Abelian Varieties with Complex Multiplication (for Pedestrians)

J. S. Milne

The main theorem of Shimura and Taniyama (see [13, Thm 5.15]) describes the action of an automorphism τ of $\mathbb{C}$ on an abelian variety of CM-type and its torsion points in the case that τ fixes the reflex field of the variety. In his Corvallis article [6], Langlands made a conjecture concerning conjugates of Shimura varieties that (see [8]) leads to a conjectural description of the action of τ on the variety and its torsion points for <u>all</u> τ. Recently (July, 1981) Deligne proved this conjecture (see [3]). Deligne expresses his result as an identity between two pro-reductive groups, the Taniyama group of Langlands 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]) gave a more down-to-earth conjecture than that stated in [8] and partially proved his conjecture.

The purpose of these notes is to use Deligne's ideas to give as direct a proof as possible of the conjecture in the form stated by Tate. It is also ~~shown~~ checked that the three forms of the conjecture, those in [3], [8], and [15], are compatible. Also, Tate's ideas are used to simplify the construction of the Taniyama group. In the first three sections I have followed Tate's manuscript [15] very closely, sometimes word-for-word.

These notes are a rough write-up of two of my lectures at the conference on Shimura Varieties, Vancouver, 17–25 Aug 1981. In 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 conjugates of Shimura varieties for most (perhaps all) Shimura varieties.

<u>Notation</u>: $\mathrm{rec}_E : \mathbb{A}_E^\times \longrightarrow \mathrm{Gal}(E^{ab}/E)$ is normalised so that a uniformizing parameter corresponds to the inverse of the usual (arithmetic) Frobenius. When E is totally complex, rec_E factors into $\mathbb{A}_E^\times \longrightarrow \mathbb{A}_E^{f\times}/E^\times \xrightarrow{r_E} \mathrm{Gal}(E^{ab}/E)$.

$\chi : \mathrm{Aut}(\mathbb{C}) \longrightarrow \mathbb{A}^{f\times}$ is defined by $\tau\zeta = \zeta^{\chi(\tau)}$, $\zeta^N = 1$.

$\left.\right\}\ r_E \circ \chi = V_{E/\mathbb{Q}}$

$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$, $\mathbb{A}^f = \hat{\mathbb{Z}} \otimes \mathbb{Q}$, $\mathbb{A}_E^f = \mathbb{A}^f \otimes E$, $\mathbb{A}_E = \mathbb{A}_E^f \times (E \otimes \mathbb{R})$.

ι (iota) = complex conjugation.

If $E \subset \mathbb{C}$, then E^{ab} and $\bar{E}$ are closures in $\mathbb{C}$

If T is a torus $/E$, $X_*(T) = \mathrm{Hom}_{\bar{E}}(\mathbb{G}_m, T)$.

Be wary of the signs!

§1 Statement of the theorem

Let A be an abelian variety over $\mathbb{C}$, and let K be a subfield of $\mathrm{End}(A) \otimes \mathbb{Q}$ 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 1 over K.) The representation of K on the tangent space to A at zero is of the form $\bigoplus_{\phi \in \Phi} \phi$ with Φ a subset of $\mathrm{Hom}(K, \mathbb{C})$. The pair (K, Φ) is a CM-type, i.e., K is a CM-field and $\mathrm{Hom}(K, \mathbb{C}) = \Phi \cup \iota\Phi$.

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

$$(x, y) \longmapsto \psi(x, iy) \; : \; H_1(A, \mathbb{R}) \times H_1(A, \mathbb{R}) \longrightarrow \mathbb{R}$$

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

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

a Riemann form with this property always exists.

Let $\mathbb{C}^{\Phi}$ be the set of complex-valued functions on Φ and embed K into $\mathbb{C}^{\Phi}$ through the natural map $a \longmapsto (\phi(a), \dots)_{\phi \in \Phi}$; let $R = K \cap \mathrm{End}(A)$. There then exist a $\mathbb{Z}$-lattice $\mathfrak{a}$ in K stable under R, an element $t \in K^{\times}$, and an R-linear analytic isomorphism $\theta : \mathbb{C}^{\Phi}/\mathfrak{a} \xrightarrow{\approx} A$ such that $\psi(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(t\, x \cdot \iota y)$ where, in the last equation, we have used θ to identify $H_1(A, \mathbb{Q})$ ~~$\mathfrak{a} \otimes \mathbb{Q}$ with~~ with $\mathfrak{a} \otimes \mathbb{Q} = K$. The variety is said to be of type $(K, \Phi; \mathfrak{a}, t)$ relative to θ. The type determines the triple $(A, K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}, \psi)$ up to isomorphism. Conversely, the triple determines the type up to a change of the following form: if θ is replaced by $\theta \circ a^{-1}$, $a \in K^\times$, then the type becomes $(K, \Phi; a\mathfrak{a}, t/a.\iota a)$.

Let $\tau \in \mathrm{Aut}(\mathbb{C})$. Then $K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ induces a map $K \hookrightarrow \mathrm{End}(\tau A) \otimes \mathbb{Q}$, so that τA also has complex multiplication by K. The form ψ is associated with a divisor D on A, and we let $\tau\psi$ be the Riemann form for τA associated with τD. It has the following characterization: after multiplying ψ with a nonzero rational number, we can assume that it takes integral values on $H_1(A, \mathbb{Z})$; define ψ_m to be the pairing $A_m \times A_m \to \mu_m$, $(x, y) \longmapsto \exp(2\pi i \psi(x,y)/m)$; 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, Φ) a map $f_\Phi : \mathrm{Aut}(\mathbb{C}) \longrightarrow \mathbb{A}_K^{f\times}/K^\times$ such that $f_\Phi(\tau).\iota f_\Phi(\tau) = \chi(\tau) K^\times$, all $\tau \in \mathrm{Aut}(\mathbb{C})$. We can now state the new main theorem of complex multiplication in the form first appearing (as a conjecture) in Tate [15].

<u>Theorem</u> 1.1 (Shimura, Taniyama, Langlands, Deligne). Suppose A has type $(K, \Phi; \mathfrak{a}, t)$ relative to $\theta : \mathbb{C}^\Phi/\mathfrak{a} \xrightarrow{\approx} A$. Let $\tau \in \mathrm{Aut}(\mathbb{C})$ and let $f \in \mathbb{A}_K^{f\times}$ lie in $f_\Phi(\tau)$.

(a) The variety τA has type $(K, \tau\Phi; f\mathfrak{a}, t\chi(\tau)/f.\iota f)$ relative to θ' say.

(b) It is possible to choose θ' so that

$$\begin{tikzcd}
\mathbb{A}_K^f \arrow[r] \arrow[d, "f"] & \mathbb{A}_K^f/\mathfrak{a} \otimes \hat{\mathbb{Z}} = K/\mathfrak{a} \arrow[r, "\theta"] & A_{tors} \arrow[d] \\
\mathbb{A}_K^f \arrow[r] & \mathbb{A}_K^f/f\mathfrak{a} \otimes \hat{\mathbb{Z}} = K/f\mathfrak{a} \arrow[r, "\theta'"] & \tau A_{tors}
\end{tikzcd}$$

commutes, where A_{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 τ fixes the reflex field of (K, Φ) then the theorem becomes the old main theorem of complex multiplication, proved by Shimura and Taniyama (see (2.8) below). This case is used in the proof of the general result.

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

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

We now ~~restate~~ restate the theorem in more invariant form. Let

$$TA \overset{df}{=} \varprojlim A_m = \varprojlim \left(\tfrac{1}{m} H_1(A,\mathbb{Z})/H_1(A,\mathbb{Z})\right) = H_1(A, \hat{\mathbb{Z}}),$$

and let $V^f A = TA \otimes \mathbb{Q} = H_1(A, \mathbb{Q}) \otimes \mathbb{A}^f$. Then ψ gives rise to a pairing

$$\psi^f = \varprojlim \psi_m : V^f A \times V^f A \longrightarrow \mathbb{Q}_\ell(1)$$

where $\mathbb{Q}_\ell(1) = (\varprojlim \mu_m(\mathbb{C})) \otimes \mathbb{Q}$.

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

(a) τA is of type $(K, \tau\Phi)$;

(b) there is a K-linear isomorphism $\alpha : H_1(A,\mathbb{Q}) \longrightarrow H_1(\tau A, \mathbb{Q})$ such that

(i) $\psi\left(\frac{\chi(\tau)}{f.\iota f}\, x, y\right) = \tau\psi(\alpha x, \alpha y)$, $\quad x, y \in H_1(A,\mathbb{Q})$;

(ii)
$$\begin{tikzcd} V^f(A) \arrow[r, "f"] \arrow[dr, "\tau"'] & V^f(A) \arrow[d, "\alpha\otimes 1"] \\ & V^f(\tau A) \end{tikzcd}$$

commutes.

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

Proof: Let θ and θ' be as in (1.1), and let $\theta_1 : K \xrightarrow{\approx} H_1(A,\mathbb{Q})$ and $\theta_1' : K \xrightarrow{\approx} H_1(\tau A, \mathbb{Q})$ be the maps induced by θ and θ'. Then

$$\psi(\theta_1(x), \theta_1(y)) = Tr(t x . \iota y)$$

$$\tau\psi(\theta_1'(x), \theta_1'(y)) = Tr(t\chi x.\iota y) \quad \text{where} \quad \chi = \chi(\tau)/f.\iota f$$

and

$$\begin{tikzcd} \mathbb{A}^f_K \arrow[r, "\theta_1"] \arrow[d, "f"] & V^f(A) \arrow[d, "\tau"] \\ \mathbb{A}^f_K \arrow[r, "\theta_1'"] & V^f(\tau A) \end{tikzcd}$$

commutes. Let $\alpha = \theta_1' \circ \theta_1^{-1}$; then

$$\tau\psi(\alpha x, \alpha y) = Tr(t\chi\, \theta_1^{-1}(x) . \iota\theta_1^{-1}(y)) = \psi(\chi x, y)$$

and

$$\tau = \theta_1' \circ f \circ \theta_1^{-1} = \theta_1' \circ \theta_1^{-1} \circ f = \alpha \circ f .$$

Conversely, let α be as in (1.3) and choose θ_1' so that $\alpha = \theta_1' \circ \theta_1^{-1}$. It is then easy to check (1.1).

§2 Definition of $f_\Phi(\tau)$.

Let (K,Φ) 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 $w_\rho \in \mathrm{Aut}(\mathbb{C})$, one for each $\rho \in \mathrm{Hom}(K,\mathbb{C})$, such that

(Better, choose w_ρ to e. line ρ

$$w_\rho \circ i \,|\, K = \rho \quad , \quad w_{\iota\rho} = \iota w_\rho .$$

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

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

<u>Lemma</u> 2.1. F_Φ is independent of the choice of $\{w_\rho\}$.

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

<u>Lemma</u> 2.2. F_Φ is independent of the choice of i (and $K \hookrightarrow \mathbb{C}$).

<u>Proof</u>: Any other choice is of the form $i' = \sigma \circ i$, $\sigma \in \mathrm{Aut}(\mathbb{C})$. Take $w'_\rho = w_\rho \circ \sigma^{-1}$, and then

$$F'_\Phi(\tau) = \prod i'^{-1} \circ (\sigma w_{\tau\phi}^{-1}\, \tau\, w_\phi\, \sigma^{-1}) \circ i' = F_\Phi(\tau).$$

Thus we can suppose $K \subset \mathbb{C}$ and ignore i; then

$$F_\Phi(\tau) = \prod_{\phi\in\Phi} w_{\tau\phi}^{-1}\,\tau\, w_\phi \qquad \text{mod } \mathrm{Aut}(\mathbb{C}/K^{ab}).$$

<u>Proposition</u> 2.3. For any $\tau\in\mathrm{Aut}(\mathbb{C})$, there is a unique $f_\Phi(\tau)\in\mathbb{A}_K^{f\times}/K^\times$ such that

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

(b) $f_\Phi(\tau).\iota f_\Phi(\tau) = \chi(\tau)K^\times$.

<u>Proof</u>: Since r_K is surjective, there is an $f\in\mathbb{A}_K^{f\times}/K^\times$ such that $r_K(f) = F_\Phi(\tau)$. We have

$$\begin{aligned} r_K(f.\iota f) = r_K(f).r_K(\iota f) &= r_K(f).\iota r_K(f)\iota^{-1} \\ &= F_\Phi(\tau).F_{\iota\Phi}(\tau) \\ &= V_{K/\mathbb{Q}}(\tau), \end{aligned}$$

where $V_{K/\mathbb{Q}}: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})^{ab}\longrightarrow\mathrm{Gal}(\bar{\mathbb{Q}}/K)^{ab}$ is the transfer (Verlagerung) map. As $V_{K/\mathbb{Q}} = r_K\circ\chi$ it follows that $f.\iota f = \chi(\tau)K^\times \bmod (\mathrm{Ker}\, r_K)$. The next lemma shows that $1+\iota$ acts bijectively on $\mathrm{Ker}(r_K)$, and so there is a unique $a\in\mathrm{Ker}\, r_K$ such that $a.\iota a = (f.\iota f/\chi(\tau))K^\times$; we must take $f_\Phi(\tau) = f/a$.

<u>Lemma</u> 2.4. $\mathrm{Ker}(r_K: \mathbb{A}_K^{f\times}/K^\times\longrightarrow\mathrm{Gal}(K^{ab}/K))$ is uniquely divisible by all integers, and its elements are fixed by ι.

<u>Proof</u>: The kernel of r_K is $\bar{K}^\times/K^\times$ where $\bar{K}^\times$ is the closure of $K^\times$ in $\mathbb{A}_K^{f\times}$. It is also equal to $\bar{U}/U$ for any subgroup U of $O_K^\times$ of finite index. A theorem of Chevalley (see [~~K~~, 3.5])

Serre, Izv. Akad. Nauk SSSR 28 (1964) 3-20 shows that $\mathbb{A}_K^{f\times}$ induces the pro-finite topology on U. If we take U to be contained in the real subfield of K and torsion-free, then it is clear that $\bar{U}/U$ is fixed by ι and (being isomorphic to $(\hat{\mathbb{Z}}/\mathbb{Z})^{\dim(A)}$) uniquely divisible.

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

<u>Proposition</u> 2.7. The maps $f_\Phi : \mathrm{Aut}(\mathbb{C}) \longrightarrow \mathbb{A}^{f\times}/K^\times$ have the following properties:

(a) $f_\Phi(\sigma\tau) = f_{\tau\Phi}(\sigma)\, f_\Phi(\tau)$;

(b) $f_{\Phi(\tau^{-1}|K)}(\sigma) = \tau f_\Phi(\sigma) \quad$ if $\tau K = K$;

(c) $f_\Phi(\iota) = 1$.

<u>Proof</u>: Let $f = f_{\tau\Phi}(\sigma)\, f_\Phi(\tau)$. Then

$$r_K(f) = F_{\tau\Phi}(\sigma)\, F_\Phi(\sigma) = \prod_{\phi\in\Phi} w_{\sigma\tau\phi}^{-1}\, \sigma w_{\tau\phi}\, w_{\tau\phi}^{-1}\, \tau w_\phi = \overset{F_\Phi(\sigma\tau)}{\cancel{r_K(f_\Phi(\sigma\tau))}}.$$

and $f \cdot \iota f = \chi(\sigma)\chi(\tau)K^\times = \chi(\sigma\tau)K^\times$. 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, Φ), so that $\mathrm{Aut}(\mathbb{C}/E) = \{\tau \in \mathrm{Aut}(\mathbb{C}) \mid \tau\Phi = \Phi\}$. Then $\Phi\,\mathrm{Aut}(\mathbb{C}/K)$ is stable under the left action of $\mathrm{Aut}(\mathbb{C}/E)$ and we write

$$\mathrm{Aut}(\mathbb{C}/K)\,\Phi^{-1} = \bigcup \psi\, \mathrm{Aut}(\mathbb{C}/E) \qquad \text{(disjoint union)};$$

the set $\Psi = \{\psi \mid E\}$, is a CM-type for E, and $(E, \cancel{\phi}\Psi)$ is the reflex of (K, Φ). The map $a \mapsto \prod_{\psi \in \Psi} \psi(a) : E \to \mathbb{C}$ ~~defines~~ factors through K and defines a morphism of algebraic tori $\Psi^{\times} : E^{\times} \to K^{\times}$. The (old) main theorem of complex multiplication states the following: let $\tau \in \mathrm{Aut}(\mathbb{C}/E)$, and let $a \in \mathbb{A}_E^{f\times}/E^{\times}$ be such that $r_E(a) = \tau$; then (1.1) is true after f has been replaced by $\Psi^{\times}(a)$. (See [13, Thm 5.15]; the sign differences result from different conventions for the reciprocity law and the action of Galois groups.) The next result shows that this is in agreement with (1.1).

<u>Proposition</u> 2.8. For any $\tau \in \mathrm{Aut}(\mathbb{C}/E)$, and $a \in \mathbb{A}_E^{f\times}/E^{\times}$ such that $r_E(a) = \tau$, $\Psi^{\times}(a) \in f_{\Phi}(\tau)$.

<u>Proof</u>: Partition Φ into orbits, $\Phi = \bigcup_j \Phi_j$, for the left action of $\mathrm{Aut}(\mathbb{C}/E)$. Then $\mathrm{Aut}(\mathbb{C}/K)\,\Phi^{-1} = \bigcup_j \mathrm{Aut}(\mathbb{C}/K)\,\Phi_j^{-1}$, and

$$\mathrm{Aut}(\mathbb{C}/K)\,\Phi_j^{-1} = \mathrm{Aut}(\mathbb{C}/K)(\sigma_j^{-1}\,\mathrm{Aut}(\mathbb{C}/E)) = (\mathrm{Hom}_K(L_j, \mathbb{C}) \circ \sigma_j^{-1})\,\mathrm{Aut}(\mathbb{C}/E)$$

where σ_j is any element of ~~Aut(C/E)~~ $\mathrm{Aut}(\mathbb{C})$ such that $\sigma_j|K \in \Phi_j$ and $L_j = (\sigma_j^{-1}E)K$. Then $\Psi^{\times}(a) = \prod b_j$, with $b_j = N_{L_j/K}(\sigma_j^{-1}(a))$. Let $F_j(\tau) = \prod_{\phi \in \Phi_j} w_{\tau\phi}^{-1}\, \tau\, w_{\phi} \pmod{\mathrm{Aut}(\mathbb{C}/K^{ab})}$. We begin by showing that

$F_j(\tau) = r_K(b_j)$.

The basic properties of Artin's reciprocity law show that

$$\begin{array}{ccccccc}
\mathbb{A}_E^{f\times} & \hookrightarrow & \mathbb{A}_{\sigma L_j}^{f\times} & \xrightarrow{\sigma_j^{-1}} & \mathbb{A}_{L_j}^{f\times} & \xrightarrow{N_{L_j/K}} & \mathbb{A}_K^{f\times} \\
\downarrow r_E & & \downarrow r_{\sigma L_j} & & \downarrow r_{L_j} & & \downarrow r_K \\
\mathrm{Gal}(E^{ab}/E) & \xrightarrow{V_{\sigma L_j/E}} & \sigma_j \mathrm{Gal}(L_j^{ab}/L_j)\sigma_j^{-1} & \xrightarrow{\mathrm{ad}\,\sigma_j^{-1}} & \mathrm{Gal}(L_j^{ab}/L_j) & \xrightarrow{\text{rest.}} & \mathrm{Gal}(K^{ab}/K)
\end{array}$$

commutes. Therefore $r_K(b_j)$ is the image of $r_E(a)$ by the three maps in the bottom row of the diagram. Consider $\{t_\phi \mid t_\phi = w_\phi \sigma_j^{-1}, \phi \in \Phi_j\}$; this is a set of coset representatives for $\sigma_j \mathrm{Aut}(\mathbb{C}/L_j)\sigma_j^{-1}$ ~~Aut(C/E)~~ in $\mathrm{Aut}(\mathbb{C}/E)$, and so $F_j(\tau) = \prod_{\phi\in\Phi_j} \sigma_j^{-1} t_{\tau\phi}^{-1}\, \tau\, t_\phi\, \sigma_j = \sigma_j^{-1}\, V(\tau)\, \sigma_j \pmod{\mathrm{Aut}(\mathbb{C}/K^{ab})}$.

~~Thus~~ $\cancel{r_K(f_\Phi(\tau)) = F_\Phi(\tau) = \prod F_j(\tau) = \prod r_K(b_j) = r_K(\ldots)}$ [illegible]

Thus $r_K(\Psi^\times(a)) = \prod r_K(b_j) = \prod F_j(\tau) = F_\Phi(\tau)$. Clearly $\Psi^\times(a)\cdot \iota\Psi^\times(a) \in \chi(\tau)K^\times$, and so this shows that $a \in f_\Phi(\tau)$.

§3 Start of the proof; Tate's result

We shall work with the statement (1.2) rather than (1.1). The variety τA has type $(K, \tau\Phi)$ because $\tau\Phi$ describes the action of K on the tangent space to τA at zero. Choose any K-linear isomorphism $\alpha: H_1(A, \mathbb{Q}) \xrightarrow{\simeq} H_1(\tau A, \mathbb{Q})$. Then

$$V^f(A) \xrightarrow{\tau} V^f(\tau A) \xrightarrow{(\alpha\otimes 1)^{-1}} V^f(A)$$

is an $\mathbb{A}_K^f$-linear isomorphism, and hence is multiplication by some $g \in \mathbb{A}_K^{f\times}$; thus $(\alpha\otimes 1)\circ g = \tau$.

<u>Lemma</u> 3.1. For this g, we have

$$(\alpha\psi)\left(\frac{\chi(\tau)}{g.\iota g}\, x, y\right) = (\tau\psi)(x, y), \qquad \text{all } x, y \in V^f(A).$$

<u>Proof</u>: By definition,

$$(\tau\psi)(\tau x, \tau y) = \tau(\psi(x,y)) \qquad x, y \in V^f(A)$$

$$(\alpha\psi)(\alpha x, \alpha y) = \psi(x, y) \qquad x, y \in V^f(A).$$

On replacing x and y by gx and gy in the second equality, we find

$$(\alpha\psi)(\tau x, \tau y) = \psi(gx, gy) = \psi((g.\iota g)x, y).$$

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

<u>Remark</u> 3.2. On taking $x, y \in H_1(A, \mathbb{Q})$ in (3.1), we can deduce that $\chi(\tau)/g.\iota g \in K^\times$; therefore $g.\iota g \equiv \chi(\tau) \mod K^\times$.

The only choice involved in the definition of g is that of α, and α is determined up to multiplication by an element of $K^\times$. Thus the class of g in $\mathbb{A}_K^{f\times}/K^\times$ depends only on A and τ. In fact it depends only on (K,Φ) and τ, because any other abelian variety of type (K,Φ) is isogenous to A and leads to the same class $gK^\times$. We define $g_\Phi(\tau) = gK^\times \in \mathbb{A}_K^{f\times}/K^\times$.

Proposition 3.3. The maps $g_\Phi : \mathrm{Aut}(\mathbb{C}) \longrightarrow \mathbb{A}_K^{f\times}/K^\times$ have the following properties:

(a) $g_\Phi(\sigma\tau) = g_{\tau\Phi}(\sigma)\, g_\Phi(\tau)$;

(b) $g_{\Phi(\tau^{-1}|K)}(\sigma) = \tau g_\Phi(\sigma)$ if $\tau K = K$;

(c) $g_\Phi(\iota) = 1$;

(d) $g_\Phi(\tau)\cdot \iota g_\Phi(\tau) = \chi(\tau)K^\times$.

Proof: (a) Choose K-linear isomorphisms $\alpha : H_1(A,\mathbb{Q}) \longrightarrow H_1(\tau A,\mathbb{Q})$ and $\beta : H_1(\tau A,\mathbb{Q}) \longrightarrow H_1(\sigma\tau A,\mathbb{Q})$, and let $g = (\alpha\otimes 1)^{-1}\circ\tau$ and $g_\tau = (\beta\otimes 1)^{-1}\circ\sigma$ so that g and g_τ represent $g_\Phi(\tau)$ and $g_{\tau\phi}(\sigma)$ respectively. Then

$$(\beta\alpha)\otimes 1\circ(g_\tau g) = (\beta\otimes 1)\circ g_\tau\circ(\alpha\otimes 1)\circ g = \sigma\tau,$$

which shows that $g_\tau g$ represents $g_\Phi(\sigma\tau)$.

(b) If $(A, K \hookrightarrow \mathrm{End}(A)\otimes\mathbb{Q})$ has type (K,Φ), then $(A, K \xrightarrow{\tau^{-1}} K \to \mathrm{End}(A)\otimes\mathbb{Q})$ has type $(K, \Phi\tau^{-1})$. The formula in (b) can be proved by transport of structure.

(c) Complex conjugation $\iota : A \longrightarrow \iota A$ is a homeomorphism (relative to the complex topology) and so induces a K-linear isomorphism $\iota_1 : H_1(A,\mathbb{Q}) \to H_1(\iota A,\mathbb{Q})$. The map $\iota_1\otimes 1 : V^f(A) \to V^f(\iota A)$ is ι again, and so on taking $\alpha = \iota_1$ we find $g = 1$.

(d) This is proved in (3.2).

Theorem 1.2 (hence also 1.1) becomes true if f_Φ is replaced by g_Φ. Our task is to show that $f_\Phi = g_\Phi$. To this end we set
$$e_\Phi(\tau) = g_\Phi(\tau)/f_\Phi(\tau) \in \mathbb{A}_K^{f\times}/K^\times.$$

<u>Proposition</u> 3.4 The maps $e_\Phi : \mathrm{Aut}(\mathbb{C}) \longrightarrow \mathbb{A}_K^{f\times}/K^\times$ have the following properties:

(a) $e_\Phi(\sigma\tau) = e_{\tau\Phi}(\sigma)\, e_\Phi(\tau)$;

(b) $e_{\Phi(\tau^{-1}|K)}(\sigma) = \tau e_\Phi(\sigma)$ if $\tau K = K$;

(c) $e_\Phi(\iota) = 1$;

(d) $e_\Phi(\tau) \cdot \iota e_\Phi(\tau) = 1$;

(e) $e_\Phi(\tau) = 1$ if $\tau\Phi = \Phi$.

<u>Proof</u>: (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 $\tau\Phi = \Phi$ in (e) means that τ fixes the reflex field of (K, Φ) and, as we observed in §2, the theorems are known to hold in that case, which means that $f_\Phi(\tau) = g_\Phi(\tau)$.

<u>Proposition</u> 3.5 Let K_0 be the maximal real subfield of K; then $e_\Phi(\tau) \in \mathbb{A}_{K_0}^{f\times}/K_0^\times$ and $e_\Phi(\tau)^2 = 1$; moreover $e_\Phi(\tau)$ depends only on the effect of τ on K_0, and is 1 if $\tau|K_0 = \mathrm{id}$.

<u>Proof</u>: Replacing τ by $\sigma^{-1}\tau$ in (a), we find using (e) that $e_\Phi(\tau) = e_\Phi(\sigma)$ if $\tau\Phi = \sigma\Phi$, i.e., $e_\Phi(\tau)$ depends only on the restriction of τ to the reflex field of (K, Φ). From (b) with $\tau = \iota$ we find using $\iota\Phi = \Phi\iota$ that $e_{\iota\Phi}(\sigma) = \iota e_\Phi(\sigma)$. Putting $\tau = \iota$, then $\sigma = \iota$,

in (a), we find that $e_\Phi(\sigma\iota) = \iota e_\Phi(\sigma)$ and $e_\Phi(\iota\tau) = e_\Phi(\tau)$. Since $\iota\tau$ and $\tau\iota$ have the same effect on E we conclude $e_\Phi(\tau) = \iota e_\Phi(\tau)$. Thus $e_\Phi(\tau) \in (\mathbb{A}_K^{f\times}/K^\times)^{\langle\iota\rangle} = \mathbb{A}_{K_0}^{f\times}/K_0^\times$, where ~~is the subgroup of~~ $\langle\iota\rangle = \mathrm{Gal}(K/K_0)$, and (d) shows that $e(\tau)^2 = 1$.

<u>Corollary</u> 3.6. Part (a) of (1.1) is true; part (b) of (1.1) becomes true when f is replaced by ef with $e \in \mathbb{A}_{K_0}^{f\times}$, $e^2 = 1$.

<u>Proof</u>: Let $e \in e_\Phi(\tau)$. Then $e^2 \in K_0^\times$ and, since an element of $K_0^\times$ that ~~which~~ is a square locally at ~~of~~ all finite primes is a square, we can correct e to achieve $e^2 = 1$. ~~Then (1.1)~~ Now (1.1) is true with f replaced by ef, 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 $e_\Phi(\tau)$. The universal e is a map into the Serre group. In §4 we review some of the theory concerning the Serre group, and in (5.1) we state the existence of e. The proof of (5.1), which requires Deligne's result [4] 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 Serre group

Let E be a CM-field. The *Serre group* corresponding to E is a pair (S^E, μ^E) comprising a $\mathbb{Q}$-rational torus S^E and a cocharacter $\mu^E \in X_*(S^E)$ defined over E whose weight $w^E \overset{df}{=} -(\iota+1)\mu^E$ is defined over $\mathbb{Q}$. It is characterized by having the following universal property: for any $\mathbb{Q}$-rational torus T and $\mu \in X_*(T)$ defined over E whose weight is $\mathbb{Q}$-rational, there is a unique $\mathbb{Q}$-rational homomorphism $\rho_\mu : S^E \longrightarrow T$ such that $\rho_\mu \circ \mu^E = \mu$.

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

$$X^*(S^E) = \{\chi \in X^*(E^\times) \mid (\tau-1)(\iota+1)\chi = 0, \text{ all } \tau \in \mathrm{Aut}(\mathbb{C})\}$$

$$X^*(\mu^E) = \textstyle\sum n_\rho[\rho] \longmapsto n_1 \; : \; X^*(S^E) \longrightarrow \mathbb{Z}$$

because this pair has a universal property dual to that of (S^E, μ^E). In particular, there is a canonical map $E^\times \twoheadrightarrow S^E$ (equal to $N_{E/\mathbb{Q}} \cdot \mathrm{Res}_{E/\mathbb{Q}}(\mu^E)$), and it is known (cf. [11, II]) that the kernel of this map is the Zariski closure of any sufficiently small subgroup U of finite index in $\mathcal{O}_E^\times$.

When E is Galois over $\mathbb{Q}$, the action of $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ on E defines an automorphism $\underset{\sim}{\sigma}$ of the torus S^E, and $X_*(\underset{\sim}{\sigma})$ is $\sum n_\rho[\rho] \longmapsto \sum n_\rho[\rho\sigma]$.

<u>Lemma 4.1</u>. Let E_0 be the maximal real subfield of E; there is an exact sequence of algebraic tori

$$1 \longrightarrow E_0^\times \xrightarrow{\binom{\text{incl.}}{N_{E_0/\mathbb{Q}}}} E^\times \times \mathbb{Q}^\times \xrightarrow{(\text{can.},\, w^E)} S^E \longrightarrow 1.$$

Proof: It suffices to show that the sequence becomes exact after the functor ~~X~~ X^* has been applied. As

$$X^*(E_0^\times) = \{\textstyle\sum n_{\rho'}[\rho'] \mid \rho' \in \mathrm{Hom}(E_0, \mathbb{C})\}$$

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

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

$$X^*\left(\binom{\text{incl}}{N_{E_0/\mathbb{Q}}}\right) = \textstyle\sum n_\rho[\rho] + n \longmapsto \sum n_\rho[\rho|E_0] + n\sum_{\rho'}[\rho']$$

$$X^*((\text{can}, w^E)) = \textstyle\sum n_\rho[\rho] \longmapsto \sum n_\rho[\rho] - (n_1 + n_\iota)$$

this is trivial.

Lemma 4.2. The map $N_{E/\mathbb{Q}}: E^\times \longrightarrow \mathbb{Q}^\times$ factors through S^E, and gives rise to a commutative diagram

$$\begin{tikzcd} S^E \arrow[rr, "1+\iota"] \arrow[dr, "N_{E/\mathbb{Q}}"'] & & S^E \\ & \mathbb{Q}^\times \arrow[ur, "-w^E"'] & \end{tikzcd}$$

Proof: $X^*(N_{E/\mathbb{Q}})$ is $n \longmapsto n\sum[\rho]$, which clearly factors through ~~X~~ $X^*(S^E) \subset X^*(E^\times)$. Moreover, the endomorphisms

$$X^*(-w^E \circ N_{E/\mathbb{Q}}) = \left(\textstyle\sum n_\rho[\rho] \longmapsto n_1 + n_\iota \longmapsto (n_1 + n_\iota)\sum n_\rho[\rho]\right)$$

$$X^*(1+\iota) = \left(\textstyle\sum n_\rho[\rho] \longmapsto \sum n_\rho([\rho] + [\iota\rho]) \longmapsto \sum(n_\rho + n_{\iota\rho})[\rho] = (n_1 + n_\iota)\sum[\rho]\right)$$

are equal.

Let $E_1 \supset E_2$ be CM-fields. The norm map $E_1^\times \longrightarrow E_2^\times$ induces a norm map $N_{E_1/E_2}: S^{E_1} \longrightarrow S^{E_2}$ which is the unique $\mathbb{Q}$-rational homomorphism such that $N_{E_1/E_2} \circ \mu^{E_1} = \mu^{E_2}$. The following diagram commutes:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & (E_1)^\times_\circ & \longrightarrow & E_1^\times \times \mathbb{Q}^\times & \longrightarrow & S^{E_1} & \longrightarrow & 1 \\
 & & \downarrow N & & \downarrow N \times id & & \downarrow N_{E_1/E_2} & & \\
1 & \longrightarrow & (E_2)^\times_\circ & \longrightarrow & E_2^\times \times \mathbb{Q}^\times & \longrightarrow & S^{E_2} & \longrightarrow & 1 .
\end{array}$$

<u>Remark</u> 4.3. The Serre group is defined for all fields of finite degree over $\mathbb{Q}$. If L contains a CM-field ~~then~~ and E is the maximal such subfield, then $N_{L/E}: S^L \xrightarrow{\approx} S^E$; otherwise $N_{L/\mathbb{Q}}: S^L \xrightarrow{\approx} S^{\mathbb{Q}} = \mathbb{Q}^\times$.

Let (K, Φ) be a CM-type with $K \subset \mathbb{C}$. ~~Let~~ Write $T = \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_m$, and define $\mu_\Phi \in X_*(T)$ by the condition

$$\begin{aligned}
[\rho] \circ \mu_\Phi &= id \quad , \rho \in \Phi \\
&= 1 \quad , \rho \notin \Phi .
\end{aligned}$$

Thus μ_Φ is the map

$$\begin{array}{ccc}
\mathbb{C}^\times & \longrightarrow & T(\mathbb{C}) = (K \otimes \mathbb{C})^\times = \prod_{\phi \in \Phi} \mathbb{C}^\times \times \prod_{\phi \notin \Phi} \mathbb{C}^\times \\
z & \longmapsto & (z, z, \dots, z; 1, \dots, 1) .
\end{array}$$

The weight of μ_Φ is the map induced by $x \mapsto x^{-1}: \mathbb{Q}^\times \hookrightarrow K^\times$, which is defined over $\mathbb{Q}$, and μ_Φ itself is defined over the reflex field of (K, Φ). There is therefore, for any CM-field E containing the reflex field of (K, Φ), a unique $\mathbb{Q}$-rational homomorphism $\rho_\Phi: S^E \longrightarrow T$ such that $\mu_\Phi = \rho_\Phi \circ \mu^E$. From now on we assume E to be Galois over $\mathbb{Q}$.

<u>Lemma</u> 4.4 (a) $\quad \tau \mu_\Phi = \mu_{\tau\Phi} \quad , \tau \in \mathrm{Aut}(\mathbb{C})$.

(b) Let $\tau \in \mathrm{Aut}(\mathbb{C})$ be such that $\tau K = K$, so that τ induces an automorphism $\underset{\sim}{\tau}$ of T; then $\underset{\sim}{\tau} \circ \mu_\Phi = \mu_{\Phi\tau^{-1}}$.

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

$$[\rho](\underset{\sim}{\tau}(x)) = \tau([\tau^{-1}\rho](x)) \quad , x \in T(\mathbb{C}), \ \rho \in \mathrm{Hom}(K, \mathbb{C}).$$

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

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

By definition, $[\tau^{-1}\rho]\,\mu_\Phi(\tau^{-1}z) = \tau^{-1}z$ if $\tau^{-1}\rho \in \Phi$

$= 1$ if $\tau^{-1}\rho \notin \Phi$.

Thus $[\rho] \circ (\tau\,\mu_\Phi) = id$ $\rho \in \tau\Phi$

$= 1$ $\rho \notin \tau\Phi$

which proves (a).

(b) $[\rho] \circ \underset{\sim}{\tau} \circ \mu_\Phi = [\rho\tau] \circ \mu_\Phi = id$ if $\rho\tau \in \Phi$

$= 1$ if $\rho\tau \notin \Phi$.

Thus (b) is clear.

Proposition 4.5 (a) For any $\tau \in \mathrm{Aut}(\mathbb{C})$, $\rho_\Phi \circ \underset{\sim}{\tau}^{-1} = \rho_{\tau\Phi}$.

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

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

$$\rho_\Phi \circ \underset{\sim}{\tau}^{-1} \circ \mu^E = \rho_\Phi \circ (\tau\mu^E) = \tau(\rho_\Phi \circ \mu^E) \qquad (\rho_\Phi \text{ is } \mathbb{Q}\text{-rational})$$

$$= \tau\mu_\Phi \qquad (\text{definition of } \rho_\Phi)$$

$$= \mu_{\tau\Phi} \qquad (4.4a),$$

~~and this~~ which implies that $\rho_\Phi \circ \tau^{-1} = \rho_{\tau\Phi}$. It remains to show that $X^*(\underset{\sim}{\tau} \circ \mu^E) = X^*(\tau\mu^E)$, but

$$X^*(\tau^{-1}\circ\mu^E) = X^*(\mu^E)\circ X^*(\tau^{-1}) = \left(\textstyle\sum n_\rho[\rho] \longmapsto \sum n_\rho[\rho\tau^{-1}] \longmapsto n_\tau\right)$$

and $X^*(\tau\mu^E) = \tau(X^*(\mu^E)) = \left(\sum n_\rho[\rho] \longmapsto \sum n_\rho[\tau^{-1}\rho] \longmapsto n_\tau\right)$.

(b) $\tau\circ\rho_\Phi\circ\mu^E = \tau\circ\mu_\Phi$ (definition of ρ_Φ)

$\qquad = \mu_{\Phi\tau^{-1}}$ (4.4b).

Proposition 4.6. For $E_1 \supset E_2$,

$$\begin{tikzcd} S^{E_1} \arrow[d, "N_{E_1/E_2}"'] \arrow[dr, "\rho_\Phi"] & \\ S^{E_2} \arrow[r, "\rho_\Phi"'] & T \end{tikzcd}$$

commutes.

Proof: $((\rho_\Phi)_2\circ N_{E_1/E_2})\circ\mu^{E_1} = (\rho_\Phi)_2\circ\mu^{E_2} = \mu_\Phi$.

Proposition 4.7. Let E be a CM-field, Galois over $\mathbb{Q}$, and consider all maps ρ_Φ for ~~(K,Φ)~~ Φ running through the CM-types on E; then $\bigcap \operatorname{Ker}\rho_\Phi = 1$.

Proof: We have to show that $\sum \operatorname{Im}(X^*(\rho_\Phi)) = X^*(S^E)$; but the left hand side contains $\sum_\Phi [\phi]$ 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 Φ_1 and Φ_2 be CM-types for K_1 and K_2 respectively such that $\Phi_1|K_2 = \Phi_2$. Then, for any CM-field E containing the reflex field of (K_1,Φ_1),

$$\begin{tikzcd} S^E \arrow[r, "\rho_{\Phi_1}"] \arrow[dr, "\rho_{\Phi_2}"'] & K_1 \\ & K_2 \arrow[u, hook] \end{tikzcd}$$

commutes

Proof: Let $i: K_2^\times \hookrightarrow K_1^\times$ be the inclusion map. Then $i\circ\mu_{\Phi_2} = \mu_{\Phi_1}$ and so $i\circ\rho_{\Phi_2}\circ\mu^E = i\circ\mu_{\Phi_2} = \mu_{\Phi_1}$, which shows that $i\circ\rho_{\Phi_2} = \rho_{\Phi_1}$.

§5 Definition of ~~the 1-cocycle~~ e^E

Proposition 5.1. ~~Let E~~ Let $E \subset \mathbb{C}$ be a CM-field, Galois over $\mathbb{Q}$. Then there exists a unique ~~homomorphism~~ map $e^E : \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$ such that, for all CM-types (K,Φ) ~~such that~~ whose reflex fields are ~~is~~ contained in E, $e_\Phi(\tau) = \rho_\Phi(e(\tau))$.

Proof: The existence of e^E will be shown in §7 and §8. The uniqueness follows from (4.7) for this shows that there is an injection $S^E \xhookrightarrow{(\rho_\Phi)} \prod T_\Phi$ where $T_\Phi = \mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$ and the product is over all CM-types on E. Thus $S^E(\mathbb{A}^f)/S^E(\mathbb{Q}) \hookrightarrow \prod T_\Phi(\mathbb{A}^f)/T_\Phi(\mathbb{Q}) = \prod \mathbb{A}_E^{f\times}/E^\times$, and so any element $a \in S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$ is determined by the set $(\rho_\Phi(a))$.

Proposition 5.2. The family of maps $e^E : \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$ has the following properties:

(a) $e^E(\sigma\tau) = \underset{\sim}{\tau}^{-1} e^E(\sigma) . e^E(\tau)$, $\quad \sigma, \tau \in \mathrm{Aut}(\mathbb{C})$;

(b) if $E_1 \supset E_2$, then

$$\begin{tikzcd} \mathrm{Aut}(\mathbb{C}) \arrow[r, "e^{E_1}"] \arrow[dr, "e^{E_2}"'] & S^{E_1}(\mathbb{A}^f)/S^{E_1}(\mathbb{Q}) \arrow[d] \\ & S^{E_2}(\mathbb{A}^f)/S^{E_2}(\mathbb{Q}) \end{tikzcd}$$

commutes;

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

(d) $e(\tau) . \underset{\sim}{\iota} e(\tau) = 1$, $\quad \tau \in \mathrm{Aut}(\mathbb{C})$;

(e) $e^E \mid \mathrm{Aut}(\mathbb{C}/E) = 1$.

Proof: We have to check that $\rho_\Phi(e(\sigma\tau)) = \rho_\Phi(\underset{\sim}{\tau}^{-1} e(\sigma) . e(\tau))$, for all (K,Φ).

But $\rho_\Phi(e^E(\sigma\tau)) = e_\Phi(\sigma\tau)$ and $\rho_\Phi(\tilde{\tau}^{-1}e^E(\sigma), e^E(\tau)) = \rho_\Phi(\tilde{\tau}^{-1}e^E(\sigma))\,\rho_\Phi(e^E(\tau))$
$= \rho_{\tau\Phi}(e^E(\sigma)).\,\rho_\Phi(e^E(\tau)) = e_{\tau\Phi}(\sigma)\, e_\Phi(\tau)$; thus the equality follows from (3.4a).

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

(c) $\rho_\Phi(e^E(\iota)) = e_\Phi(\iota) = 1$ (by 3.4c), and so $e^E(\iota) = 1$.

(d) Follows from (3.4d).

(e) Assume τ fixes E ; then $\tau\Phi = \Phi$ whenever E contains the reflex field of (K, Φ), and so $\rho_\Phi(e^E(\tau)) = e^*_\Phi(\tau) = 1$ by (5.2e).

<u>Remark</u> 5.3. (a) Define $\varepsilon^E(\tau) = e(\tau^{-1})^{-1}$; then the maps ε^E satisfy the same conditions (b), (c), (d), and (e) of (5.2) as e^E, but (a) becomes the condition $\varepsilon^E(\sigma\tau) = \sigma\,\varepsilon^E(\tau).\,\varepsilon^E(\sigma)$: $\varepsilon^E(\sigma)$ is a crossed homomorphism.

(b) Condition (b) shows that e^E determines $e^{E'}$ for all $E' \subset E$. We extend the definition of e^E to all CM-fields $E \subset \mathbb{C}$ by letting $e^E = N_{E_1/E} \circ e^{E_1}$ for any Galois CM-field E_1 containing E.

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

$$\begin{tikzcd}
\mathrm{Aut}(\mathbb{C}) \arrow[r, "e^E"] \arrow[dr, "e^{\mathbb{Q}[i]}=1"'] & S^E(\mathbb{A}^f)/S^E(\mathbb{Q}) \arrow[r, "1+\iota"] \arrow[d, "N_{E/\mathbb{Q}[i]}"] \arrow[dr, "N_{E/\mathbb{Q}}"] \arrow[dr, phantom, "(4.2)"] & S^E(\mathbb{A}^f)/S^E(\mathbb{Q}) \\
 & S^{\mathbb{Q}[i]}(\mathbb{A}^f)/S^{\mathbb{Q}[i]}(\mathbb{Q}) \arrow[r, "N_{\mathbb{Q}[i]/\mathbb{Q}}"] & S^{\mathbb{Q}}(\mathbb{A}^f)/S^{\mathbb{Q}}(\mathbb{Q}) \arrow[u, "w^E"']
\end{tikzcd}$$

(we can assume $E \supset \mathbb{Q}[i]$); $S^{\mathbb{Q}[i]} = \mathbb{Q}[i]^\times$, $S^{\mathbb{Q}} = \mathbb{Q}^\times$). In his (original) letter to Langlands (see [23]) Deligne showed that the difference between the motivic Galois group and the Taniyama group was measured by a family of crossed homomorphisms (e^E) having properties (b), (c), and (e) of (5.2). After seeing Tate's result he used the above argument to show that his maps e^E had the same properties as Tate's $e_\Phi(\tau)$, viz $e^E(\tau).\iota e^E(\tau)=1$, $e^E(\tau)^2=1$.

§6 Proof that $e=1$

Proposition 6.1. Suppose there are given crossed homomorphisms $e^E: \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$, one for each CM-field $E \subset \mathbb{C}$, such that

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

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

(c) if $E_1 \supset E_2$ then

$$\begin{tikzcd} \mathrm{Aut}(\mathbb{C}/\mathbb{Q}) \arrow[r, "e^{E_1}"] \arrow[dr, "e^{E_2}"'] & S^{E_1}(\mathbb{A}^f)/S^{E_1}(\mathbb{Q}) \arrow[d, "N_{E_1/E_2}"] \\ & S^{E_2}(\mathbb{A}^f)/S^{E_2}(\mathbb{Q}) \end{tikzcd}$$

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, in particular for those that are Galois over $\mathbb{Q}$.

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, $e^E(\iota\tau) = e^E(\tau\iota)$ for all $\tau \in \mathrm{Aut}(\mathbb{C})$. ~~Thus~~ Since

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

we conclude that $\iota e^E(\tau) = e^E(\tau)$, ~~then~~

Lemma 6.2. Assume that E is Galois over $\mathbb{Q}$, and let $\langle\iota\rangle$ be the subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ generated by $\iota|E$.

~~Lemma 6.3. Let $\langle\iota\rangle$ be the subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ generated by $\iota \in E_0$~~

(a) There is an exact commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d] & S^E(\mathbb{Q})^{\langle\iota\rangle} \arrow[r] \arrow[d] & \mu_2(E_0) \arrow[r, "N_{E_0/\mathbb{Q}}"] \arrow[d] & \mu_2(\mathbb{Q}) \arrow[d] \\
1 \arrow[r] & \mathbb{A}^{f\times} \arrow[r] & S^E(\mathbb{A}^f)^{\langle\iota\rangle} \arrow[r] & \mu_2(\mathbb{A}^f_{E_0}) \arrow[r, "N"] & \mu_2(\mathbb{A}^f)
\end{tikzcd}$$

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

(b) The canonical map

$$H^1(\langle\iota\rangle, S^E(\mathbb{Q})) \longrightarrow H^1(\langle\iota\rangle, S^E(\mathbb{A}^f))$$

is injective.

Proof: From (4.1) we obtain cohomology sequences

$$\begin{tikzcd}[column sep=small]
1 \arrow[r] & E_0^{\times} \arrow[r] \arrow[d] & E_0^{\times} \times \mathbb{Q}^{\times} \arrow[r] \arrow[d] & S^E(\mathbb{Q})^{\langle\iota\rangle} \arrow[r] \arrow[d] & \mu_2(E_0) \arrow[r, "N"] \arrow[d] & \mu_2(\mathbb{Q}) \arrow[r] \arrow[d] & H^1(\langle\iota\rangle, S^E(\mathbb{Q})) \arrow[r] \arrow[d] & E_0^{\times}/E_0^{\times 2} \arrow[d] \\
1 \arrow[r] & \mathbb{A}^{f\times}_{E_0} \arrow[r] & \mathbb{A}^{f\times}_{E_0} \times \mathbb{A}^{f\times} \arrow[r] & S^E(\mathbb{A}^f)^{\langle\iota\rangle} \arrow[r] & \mu_2(\mathbb{A}^f_{E_0}) \arrow[r, "N"] & \mu_2(\mathbb{A}^f) \arrow[r] & H^1(\langle\iota\rangle, S^E(\mathbb{A}^f)) \arrow[r] & \mathbb{A}^{f\times}_{E_0}/\mathbb{A}^{f\times 2}_{E_0}
\end{tikzcd}$$

It is easy to ~~see~~ extract from this the diagram in (a). Let $\gamma \in H^1(\langle\iota\rangle, S^E(\mathbb{Q}))$ map to zero in $H^1(\langle\iota\rangle, S^E(\mathbb{A}^f))$. As $E_0^{\times}/E_0^{\times 2} \longrightarrow \mathbb{A}^{f\times}_{E_0}/\mathbb{A}^{f\times 2}_{E_0}$ is injective (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 γ is the image of $\pm 1 \in \mu_2(\mathbb{Q})$. The map $N_{E_0/\mathbb{Q}} : \mu_2(E_0) \longrightarrow \mu_2(\mathbb{Q})$ sends -1 to $(-1)^{[E_0:\mathbb{Q}]}$. ~~If $[E_0$~~ If $[E_0 : \mathbb{Q}]$ is odd, it is surjective, and therefore $\gamma = 0$. Suppose therefore that $[E_0 : \mathbb{Q}]$ is even, and ~~let γ be~~ that γ is the image of -1. The assumption that γ maps to zero in $H^1(\langle\iota\rangle, S^E(\mathbb{A}^f))$ then implies that $-1 \in \mathbb{Q}_\ell$ is in the image of $N : E_0 \otimes \mathbb{Q}_\ell \longrightarrow \mathbb{Q}_\ell$ for all ℓ; but this is impossible, since for some ℓ, $[E_{0v} : \mathbb{Q}_\ell]$ will be even for one (hence all) v dividing ℓ.

Part (b) of the lemma shows that

$$S^E(\mathbb{A}^f)^{\langle\iota\rangle} / S^E(\mathbb{Q})^{\langle\iota\rangle} = (S^E(\mathbb{A}^f)/S^E(\mathbb{Q}))^{\langle\iota\rangle}.$$

The condition $\iota e^E(\tau) = e^E(\tau)$ 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

$$1 \longrightarrow \mathbb{A}^{f\times}/\mathbb{Q}^\times \xrightarrow{w} S^E(\mathbb{A}^f)^{\langle\iota\rangle}/S^E(\mathbb{Q})^{\langle\iota\rangle} \longrightarrow \mu_2(\mathbb{A}^f_{E_0})/\mu_2(E_0).$$

Now assume that $E \supset \mathbb{Q}[i]$ so that $E = E_0[i]$. We show first that the image of $e^E(\tau)$ in $\mu_2(\mathbb{A}^f_{E_0})/\mu_2(E_0)$ is 1. Let ε represent the image; then $\varepsilon = (\varepsilon_v)$, $\varepsilon_v = \pm 1$, and ε itself is defined up to sign. We shall show that, for any two primes v_1 and v_2, $\varepsilon_{v_1} = \varepsilon_{v_2}$. Choose a totally real quadratic extension E_0' of E_0 in which v_1 and v_2 remain prime, and let $E' = E_0'[i]$. Let ε' represent the image of $e^{E'}(\tau)$ in $\mu_2(\mathbb{A}^f_{E_0'})/\mu_2(E_0')$. 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 $v_i' | v_i$, then $N_{E'_{0,v_i'}/E_{0,v_i}} = 1$, for $i = 1, 2$.

It follows that e^E factors through $w(\mathbb{A}^{f\times}/\mathbb{Q}^\times)$. Consider

$$\begin{array}{lccccc}
E & 1 \longrightarrow & \mathbb{A}^{f\times}/\mathbb{Q}^\times & \xrightarrow{w} & S^E(\mathbb{A}^f)/S^E(\mathbb{Q}) \\
 & & \downarrow{\scriptstyle id} & & \downarrow \\
\mathbb{Q}[i] & 1 \longrightarrow & \mathbb{A}^{f\times}/\mathbb{Q}^\times & \xrightarrow{w} & S^{\mathbb{Q}[i]}(\mathbb{A}^f)/S^{\mathbb{Q}[i]}(\mathbb{Q})
\end{array}$$

According to (c), $e^E(\tau)$ maps to $e^{\mathbb{Q}[i]}(\tau)$, which according to (d), is 1. As $e^E(\tau)$ lies in $\mathbb{A}^{f\times}/\mathbb{Q}^\times$, and the map from there into $S^{\mathbb{Q}[i]}(\mathbb{A}^f)/S^{\mathbb{Q}[i]}(\mathbb{Q})$ is injective, this shows that $e^E(\tau) = 1$.

Remark 6.7. The argument used in the penultimate paragraph of the above proof is that used by Shih [12, p101] 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 f^E

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

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

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{A}_E^{\times}/E^{\times} \arrow[r] \arrow[d, "\mathrm{rec}_E"] & W_{E/\mathbb{Q}} \arrow[r] \arrow[d] & \mathrm{Hom}(E,\mathbb{C}) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathrm{Gal}(E^{ab}/E) \arrow[r] & \mathrm{Hom}(E^{ab},\mathbb{C}) \arrow[r] & \mathrm{Hom}(E,\mathbb{C}) \arrow[r] & 1
\end{tikzcd}$$

(see [15]). Assume that E is totally complex. Then $E_\infty^{\times} E^{\times} \subset \mathrm{Ker}(\mathrm{rec}_E)$, and so we can divide out by this group and its image in $W_{E/\mathbb{Q}}$ to obtain an exact commutative diagram,

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{A}_E^{f\times}/E^{\times} \arrow[r] \arrow[d, "r_E"] & W^f_{E/\mathbb{Q}} \arrow[r] \arrow[d] & \mathrm{Hom}(E,\mathbb{C}) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathrm{Gal}(E^{ab}/E) \arrow[r] & \mathrm{Hom}(E^{ab},\mathbb{C}) \arrow[r] & \mathrm{Hom}(E,\mathbb{C}) \arrow[r] & 1
\end{tikzcd}$$

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

$$w_\sigma | E = \sigma, \quad w_{\iota\sigma} = \tilde{\iota} w_\sigma \text{ all } \sigma, \text{ where } \tilde{\iota} \text{ maps to } \iota \in \mathrm{Hom}(E^{ab},\mathbb{C}).$$

(Cf. §2) Let $\tau \in \mathrm{Aut}(\mathbb{C})$ and let $\tilde{\tau} \in W^f_{E/\mathbb{Q}}$ map to $\tau | E^{ab}$. Then $w_{\tau\sigma}^{-1} \tilde{\tau} w_\sigma \in \mathbb{A}_E^f$, and we define

$$f(\tau) = \prod_{\sigma \in \mathrm{Hom}(E,\mathbb{C})} (\sigma^{-1}\mu^E)(w_{\tau\sigma}^{-1}\tilde{\tau} w_\sigma) \mod S^E(E^{*})$$

Thus f is a map $\mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}_E^f)/S^E(E)$.

<u>Proposition</u> 7.1. Let (K,Φ) be a CM-type whose reflex field is contained in E, and let $T = \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_m$. Identify

$T(\mathbb{A}^f)/T(\mathbb{Q})$ with a subgroup of $T(\mathbb{A}^f_E)/T(E)$. Then

$$\rho_\Phi(f(\tau)) = f_\Phi(\tau).$$

Proof: Because of (4.8), it suffices to show this with $K = E$.

Lemma 7.2. With the above notations,

$$f_\Phi(\tau) = \prod_{\phi\in\Phi} w_{\tau\phi}^{-1}\,\tilde{\tau}\, w_\phi \mod E^\times.$$

Proof. ~~Clearly~~ Let f' denote the right hand side. Then $r_E(f') = F_\Phi(\tau)$ (obviously), and the same argument as in the proof of (2.3) shows that $f' \cdot \iota f' = \chi(\tau)$.

We now assume $E = K$, $E/\mathbb{Q}$ Galois

Interchange $\sigma \leftrightarrow \rho$

Write i for the map $T(\mathbb{Q}) \longrightarrow T(E)$ induced by $\mathbb{Q} \hookrightarrow E$; then, for any $\rho \in \mathrm{Hom}(E, \mathbb{C})$ and $a \in T(\mathbb{Q}) = E^\times$, $[\rho](i(a)) = \rho a$. Thus $[\rho](i(f_\Phi(\tau))) = \rho f_\Phi(\tau) = f_{\Phi\rho^{-1}}(\tau)$ by (2.7b). On the other hand,

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

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

$$= [\rho]\Big(\prod_\sigma \sigma^{-1}\mu_\Phi (w_{\tau\sigma}^{-1}\tilde{\tau} w_\sigma)\Big)$$

$$= \prod_\sigma ([\rho]\circ \mu_{\sigma^{-1}\Phi})(w_{\tau\sigma}^{-1}\tilde{\tau} w_\sigma) \qquad \text{(by 4.4a)}$$

$$= \prod_{\sigma \text{ s.t. } \rho\in\sigma^{-1}\Phi} w_{\tau\sigma}^{-1}\tilde{\tau} w_\sigma$$

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

$$= f_{\Phi\rho^{-1}}(\tau).$$

~~The rest of this section is not required for the proof of (1.1).~~

<u>Corollary</u> 7.3. (a) $f(\tau)$ depends only on E and τ; we have therefore defined maps $f^E : \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f_E)/S^E(E)$, one for each CM-field E (Galois over $\mathbb{Q}$).

(b) $f^E(\sigma\tau) = \tilde{\tau}^{-1} f^E(\sigma) . f^E(\tau)$, $\sigma, \tau \in \mathrm{Aut}(\mathbb{C})$;

(c) if $E_1 \supset E_2$, then

$$\begin{tikzcd} \mathrm{Aut}(\mathbb{C}) \arrow[r, "e^{E_1}"] \arrow[dr, "e^{E_2}"'] & S^{E_1}(\mathbb{A}^f)/S^{E_1}(\mathbb{Q}) \arrow[d] \\ & S^{E_2}(\mathbb{A}^f)/S^{E_2}(\mathbb{Q}) \end{tikzcd}$$

commutes;

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

(e) $f^E(\tau) . \tilde{\iota} f^E(\tau) = w^E(\tau)^{-1}$;

(f) $\sigma f^E(\tau) = f^E(\tau)$ for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$.

<u>Proof</u>: (a) $f(\tau)$ is the unique element of $S^E(\mathbb{A}^f_E)/S^E(E)$ such that $\rho_\Phi(f(\tau)) = f_\Phi(\tau)$ for all (K, Φ). (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) $\rho_\Phi(\sigma f^E(\tau)) = \sigma(\rho_\Phi(f^E(\tau))) = \sigma f^E_\Phi(\tau) = f^E_\Phi(\tau)$.

<u>Remark</u> 7.4 Let $\bar{w}_\sigma \in W^f_{E/\mathbb{Q}}$ be such that

$$\bar{w}_\sigma | E = \sigma, \quad \bar{w}_{\sigma\iota} = \bar{w}_\sigma \tilde{\iota}.$$

Then [6], [9], $\bar{b}(\tau)$ is defined by

$$\bar{b}(\tau) = \prod_{\sigma \in \mathrm{Gal}(E/\mathbb{Q})} \sigma \mu^E(\bar{w}_\sigma \tilde{\tau} \bar{w}^{-1}_{\sigma\tau}) \quad (\mathrm{mod}\ S^E(E))$$

Let $w_\sigma = \bar{w}^{-1}_{\sigma^{-1}}$; then $w_\sigma | E = \sigma$ and $w_{\iota\sigma} = \tilde{\iota} w_\sigma$; moreover

$$\bar{b}(\tau^{-1})^{-1} = \prod_{\sigma \in \mathrm{Gal}(E/\mathbb{Q})} \sigma \mu^E(w^{-1}_{\sigma^{-1}\tau} \tilde{\tau} w_{\sigma^{-1}}) = f^E(\tau).$$

Thus, in the notation of [9, 2.9], $f^E(\tau) = \bar{\beta}(\tau)$.

§8 Definition of g^E

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

Proposition 8.1. Let $E \subset \mathbb{C}$ be a CM-field. There exists a unique map $g^E : \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f_E)/S^E(E)$ with the following property: for any CM-type (K, Φ) whose reflex field is contained in E,

$$\rho_\Phi(g^E(\tau)) = g_\Phi(\tau)$$

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

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 $H^s(X,\mathbb{Q})(r) = H^s(X, (2\pi i)^r\mathbb{Q})$ (cohomology with respect to the complex topology). A Hodge cycle on A is an element $s \in H^{2p}(A^k, \mathbb{Q})(p)$, some p, k, that is of type (p,p), i.e., under the embedding $(2\pi i)^p\mathbb{Q} \hookrightarrow \mathbb{C}$, s maps into $H^{p,p} \subset H^{2p}(X, \mathbb{C})$. Recall that $H^r(A^k, \mathbb{Q}) = \Lambda^r(\oplus^k H_1(A,\mathbb{Q})^\vee)$, and so $GL(H_1(A,\mathbb{Q}))$ acts by transport of structure on $H^r(A^k, \mathbb{Q})$. The Mumford-Tate group $MT(A)$ of A is the largest $\mathbb{Q}$-rational algebraic subgroup of $GL(H_1(A,\mathbb{Q}))$ such that

$$MT(A)(\mathbb{Q}) = \{\alpha \in GL(H_1(A,\mathbb{Q})) \mid \exists\, \nu(\alpha) \in \mathbb{Q}^\times \text{ s.t. } \alpha s = \nu(\alpha)^p s,$$

for any Hodge cycle s on A (of type (p,p))$\}$.

Lemma 8.2. Assume A is of CM-type (K, Φ), where the reflex field of (K, Φ) is contained in E. Then the image of $\rho_\Phi : S^E \longrightarrow K^\times \subset GL(H_1(A, \mathbb{Q}))$ is equal to $MT(A)$.

Proof. Cf. [4, §3.4].

Write $H^{2p}(A^k, \mathbb{A}^f)(p) = H^{2p}(A^k, \mathbb{Q})(p) \otimes \mathbb{A}^f$. Then there is a canonical isomorphism

$$H^{2p}(A^k, \mathbb{A}^f)(p) \xrightarrow{\approx} \Lambda^r(\oplus^k V^f(A)^\vee)$$

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

<u>Theorem</u> 8.3. Let $s \in H^{2p}(A^k, \mathbb{Q})(p)$ be a Hodge cycle on A, and let s^f be the image of s in $H^{2p}(A^k, \mathbb{A}^f)(p)$; then for any $\tau \in$ Aut$(\mathbb{C})$ there exists a Hodge cycle s_1 on τA whose image in $H^{2p}(A^k, \mathbb{A}^f)(p)$ is τs^f.

DMOS <u>Proof</u>: See [4]

The cycle s_1 of the theorem will be written τs.

<u>Proposition</u> 8.4. With the notations of (8.2), there exists a K-linear isomorphism $\alpha : H_1(A, E) \xrightarrow{\approx} H_1(\tau A, E)$ such that $\alpha(s) = \nu(\alpha)^r \tau(s)$, for all Hodge cycles s on A (of type (p,p)).

<u>Proof</u>: For any $\mathbb{Q}$-algebra R, let

$$P(R) = \{\alpha : H_1(A,R) \xrightarrow{\approx} H_1(\tau A, R) \mid \alpha(s) = \nu(\alpha)^r \tau(s), \text{all } s\}.$$

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 $\tau : H_1(A, \mathbb{A}^f) \to H_1(\tau A)$ in $P(\mathbb{A}^f)$ shows that P is a torsor. It therefore corresponds to an element of $H^1(\mathbb{Q}, MT(A))$. But $MT(A)_E \approx \mathbb{G}_m \times \cdots \times \mathbb{G}_m$, and so $H^1(E, MT(A)) = 0$ by Hilbert's theorem 90.

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

$$V^f(A) \otimes E \xrightarrow{\tau} V^f(\tau A) \otimes E \xrightarrow{(\alpha\otimes 1)^{-1}} V^f(A) \otimes E$$

is an $\mathbb{A}^f_E$-linear isomorphism and sends a Hodge cycle s of type (p,p) to $\nu^p s$, some $\nu \in \mathbb{A}^{f\times}_E$. Therefore it is multiplication by an element $g \in MT(A)(\mathbb{A}^f_E) = S^E(\mathbb{A}^f_E)$. The class $g(\tau)$ of g in $S^E(\mathbb{A}^f_E)/S^E(E)$ has the properties required for (8.1).

The map $g : \mathrm{Aut}(\mathbb{C}) \longrightarrow S^E(\mathbb{A}^f_E)/S^E(E)$ has the same properties as those listed for f in (7.3). In particular, $g(\tau)$ is fixed by $\mathrm{Gal}(E/\mathbb{Q})$. Set

$$e(\tau) = g(\tau)/f(\tau).$$

Then $e(\tau) \in S^E(\mathbb{A}^f_E)/S^E(E)^{\mathrm{Gal}(E/\mathbb{Q})}$, and it remains to show that it lies in $S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$.

<u>Proposition</u> 8.5. $e(\tau)$ lies in $S^E(\mathbb{A}^f)/S^E(\mathbb{Q})$.

<u>Proof</u>: There is a cohomology sequence

$$0 \longrightarrow S^E(\mathbb{Q}) \longrightarrow S^E(\mathbb{A}^f) \longrightarrow (S^E(\mathbb{A}^f_E)/S^E(E))^{\mathrm{Gal}(E/\mathbb{Q})} \longrightarrow H^1(\mathbb{Q}, S^E).$$

Thus we have to show that the image γ of $e(\tau)$ in $H^1(\mathbb{Q}, S^E)$ is zero. But $H^1(\mathbb{Q}, S^E) \hookrightarrow \prod_{\ell,\infty} H^1(\mathbb{Q}_\ell, S^E)$, as follows easily from (2.1), and the image of $e(\tau)$ in $H^1(\mathbb{Q}_\ell, S^E)$ is obviously zero for all finite ℓ. It remains to check that the image of γ in $H^1(\mathbb{R}, S^E)$ is zero. Let

$$T = \{ a \in \prod_{\text{CM-types on } E} E^\times \mid a \cdot \iota a \in \mathbb{Q}^\times \} \qquad (\text{torus over } \mathbb{Q})$$

Lemma 8.6. The image of γ in $H^1(\mathbb{Q}, T)$ is zero.

Proof: In the proof (3.6) it is shown that the image of e in $T(\mathbb{A}_E^f)/T(E)$ lifts to an element $\varepsilon \in T(\mathbb{A}_{\mathbb{Q}}^f)$. The image of γ in $H^1(\mathbb{Q}, T)$ is represented by the cocycle $\sigma \mapsto \sigma\varepsilon - \varepsilon = 0$.

Lemma 8.7. The map $H^1(\mathbb{R}, S^E) \longrightarrow H^1(\mathbb{R}, T)$ is injective.

Proof: There is a norm map $a \mapsto a.\iota a : T \twoheadrightarrow \mathbb{G}_m$, and we define ST and $SMT(A)$ to make the rows in

$$\begin{array}{ccccccccc} 1 & \longrightarrow & SMT(A) & \longrightarrow & MT(A) & \longrightarrow & \mathbb{G}_m & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & ST & \longrightarrow & T & \xrightarrow{N} & \mathbb{G}_m & \longrightarrow & 1 \end{array}$$

exact. (Here $A = \prod A_{\mathfrak{z}}$). This diagram gives rise to an exact commutative diagram

$$\begin{array}{ccccccc} \mathbb{R}^\times & \longrightarrow & H^1(\mathbb{R}, SMT) & \longrightarrow & H^1(\mathbb{R}, MT) & \longrightarrow & 0 \\ \| & & \downarrow & & \downarrow & & \\ \mathbb{R}^\times & \longrightarrow & H^1(\mathbb{R}, ST) & \longrightarrow & H^1(\mathbb{R}, T) & \longrightarrow & 0 \end{array}$$

Note that ST (and hence SMT) are anisotropic over $\mathbb{R}$; ~~then~~ hence, $H^1(\mathbb{R}, SMT) = SMT(\mathbb{C})_2$ and $H^1(\mathbb{R}, ST) = ST(\mathbb{C})_2$, and so $H^1(\mathbb{R}, SMT) \hookrightarrow H^1(\mathbb{R}, ST)$. 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 $e_{\Phi}(\tau)$ 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 [8].

<u>Theorem</u> 9.1. Let A be an abelian variety of CM-type (K, Φ); let $\tau \in \mathrm{Aut}(\mathbb{C})$, and let $f \in f(\tau)$. Then

(a) τA is of type $(K, \tau\Phi)$;

(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, Φ), such that

(i) $\alpha(s) = \nu(\alpha)^p \tau(s)$, for all Hodge cycles s on A, where $\nu(\alpha) \in \mathbb{Q}^\times$ and $2p$ is the degree of s;

(ii)
$$\begin{tikzcd} V^f(A)\otimes E \arrow[r, "\rho_\Phi(f)"] \arrow[dr, "\tau"'] & V^f(A)\otimes E \arrow[d, "\alpha\otimes 1"] \\ & V^f(\tau A)\otimes E \end{tikzcd} \qquad (\rho_\Phi(f) \in \mathbb{A}^{f\times}_{K\otimes E})$$

commutes.

<u>Proof</u>. The theorem is true (by definition) if $f(\tau)$ is replaced by $g(\tau)$, but we have shown that $g(\tau) = f(\tau)$.

<u>Remark</u> 9.2. Let T be a torus such that
$$MT(A) \subset T \subset \{a \in K^\times \mid a \cdot \iota a \in \mathbb{Q}^\times\}.$$
Then the Shimura variety $Sh(T, \{h\})$ is, in a natural way, a moduli scheme ~~variety~~ and the (new) main theorem of complex multiplication gives a description of the action of $\mathrm{Aut}(\mathbb{C})$ on $Sh(T, \{h\})$ (see [10, §6]).

<u>Remark</u> 9.3. Out of his study of the zeta functions of Shimura varieties, Langlands [6] 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 ~~Sh(G,X)~~ a Shimura variety $Sh(G,X)$ depends only on (G^{der}, X). Thus similar methods to those used in [1] can be used to ~~prove~~ prove Langlands's conjecture for exactly those Shimura varieties for which Shimura's conjecture is proved in [1].

§10 The Taniyama group

By an extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^E ~~we mean~~ with finite-adelic splitting we mean an exact sequence

$$1 \longrightarrow S^E \longrightarrow T^E \xrightarrow{\pi^E} \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1$$

of pro-algebraic groups over $\mathbb{Q}$ ($\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is to be regarded as a constant pro-algebraic group) together with a continuous ~~map~~ homomorphism $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{sp^E} T^E(\mathbb{A}^f)$ such that $sp^E \cdot \pi^E = id$.) Assume $E \subset \mathbb{C}$ is Galois over $\mathbb{Q}$, and a CM-field.

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

<u>Proposition</u> 10.1 (a) Let (T^E, sp^E) be an extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^E with finite-adelic splitting. Choose a section ~~$E: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to T^E$)~~ $a^E : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow (T^E)_E$ that is a morphism of pro-algebraic groups. Define $h(\tau) \in S^E(\mathbb{A}^f_E)/S^E(E)$ to be the class of $sp^E(\tau)\, a^E(\tau)^{-1}$.

(i) $h(\tau)$ is well-defined;

(ii) $\sigma\, h(\tau) = h(\tau)$, $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$;

(iii) $h(\tau_1\tau_2) = h(\tau_1) . \underset{\sim}{\tau_1}\, h(\tau_2)$, $\tau_1, \tau_2 \in$ ~~$\mathbb{A}$~~ $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$;

(iv) h lifts to a continuous map $h' : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to S^E(\mathbb{A}^f_E)$ such that the map $(\tau_1, \tau_2) \longmapsto d_{\tau_1,\tau_2} \overset{df}{=} h'(\tau_1) . \underset{\sim}{\tau_1}\, h'(\tau_2) . h'(\tau_1\tau_2)^{-1}$ is locally constant.

(b) Let $h : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow S^E(\mathbb{A}^f_E)/S^E(E)$ be a map satisfying conditions (i), (ii), (iii), (iv); then h arises from a unique extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^E with finite-adelic splitting

<u>Proof</u>. Easy; see [9, §2].

Let $S = \varprojlim S^E$, where E runs through the CM-fields $E \subset \mathbb{C}$ that are Galois over $\mathbb{Q}$. By an extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S with finite-adelic splittings, we mean a projective system of extensions of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^E with finite-adelic splitting, i.e., a family

$$\begin{array}{ccccccccc}
1 & \longrightarrow & S^{E_1} & \longrightarrow & T^{E_1} & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & 1 \\
 & & \downarrow N_{E_1/E_2} & & \downarrow N_{E_1/E_2} & & \| & & \\
1 & \longrightarrow & S^{E_2} & \longrightarrow & T^{E_2} & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & 1
\end{array}$$

$$\begin{tikzcd}
T^{E_1}(\mathbb{A}^f) \arrow[d, "N_{E_1/E_2}"] & \\
T^{E_2}(\mathbb{A}^f) & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[ul, "sp^{E_1}"'] \arrow[l, "sp^{E_2}"]
\end{tikzcd}$$

of commutative diagrams.

<u>Theorem</u> 10.2. Let T_1 and T_2 be two extensions of ~~S~~ $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S with finite-adelic splittings. Assume,

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

$$\begin{array}{ccccccccc}
1 & \longrightarrow & S^E & \longrightarrow & {}_E T_i^E & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/E) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & S^E & \longrightarrow & M^E & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/E)^{ab} & \longrightarrow & 1
\end{array}$$

compatible with the finite-adelic splittings, where ${}_E T^E$ is the inverse image of $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ in T^E and the lower row is the extension constructed in Serre [11, II].

(b) For each $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\pi_1^{-1}(\tau) \simeq \pi_2^{-1}(\tau)$ as S^E-torsors

(c) $sp^E(\iota) \in T_i^E(\mathbb{Q})$, $i = 1, 2$.

Then there is a unique family of isomorphisms $\phi^E : T_1^E \longrightarrow T_2^E$ making the following diagrams commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S^E & \longrightarrow & T_1^E & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & 1 \\ & & \| & & \downarrow \phi^E & & \| & & \\ 1 & \longrightarrow & S^E & \longrightarrow & T_2^E & \longrightarrow & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & 1 \end{array}$$

$$\begin{array}{ccc} T_1^{E_1} & \xrightarrow{N_{E_1/E_2}} & T_1^{E_2} \\ \downarrow \phi^{E_1} & & \downarrow \phi^{E_2} \\ T_2^{E_1} & \xrightarrow{N_{E_1/E_2}} & T_2^{E_2} \end{array} \qquad \begin{array}{ccc} T_1^E(\mathbb{A}^f) & \xleftarrow{sp_1^E} & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \\ \downarrow & & \| \\ T_2^E(\mathbb{A}^f) & \xleftarrow{sp_2^E} & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \end{array}$$

<u>Proof</u>: 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 the family (e^E), where $e^E = h_1^E / h_2^E$, satisfy the hypotheses of (6.1). Thus $h_1^E = h_2^E$ for all E, and we apply (10.1b).

<u>Definition</u> 10.3. The extension corresponding to the family of maps (f^E) defined in (7.3) is called the Taniyama group. (rather $\tau \mapsto f^E(\tau)^{-1}$)

<u>Remark</u> 10.4. In [3] Deligne proves the following:

(a) let M be the group associated with the Tannakian category of motives over $\mathbb{Q}$ generated by Artin motives and abelian varieties of potential CM-type; then M is an extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S with finite-adelic splitting in the sense defined above. (From a more naive point of view, M is the extension defined by the maps (g^E) of §8.)

(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 ~~combd~~ combine 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) main 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)).

§11 Zeta functions

Lemma 11.1. There exists a commutative diagram

$$\begin{tikzcd} T^E(\mathbb{C}) & W_{\mathbb{Q}} \arrow[l, "sp_\infty^E"'] \arrow[d] \\ T^E(\mathbb{Q}) \arrow[u, hook] \arrow[r] & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \end{tikzcd}$$

where $W_{\mathbb{Q}}$ is the Weil group of $\mathbb{Q}$ and T is the Taniyama group.

Proof: easy; see [9, 3.17].

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

(a) $\rho_f \overset{\mathrm{df}}{=} \rho \circ sp^E : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(V^f(A))$ describes the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $V^f(A)$;

(b) $L(s, A/\mathbb{Q}) = L(s, \rho_\infty)$ where $\rho_\infty = \rho \circ sp_\infty^E$ is a complex representation of W_E.

Proof: The existence of ρ is obvious from the interpretation of T as the motivic Galois group M (see 10.4a) or, more namely, ~~to~~ as the extension corresponding to $(g^{E(\tau)^{-1}})$.

<u>Remark</u> 11.3. The proof ~~of~~ of (11.2) does not require the full strength of ~~#~~ Deligne's results, and in fact is proved by Deligne in [2]. Subsequently Yoshida [16] found another ~~proof~~ proof that $L(s, A/\mathbb{Q}) = L(s, \rho_\infty)$ for <u>some</u> complex representation ρ_∞ of $W_{\mathbb{Q}}$. When $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ stabilizes $K \subset End(A_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$, this last result was proved independently by ~~the~~ Milne [7] (all primes) and Shimura [14] (good primes only).

19/9/81

References

1. P. Deligne : Variétés de Shimura . Corvallis 1977.

2. ——— : Letter to Langlands 10 April 1979

3. ——— : Motifs et groupe de Taniyama (completion of [2]) To appear in [5]

4. ——— (Notes by J S Milne) : Hodge cycles on abelian varieties . To appear in [5]

5. Deligne, Milne, Ogus, Shih : Hodge Cycles, Motives, and Shimura Varieties . Submitted to Springer L.N.

6. Langlands : Corvallis 1977

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

8. Milne + Shih : Shimura Varieties : Conjugates and the Action of Complex Conjugation . 154pp (1979). Revised + published as [9], [10], + Annals 1981

9. ——— : Langlands's construction of the Taniyama group. To appear in [5] 1982a

10. ——— : Conjugates of Shimura Varieties : To appear in [5]. 1982b

11. Serre : l-adic Representations : Benjamin

12. Shih : Annals 103 (1976) 81-102

13. Shimura : Book 1971

14. ——— : Annals 94 (1971) 504-533

15. Tate : On conjugation of abelian varieties of CM-type Ms 8pp April 1981

16. Yoshida : Annals (1981).