small subgroup $U$ of finite index in $O^E$.

When $E$ is Galois over $Q$, the action of $\sigma \in \text{Gal}(E/Q)$ on $E$ defines an automorphism $\sigma$ of the torus $S^E$, and $X_*(\sigma)$ is

$$\sum \eta_{\rho} [\rho] \mapsto \sum \eta_{\rho} [\rho \circ \sigma].$$

**Lemma 4.1.** Let $E_0$ be the maximal real subfield of $E$; there is an exact sequence of algebraic tori
Proof: It suffices to show that the sequence becomes exact after the functor $X^*$ has been applied. As

$X^*(E'_0) = \{ \sum n_{\rho'} [\rho'] \mid \rho' \in \text{Hom}(E'_0, \mathbb{C}) \}$

$X^*(E^x \times Q^x) = \{ \sum n_{\rho} [\rho] + n \mid \rho \in \text{Hom}(E, \mathbb{C}) \}$

$X^*(S^E) = \{ \sum n_{\rho} [\rho] \mid n_{\rho} + \gamma_{\rho} = \text{constant} \}$

$X^*(\text{incl} \cdot \rho) = \sum n_{\rho} [\rho] + n \mapsto \sum n_{\rho} [\rho \mid E_0] + n \sum [\rho']$

$X^*(\text{can}, w^E) = \sum n_{\rho} [\rho] \mapsto \sum n_{\rho} [\rho] - (n_i + n_i)$

This is trivial.

Lemma 4.2 The map $N_{E/Q} : E^x \to \phi^x$ factors through $S^E$, and give rise to a commutative diagram

\[
\begin{array}{ccc}
S^E & \xrightarrow{i+1} & S^E \\
\downarrow N_{E/Q} & & \downarrow \phi^E \\
Q^x & \xrightarrow{w^E} & \\
\end{array}
\]

Proof: $X^*(N_{E/Q}) = n \mapsto n \sum [\rho]$, which clearly factors through $X^*(S^E) \subset X^*(E^x)$. Moreover, the endomorphisms

$X^*(w^E \cdot N_{E/Q}) = (\sum n_{\rho} [\rho] \mapsto n + n_i \mapsto (n + n_i) \sum n_{\rho} [\rho])$

$X^*(i+1) = (\sum n_{\rho} [\rho] \mapsto \sum n_{\rho} [\rho] + [\rho] \mapsto \sum (n_{\rho} + n_{\rho}) [\rho] = (n_i + n_i) \sum [\rho]$ are equal.

Let $E_1 > E_2$ be CM fields. The norm map $E_1^x \to E_2^x$ induces a norm map $N_{E_1/E_2} : S_{E_1}^x \to S_{E_2}^x$, which is the unique $\phi$-rational homomorphism such that $N_{E_1/E_2} \cdot \phi^{E_1} = \phi^{E_2}$. The following diagram
Commutes:
\[
1 \rightarrow (E,)^{x} \rightarrow E^{x} \times Q^{x} \rightarrow S^{E} \rightarrow 1
\]
\[
\downarrow N \quad \downarrow N \times \text{id} \quad \downarrow N_{E, E_{L}}
\]
\[
1 \rightarrow (E_{L})^{x} \rightarrow E_{L}^{x} \times Q^{x} \rightarrow S^{E_{L}} \rightarrow 1.
\]

Remark 4.3. The dense group is defined for all fields of finite degree over \(Q\). If \(L\) contains a CM-field \(E_{L}\) and \(E\) is the maximal such subfield, then \(N_{L/E} : S^{L} \rightarrow S^{E}\); otherwise \(N_{L/Q} : S^{L} \rightarrow S^{Q} = Q^{x}\).

\[
\text{Let } (K, \mathfrak{f}) \text{ be a CM-type. \(\widehat{\mathbf{T}}\) Write } T = \text{Res}_{K/Q} G_{m}, \text{ and define } \mu_{\mathfrak{f}} \in X_{x}(T) \text{ by the condition}
\]
\[
\rho \circ \mu_{\mathfrak{f}} = \text{id}, \quad \rho \in \mathfrak{f}
\]
\[
= 1, \quad \rho \notin \mathfrak{f}.
\]
Thus \(\mu_{\mathfrak{f}}\) is the map
\[
\mathbf{C}^{x} \longrightarrow T^{x}(C) = (K \otimes C)^{x} = \prod_{\mathfrak{p} \in \mathfrak{f}} C^{x} \times \prod_{\mathfrak{p} \notin \mathfrak{f}} C^{x}
\]
\[
z \longrightarrow (z, z, ..., z, 1, 1, ..., 1).
\]
The weight of \(\mu_{\mathfrak{f}}\) is the map induced by \(x \rightarrow x^{-1} : Q^{x} \rightarrow K^{x}\), which is defined over \(Q\), and \(\mu_{\mathfrak{f}}\) itself is defined over the reflex field of \((K, \mathfrak{f})\). Thus it is therefore, for any CM-field \(E\) containing the reflex field of \((K, \mathfrak{f})\), a unique \(Q\)-rational homomorphism \(\rho_{\mathfrak{f}} : S^{E} \rightarrow T\) such that \(\mu_{\mathfrak{f}} = \rho_{\mathfrak{f}} \circ \mu_{E}\). From now on we assume \(E\) to be \(K\).

Lemma 4.4 (c) \(\forall \mu_{\mathfrak{f}} = \mu_{\mathfrak{f}} z z = \text{Aut}(C)\).
(b) Let $\tau \in \text{Aut}(C)$ be such that $\tau K = K$, so that $\tau$ induces an automorphism $\tau$ of $T$; then $\tau \circ \sigma = \sigma \circ \tau^{-1}$.

**Proof:** (a) We shall need to use the formula

$$[\rho](\tau(\xi(x))) = \tau([\tau^{-1} \rho](x)), \quad x \in T(C), \quad \rho \in \text{Hom}(K, C).$$

Let $\rho \in \text{Hom}(K, C)$; then

$$[\rho](\tau(\xi(z))) = [\rho](\tau(\mu_{\xi}(\tau^{-1}(z)))) = \tau([\tau^{-1} \rho](\mu_{\xi}(\tau^{-1}(z)))).$$

By definition, $[\tau^{-1} \rho](\mu_{\xi}(\tau^{-1}(z))) = \tau^{-1} \rho \neq \phi$.

$$= 1 \quad \text{if} \quad \tau^{-1} \rho \notin \phi.$$ 

Thus

$$[\rho] \cdot (\tau \mu_{\xi}) = \text{id} \quad \rho \in \tau \phi$$

$$= 1 \quad \rho \notin \tau \phi,$$

which proves (a).

(b) $[\rho \tau] \cdot (\tau \mu_{\xi}) = [\rho \tau] \cdot \mu_{\xi} = \text{id} \quad \forall \phi \rho \tau \in \phi$

$= 1 \quad \rho \tau \notin \phi.$

Thus (b) is clear.

**Proposition 4.5** (a) For any $\tau \in \text{Aut}(C)$, $\rho_{\tau} \circ \tau^{-1} = \rho_{\tau}$.

(b) If $\tau K = K$, then $\tau \circ \rho_{\tau} = \rho_{\tau} \circ \tau^{-1}$.

**Proof** (a) We shall show that $\tau^{-1} \circ \mu_{E} = \tau(\mu_{E}^{E})$; from this it follows that

$$\rho_{\tau} \circ \tau^{-1} \circ \mu_{E} = \rho_{\tau} \circ (\tau(\mu_{E}^{E})) = \tau(\rho_{\tau} \circ \mu_{E}^{E}) \quad (\rho_{\tau} \text{ is $\tau$-rational})$$

$$= \tau \mu_{\xi} \quad \text{(definition of } \rho_{\xi})$$

$$= \mu_{\tau \xi} \quad (4.40),$$

and this which implies that $\rho_{\tau} \circ \tau^{-1} = \rho_{\tau \xi}$. It remains to show that $X^{*}(\tau \circ \mu_{E}) = X^{*}(\mu_{E})$, but
\[ X^*(\tau, \mu^E) = X^*(\mu^E) \circ X^*(\tau^{-1}) = (\sum \eta_{\rho}[\mathcal{P}] \mapsto \sum \eta_{\rho}[\tau^{-1}\mathcal{P}] \mapsto \eta_{\tau}) \]

and \[ X^*(\tau \mu^E) = \tau \left( X^*(\mu^E) \right) = (\sum \eta_{\rho}[\mathcal{P}] \mapsto \sum \eta_{\rho}[\tau^{-1}\mathcal{P}] \mapsto \eta_{\tau}) \].

(b) \[ \tau \circ \rho_{\mathcal{P}} \circ \mu^E = \tau \circ \mu_{\mathcal{P}} \]

(definition of \( \rho_{\mathcal{P}} \))

\[ = \mu_{\tau^{-1}} \] (4.4b).

**Proposition 4.6.** For \( E_1 \supset E_2 \),

\[ S^{E_1} \xrightarrow{\rho_{\mathcal{P}}} \]

commutes.

\[ \downarrow N_{E_1/E_2} \]

\[ S^{E_1} \xrightarrow{\rho_{\mathcal{P}}} T \]

**Proof:** \[ (\rho_{\mathcal{P}})_2 \circ N_{E_1/E_2} \circ \mu^{E_1} = (\rho_{\mathcal{P}})_2 \circ \mu^{E_2} = \mu_{\mathcal{P}}. \]

Let \( E \) be a CM-field, Galois over \( \mathbb{Q}_{\mathcal{P}} \).

**Proposition 4.7.** \( \lambda \), and consider all maps \( \rho_{\mathcal{P}} \) for \( \lambda \) running through the CM-types on \( E \); then \( \bigwedge \ker \rho_{\mathcal{P}} = 1 \).

**Proof:** We have to show that \( \sum \text{Im}(x^*(\rho_{\mathcal{P}})) = X^*(S^E) \), but the left-hand side contains \( \sum \mathcal{P} \mathcal{P} \) for all CM-types on \( E \), and these elements generate \( X^*(S^E) \).

**Proposition 4.8.** Let \( K_1 \supset K_2 \) be CM-fields and let \( \mathcal{P}_1 \) and \( \mathcal{P}_2 \) be CM-types for \( K_1 \) and \( K_2 \) respectively such that \( \mathcal{P}_1 | K_2 = \mathcal{P}_2 \). Then, for any CM-field \( E \) containing the reflex field of \( (K_1, \mathcal{P}_1) \),

\[ S^E \xrightarrow{\rho_{\mathcal{P}_1}} K_1 \]

commutes.

**Proof:** Let \( i : K_2^x \to K_1^x \) be the inclusion map. Then \( i \circ \mu_{\mathcal{P}_2} = \mu_{\mathcal{P}_1} \), and so \( i \circ \rho_{\mathcal{P}_2} \circ \mu^E = i \circ \mu_{\mathcal{P}_2} = \mu_{\mathcal{P}_1} \), which shows that \( i \circ \rho_{\mathcal{P}_2} = \rho_{\mathcal{P}_1} \).
§5. Definition of $\xi$

Proposition 5.1. Let $E \subseteq \mathbb{C}$ be a CM-field, Galois over $\mathbb{Q}$. Then there exists a unique homomorphism $e^E : \text{Aut}(C) \to S^E(A^f) / S^E(\mathbb{Q})$ such that, for all CM-types $(K, \pi)$ with reflex fields $E$ contained in $E$, $e^E_\pi(\tau) = \rho^\pi_\pi(e(\tau))$.

Proof: The existence of $e^E$ will be shown in §7 and §8. The uniqueness follows from (6.7). For this shows that there is an injection $\xi \to \prod \mathbf{T}_\pi$ where $\mathbf{T}_\pi = \text{Res}_{E/\mathbb{Q}} \mathbb{G}_m$ and the product is over all CM-types on $E$. Thus $S^E(A^f) / S^E(\mathbb{Q}) \to \prod \mathbf{T}_\pi(A^f)/\mathbb{Q} = \prod \mathbf{A}^f_{E}/E^f$, and so any element $\alpha \in S^E(A^f) / S^E(\mathbb{Q})$ is determined by the set $\rho^\pi_\pi(\alpha)$.

Proposition 5.2. The family of maps $e^E : \text{Aut}(C) \to S^E(A^f) / S^E(\mathbb{Q})$

have the following properties:

(a) $e^E(\sigma \tau) = e^E(\sigma)^{e^E(\tau)}$, $\sigma, \tau \in \text{Aut}(E)$;

(b) if $E_1 \subseteq E_2$, then $\text{Aut}(C) \xrightarrow{e^E_{E_1}} S^{E_1}(A^f) / S^{E_1}(\mathbb{Q})$ commutes;

(c) $e^E(1) = 1$;

(d) $e^E(\tau) \cdot e^E(\tau) = 1$, $\tau \in \text{Aut}(E)$;

(e) $e^E : \text{Aut}(C/E) \to S^E(A^f) / S^E(\mathbb{Q})$

Proof: We have to check that $\rho^\pi_\pi(e(\sigma \tau)) = \rho^\pi_\pi(e(\tau)^{e^E(\sigma)} \cdot e(\tau))$, for all $(K, \pi)$. 


But \( \rho \circ (\mathcal{E}(r^2)) = \mathcal{E}(r^2) \) and \( \rho \circ (\mathcal{E}^{-1}(r), \mathcal{E}(r)) = \rho \circ (\mathcal{E}^{-1}(r), \mathcal{E}(r)) \rho \circ (\mathcal{E}(r)) \)
\[ = \mathcal{E}(r^2) \mathcal{E}(r^2) \mathcal{E}(r) = \mathcal{E}(r) \mathcal{E}(r) \mathcal{E}(r) \] Thus the equality follows from (3.4a).

(b) This follows from (4.6) and the definition of \( E \).

(c) \( \mathcal{E}(\mathcal{E}(r)) = \mathcal{E}(r) = 1 \) (by 3.4c), and so \( \mathcal{E}(r) = 1 \).

(d) Follows from (3.4d).

(e) Assume \( \tau \) fixed \( E \); then \( \tau \mathcal{E} = \mathcal{E} \) whenever \( E \) contains the reflex field of \((K, \mathcal{E})\), and so \( \rho \circ (\mathcal{E}(r)) = \mathcal{E}(r) = 1 \) by (5.2.6).

Remark 5.3. (a) Define \( \mathcal{E}(r) = \mathcal{E}(r)^{-1} \); then the maps \( \mathcal{E}(r) \) satisfy the same conditions (b), (c), (d), and (e) of (5.2) as \( E \), but (d) becomes the condition \( \mathcal{E}(r) \mathcal{E}(r) = \mathcal{E}(r^2) \). \( \mathcal{E}(r) : \mathcal{E}(r) \) is a crossed homomorphism.

(b) Condition (b) shows that \( E \) determines \( \mathcal{E}(r) \) for all \( E \). We extend the definition of \( E \) to all CM-fields \( E \) in \( \mathcal{E} \) by letting \( E = N_{E/\mathcal{E}} \mathcal{E} \). For any Galois CM-field \( E \), containing \( \mathcal{E}(r) \).

(c) Part (d) of (5.2) follows from the remaining parts, as is clear from the following diagram:

\[
\begin{array}{ccc}
\text{Aut}(\mathcal{E}) & \frac{\mathcal{E}(r)}{\mathcal{E}(r)} & \frac{\mathcal{E}(r)}{\mathcal{E}(r)} \\
\downarrow \text{N.E/\mathcal{E}} & \downarrow \text{N.E/\mathcal{E}} & \downarrow \text{N.E/\mathcal{E}} \\
\frac{\mathcal{E}(r)}{\mathcal{E}(r)} & \frac{\mathcal{E}(r)}{\mathcal{E}(r)} & \frac{\mathcal{E}(r)}{\mathcal{E}(r)}
\end{array}
\]

(we can assume \( E \) \( \neq \mathcal{E}(r) \); \( \mathcal{E}(r)^2 = \mathcal{E}(r)^2 \), \( \mathcal{E}(r)^2 = \mathcal{E}(r)^2 \)). In his (original) letter to Longlands (see 5.23) Deligne showed that the difference between the motivic Galois group and the Tannakian group.
was measured by a family of crossed homomorphisms \((c^E)\) having properties (b), (c), and (c) of (5.2). After seeing Tate's result he used the above argument to show that his map \(c^E\) had the same properties as Tate's \(d^E(x)\), viz. \(c^E(\tau) \cdot e^F(\tau) = 1\), \(c^E(\tau)^2 = 1\).
§6 Proof that $e=1$

**Proposition 6.1.** Suppose there are given crossed homomorphisms

$$ e^E : \text{Aut}(C) \rightarrow S^E(A^f) / S^E(Q) , \text{ one for each CM-field } E^c_E , \text{ such that} $$

(a) $e^E(1) = 1$, all $E$;

(b) $e^E | e^E | \text{Aut}(C/E) = 1$ ;

(c) if $E_1 \supsetneq E_2$, then $e^{E_1} : \text{Aut}(C/Q) \rightarrow S^{E_1}(A^f) / S^{E_1}(Q)$

$$ e^{E_2} \downarrow_{\text{NE, } E_2} \quad \text{commutes.} $$

Then $e^E = 1$ — i.e. $e^E(\tau) = 1$ — for all $E$.

**Proof:** Clearly it suffices to show that $e^E = 1$ for all sufficiently large $E_\tau$, in particular for those that are Galois over $Q$.

The crossed homomorphism condition is that

$$ e(\sigma \tau) = \sigma e(\tau) \cdot e(\sigma). $$

Condition (b) implies that $e^E(\tau) = e^E(\tau')$ if $\tau | E = \tau' | E$. In particular,

$$ e^E(1) = e^E(1) \text{ for all } \tau \in \text{Aut}(C). $$

Since

$$\begin{cases} e^E(\tau) = \tau e^E(1) \cdot e^E(\tau) = e^E(\tau) \\ e^E(1) = 1 e^E(1) \cdot e^E(1) = e^E(1) \end{cases}$$

we conclude that $e^E(\tau) = e^E(\tau)$.

**Lemma 6.2.** Assume that $E$ is Galois over $Q$, and let $<\tau>$ be the subgroup of $\text{Gal}(E/Q)$ generated by $\tau E$.
Lemma 6.4. Let \( \mathcal{E}_0 \) be the 
subgroup of \( \text{Gal}(E/Q) \) generated by \( \sigma \).

(a) There is an exact commutative diagram

\[
1 \to \mathbb{Q}^x \to S^E(\mathbb{Q}) \to \mu_2(E) \to \mu_2(Q) \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
1 \to A^f \to S^E(A^f) \to \mu_2(A) \to \mu_2(Q^f)
\]

where \( \mu_2(R) \) denotes the set of square roots of 1 in a ring \( R \).

(b) The canonical map

\[
H^1(\langle \sigma \rangle, S^E(\mathbb{Q})) \to H^1(\langle \sigma \rangle, S^E(A^f))
\]

is injective.

Proof: From (4.1) we obtain cohomology sequences

\[
1 \to E_0^x \to E_0^x \times \mathbb{Q} \to S^E(\mathbb{Q}) \to \mu_2(E) \to H^1(\langle \sigma \rangle, S^E(\mathbb{Q})) \to E_0^x / E_0^{x^2}
\]

It is easy to extract from this the diagram in (a). Let \( \gamma \in H^1(\langle \sigma \rangle, S^E(\mathbb{Q})) \) map to zero in \( H^1(\langle \sigma \rangle, S^E(A^f)) \). As \( E_0^x / E_0^{x^2} \to A_0^x / A_0^{x^2} \) is surjective (an element of \( E_0 \) that is a square in \( E_0/V \) for all finite primes \( v \) is a square in \( E_0 ) \), we see that \( \gamma \) is the image of \( \pm 1 \in \mu_2(Q) \). The map \( N_{E_0/Q} : \mu_2(E) \to \mu_2(Q) \) sends \( -1 \) to \( (-1)^{[E_0 : Q]} \).

If \( [E_0 : Q] \) is odd, it is surjective, and therefore \( \gamma = 0 \).

Suppose therefore that \( [E_0 : Q] \) is even, and that \( \gamma \) is the image of \(-1\). The assumption that \( \gamma \) maps to zero in \( H^1(\langle \sigma \rangle, S^E(A^f)) \) then implies that \( -1 \in \mathbb{Q}^e \) is the image of \( N : E_0 \to \mathbb{Q}^e \) for all \( v \).

But this is impossible, since for some \( l \), \([E_0/y : \mathbb{Q}_e] \) will be even for one (hence all) \( y \) dividing \( l \).
Part (b) of the lemma shows that
\[ S^E(A^f) \langle angle / S^E(Q) \langle angle = (S^E(A^f)/S^E(Q)) \langle angle \]
The condition \( e^E(\tau) = e^E(\bar{\tau}) \) shows that \( e^E \) maps into the right hand group, and we shall henceforth regard it as mapping into the left hand group.
From part (a) we can extract an exact sequence
\[ 1 \rightarrow A^f / Q^x \rightarrow S^E(A^f) \langle angle / S^E(Q) \langle angle \rightarrow \mu(E_0^f) / \mu(E_0) \rightarrow 1. \]
Now assume that \( E > Q[i] \) so that \( E = E_0[i] \). We show first that the image of \( e^E(\tau) \) in \( \mu(E_0^f) / \mu(E_0) \) is 1. Let \( \varepsilon \) represent the image; then \( \varepsilon = (\varepsilon_v) \), \( \varepsilon_v = \pm 1 \), and \( \varepsilon \) itself is defined up to sign. We shall show that, for any two primes \( v, \bar{v} \), \( \varepsilon_v = \varepsilon_{\bar{v}} \). Choose a totally real quadratic extension \( E_0' \) of \( E_0 \) in which \( v, \bar{v} \) remain prime, and let \( E' = E_0'[i] \). Let \( \varepsilon' \) represent the image of \( e^{E'}(\tau) \) in \( \mu(E_0^f) / \mu(E_0') \). Then condition (c) shows that \( N_{E_0'/E_0} \varepsilon' \) represents the image of \( e^E(\tau) \), and so \( N_{E_0'/E_0} \varepsilon = \pm \varepsilon \). But if \( v | v, \bar{v} \), then \( N_{E_0'/E_0} \varepsilon = 1 \), for \( i = 1, 2 \).
It follows that \( e^E \) factors through \( (A^f / Q^x) \). Consider
\[ E \rightarrow A^f / Q^x \rightarrow S^E(A^f) / S^E(Q) \rightarrow \mu(E_0^f) / \mu(E_0) \rightarrow 1. \]
According to (c), \( e^E(\tau) \) maps to \( e^{Q[i]}(\tau') \), which according to (d) is 1.
\( e^E(\tau) \) lies in \( A^f / Q^x \), and the map from there into \( S^{Q[i]}(A^f) / S^{Q[i]}(Q) \) is injective, thus shows that \( e^E(\tau) = 1 \).

Remark 6.7. The argument used in the benultimate paragraph of the above proof is that used by Shih [12, p.101] to complete his proof of his special case of (1.1). For the argument in the final paragraph, cf. 5.3c.
These two arguments were all that was lacking in the original version [2] of [3].
§7. Definition of $S^E$

We begin the proof of (5.1) by showing that there is a universal $f$, giving rise to the $f_S$.

Let $E \subset C$. The Weil group $W_{E/Q}$ of $E/Q$ acts on an exact commutative diagram

$$
1 \rightarrow A^x_E / E^x \rightarrow W_{E/Q} \rightarrow \text{Hom}(E, C) \rightarrow 1
\downarrow \gamma \text{rec}_E
\downarrow
1 \rightarrow \text{Sel}(E^{ab}/E) \rightarrow \text{Hom}(E^{ab}, C) \rightarrow \text{Hom}(E, C) \rightarrow 1.
$$

(see [157]). Assume that $E$ is totally complex. Then $E^x \subset E^{ab} \subset \ker(\text{rec}_E)$, and so we can divide out by this group and its image in $W_{E/Q}$ to obtain an exact commutative diagram

$$
1 \rightarrow A^x_E / E^x \rightarrow W^f_{E/Q} \rightarrow \text{Hom}(E, C) \rightarrow 1
\downarrow
1 \rightarrow \text{Sel}(E^{ab}/E) \rightarrow \text{Hom}(E^{ab}, C) \rightarrow \text{Hom}(E, C) \rightarrow 1
$$

Assume now that $E$ is a CM-field. The cocharacter $\mu^E$ is defined over $E$, and gives rise to a map $\mu^E(R) : R^{x} \rightarrow S^E(R)$ for any $E$-algebra $R$. Choose elements $w_{\sigma} \in W^f_{E/Q}$, one for each $\sigma \in \text{Gal} \circ \text{Hom}(E, C)$, such that

$$
w_{\sigma} | E = \sigma, \quad w_{\sigma} = i w_{\sigma} \quad \text{all } \sigma, \quad \text{where } i \text{ maps } z \in \text{Hom}(E^{ab}, C).
$$

(Cf. §2) Let $\tau \in \text{Aut}(C)$ and let $\tau \in W^f_{E/Q}$ such that $E \tau \subset E^{ab}$. Then $w_{\tau^*} = i w_{\sigma} \in A^x_E$, and we define

$$
f(\tau) = \prod_{\sigma \in \text{Gal} \circ \text{Hom}(E, C)} (\sigma^{-1} \mu^E) (w_{\sigma} - \tau w_{\sigma}) \bmod S^E(E^{x})
$$

Thus $f$ is a map $\text{Aut}(C) \rightarrow S^E(A^x_E) / S^E(E)$.

**Proposition 7.1.** Let $(K, \tilde{f})$ be a CM-type whose reflex field is contained in $E$, and let $T = \text{Res}_{K/Q} \text{Gal}_m$. Identify
Let $f$ denote the right hand side. Then $r_E(f') = f' f(\tau)$ (obviously), and the same argument as in the proof of (2.3) shows that $f' f' = \chi(\tau)$.

Write $i$ for the map $T(\mathbb{Q}) \to T(E)$ induced by $\mathbb{Q} \to E$; then, for any $\rho \in \text{Hom}(K, E, C)$ and $a \in T(\mathbb{Q}) = E^\times$,

$$[\rho] (i(a)) = \rho a.$$ 

Thus $i [\rho] (i (f(\tau))) = \rho [\bar{f} (\tau)] = f \rho^{-1} (\tau)$ by (2.7b). On the other hand,

$$[\rho] (\rho [\bar{f} (\tau)]) = \prod_{\sigma} [\rho] \prod_{\sigma} \rho \circ (\sigma \circ \mu E) (w_{\sigma}^{-1} \bar{\tau} w_{\sigma})$$

$$= \prod_{\sigma} \rho (\sigma \circ \mu E) (w_{\sigma}^{-1} \bar{\tau} w_{\sigma})$$

$$= \prod_{\sigma} (w_{\sigma}^{-1} \bar{\tau} w_{\sigma})$$

$$= \prod_{\sigma \text{st. } \rho \circ \mu E} w_{\sigma}^{-1} \bar{\tau} w_{\sigma}$$

$$= \prod_{\sigma \in \bar{\rho}^{-1}} w_{\sigma}^{-1} \bar{\tau} w_{\sigma}$$

$$= f \rho^{-1} (\tau).$$
Corollary 7.3. (a) \( f(\tau) \) depends only on \( E \) and \( \tau \); we have therefore defined maps \( f^E : \text{Aut}(C) \to SE(A_E^f)/SE(E) \), one for each CM-field \( E \) (below over \( \mathcal{O} \)).

(b) \( f^E(\sigma \tau) = \sigma^{-1} f^E(\sigma) f^E(\tau), \quad \sigma, \tau \in \text{Aut}(C) \);

(c) If \( E_1 \supset E_2 \), then \( \text{Aut}(C) \xrightarrow{e_{E_1}} SE_1(A_f^E)/SE_2(E_2) \) commutes;

(d) \( f^E(1) = 1 \);

(e) \( f^E(\tau)^{-1} f^E(\tau) = \omega^E(\tau) \);

(f) \( \sigma f^E(\tau) = f^E(\tau) \) for all \( \sigma \in \text{Gal}(E/\mathcal{O}) \).

Proof. (a) \( f(\tau) \) is the unique element of \( SE(A_E^f)/SE(E) \) such that \( \rho(\tau \tau) = f^E(\tau) \) for all \((K, \mathfrak{H})\). (Cf. the proof of the uniqueness of \( e^E \) in (5.1).)

(b), (c), (d), (e). These are proved as (a), (b), (c), (d) of (5.2).

(f) \( \rho(\tau \tau) = \sigma \rho(\tau \tau) = \sigma f^E(\tau) = f^E(\tau) \).

Remark 7.4. Let \( \tilde{W}_\sigma \in W_{E/\mathcal{O}}^f \) be such that
\[
\tilde{W}_\sigma |E = \sigma, \quad \tilde{W}_\sigma^{-1} = \tilde{W}_\sigma^{-1}.
\]

Then \([6, 9, 2.9] \), \( \tilde{b}(\tau) \) is defined by
\[
\tilde{b}(\tau) = \prod_{\tau \in \text{Gal}(E/\mathcal{O})} \sigma \mu^E(\tilde{W}_\sigma^{-1} \tilde{W}_\sigma^{-1}) \pmod{SE(E)}.
\]

Let \( W_\sigma = \tilde{W}_\sigma^{-1} \); then \( W_\sigma |E = \sigma \) and \( W_\sigma^{-1} = \tilde{W}_\sigma^{-1} \); moreover
\[
\tilde{b}(\tau^{-1})^{-1} = \prod_{\tau \in \text{Gal}(E/\mathcal{O})} \sigma \mu^E(W_\sigma^{-1} \tilde{W}_\sigma^{-1}) = f^E(\tau).
\]

Thus, in the notation of \([9, 2.9] \), \( f^E(\tau) = \tilde{b}(\tau) \).
Definition of $g^E$

We complete the proof of (5.1) by showing that there is a universal $g$ giving rise to all $g^E$.

Proposition 8.1. Let $E \subseteq \mathbb{C}$ be a CM-field. There exists a unique map $g^E : \text{Aut}(E) \to S^E(\mathbb{A}_E^f) / S^E(E)$ with the following property: for any CM-type $(K, \Phi)$ whose reflex field is contained in $E$,

$$g^E(\rho_E^f(\tau)) = g_K^f(\tau)$$

in $T(\mathbb{A}_E^f) / T(E)$, where $T = \text{Res}_{K/\mathbb{Q}} \mathbb{G}_m$.

Proof: The uniqueness follows from (4.7). For the existence we need the notion of a Hodge cycle.

For any variety $X$ over $\mathbb{C}$, write $H^\cdot(X, \mathbb{Q})(r) = H^\cdot(X, (2\pi i)^r \mathbb{Q})$ (cohomology with respect to the complex topology). A Hodge cycle on $A$ is an element $s \in H^p(A^k, \mathbb{Q})(r)$, some $p, k$, that is of type $(p, p)$, i.e., under the embedding $(2\pi i)^r \mathbb{Q} \hookrightarrow \mathbb{C}$, $s$ maps into $H^{p, p} \subset H^{p, p}(X, \mathbb{C})$. Recall that $H^\cdot(A^k, \mathbb{Q}) = \bigoplus H^\cdot(A, \mathbb{Q})^\vee$, and so $GL(H(A, \mathbb{Q}))$ acts by transport of structure on $H^\cdot(A^k, \mathbb{Q})$. The Mumford-Tate group $MT(A)$ of $A$ is the largest $\mathbb{Q}$-rational algebraic subgroup of $GL(H(A, \mathbb{Q}))$ such that

$$MT(A) \mathbb{Q} = \{ g \in GL(H(A, \mathbb{Q})) \mid g \alpha s = \alpha^r g \text{ for all } s \in D(A)^s \}.$$  

For any Hodge cycle $s$ on $A$ (of type $(p, p)$),

Lemma 8.2. Assume $A$ is of CM-type $(K, \Phi)$, where the reflex field of $(K, \Phi)$ is contained in $E$. Then the image of $\rho_E^f : S^E \to K^\times \subset GL(H(A, \mathbb{Q}))$ is equal to $MT(A)$.

Proof. Cf. [4, 3.4.3].
With $H^{2p}(A^k, A^f)(p) = H^{2p}(A^k, \mathbb{Q})(p) \otimes \mathbb{A}^f$. Then there is a canonical isomorphism

$$H^{2p}(A^k, A^f)(p) \cong A^k \left( \bigoplus V^f(\mathbb{A})^\vee \right)$$

and so the action of $\mathfrak{g} \cdot \text{Aut}(\mathbb{C})$ on $V^f(\mathbb{A})$ gives rise to an action on $H^{2p}(A^k, A^f)(p)$. We shall need to use the following important result of Deligne.

**Theorem 8.3.** Let $s \in H^{2p}(A^k, \mathbb{Q})(p)$ be a Hodge cycle in $A$, and let $s^\tau$ be the image of $s$ in $H^{2p}(A^k, A^f)(p)$; then for any $\tau \in \text{Aut}(\mathbb{C})$ there exists a Hodge cycle $s$, on $\tau A$ whose image in $H^{2p}(A^k, A^f)(p)$ is $\tau s$.

**Proof:** See [1, 43]

The cycle $s$, of the theorem will be written $\tau s$.

**Proposition 8.4.** With the notations of (8.2), there exists a linear isomorphism $\varphi : H^1(A, E) \cong H^1(\tau A, E)$ such that $\varphi(s) = \varphi(x) \otimes \tau(s)$, for all Hodge cycles $s$ on $A$ (of type $(p, p)$).

**Proof:** For any $\mathbb{Q}$-algebra $R$, let $P(R) = \{ x : H^1(A, R) \rightarrow H^1(\tau A, R) | \varphi(s) = \varphi(x) \otimes \tau(s) \}$, all $s$.

Then $P(R)$ is either empty or is a principal homogeneous space over $MT(A)(R)$. Thus $P$ is either the empty scheme or is a torsor for $MT(A)$. The existence of $\tau : H^1(A, A^f) \rightarrow H^1(A^k)$ in $P(\mathbb{A})$ shows that $P$ is a torsor. It therefore corresponds to an element of $H^1(\mathbb{Q}, MT(A))$. But $MT(A) \cong \mathbb{G}_m \times \cdots \times \mathbb{G}_m$, and so $H^1(\mathbb{Q}, MT(A)) = 0$ by Hilbert's theorem 90.

Both (8.2) and (8.4) obviously also apply to products of
abelian varieties of CM-type. Let $A = \prod A_{\varphi}$, where $\varphi$ runs through the CM-types on $E$ and $A_{\varphi}$ is a type $(E, \varphi)$. Then $\rho : S^E \rightarrow MT(A)$. Choose $a \in (7.4)$. Then

$$V^f(A) \otimes E \rightarrow V^f(A) \otimes E \xrightarrow{(\otimes 1)} V^f(A) \otimes E$$

as an $A_{\varphi}$-linear isomorphism and sends a Hodge cycle of type $(p, p)$ to $\otimes s$, some $s \in A_{\varphi}^{\times}$. Therefore it is multiplication by an element $\otimes 1 \in MT(A)(A_{\varphi}) = S^E(A_{\varphi})$. The class $\otimes 1$ of $\otimes 1$ in $S^E(A_{\varphi})/S^E(E)$ has the properties required for (7.1).

The map $g : \text{Aut}(C) \rightarrow S^E(A_{\varphi})/S^E(E)$ has the same properties as those listed for $f$ in (7.3). In particular, $g(\tau)$ is fixed by $\text{Gal}(E/Q)$. Let $\tau(\tau) = g(\tau)/f(\tau)$.

Then $e(\tau) \in S^E(A_{\varphi})/S^E(E)$, and it remains to show that it lies in $S^E(A_{\varphi})/S^E(Q)$.

**Proposition 8.5.** $e(\tau)$ lies in $S^E(A_{\varphi})/S^E(Q)$.

**Proof.** There is a cohomology sequence

$$0 \rightarrow S^E(Q) \rightarrow S^E(A_{\varphi}) \rightarrow (S^E(A_{\varphi})/S^E(E)) \xrightarrow{\text{Gal}(E/Q)} H^1(Q, S^E).$$

Thus we have to show that the image of $e(\tau)$ in $H^1(Q, S^E)$ is zero. But $H^1(Q, S^E) \rightarrow H^1(Q, S^E)$, as follows easily from (4.1), and the image of $e(\tau)$ in $H^1(Q, S^E)$ is obviously zero for all finite $H$. It remains to check that the class $\otimes 1$ of $\otimes 1$ in $H^1(Q, S^E)$ is zero. Let

$$T = \{ a \in \prod E^x \mid a \otimes \in Q^{x} \text{ for some } \varphi \}$$

be the torsion over $Q$. Then
Lemma 8.6. The image of $a$ in $H^1(\Phi, T)$ is zero.

Proof: In the proof (3.6), it is shown that the image of $a$ in $T(A_{\phi}^g) / T(E)$ lifts to an element $s \in T(A_{\phi}^{g_0})$. The image of $a$ in $H^1(\Phi, T)$ is represented by the cocycle $c \mapsto s \Phi - e = 0$.

Lemma 8.7. The map $\Phi : H^1(\mathbb{R}, S^F) \to H^1(\mathbb{R}, T)$ is injective.

Proof: There is a commutative diagram:

\[
\begin{array}{ccc}
1 & \to & SMT(N) & \to & MT(N) & \to & \mathbb{G}_m & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \to & ST & \to & T & \to & \mathbb{G}_m & \to & 1 \\
\end{array}
\]

exact. (Here $A = \prod A_{\phi}$. The diagram gives rise to an exact commutative diagram:

\[
\begin{array}{ccc}
\mathbb{R}^x & \to & H^1(\mathbb{R}, SMT) & \to & H^1(\mathbb{R}, MT) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{R}^x & \to & H^1(\mathbb{R}, ST) & \to & H^1(\mathbb{R}, T) & \to & 0 \\
\end{array}
\]

Note that $ST$ (and hence $SMT$) is an isomorphism over $\mathbb{R}$; hence, $H^1(\mathbb{R}, SMT) = SMT(C)$ and $H^1(\mathbb{R}, ST) = ST(C)$, and so $H^1(\mathbb{R}, SMT) \to H^1(\mathbb{R}, ST)$. The five-lemma now completes the proof.

(See also [10, §5].)

Remark 8.8. It seems to be essential to make use of Hodge cycles, and consequently Shimura varieties (which are used in the proof of 8.3) in order to show the $c_{\phi}(e)$ have the correct functorial properties. Note that Shih [12] also needed to use Shimura varieties to prove his case of the theorem.
§9 Re-statement of the theorem

The following statement of the main theorem of complex multiplication first appeared (as a conjecture) in Milne-Shih [83].

Theorem 9.1. Let $A$ be an abelian variety of CM-type $(K, \mathfrak{f})$; let $\tau \in \text{Aut}(E)$, and let $f \notin F(\tau)$. Then

(a) $\tau A$ is of type $(K, \mathfrak{f})$;
(b) there is a $K$-linear isomorphism $\alpha : H_1(A, E) \to H_1(\tau A, E)$,

where $E$ is the reflex field of $(K, \mathfrak{f})$, such that

(i) $\alpha(s) = v(\alpha)^p \tau(s)$, for all Hodge cycles $s$ in $A$,

(ii) $v_f(A) \otimes E \xrightarrow{\rho_{\mathfrak{f}}(\tau)} v_f(A) \otimes E$

commutes.

Proof. The theorem is true (by definition) if $s(\tau)$ is replaced by $\tilde{g}(\tau)$, but we have shown that $g(\tau) = f(\tau)$.

Remark 9.2. Let $T$ be a torus such that

$MT(A) \subset T \subset \mathfrak{g} \subset K^x | a.a \in \mathfrak{g}^x$.

Then the Shimura variety $SH(T, \mathfrak{g})$ is, in a natural way, a moduli scheme, and the (new) main theorem of complex multiplication gives a description of the action of $\text{Aut}(E)$ on $SH(T, \mathfrak{g})$ (see [10, §6]).

Remark 9.3. Out of his study of the zeta functions of Shimura varieties, Langlands [563] was led to
a conjecture concerning the conjugates of Shimura varieties. The conjecture is trivial for the Shimura varieties associated with tori, but in [10] it is shown that for groups of symplectic similitudes the conjecture is equivalent to (9.1). It is also shown in [10] that the validity of the conjecture for \( \operatorname{Sh}(G, X) \), a Shimura variety, depends only on \( (G^\text{der}, X) \). Thus, similar methods to those used in [13] can be used to prove Langlands's conjecture for exactly those Shimura varieties for which Shimura's conjecture is proved in [13].
§10 The Zariski $G$-group

By an extension $\varpi : \text{Gal}(\overline{Q}/Q) \to S^E$ with finite-adic splitting, we mean an exact sequence

$$1 \to S^E \to T_E \xrightarrow{\pi^E} \text{Gal}(\overline{Q}/Q) \to 1$$

of prof-algebraic groups over $Q$ ($\text{Gal}(\overline{Q}/Q)$ is to be regarded as a constant prof-algebraic group) together with a continuous homomorphism $\varpi : \text{Gal}(\overline{Q}/Q) \to T_E(A^f)_E$ such that $\varpi \cdot \pi^E = \text{id}$.

We always assume that the action of $\text{Gal}(\overline{Q}/Q)$ on $S^E$ given by the extension is the natural action.

**Proposition 10.1.** (a) Let $(T_E, \varpi^E)$ be an extension of $\text{Gal}(\overline{Q}/Q)$ by $S^E$ with finite-adic splitting. Choose a section $a^E : \text{Gal}(\overline{Q}/Q) \to (T_E)_E$ that is a morphism of prof-algebraic groups. Define $h(\tau) \in S^E(A^f_E) / S^F(E)$ to be the class of $\varpi(\tau) \cdot a^E(\tau)^{-1}$.

1. $h(\tau)$ is well-defined;
2. $\sigma \cdot h(\tau) = h(\tau) \cdot \sigma \in S^E(E/Q)$;
3. $h(\tau_1 \cdot \tau_2) = h(\tau_1) \cdot h(\tau_2)$, $\tau_1, \tau_2 \in \text{Gal}(\overline{Q}/Q)$;
4. $h$ lifts to a continuous map $h' : \text{Gal}(\overline{Q}/Q) \to S^E(A^f_E)$ such that the map $(\tau_1, \tau_2) \mapsto d_{\tau_1, \tau_2}^{f_{\ref{5b}}} = h'(\tau_2)^* \cdot h'(\tau_1)^{-1}$ is locally constant.

(b) Let $h : \text{Gal}(\overline{Q}/Q) \to S^E(A^f_E) / S^E(E)$ be a map satisfying conditions (1), (3), (iii), (iv); then $h$ arises from a unique extension of $\text{Gal}(\overline{Q}/Q)$ by $S^E$ with finite-adic splitting.

**Proof.** Easy; see [9, §52].
Let $S = \lim_{\rightarrow} S^E$, where $E$ runs through the CM-fields $E \subset E$ that are Galois over $Q$. By an extension of $\text{Gal}(\overline{Q}/Q)$ by $S$, we mean a projective system of extensions of $\text{Gal}(\overline{Q}/Q)$ by $S^E$ with finitely-adic splitting, i.e., a family

$$
1 \rightarrow S^{E_1} \rightarrow T^{E_1} \rightarrow \text{Gal}(\overline{Q}/Q) \rightarrow 1
$$

$$
\downarrow N_{E_1/E_2} \quad \downarrow N_{E_1/E_2} \quad \parallel
$$

$$
1 \rightarrow S^{E_2} \rightarrow T^{E_2} \rightarrow \text{Gal}(\overline{Q}/Q) \rightarrow 1
$$

of commutative diagrams.

**Theorem 10.2.** Let $T_1$ and $T_2$ be two extensions of $S^E \subset \text{Gal}(\overline{Q}/Q)$ by $S$ with finitely-adic splittings. Assume,

(a) For each $E$, and $i=1, 2$, there exists a commutative diagram

$$
1 \rightarrow S^{E} \rightarrow E^{T_i \subset E} \rightarrow \text{Gal}(\overline{Q}/E) \rightarrow 1
$$

$$
\parallel \quad \downarrow \quad \parallel
$$

$$
1 \rightarrow S^{E} \rightarrow M^{E} \rightarrow \text{Gal}(\overline{Q}/E) \rightarrow 1
$$

compatible with the finitely-adic splittings, where $T^{E}_{\leftarrow E}$ is the inverse image of $\text{Gal}(\overline{Q}/E)$ in $T^{E}$, and the lower row is the extension constructed in [IV, II].

(b) For each $i \in \text{Gal}(\overline{Q}/Q)$, $\pi^{-1}_i(\tau) \cong \pi^{-1}_i(\tau)$ on $S^{E}$.
(c) $s_p^E(i) \in T_i^E(\overline{Q}/Q)$, $i = 1, 2$.

Then there is a unique family of isomorphisms $\phi^E: T_i^E \rightarrow T_2^E$ making the following diagrams commute:

\[
\begin{array}{ccc}
1 & \rightarrow & S^E \\
\downarrow & & \downarrow \\
1 & \rightarrow & S^E \\
\end{array}
\quad
\begin{array}{ccc}
T_i^E & \rightarrow & \text{Gal}(\overline{Q}/Q) \\
\downarrow \phi^E & & \downarrow \phi^E \\
T_2^E & \rightarrow & \text{Gal}(\overline{Q}/Q) \\
\end{array}
\]

Proof: Let $(h_1^E)$ and $(h_2^E)$ be the families of maps corresponding as in (10.1a) to $T_1$ and $T_2$. The hypotheses of the theorem imply that $\phi^E$ the families $(c^E)$, where $c^E = h_1^E / h_2^E$, satisfy the hypotheses of (6.1). Thus $h_1^E = h_2^E$ for all $E$, and we apply (10.1b).

**Definition 10.3.** The extension corresponding to the family of maps $(\phi^E)$ defined in (7.3) is called the Zariski theory.

**Remark 10.4.** In [3] Deligne proves the following:

(a) Let $\mathcal{M}$ be the group associated with the Zariski category of motives over $\mathbb{Q}$ generated by Artin motives and
abelian varieties of potential CM-type; then $M$ is an extension of $\text{Gal}(\bar{Q}/Q)$ by $S$ with finite-adélic splitting in the sense defined above. (From a more naive point of view, $M$ is the extension defined by the mate $(q^E)$ of $q$.)

(b) Theorem (10.2), by essentially the same argument as we have given in §6, except expressed directly in terms of the extensions rather than the cocycles.

These two results combined to show that the motivic Galois group is isomorphic to the explicitly constructed Taniyama group (as extensions...). This can be regarded as another statement of the (new) mean theorem of complex multiplication.

Note however that without the Taniyama group, Deligne's results say very little. This is why I have included Langlands as one of the main contributors to the proof of (1.1), even though he never explicitly considered abelian varieties with complex multiplication! (and neither he nor Deligne explicitly considered a statement like (1.1)).
Lemma 11.1. There exists a commutative diagram

\[
\begin{array}{ccc}
T^E(C) & \xrightarrow{\rho \circ \sp_E} & W_{E/\mathbb{Q}} \\
\uparrow & & \downarrow \\
T^E(\mathbb{Q}) & \longrightarrow & \Gal(\overline{\mathbb{Q}}/\mathbb{Q})
\end{array}
\]

where \( W_{E/\mathbb{Q}} \) is the Weil group of \( E \) and \( T^E \) is the Tamagawa group.

Proof: easy; see \([9, 317]\).

Theorem 11.2. Let \( A \) be an abelian variety over \( \mathbb{Q} \) of potential CM-type \((K, \mathfrak{f})\). Let \( E \) be a CM-field containing the reflex field of \((K, \mathfrak{f})\). Then there exists a representation \( \rho : T^E \rightarrow \Aut(H^1(A_{\mathbb{C}}, \mathbb{Q})) \Aut(H_1(A_{\mathbb{C}}, \mathbb{Q})) \) such that

1. \( \rho \circ \sp^E = \Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \Aut(V^f(A)) \)

which describes the action of \( \Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \) on \( V^f(A) \);

2. \( L(s, A/\mathbb{Q}) = L(s, \rho_{\alpha}) \) where \( \rho_{\alpha} = \rho \circ \sp^E_{\alpha} \) is a complex representation of \( W_E \).

Proof: The existence of \( \rho \) is obvious from the interpretation of \( T^E \) as the motive Galois group \( M \) (see 10.4a) or, more
Remark 11.3. The proof of (11.2) does not require the full strength of Deligne's results, and in fact is proved by Deligne in [27]. Subsequently, Yoshida [165] found another proof that $L(s, A/Q) = L(s, \rho_\infty)$ for some complex representation $\rho_\infty$ of $W_d$. When $\text{Gal} (\overline{Q}/Q)$ stabilizes $K < \text{End}(A) \otimes Q$, this last result was proved independently by Miedema [173] (all forms) and Shimura [147] (good forms only).
References


2. ——: Letter to Langlands 10 April 1979

3. ——: Motifs et groupe de Taniyama (Completion of E23) To appear in [53]

4. —— (Notes by J.S. Milne): Hodge cycles on abelian varieties. To appear in [53]


6. Langlands: Corvallis 1977

7. Milne: Inventiones 17 (1972) 177-190


11. Serre: Linear Representations, Benjamin


14. ——: Annals 94 (1971) 504-533

15. Tate: On congruence of abelian varieties of CM-type. Ma 8 pp 10 April 1971