ABELIAN VARIETIES OVER Q AND MODULAR FORMS

Kenneth A. Ribet

University of California, Berkeley

1. Introduction.

Let C be an elliptic curve over $\mathbf{Q}$. Let N be the conductor of C. The Taniyama conjecture asserts that there is a non-constant map of algebraic curves $X_o(N) \to C$ which is defined over $\mathbf{Q}$. Here, $X_o(N)$ is the standard modular curve associated with the problem of classifying elliptic curves E together with cyclic subgroups of E having order N.

The Taniyama conjecture may be reformulated in various ways. For example, let $X_1(M)$ be the modular curve associated with the problem of classifying elliptic curves E along with a point of order M on E. One knows that if there is a non-constant map $X_1(M) \to C$ over $\mathbf{Q}$ for some $M \geq 1$, then there is a non-constant map $X_o(N) \to C$. (For a result in this direction, see [11].)

In a recent article [12], B. Mazur introduced another type of reformulation. Mazur says that C possesses a "hyperbolic uniformization of arithmetic type" if there is a non-constant map over the complex field $\pi\colon X_1(M)_{\mathbf{C}} \to C_{\mathbf{C}}$ for some $M \geq 1$. The map π is not required to be defined over $\mathbf{Q}$. In [12, Appendix], Mazur proves: Suppose that there is a non-constant map $\pi\colon X_1(M)_{\mathbf{C}} \to C_{\mathbf{C}}$. Then there is a non-constant map $\pi'\colon X_1(M') \to C$ over $\mathbf{Q}$, where M' is a suitable positive integer (which may be different from M). As mentioned above, it follows easily from the existence of π' that C satisfies Taniyama's conjecture. We thus arrive at the following conclusion:

(1.1) Theorem [Mazur]. *Let C be an elliptic curve over $\mathbf{Q}$. Then C satisfies Taniyama's conjecture if and only if C admits a hyperbolic uniformization of arithmetic type over $\mathbf{C}$.*

In connection with [12], Serre asked for a conjectural characterization of elliptic curves over $\mathbf{C}$ which admit a hyperbolic uniformization of arithmetic type. All such curves are defined over $\overline{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Thus one wishes to characterize those elliptic curves over $\overline{\mathbf{Q}}$ which are quotients of some modular

This manuscript was written in conjunction with the author's lectures at the seventh KAIST mathematics workshop in Taejon, Korea (August 11–14, 1992). The author describes work which was begun during his visits to the Hebrew University of Jerusalem and the Université de Paris XI (Orsay). It is a pleasure to thank these institutions for their hospitality. The author wishes to thank J-P. Serre for suggesting the problem and for pointing out the relevance of Tate's theorem (Theorem 6.3 below.) The author was supported in part by NSF Grant #DMS 88-06815.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

curve $X_1(M)$. Equivalently, one wishes to study the set of elliptic curves which are quotients of the Jacobian $J_1(N)_{\overline{\mathbf{Q}}}$ of $X_1(N)_{\overline{\mathbf{Q}}}$, for some $N \geq 1$. It is well known that all complex multiplication elliptic curves have this property; this follows from [26, Th. 1]. Hence we are principally interested in elliptic curves $C/\overline{\mathbf{Q}}$ without complex multiplication.

In this article, we introduce the concept of an abelian variety over $\mathbf{Q}$ which is of "$\mathbf{GL}_2$-type." Roughly speaking, this is an abelian variety over $\mathbf{Q}$ whose algebra of $\mathbf{Q}$-endomorphisms is a number field of degree equal to the dimension of the abelian variety. It is easy to see that $J_1(N)$ decomposes up to isogeny over $\mathbf{Q}$ as a product of such abelian varieties. Hence any $C/\overline{\mathbf{Q}}$ which is a quotient of some $J_1(N)$ is a quotient (over $\overline{\mathbf{Q}}$) of an abelian variety of $\mathbf{GL}_2$-type over $\mathbf{Q}$.

We prove in this article the following facts (the third is a simple corollary of the first two):

1. Let C be an elliptic curve over $\overline{\mathbf{Q}}$ without complex multiplication. Then C is a quotient of an abelian variety of $\mathbf{GL}_2$-type over $\mathbf{Q}$ if and only if C is isogenous to each of its Galois conjugates ${}^{\sigma}C$ with $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. (If C has this latter property, we say that C is a "$\mathbf{Q}$-curve." The terminology is borrowed from Gross [7].)
2. Assume Serre's conjecture [24, (3.2.4$_?$)] on representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then every abelian variety of $\mathbf{GL}_2$-type over $\mathbf{Q}$ is a quotient of $J_1(N)$ for some $N \geq 1$.
3. Let $C/\overline{\mathbf{Q}}$ be an elliptic curve without complex multiplication. If C is a quotient of $J_1(N)_{\overline{\mathbf{Q}}}$ for some N, then C is a $\mathbf{Q}$-curve. Conversely, suppose that C is a $\mathbf{Q}$-curve. Then if the conjecture [24, (3.2.4$_?$)] is correct, C is a quotient of $J_1(N)_{\overline{\mathbf{Q}}}$ for some N.

In summary, we arrive at a conjectural characterization of elliptic curves over $\overline{\mathbf{Q}}$ which are quotients of modular curves $X_1(N)$: they are exactly the $\mathbf{Q}$-curves in the sense indicated above. This characterization was predicted by Serre.

2. Abelian varieties over $\mathbf{Q}$ of $\mathbf{GL}_2$-type.

We will be concerned with abelian varieties over $\mathbf{Q}$ which admit actions of number fields that are "as large as possible." We first quantify this concept.

Suppose that A is an abelian variety over $\mathbf{Q}$ and that E is a number field acting on A up to isogeny over $\mathbf{Q}$:

$$E \hookrightarrow \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_{\mathbf{Q}}(A).$$

By functoriality, E acts on the space of tangent vectors $\mathrm{Lie}(A/\mathbf{Q})$, which is a $\mathbf{Q}$-vector space of dimension $\dim A$. (For an account of the Lie algebra attached to a group scheme over a field, see for example [14, §11].) The dimension of this vector space is therefore a multiple of $[E\colon \mathbf{Q}]$, so that we have $[E\colon \mathbf{Q}] \mid \dim A$. In particular, $[E\colon \mathbf{Q}] \leq \dim A$.

This observation motivates the study of abelian varieties $A/\mathbf{Q}$ whose endomorphism algebras contain number fields of maximal dimension $\dim A$. If E is a number field of degree $\dim A$ which is contained in $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$, then the Tate modules $V_\ell(A)$ associated with A are free of rank two over $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. Accordingly, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $V_\ell(A)$ defines a representation with values in $\mathbf{GL}(2, E \otimes \mathbf{Q}_\ell)$. We say that A is of "$\mathbf{GL}_2$-type."

Suppose that B is of $\mathbf{GL}_2$-type, and that $F \subseteq \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(B)$ is a number field of degree $\dim B$. Let E be a number field containing F, and let $n = [E\colon F]$. After choosing a basis for E over F, we find an embedding $E \subseteq M(n, F)$ of E into the ring of n by n matrices over F. Since $M(n, F)$ acts naturally up to isogeny on $A := B \times \cdots \times B$ (n factors), we obtain an embedding $E \subseteq \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$. Hence A is again of $\mathbf{GL}_2$-type. (We can summarize the situation by writing $A = E \otimes_F B$.)

We say that an abelian variety $A/\mathbf{Q}$ of $\mathbf{GL}_2$-type is *primitive* if it is not isogenous over $\mathbf{Q}$ to an abelian variety obtained by this matrix construction, relative to an extension E/F of degree $n > 1$ (cf. [31, §8.2]).

(2.1) Theorem. *Let A be an abelian variety of $\mathbf{GL}_2$-type over $\mathbf{Q}$. Then the following conditions are equivalent: (i) A is primitive; (ii) $A/\mathbf{Q}$ is simple; (iii) the endomorphism algebra of $A/\mathbf{Q}$ is a number field whose degree coincides with the dimension of A.*

Proof. Let E be a number field of degree $\dim A$ which is contained in the $\mathbf{Q}$-algebra $\mathcal{X} := \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_{\mathbf{Q}}(A)$. Let D be the commutant of E in $\mathcal{X}$. We claim that D is a division algebra (cf. [16, Th. 2.3]).

To prove the claim, we must show that each non-zero $\mathbf{Q}$-endomorphism of A which commutes with E is an isogeny. Let λ be such an endomorphism and let B be the image of λ. Then B is a non-zero abelian subvariety of A. The field E operates on B (up to isogeny), and thereby acts by functoriality on the $\mathbf{Q}$-vector space $\mathrm{Lie}(B/\mathbf{Q})$. The dimension of $\mathrm{Lie}(B/\mathbf{Q})$ is accordingly a multiple of $[E\colon \mathbf{Q}]$; on the other hand, it coincides with $\dim B$. Hence $B = A$, so that λ is an isogeny.

The Lie algebra $\mathrm{Lie}(A/\mathbf{Q})$ may now be viewed as a D-vector space. Because of this, the dimension of $\mathrm{Lie}(A/\mathbf{Q})$ is a multiple of $\dim_{\mathbf{Q}}(D)$. In other words, we have $\dim(D) \mid \dim(E)$. This gives the equality $D = E$; i.e., it shows that E is its own commutant in $\mathcal{X}$.

In particular, the center F of $\mathcal{X}$ is a subfield of E. We have then $\mathcal{X} \approx M(n, Q)$, where Q is a division algebra with center F. If Q has dimension t^2 over F, then $nt = [E\colon F]$. This follows from the fact that E is a maximal commutative semisimple subalgebra of $\mathcal{X}$, which in turn follows from the statement that E is its own commutant in $\mathcal{X}$.

The structure of $\mathcal{X}$ shows that A is isogenous (over $\mathbf{Q}$) to a product of n copies of an abelian variety B whose algebra of $\mathbf{Q}$-endomorphisms is isomorphic to Q. The same Lie algebra argument we have already used shows that $\dim_{\mathbf{Q}}(Q) \mid \dim(B)$, so that $n \cdot \dim_{\mathbf{Q}}(Q) \mid \dim(A)$. This gives the divisibility $nt^2[F\colon \mathbf{Q}] \mid [E\colon \mathbf{Q}]$, which implies $nt^2 \mid nt$. One deduces that $t = 1$, i.e., that $Q = F$, and obtains the equality $n = [E\colon F]$. Hence the dimension of B coincides with the degree of F over $\mathbf{Q}$. Also, we have $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A) \approx M(n, F)$.

In other words, A is obtained from B and F by the construction we outlined above. The equivalence of the three statements in the theorem is now clear: each assertion is equivalent to the equality $n = 1$. ∎

3. ℓ-ADIC REPRESENTATIONS ATTACHED TO PRIMITIVE ABELIAN VARIETIES OVER $\mathbf{Q}$ OF $\mathbf{GL}_2$-TYPE.

In what follows, we study primitive abelian varieties of $\mathbf{GL}_2$-type over $\mathbf{Q}$. Since we never encounter such abelian varieties which are not primitive in the above sense, we will often drop the word "primitive" and refer simply to abelian varieties over $\mathbf{Q}$ of $\mathbf{GL}_2$-type.

To motivate the study of these varieties, we first allude to the existence of a large class of examples of (primitive) abelian varieties of $\mathbf{GL}_2$-type over $\mathbf{Q}$. Suppose that $f = \sum a_n q^n$ is a normalized cuspidal eigenform of weight two on a subgroup of $\mathbf{SL}(2,\mathbf{Z})$ of the form $\Gamma_1(N)$. Then Shimura [27, Th. 7.14] associates to f an abelian variety $A = A_f$ over $\mathbf{Q}$ together with an action on A of the field $E = \mathbf{Q}(\dots, a_n, \dots)$. The variety A_f may be constructed as a quotient of $J_1(N)$, the Jacobian of the standard modular curve $X_1(N)$ [29]. The dimension of A and the degree of E are equal. It is well known (and easy to show) that E is the full algebra of endomorphisms of A which are defined over $\mathbf{Q}$ [19, Cor. 4.2]. Thus, A is of $\mathbf{GL}_2$-type over $\mathbf{Q}$. For each $N \geq 1$, the Jacobian $J_1(N)$ is isogenous to a product of abelian varieties of the form A_f [19, Prop. 2.3].

In §4, we study the converse problem: Suppose that $A/\mathbf{Q}$ is of $\mathbf{GL}_2$-type. Is A isogenous to a quotient of $J_1(N)$, for some $N \geq 1$? We show that an affirmative answer is implied by conjecture ($3.2.4_?$) of Serre's article [24] on modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

We now begin the study of Galois representations attached to $\mathbf{GL}_2$-type abelian varieties over $\mathbf{Q}$. Suppose that A is such an abelian variety. Let E be the endomorphism algebra of $A/\mathbf{Q}$. Then E is a number field which is either a totally real number field or a "CM field," since each $\mathbf{Q}$-polarization of A defines a positive involution on E.

Recall that for each prime number ℓ, the Tate module $V_\ell = V_\ell(A)$ is free of rank two over $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. For each prime $\lambda \mid \ell$ of E, let E_λ be the completion of E at λ, and set $V_\lambda := V_\ell \otimes_{E\otimes\mathbf{Q}_\ell} E_\lambda$. Thus V_λ is a two-dimensional vector space over E_λ, and V_ℓ is the direct sum of the V_λ with $\lambda \mid \ell$. The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on V_λ defines a "λ-adic representation" ρ_λ. One knows that the collection (ρ_λ) (as λ ranges over the set of finite primes of E) forms a strictly compatible system of E-rational representations whose exceptional set is the set of prime numbers at which A has bad reduction. (For background on this material, see [25, §11.10] and perhaps [17, Ch. II].) We will prove some facts about the λ-adic representations ρ_λ and their reductions mod λ.

For each λ, let $\delta_\lambda\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to E_\lambda^*$ be the determinant of ρ_λ. The δ_λ form a compatible system of E-rational one-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In the case where E is totally real, we have $\det \rho_\lambda = \chi_\ell$, where

$$\chi_\ell\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_\ell^*$$

is the ℓ-adic cyclotomic character, and where ℓ is the prime of $\mathbf{Q}$ lying below λ [17, Lemma 4.5.1]. This formula must be modified slightly in the case where E is allowed to be a CM-field:

(3.1) Lemma. *There is a character of finite order* $\epsilon\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to E^*$ *such that* $\delta_\lambda = \epsilon\chi_\ell$ *for each finite prime* λ *of* E*. This character is unramified at each prime which is a prime of good reduction for* A*.*

Proof. Since the abelian representations δ_λ arise from an abelian variety, they have the Hodge-Tate property. It follows that they are locally algebraic in the sense of [21, Ch. III]; see [21, p. III-50] and [17, Prop. 1.5.3]. One deduces that the family δ_λ is associated with an E-valued Grossencharacter of type A_o of the field $\mathbf{Q}$ [17, p. 761]. Since the type-A_o Grossencharacters of $\mathbf{Q}$ are just products of Dirichlet characters with powers of the "norm" character, there is an integer n and an E-valued Dirichlet character ϵ so that we have $\delta_\lambda = \epsilon\chi_\ell^n$ for each λ. Here, ℓ again denotes the residue characteristic of λ. (We will use the association $\ell \leftrightarrow \lambda$ from time to time without comment.) We have blurred the distinction between characters of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of finite order and Dirichlet characters: if ϵ is a Dirichlet character, then its Galois-theoretic avatar takes the value $\epsilon(p)$ on a Frobenius element for p in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

By the criterion of Néron-Ogg-Shafarevich, ρ_λ is ramified at a prime $p \neq \ell$ if and only if A has bad reduction at p. Thus, δ_λ is unramified at a prime $p \neq \ell$ if A has good reduction at p. In other words, if p is a prime of good reduction for A, and if $\ell \neq p$, then $\epsilon\chi_\ell^n$ is unramified at p. Since χ_ℓ is unramified at p, ϵ is unramified at p.

It remains to check that $n = 1$. For this, fix a prime number ℓ. It is well known that the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\det_{\mathbf{Q}_\ell}(V_\ell)$ is given by the character $\chi_\ell^{\dim(A)} = \chi_\ell^{[E:\,\mathbf{Q}]}$. On the other hand, the determinant of the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on V_ℓ is given by the character

$$\prod_{\lambda|\ell} \mathbf{N}_{E_\lambda/\mathbf{Q}_\ell}(\delta_\lambda) = \mathbf{N}_{E/\mathbf{Q}}(\epsilon)\cdot\chi_\ell^{n\cdot[E:\,\mathbf{Q}]}.$$

(Here, $\mathbf{N}$ denotes a norm.) Since χ_ℓ has infinite order, we deduce that $\mathbf{N}(\epsilon) = 1$ and that $n = 1$. ■

(3.2) Lemma. *Each character δ_λ is odd in the sense that it takes the value -1 on complex conjugations in* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

[Since χ_ℓ is an odd character, the Lemma may be reformulated as the statement that $\epsilon(-1) = +1$.] For the proof, we use the comparison isomorphism

$$V_\lambda \approx H_1(A(\mathbf{C}), \mathbf{Q}) \otimes_E E_\lambda$$

resulting from an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. In this view of V_λ, the complex conjugation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on V_λ as $F_\infty \otimes 1$, where F_∞ is the standard "real Frobenius" on $H_1(A(\mathbf{C}), \mathbf{Q})$ (cf. [4, §0.2]). In particular, δ_λ is odd if and only if we have $\det F_\infty = -1$, where the determinant is taken relative to the E-linear action of F_∞ on $H_1(A(\mathbf{C}), \mathbf{Q})$.

Since F_∞ is an involution, and $H_1(A(\mathbf{C}), \mathbf{Q})$ has dimension two, the indicated determinant is $+1$ if and only if F_∞ acts as a scalar ($= \pm 1$) on $H_1(A(\mathbf{C}), \mathbf{Q})$. To prove that F_∞ does *not* act as a scalar, we recall that $F_\infty \otimes 1$ permutes the two subspaces $H_{0,1}$ and $H_{1,0}$ of $H_1(A(\mathbf{C}), \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$ in the Hodge decomposition of $H_1(A(\mathbf{C}), \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$. ■

(3.3) Proposition. *For each λ, ρ_λ is an absolutely irreducible two dimensional representation of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *over E_λ. We have* $\mathrm{End}_{\mathbf{Q}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]} V_\lambda = E_\lambda$.

Proof. Faltings [5] proved that V_ℓ is a semisimple $\mathbf{Q}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module whose commutant is $E \otimes \mathbf{Q}_\ell$. (This is the Tate conjecture for endomorphisms of A.)

Since V_ℓ is the product of the V_λ with $\lambda \mid \ell$, each module V_λ is semisimple over $\mathbf{Q}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ and satisfies $\mathrm{End}_{\mathbf{Q}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]} V_\lambda = E_\lambda$. This implies that V_λ is simple over E_λ, and that $\mathrm{End}_{E_\lambda} V_\lambda = E_\lambda$. The absolute irreducibility follows. ■

For each prime p at which A has good reduction, let a_p be the element of E such that

$$a_p = \mathrm{tr}_{E_\lambda}(\mathrm{Frob}_p \mid V_\lambda)$$

whenever $\ell \neq p$. Let $^-$ denote the canonical involution on E: this involution is the identity if E is totally real, and the "complex conjugation" on E if E is a CM field. The involution $^-$ is the Rosati involution on E induced by every polarization of $A/\mathbf{Q}$.

(3.4) Proposition. *We have $a_p = \overline{a}_p \epsilon(p)$ for each prime p of good reduction.*

Proof. Let ℓ be a prime number. Let $\sigma\colon E \hookrightarrow \overline{\mathbf{Q}}_\ell$ be an embedding of fields, and let $\bar\sigma$ be the conjugate embedding $x \mapsto \sigma(\overline{x})$. Let $V_\sigma = V_\ell \otimes_{E\otimes\mathbf{Q}_\ell} \overline{\mathbf{Q}}_\ell$, where the tensor product is taken relative to the map of $\mathbf{Q}_\ell$-algebras $E \otimes \mathbf{Q}_\ell \to \overline{\mathbf{Q}}_\ell$ induced by σ. Define $V_{\bar\sigma}$ similarly, using $\bar\sigma$.

Fix a polarization of A defined over $\mathbf{Q}$. The associated e_{ℓ^ν}-pairings of Weil induce a bilinear map $\langle\ ,\ \rangle\colon V_\ell \times V_\ell \to \mathbf{Q}_\ell(1)$, where $\mathbf{Q}_\ell(1)$ is (as usual) the $\mathbf{Q}_\ell$-adic Tate module attached to the ℓ-power roots of unity in $\overline{\mathbf{Q}}$. We have $\langle ex, y\rangle = \langle x, \overline{e}x\rangle$ for $e \in E$ and $x, y \in V_\ell$. Further, this pairing is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant in the sense that we have $\langle {}^g x, {}^g y\rangle = {}^g\langle x, y\rangle$ for $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. After extending scalars from $\mathbf{Q}_\ell$ to $\overline{\mathbf{Q}}_\ell$, we find an isomorphism of $\overline{\mathbf{Q}}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-modules

$$V_{\bar\sigma} \approx \mathrm{Hom}(V_\sigma, \overline{\mathbf{Q}}_\ell(1)).$$

Now (3.1) implies that the determinant of V_σ is a one-dimensional $\overline{\mathbf{Q}}_\ell$-vector space on which $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts by the character ${}^\sigma\epsilon\chi_\ell$. Since V_σ is of dimension two, this gives

$$\mathrm{Hom}(V_\sigma, \overline{\mathbf{Q}}_\ell({}^\sigma\epsilon\chi_\ell)) \approx V_\sigma.$$

In view of the fact that $\mathrm{Hom}(V_\sigma, \overline{\mathbf{Q}}_\ell({}^\sigma\epsilon\chi_\ell))$ is the twist by ${}^\sigma\epsilon$ of $\mathrm{Hom}(V_\sigma, \overline{\mathbf{Q}}_\ell(1))$, we get $V_\sigma \approx V_{\bar\sigma}({}^\sigma\epsilon)$. For $p \neq \ell$ a prime of good reduction, the trace of Frob_p acting on V_σ is $\sigma(a_p)$, and similarly the trace of Frob_p acting on $V_{\bar\sigma}({}^\sigma\epsilon)$ is ${}^\sigma\epsilon(p)\bar\sigma(a_p) = {}^\sigma\epsilon(p)\sigma(\overline{a}_p)$. This gives $a_p = \epsilon(p)\overline{a}_p$, as required. ■

(3.5) Proposition. *Let S be a finite set of prime numbers including the set of primes at which A has bad reduction. Then the field E is generated over $\mathbf{Q}$ by the a_p with $p \notin S$.*

Proof. The Proposition follows from the Tate Conjecture for endomorphisms of A by a simple argument, which we now sketch (see [17, pp. 788–789] for more details). Choose a prime number ℓ, and observe that $\mathrm{End}_{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})} V_\ell = E \otimes \mathbf{Q}_\ell$ because of Faltings's results quoted in the proof of (3.3). Let $\overline{V}_\ell = V_\ell \otimes \overline{\mathbf{Q}}_\ell$; then as a consequence we have $\mathrm{End}_{\overline{\mathbf{Q}}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]} \overline{V}_\ell = E \otimes \overline{\mathbf{Q}}_\ell$. In addition, the semisimplicity of the V_ℓ implies that $\overline{V}_\ell$ is semisimple as a $\overline{\mathbf{Q}}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. For each $\sigma\colon E \hookrightarrow \overline{\mathbf{Q}}_\ell$, let V_σ be as above. Then the V_σ are simple $\overline{\mathbf{Q}}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-modules, and they are pairwise non-isomorphic. Indeed, they are a priori semisimple, but the commutant of their product is $\prod_\sigma \overline{\mathbf{Q}}_\ell$. It follows that their traces are pairwise distinct. Since the trace of Frob_p acting on V_σ is $\sigma(a_p)$ (for $p \notin S \cup \{\ell\}$), the Cebotarev Density Theorem implies that the functions $p \mapsto \sigma(a_p), p \notin S \cup \{\ell\}$ are pairwise distinct. ■

For the next result, fix a finite set S as in (3.5), and let F be the subfield of E generated by the numbers $a_p^2/\epsilon(p)$ with $p \notin S$.

(3.6) Proposition. *The field F is totally real. The extension E/F is abelian.*

Proof. Let $^-$ again be the canonical complex conjugation of E. For $p \notin S$, we have

$$\frac{\overline{a}_p^2}{\overline{\epsilon}(p)} = \frac{a_p^2}{\epsilon(p)^2}\epsilon(p)$$

by (3.4). The first assertion of the Proposition then follows. For the second, let $t_p = a_p^2/\epsilon(p)$. It is clear that E is contained in the extension of F (in an algebraic closure of E) obtained by adjoining to F the square roots of all t_p, and all roots of unity. This gives the second assertion. ■

We now consider the reductions of the λ-adic representations ρ_λ. To do this directly, replace A by an abelian variety which is $\mathbf{Q}$-isogenous to A and which has the property that its ring of $\mathbf{Q}$-endomorphisms is the ring of integers $\mathcal{O}$ of E. (This process does not change isomorphism classes of the λ-adic representations ρ_λ.) Write simply A for this new abelian variety. For each λ, consider the kernel $A[\lambda]$: this is the group of $\mathbf{Q}$-valued points of A which are killed by all elements of the maximal ideal λ of $\mathcal{O}$. The action of $\mathcal{O}$ on $A[\lambda]$ makes $A[\lambda]$ into a two-dimensional vector space over the residue field $\mathbf{F}_\lambda$ of λ. The $\mathbf{F}_\lambda$-linear action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $A[\lambda]$ defines a reduction $\overline{\rho}_\lambda$ of ρ_λ (cf. [17, II.2]). (There should be no confusion with the involution $^-$ which appears above.)

(3.7) Lemma. *For all but finitely many λ, the representation $\overline{\rho}_\lambda$ is absolutely irreducible.*

A result of Faltings [6, Theorem 1, page 204] implies that the following holds for almost all λ: $A[\lambda]$ is a semisimple $\mathbf{F}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ module whose commuting algebra is $\mathbf{F}_\lambda$. The Lemma follows directly from this statement. ■

4. Conjectural connection with modular forms.

We continue the discussion of §3, focusing on the possibility of linking A with modular forms, at least conjecturally. According to (3.7), $\overline{\rho}_\lambda$ is absolutely irreducible for almost all λ. For each λ such that $\overline{\rho}_\lambda$ is absolutely irreducible, conjectures of Serre [24, (3.2.3?–3.2.4?)] state that $\overline{\rho}_\lambda$ is "modular" in the sense that it arises from the space of mod ℓ cusp forms of a specific level N_λ, weight k_λ, and character ϵ_λ.

These invariants are essentially constant as functions of λ. Rather than study them for all λ, we will restrict attention to those maximal ideals λ which are odd, prime to the conductor of A, are unramified in E, and have degree one. Let Λ be the set of such ideals λ with the property that $\overline{\rho}_\lambda$ is absolutely irreducible. Lemma 3.7 implies that Λ is an infinite set.

(4.1) Lemma. *The levels N_λ are bounded as λ varies in Λ.*

Proof. It follows from the definition of N_λ that this level divides the conductor of the two-dimensional ℓ-adic representation ρ_λ. (To compare the two conductors, one can use the Hilbert Formula of [15, §I].) The conductor of ρ_λ divides the conductor of the full ℓ-adic representation $V_\ell(A)$. According to results of A. Grothendieck [8, Cor. 4.6], this latter conductor is independent of ℓ. (It is by definition the conductor of A.) ■

(4.2) Lemma. *For all $\lambda \in \Lambda$, we have $k_\lambda = 2$.*

Proof. Take $\lambda \in \Lambda$. The determinant of $\overline{\rho}_\lambda$ is the reduction mod λ of δ_λ. By (3.1), this determinant is the product of the mod ℓ cyclotomic character $\overline{\chi}_\ell$ and the reduction mod λ of ϵ. The definition of Λ shows that ℓ is a prime of good reduction for A, so that ϵ is unramified at ℓ (Lemma 3.1). Hence, if I is an inertia group for ℓ in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, we have $\det \overline{\rho}_\lambda \mid I = \overline{\chi}_\ell$.

Further, suppose that $D \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is a decomposition group for ℓ. It is clear that $\overline{\rho}_\lambda \mid D$ is finite at ℓ [24, p. 189], since A has good reduction at ℓ. Indeed, the kernel of multiplication by ℓ on $A_{\mathbf{Q}_\ell}$ extends to a finite flat group scheme $\mathcal{G}$ over $\mathbf{Z}_\ell$ because of this good reduction [8, Cor. 2.2.9]. The Zariski closure of $A[\lambda]$ in $\mathcal{G}$ then prolongs $\overline{\rho}_\lambda$ to a group scheme of type (ℓ, ℓ) over $\mathbf{Z}_\ell$.

By Proposition 4 of [24, §2.8], we find that $k_\lambda = 2$. ■

(4.3) Lemma. *For all but finitely many $\lambda \in \Lambda$, we have $\epsilon_\lambda = \epsilon$.*

One checks easily that $\epsilon_\lambda = \epsilon$ whenever ℓ is prime to the order of ϵ. We omit the details, since Lemma 4.3 will not be used below. ■

(4.4) Theorem. *Let A be an abelian variety over $\mathbf{Q}$ of $\mathbf{GL}_2$-type. Assume Serre's conjecture* [24, (3.2.4?)] *on representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Then A is isogenous to a $\mathbf{Q}$-simple factor of $J_1(N)$, for some $N \geq 1$.*

Proof. Applying [24, (3.2.4?)] to the representations $\overline{\rho}_\lambda$ with $\lambda \in \Lambda$, we find that each $\overline{\rho}_\lambda$ arises from a newform of weight $k_\lambda = 2$ and level dividing N_λ. Since the N_λ's are bounded (Lemma 4.1), there are only a finite number of such newforms.

Hence there is a fixed newform $f = \sum a_n q^n$ which gives rise to an infinite number of the $\overline{\rho}_\lambda$'s. Explicitly, we have the following situation. Let R be the ring of integers of the field $\mathbf{Q}(\ldots, a_n, \ldots)$. For an infinite number of $\lambda \in \Lambda$, there is a ring homomorphism $\varphi_\lambda \colon R \to \overline{\mathbf{F}}_\lambda$ mapping a_p to $\mathrm{tr}(\overline{\rho}_\lambda(\mathrm{Frob}_p))$ for all but finitely many primes p.

Let N be the level of f, and let A_f be the quotient of $J_1(N)$ which is associated to f. Let λ be a prime for which there is a φ_λ as above. By the Cebotarev Density Theorem, we have

$$A_f[\ell] \otimes_{R/\ell R} \overline{\mathbf{F}}_\lambda \approx A[\lambda] \otimes_{\mathbf{F}_\lambda} \overline{\mathbf{F}}_\lambda,$$

where $\overline{\mathbf{F}}_\lambda$ is regarded as an $R/\ell R$-module via φ_λ. Since $A_f[\ell] \otimes_{R/\ell R} \overline{\mathbf{F}}_\lambda$ is a quotient of $A_f[\ell] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}}_\lambda$, and since $\mathbf{F}_\lambda = \mathbf{F}_\ell$, we have

$$\mathrm{Hom}_{\overline{\mathbf{F}}_\lambda[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]}(A_f[\ell] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}}_\lambda, A[\lambda] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}}_\lambda) \neq 0.$$

It follows that $\mathrm{Hom}_{\mathbf{F}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]}(A_f[\ell], A[\lambda]) \neq 0$.

Hence we have $\mathrm{Hom}_{\mathbf{F}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]}(A_f[\ell], A[\ell]) \neq 0$ for an infinite number of prime numbers ℓ. By the theorem of Faltings quoted above, we get $\mathrm{Hom}_{\mathbf{Q}}(A_f, A) \neq 0$. Since A is a simple abelian variety over $\mathbf{Q}$, A must be a quotient of A_f. Since A_f is, in turn, a quotient of $J_1(N)$, we deduce that A is a quotient of $J_1(N)$. ∎

5. Decomposition over $\overline{\mathbf{Q}}$.

Suppose again that $A/\mathbf{Q}$ is an abelian variety of $\mathbf{GL}_2$-type, and let

$$E = \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A).$$

Let $\mathcal{X} = \mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(A)$ be the algebra of *all* endomorphisms of A.

(5.1) Proposition [Shimura]**.** *Suppose that $A_{\overline{\mathbf{Q}}}$ has a non-zero abelian subvariety of CM-type. Then $A_{\overline{\mathbf{Q}}}$ is isogenous to a power of a CM elliptic curve.*

This is Proposition 1.5 in [28]. For a generalization of this result, see Proposition 5.2 of [9]. See also the discussion in §4 of [18].

(5.2) Proposition. *Suppose that $A_{\overline{\mathbf{Q}}}$ has no non-zero abelian subvariety of CM type. Then the center of $\mathcal{X}$ is a subfield F of E. The algebra $\mathcal{X}$ is isomorphic either to a matrix ring over F, or else to a ring of matrices over a quaternion division algebra over F.*

Proof. We employ the same arguments used to prove (2.1) above and Theorem 2.3 of [16]. Let D be the commutant of E in $\mathcal{X}$. Clearly, D is a division algebra: otherwise, we can make E act on a proper non-zero abelian subvariety of $A_{\overline{\mathbf{Q}}}$, contrary to the hypothesis that no abelian subvariety of $A_{\overline{\mathbf{Q}}}$ is of CM type. Also, E is a subfield of D; it is a maximal commutative subfield because $A_{\overline{\mathbf{Q}}}$ does not have complex multiplication. Hence E is its own commutant in D. Since D is the commutant of E, we get $D = E$. In particular, the center of $\mathcal{X}$ is contained in E, so that the center is a subfield F of E.

Since $\mathcal{X}$ is now a central simple algebra over F, we have $\mathcal{X} \approx M(n, D)$, where D is now a division algebra with center F, and n is a positive integer. Suppose that D has dimension t^2 over F; then $[E\colon F] = nt$ since E is a maximal commutative subalgebra of $\mathcal{X}$. Up to isogeny, $A_{\overline{\mathbf{Q}}}$ is of the form B^n, where the endomorphism algebra of B contains D. Following an idea of J. Tunnell (cf. [20, Th. 1]), we fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and form the cohomology group $H^1(B(\mathbf{C}), \mathbf{Q})$. This is a $\mathbf{Q}$-vector space of dimension

$$2\dim(B) = \frac{2}{n}\dim(A) = \frac{2nt}{n}[F\colon \mathbf{Q}]$$

with a functorial action of D. Hence the $\mathbf{Q}$-dimension $t^2[F\colon \mathbf{Q}]$ of D divides the dimension over $\mathbf{Q}$ of $H^1(B(\mathbf{C}), \mathbf{Q})$, which is $2t[F\colon \mathbf{Q}]$. Thus $t \leq 2$, so that either $D = F$, or else D is a quaternion division algebra with center F. ∎

As in Proposition 3.6, let S be a finite set of primes containing the primes of bad reduction for A. Let F be the center of $\mathcal{X}$. Then we have:

(5.3) Theorem. *The field F is generated by the numbers $a_p^2/\epsilon(p)$ with $p \notin S$.*

In other words, the field F which appears in (3.6) is the same as the field F in (5.2).

To prove (5.3), we let ℓ be a prime which splits completely in E, so that all embeddings $E \hookrightarrow \overline{\mathbf{Q}}_\ell$ take values in $\mathbf{Q}_\ell$. Choose a finite extension K of $\mathbf{Q}$ such that all endomorphisms of A are defined over K, and let H be the corresponding open subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Replacing H be a smaller subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ if necessary, we may assume that H is contained in the kernel of ϵ. We have $\mathcal{X} \otimes \mathbf{Q}_\ell = \mathrm{End}_{\mathbf{Q}_\ell[H]} V_\ell$, by Faltings's results [5]. The center of $\mathcal{X} \otimes \mathbf{Q}_\ell$ is $F \otimes \mathbf{Q}_\ell$.

The Tate module V_ℓ decomposes as a product $\prod_\sigma V_\sigma$, where σ runs over the set Σ of embeddings $\sigma\colon E \to \mathbf{Q}_\ell$, and where $V_\sigma = V_\ell \otimes_{E\otimes\mathbf{Q}_\ell} \mathbf{Q}_\ell$, with $\mathbf{Q}_\ell$ being regarded as an $E \otimes \mathbf{Q}_\ell$ module via σ. (Cf. the proof of (3.4).) Each V_σ is a simple $\mathbf{Q}_\ell[H]$-module because A has no CM subvariety and because the action of H on V_ℓ is semisimple (Faltings). Hence $\mathrm{End}_H V_\sigma = \mathbf{Q}_\ell$ for each σ.

For each prime v of K which is prime to ℓ and the set of bad primes for A, there is a "trace of Frobenius" $t_v \in E$ associated with v. We have $\mathrm{tr}(\mathrm{Frob}_v \mid V_\sigma) = \sigma(t_v)$ for each σ. One knows for $\sigma, \tau \in \Sigma$ that V_σ and V_τ are isomorphic $\mathbf{Q}_\ell[H]$-modules if and only if $\sigma(t_v) = \tau(t_v)$ for all v, i.e., if and only if $\sigma|_L = \tau|_L$, where $L = \mathbf{Q}(\dots, t_v, \dots)$ (cf. [17, §IV.4]). This implies that the center of $\mathcal{X} \otimes \mathbf{Q}_\ell$ is $L \otimes \mathbf{Q}_\ell$. Thus $F \otimes \mathbf{Q}_\ell = L \otimes \mathbf{Q}_\ell$ (equality inside $E \otimes \mathbf{Q}_\ell$), which implies that $F = L$.

Suppose now that $\sigma = \tau$ on L, so that $V_\sigma \approx V_\tau$ as representations of H. A simple argument shows that there is a character $\varphi\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Q}_\ell^*$ such that $V_\sigma \approx V_\tau \otimes \varphi$ as $\mathbf{Q}_\ell[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-modules. The character φ is necessarily unramified at all primes $p \neq \ell$ which are primes of good reduction for A. Taking traces, we get $\sigma(a_p) = \varphi(p)\tau(a_p)$ for all such primes. By considering determinants, we get ${}^\sigma\epsilon = \varphi^2 \cdot {}^\tau\epsilon$. These two equations show that σ and τ agree on $a_p^2/\epsilon(p)$ for all good primes $p \neq \ell$.

It follows by Galois theory that we have $a_p^2/\epsilon(p) \in L$ for all good reduction primes $p \neq \ell$. Hence $a_p^2/\epsilon(p) \in F$ for all such p. By varying ℓ we obtain the inclusion $\mathbf{Q}(\dots, a_p^2/\epsilon(p), \dots) \subseteq F$, where p runs over the set of all primes of good reduction for A.

To prove the opposite inclusion, we must show that if $\sigma(a_p^2/\epsilon(p)) = \tau(a_p^2/\epsilon(p))$ for all p, then V_σ and V_τ are H-isomorphic. By the Cebotarev Density Theorem, the hypothesis implies that the functions on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ "$\mathrm{tr}^2 / \det$" are the same for V_σ and V_τ. In particular, we have $\mathrm{tr}(h|V_\sigma) = \pm\,\mathrm{tr}(h|V_\tau)$ for all $h \in H$. This equality implies that V_σ and V_τ become isomorphic after H is replaced by an open subgroup H_o of H (cf. [22, p. 324]). Since H was already chosen "sufficiently small," we find that V_σ and V_τ are indeed isomorphic as $\mathbf{Q}_\ell[H]$-modules. ■

(5.4) Corollary. *The center F of $\mathcal{X}$ is a totally real number field. The extension E/F is abelian.*

Proof. The Corollary follows from (5.3) and (3.6). ■

Let g be an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and consider the automorphism $x \mapsto {}^g x$ of $\mathcal{X}$ which is induced by g. This automorphism is necessarily inner (Skolem-Noether theorem), and it fixes E; therefore it is given by conjugation by an element $\alpha(g)$ of E^* which is well defined modulo F^*. The map $\alpha\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to E^*/F^*$ is a continuous homomorphism (cf. [20, p. 268]). It is a fact that α is unramified at all primes p at which A has semistable reduction [16, Th. 1.1].

(5.5) Theorem. *We have* $\alpha^2 \equiv \epsilon \pmod{F^*}$. *Moreover, suppose that* p *is a prime of good reduction for* A *such that* $a_p \neq 0$. *Then* $\alpha(\mathrm{Frob}_p) \equiv a_p \pmod{F^*}$.

Proof. To prove the first assertion, let ℓ be a prime which splits completely in E. We must prove that $\sigma(\alpha^2(g)/\epsilon(g)) = \tau(\alpha^2(g)/\epsilon(g))$ whenever σ and τ are embeddings $E \hookrightarrow \mathbf{Q}_\ell$ which agree on F.

If σ and τ have this property, then there is a character $\varphi\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Q}_\ell^*$ for which $V_\sigma \approx V_\tau \otimes \varphi$ (the notation is as in the proof of (5.3)). The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\mathrm{Hom}(V_\sigma, V_\tau)$ by multiplication by $\varphi(g)^{-1}$, but also by conjugation by $\alpha(g)$. Since $\alpha(g)$ acts on V_σ and V_τ by ${}^\sigma\alpha(g)$ and ${}^\tau\alpha(g)$ (respectively), $\alpha(g)$ acts on $\mathrm{Hom}(V_\sigma, V_\tau)$ by ${}^\tau\alpha(g)/{}^\sigma\alpha(g)$. Hence, $\varphi(g) = {}^\sigma\alpha(g)/{}^\tau\alpha(g)$ in $\mathbf{Q}_\ell$. On the other hand, as remarked during the proof of (5.3), we have ${}^\sigma\epsilon = \varphi^2 \cdot {}^\tau\epsilon$. The two equalities give the required conclusion

$$\sigma(\alpha^2/\epsilon) = \tau(\alpha^2/\epsilon).$$

For the second assertion, we choose $\ell \neq p$. With the notation as above, $\varphi(p) = {}^\sigma\alpha(\mathrm{Frob}_p)/{}^\tau\alpha(\mathrm{Frob}_p)$. However, we have $\sigma(a_p) = \varphi(p)\tau(a_p)$, as noted during the proof of (5.3). On comparing two formulas for $\varphi(g)$, we get $\sigma(\alpha(\mathrm{Frob}_p)/a_p) = \tau(\alpha(\mathrm{Frob}_p)/a_p)$. ∎

Remark. It should be easy to prove that the set of p for which $a_p = 0$ has density 0, since the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in $\mathrm{Aut}\, V_\sigma$ is open in $\mathrm{Aut}\, V_\sigma$, for any σ.

Let $\tilde\alpha$ be a lift of α to a function $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to E^*$. The function

$$c\colon (g_1, g_2) \mapsto \frac{\tilde\alpha(g_1)\tilde\alpha(g_2)}{\tilde\alpha(g_1 g_2)}$$

is then a 2-cocycle on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with values in F^*. (We regard F^* as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module with trivial action.) The image $[c]$ of c in $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), F^*)$ is independent of the choice of $\tilde\alpha$. Since α^2 lifts to the character ϵ, it is clear that $[c]$ has order dividing two.

Consider the map

$$\xi\colon H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), F^*) \longrightarrow H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/F), \overline{\mathbf{Q}}^*) = \mathrm{Br}\, F$$

obtained from the restriction map $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), F^*) \to H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/F), F^*)$ and the map $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/F), F^*) \to H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/F), \overline{\mathbf{Q}}^*)$ induced by the inclusion of F^* into $\overline{\mathbf{Q}}^*$. (We view $\overline{\mathbf{Q}}^*$ as a $\mathrm{Gal}(\overline{\mathbf{Q}}/F)$-module in the standard way; i.e., we use the Galois action. The notation "$\mathrm{Br}\, F$" indicates the Brauer group of F.)

(5.6) Theorem [Chi]**.** *The class of* $\mathcal{X}$ *in* $\mathrm{Br}\, F$ *coincides with* $\xi([c])$.

Proof. According to [3, Th. 3.4], the algebra $\mathcal{X}$ is isomorphic to a twisted matrix algebra $(\mathrm{End}_F\, E)(\alpha)$. Theorem 4.8 of [3] expresses $[(\mathrm{End}_F\, E)(\alpha)] \in \mathrm{Br}\, F$ as the image of a certain two-cocycle whose values are Jacobi sums. By [20, Prop. 1], the class of this Jacobi-sum cocycle coincides with the class of the two-cocycle

$$(g, h) \mapsto \tilde\alpha(h)^{g-1} = \frac{{}^g\tilde\alpha(h)}{\tilde\alpha(h)}$$

on $\mathrm{Gal}(\overline{\mathbf{Q}}/F)$. We wish to compare this with the two-cocycle

$$(g,h) \mapsto \frac{\tilde{\alpha}(g)\tilde{\alpha}(h)}{\tilde{\alpha}(gh)}.$$

The product of the two is the map

$$(g,h) \mapsto \frac{{}^g\tilde{\alpha}(h)\tilde{\alpha}(g)}{\tilde{\alpha}(gh)},$$

which is a coboundary. Hence the class of $\mathcal{X}$ in $\mathrm{Br}\,F$ is the negative of $\xi([c])$. Since $[c]$ (and $[\mathcal{X}]$) have order two, we get the Theorem as stated. ■

A final remark about $\mathcal{X}$ concerns the isogeny class of the simple factors of $A_{\overline{\mathbf{Q}}}$. We have $\mathcal{X} \approx M(n,D)$ for some positive integer n, where D is a division algebra of dimension one or four over F. Accordingly, $A_{\overline{\mathbf{Q}}}$ decomposes up to isogeny as the product of n copies a simple abelian variety B over $\overline{\mathbf{Q}}$ whose endomorphism algebra is isomorphic to D. Since A is defined over $\mathbf{Q}$, we have

$${}^gB \times \cdots \times {}^gB \;\sim\; {}^gA_{\overline{\mathbf{Q}}} \;\sim A_{\overline{\mathbf{Q}}} \;\sim B \times \cdots \times B$$

for each $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. (The sign "$\sim$" indicates an isogeny.) By the uniqueness of decomposition up to isogeny, we have ${}^gB \sim B$. One says that the isogeny class of B is "defined over $\mathbf{Q}$."

Consider the special case where $n = \dim A$, so that B is of dimension one. The elliptic curve B is then isogenous to each of its conjugates (over $\overline{\mathbf{Q}}$). Borrowing (and bending) a term used by B. H. Gross [7], we say that B is a "$\mathbf{Q}$-curve."

6. $\mathbf{Q}$-curves as factors of abelian varieties of $\mathbf{GL}_2$-type.

We have just proved: Suppose that C is an elliptic curve over $\overline{\mathbf{Q}}$ which occurs as a simple factor of a primitive abelian variety of $\mathbf{GL}_2$-type over $\mathbf{Q}$ with no complex multiplication over $\overline{\mathbf{Q}}$. Then C is a $\mathbf{Q}$-curve; it is, more precisely, a $\mathbf{Q}$-curve with no complex multiplication.

In this §, we prove the converse:

(6.1) Theorem. *Suppose that C is an elliptic curve over $\overline{\mathbf{Q}}$ with no complex multiplication. Assume that C is isogenous to each of its conjugates ${}^gC$ with $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then there is a primitive abelian variety A of $\mathbf{GL}_2$-type over $\mathbf{Q}$ such that C is a simple factor of A over $\overline{\mathbf{Q}}$.*

(6.2) Corollary. *Suppose that C is as in (6.1). Assume Serre's conjecture* [24, (3.2.4?)] *on representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Then C is a simple factor, over $\overline{\mathbf{Q}}$, of $J_1(N)$ for some $N \geq 1$.*

The Corollary follows directly from (6.1) and (4.4). ■

Proof of (6.1). Let C be as in the statement of the Theorem. We can find a model C_o of C over a number field $K \subset \overline{\mathbf{Q}}$. We may assume that $K/\mathbf{Q}$ is a Galois extension. For each $g \in \mathrm{Gal}(K/\mathbf{Q})$, C_o and ${}^gC_o$ are $\overline{\mathbf{Q}}$-isogenous. Enlarging K if necessary, we may assume that there are isogenies $\mu_g\colon {}^gC_o \to C_o$ defined over K.

The map

$$c\colon (g,h) \mapsto \mu_g {}^g\mu_h \mu_{gh}^{-1}$$

may be regarded as $\mathbf{Q}^*$-valued, since $\mathbf{Q} \otimes \mathrm{End}_K(C_o) = \mathbf{Q}$. A short computation shows that c is a two-cocycle on $\mathrm{Gal}(K/\mathbf{Q})$ with values in $\mathbf{Q}^*$. The class of c in $H^2(\mathrm{Gal}(K/\mathbf{Q}), \mathbf{Q}^*)$ is independent of the choices of the μ_g. By inflation, we may (and will) regard c as a locally constant function on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

(6.3) Theorem [Tate]**.** *Let M be the discrete* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-module* $\overline{\mathbf{Q}}^*$ *with trivial action. Then* $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), M) = 0$.

This theorem of Tate is proved as Theorem 4 in Serre's article [23], with $\overline{\mathbf{Q}}$ replaced by $\mathbf{C}$. The proof exposed by Serre begins with the observation that

$$H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{C}^*) = H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), W),$$

where W is the torsion subgroup of $\mathbf{C}^*$, i.e., the group of complex roots of unity. This observation follows from the fact that $\mathbf{C}^*/W$ is uniquely divisible. Since $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts trivially on $\mathbf{C}^*$, W is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-isomorphic to $\mathbf{Q}/\mathbf{Z}$. One proves that $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{Q}/\mathbf{Z}) = 0$; in fact, we have $H^2(\mathrm{Gal}(\overline{K}/K), \mathbf{Q}/\mathbf{Z}) = 0$ whenever K is a local or global field [23, §6.5].

Since the quotient of M by its torsion subgroup is uniquely divisible, and since the torsion subgroup of M is isomorphic to $\mathbf{Q}/\mathbf{Z}$, we obtain $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), M) = H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{Q}/\mathbf{Z}) = 0$. ∎

Because of Tate's theorem, there is a locally constant function $\alpha\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{Q}}^*$ such that we have the identity among functions $G \times G \to \overline{\mathbf{Q}}^*$

$$c(g,h) = \frac{\alpha(g)\alpha(h)}{\alpha(gh)}.$$

After again enlarging K, we may identify α with a function on $\mathrm{Gal}(K/\mathbf{Q})$ and regard g and h as elements of this Galois group.

Let E be the extension of $\mathbf{Q}$ generated by the values of α. The definition of c shows that we have

$$c(g,h)^2 = \frac{\deg \mu_g \deg \mu_h}{\deg \mu_{gh}},$$

where "deg" denotes the degree of an isogeny between elliptic curves (or, more generally, of a non-zero element of $\mathbf{Q} \otimes \mathrm{Hom}(C_1, C_2)$, where C_1 and C_2 are elliptic curves). It follows that the function

$$\epsilon\colon g \mapsto \frac{\alpha^2(g)}{\deg \mu_g}$$

is a Dirichlet character $\mathrm{Gal}(K/\mathbf{Q}) \to E^*$. Because $\alpha^2 \equiv \epsilon \pmod{\mathbf{Q}^*}$, the field E is an abelian extension of $\mathbf{Q}$ (cf. Prop. 3.6).

If one performs the analysis of §3 on the abelian variety A which we construct below, one finds (e.g., in (3.1)) another Dirichlet character called ϵ. It is very likely that the two ϵ's are equal up to "sign," i.e., possible inversion (cf. Lemma 7.1 below).

To simplify notation, let us write simply C for the elliptic curve C_o over K and $C_{\overline{\mathbf{Q}}}$ for the curve originally called C. Let B be the abelian variety $\operatorname{Res}_{K/\mathbf{Q}} C$, where "Res" is Weil's "restriction of scalars" functor [33, 13]. Then B is an abelian variety over $\mathbf{Q}$ of dimension $[K:\mathbf{Q}]$. It represents the functor on $\mathbf{Q}$-schemes $S \mapsto C(S_K)$; in particular, we have $\operatorname{Hom}_{\mathbf{Q}}(X,B) = \operatorname{Hom}_K(X_K, C)$ whenever X is an abelian variety over $\mathbf{Q}$.

Applying this formula in the special case where $X = B$, we find $\operatorname{End}_{\mathbf{Q}}(B) = \operatorname{Hom}_K(B_K, C)$. On the other hand [33, p. 5],

$$B_K = \prod_{\sigma\in\operatorname{Gal}(K/\mathbf{Q})} {}^{\sigma}C.$$

Hence we have

$$\mathbf{Q}\otimes\operatorname{End}_Q(B) = \prod_{\sigma} \mathbf{Q}\otimes\operatorname{Hom}_K({}^{\sigma}C, C).$$

Since $\mathbf{Q}\otimes\operatorname{Hom}({}^{\sigma}C, C)$ is the one-dimensional vector space generated by μ_σ, we find that $\mathcal{R} := \mathbf{Q}\otimes\operatorname{End}_{\mathbf{Q}}(B)$ may be written as $\prod \mathbf{Q}\cdot\mu_\sigma$. Let λ_σ be the element of $\mathcal{R}$ which corresponds to $\mu_\sigma\colon {}^{\sigma}C \to C$; then $\mathcal{R}$ is a $\mathbf{Q}$-algebra with vector space basis λ_σ.

(6.4) Lemma. *We have $\lambda_\sigma\lambda_\tau = c(\sigma,\tau)\lambda_{\sigma\tau}$ in $\mathcal{R}$ for $\sigma,\tau\in\operatorname{Gal}(K/\mathbf{Q})$.*

Proof. Each map λ_σ acts on $B_K = \prod_g {}^{g}C$ as a "matrix": it sends the factor ${}^{g\sigma}C$ to ${}^{g}C$ by ${}^{g}\mu_\sigma$ (cf. [7. §15]). A short computation using the identity

$$\mu_\sigma\,{}^{\sigma}\mu_\tau = c(\sigma,\tau)\mu_{\sigma\tau}$$

gives the desired formula. ∎

The algebra $\mathcal{R}$ is thus a "twisted group algebra" $\mathbf{Q}[\operatorname{Gal}(K/\mathbf{Q})]$ in which we have the multiplication table $[\sigma][\tau] = c(\sigma,\tau)[\sigma\tau]$. The obvious map of $\mathbf{Q}$-vector spaces

$$\omega\colon \mathcal{R}\to E, \qquad \lambda_\sigma\mapsto\alpha(\sigma)$$

is in fact a surjective homomorphism of $\mathbf{Q}$-algebras because of (6.4).

In [2], $\mathbf{Q}\otimes\operatorname{End}_{\mathbf{Q}}(B)$ is studied in an analogous situation where C has complex multiplication, and where K is the Hilbert class field of the field of complex multiplication. (The curve C is then a "$\mathbf{Q}$-curve" in the original sense of the term.) Criteria are given for $\mathbf{Q}\otimes\operatorname{End}_{\mathbf{Q}}(B)$ to be (i) a commutative algebra, i.e., a product of number fields, and (ii) a product of *totally real* fields. It might be interesting to formulate similar criteria in our context.

Let T be the abelian variety $\prod_\sigma C$ over K. We write C_σ for the copy of C in the σth place, so that T becomes the product $\prod C_\sigma$. We have a map $\mathcal{R}\to\mathbf{Q}\otimes\operatorname{End}T$ given as follows: For $g\in\operatorname{Gal}(K/\mathbf{Q})$, the element $\lambda_g = [g]$ of $\mathcal{R}$ acts on T by sending C_σ to $C_{g\sigma}$ by the map (of elliptic curves up to isogeny) "multiplication by $c(g,\sigma)$." One checks directly that this is a homomorphism of $\mathbf{Q}$-algebras. The variety T will be interpreted as $\mathcal{R}\otimes_{\mathbf{Q}} C$ by readers who are fond of such tensor-product constructions.

Let $\iota\colon T \xrightarrow{\sim} B_K = \prod {}^{\sigma}C$ be the isomorphism of abelian varieties up to isogeny which takes the factor C_σ of T to the factor ${}^{\sigma^{-1}}C$ of B_K, via the map ${}^{\sigma^{-1}}\mu_\sigma$.

(6.5) Proposition. *The map ι is $\mathcal{R}$-equivariant, for the action of $\mathcal{R}$ on T just defined and for the structural action of $\mathcal{R}$ on B.*

Proof. The proof of this Proposition is an uninteresting computation, which is omitted.

(6.6) Corollary. *The Lie algebra* $\mathrm{Lie}(B/\mathbf{Q})$ *is a free $\mathcal{R}$-module of rank one.*

Proof. The statement to be proved is true if and only if $\mathrm{Lie}(B_K/K)$ is free of rank one over $R\otimes_{\mathbf{Q}}K$. By (6.5), $\mathrm{Lie}(B_K/K)$ may be identified with $\mathcal{R}\otimes_{\mathbf{Q}}\mathrm{Lie}(C/K)$, with $\mathcal{R}$ operating trivially on the second factor. Hence $\mathrm{Lie}(B_K/K)$ is indeed free of rank one over $\mathcal{R}\otimes_{\mathbf{Q}} K$. ∎

To complete the proof of (6.1), we let A be the abelian variety $E\otimes_{\mathcal{R}} B$, where E is viewed as a $\mathcal{R}$-module via ω. Explicitly, use the fact that $\mathcal{R}$ is a semisimple $\mathbf{Q}$-algebra to write $\mathcal{R}$ as a direct sum of its quotient E with the kernel of the map ω. Let $\pi\in\mathcal{R}$ be the projector onto E, and let $A\subseteq B$ be the image of π, viewed as an endomorphism of A up to isogeny. (In other words, A is the image of $m\cdot\pi$, where m is a positive integer chosen so that $m\cdot\pi$ is a true endomorphism of B.) Then A is an abelian subvariety of B, defined over $\mathbf{Q}$, whose algebra of $\mathbf{Q}$-endomorphisms is E. By (6.6), E acts without multiplicity on $\mathrm{Lie}(B)$ and therefore, in particular, without multiplicity on $\mathrm{Lie}(A)$. Hence A has dimension equal to $[E\colon \mathbf{Q}]$, which means that A is of $\mathbf{GL}_2$-type. (It is clear that A is non-zero because π is non-zero.)

Since B_K is isogenous to a product of copies of C, the same holds true for A_K. Thus C is a quotient of B_K. ∎

7. $\mathbf{Q}$-curves over quadratic fields.

Suppose that C is a $\mathbf{Q}$-curve as above and that K is a quadratic field. Let σ be the non-trivial automorphism of K over $\mathbf{Q}$. Then, by hypothesis, there is a K-isogeny $\mu=\mu_\sigma\colon {}^\sigma C\to C$. We take the identity map for μ_1, where "1" is the identity automorphism of K. The cocycle c takes the value 1 on all elements of $\mathrm{Gal}(K/\mathbf{Q})\times\mathrm{Gal}(K/\mathbf{Q})$ other than (σ,σ). Its value on that pair is the non-zero integer m such that $\mu\circ{}^\sigma\mu$ is multiplication by m on C. The algebra $\mathcal{R}$ may be written $\mathbf{Q}[X]/(X^2-m)$, where X corresponds to the element of $\mathcal{R}$ we have been calling $[\sigma]$.

Let us split c by defining $\alpha\colon\ \mathrm{Gal}(K/\mathbf{Q})\to\overline{\mathbf{Q}}^*$ to be the map taking 1 to 1 and σ to a square root of m. The character

$$\theta\colon g\mapsto\frac{\alpha^2(g)}{\deg\mu_g}$$

is then trivial if m is positive and of order two if m is negative. In the case where θ is of order two, it is an isomorphism $\mathrm{Gal}(K/\mathbf{Q})\xrightarrow{\sim}\{\pm1\}$.

If m is a perfect square, then we have $E=\mathbf{Q}$ in the notation of §6. The abelian variety A is then a model of C over $\mathbf{Q}$.

Assume for the rest of this § that m is not a perfect square. Then $\mathcal{R}=E$ is a quadratic number field, and we have $B=A$ in the notation of §6. The field E is real if m is positive and imaginary if m is negative. Thus E is real if and only if θ is trivial.

The λ-adic representations of A define a Dirichlet character ϵ (Lemma 3.1). According to (3.2), ϵ is an even character. Also, ϵ is non-trivial if and only if E is imaginary (3.4). Thus ϵ if non-trivial if and only if θ is non-trivial.

(7.1) Lemma. *The characters ϵ and θ are equal.*

Proof. By (6.5), A_K is K-isogenous to the abelian variety "$E\otimes C$," i.e., to the product of two copies of C with E acting through a regular representation $E \hookrightarrow M(2, \mathbf{Q})$. In particular, the λ-adic representations of A_K are just the ℓ-adic representations of C, viewed as taking values in $\mathbf{GL}(2, E_\lambda)$ rather than in $\mathbf{GL}(2, \mathbf{Q}_\ell)$. This implies that the determinants of the $\rho_\lambda|_{\mathrm{Gal}(\overline{\mathbf{Q}}/K)}$ are the cyclotomic characters χ_ℓ. Hence ϵ is trivial on $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$, and therefore may be identified with a character of the group $\mathrm{Gal}(K/\mathbf{Q})$, whose order is two. Since θ is also a character of this latter group, and since the two characters are simultaneously non-trivial, they are equal. ■

As mentioned above, it seems very likely that Lemma 7.1 (quite possibly in the form $\epsilon = \theta^{-1}$) generalizes to the situation of §6.

(7.2) Proposition [Serre]**.** *At least one of the two quadratic fields E, K is a real quadratic field.*

Proof. We give two proofs, the first of which was communicated to the author by Serre: Assume that K is a complex quadratic field. After we embed K in $\mathbf{C}$, the automorphism σ of K becomes the restriction to K of $\bar{\ }$, complex conjugation on $\mathbf{C}$. Choose a holomorphic differential ω on C. Then $C_{\mathbf{C}}$ may be identified with the curve $\mathbf{C}/L$, with $L \subset \mathbf{C}$ the period lattice of ω. The curve ${}^\sigma C$ becomes the complex conjugate $\mathbf{C}/\bar{L}$ of C. The isogeny μ is induced by the map "multiplication by γ" on $\mathbf{C}$, for some non-zero complex number γ. The integer m may be identified with $\gamma\bar{\gamma}$, and is therefore positive. This means that E is a real quadratic field.

Another proof can be given as follows. Assume that E is an imaginary quadratic field. Then ϵ is a non-trivial character of $\mathrm{Gal}(K/\mathbf{Q})$. This character is *even* by (3.2). Therefore K is real. ■

In connection with Proposition 7.2, it is natural to ask whether each of the three possibilities allowed by the Proposition do, in fact, occur. The case where E is imaginary, so that K is real, was treated in detail by Shimura [28, §10], who constructed a family of numerical examples. This case was later studied by Serre [24, p. 208], who pointed out that Theorem 4.4 holds in this context. A situation where E is a real quadratic field and K is an imaginary quadratic field is described by Koike in [10, §1]. In this example, the abelian variety A is associated to a weight-two newform on $\Gamma_o(81)$. One has $E = \mathbf{Q}(\sqrt{3})$ and $K = \mathbf{Q}(\sqrt{-3})$.

To exhibit an example where both E and K are real, we consider the eight-dimensional complex vector space S of weight-two cusp forms on $\Gamma_o(169)$. According to [1, Table 5], one can find a (normalized) newform $f = \sum a_n q^n \in S$ whose coefficients generate a quadratic field E. Moreover, the only two such forms are f and ${}^\sigma f = \sum {}^\sigma a_n q^n$, where σ is the non-trivial automorphism of E over $\mathbf{Q}$. Since f is a form with trivial "Nebentypus" character, E is a priori a real quadratic field. In fact, the author has learned from D. Zagier that tables constructed by Cohen and Skoruppa show that $E = \mathbf{Q}(\sqrt{3})$.

Let φ be the quadratic Dirichlet character with conductor 13. Then $f \otimes \varphi := \sum \varphi(n) a_n q^n$ is again a normalized newform in S; its coefficients generate the same quadratic field E as the coefficients of f. Hence we have either $f = \varphi \otimes f$, or else ${}^\sigma f = \varphi \otimes f$. The former possibility is excluded by [18, Th. 4.5], since φ is an even character (i.e., since φ corresponds to a real quadratic field). Hence f is a form with an "extra twist" by φ: we have $\varphi \otimes f = {}^\sigma f$. Moreover, again by Theorem 4.5 of [18], f is not a form with complex multiplication.

The abelian variety $A = A_f$ associated to f satisfies $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A) = E$. According to [19] (see especially Theorem 5.1 of [19]), the full algebra $\mathcal{X} = \mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(A)$ of A coincides with its subalgebra $\mathbf{Q} \otimes \mathrm{End}_K(A) = E$, where $K = \mathbf{Q}(\sqrt{13})$ is the extension of $\mathbf{Q}$ cut out by φ. This algebra is a quaternion algebra over $\mathbf{Q}$. Since K may be embedded in $\mathbf{R}$, a well known theorem of Shimura [30, Th. 0] implies that $\mathcal{X}$ is isomorphic to the matrix algebra $M(2, \mathbf{Q})$. (Once we know that $E = \mathbf{Q}(\sqrt{3})$, we can give an alternative proof that $\mathcal{X}$ is a matrix algebra which is based on the explicit description of $\mathcal{X}$ given in [19].) Hence A becomes isogenous over K to a product $C \times C$, where C is an elliptic curve defined over K. Therefore, we are in the situation described above, with $E = \mathbf{Q}(\sqrt{3})$ and $K = \mathbf{Q}(\sqrt{13})$.

8. Descent of abelian varieties up to isogeny.

Suppose that L/K is a Galois extension of fields and that A is an abelian variety over L. A well-known theorem of Weil [32] states that A has a model over K if and only if there are isomorphisms $\mu_\sigma\colon {}^\sigma A \xrightarrow{\sim} A$ ($\sigma \in \mathrm{Gal}(L/K)$) which satisfy the compatibility condition

$$\mu_\sigma {}^\sigma\mu_\tau = \mu_{\sigma\tau}. \tag{8.1}$$

As an application of the techniques encountered in §6, we will prove an analogous criterion for abelian varieties *up to isogeny.* Namely, suppose that A is isogenous (over L) to an abelian variety B/L which has a model over K. Then one finds isomorphisms $\mu_\sigma\colon {}^\sigma A \xrightarrow{\sim} A$ of abelian varieties up to isogeny over L which satisfy the compatibility condition (8.1). Conversely, one has

(8.2) Theorem. *Suppose that there are isomorphisms of abelian varieties up to isogeny over L, $\mu\colon {}^\sigma A \xrightarrow{\sim} A$, which satisfy (8.1). Then there is an abelian variety B over K such that A is L-isogenous to B_L.*

Proof. We can, and do, assume that L is a finite extension of K. Let X be the abelian variety $X = \mathrm{Res}_{L/K} A$. Recalling the discussion of §6, we find a decomposition

$$\mathbf{Q} \otimes \mathrm{End}_K(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \mathbf{Q} \otimes \mathrm{Hom}_L({}^\sigma A, A).$$

The homomorphism μ_σ in the "σ^{th} factor" corresponds to an element $[\sigma]$ of $\mathbf{Q} \otimes \mathrm{End}_K(X)$. The element $[g]$ operates on $\prod {}^\sigma A$ as a matrix, sending ${}^{\tau g}A$ to ${}^\tau A$ by ${}^\tau\mu_g$ for each $\tau \in \mathrm{Gal}(L/K)$.

Because the analogue of $c(\sigma, \tau)$ is 1 in this context, we have simply $[\sigma][\tau] = [\sigma\tau]$ for $\sigma, \tau \in \mathrm{Gal}(L/K)$: the identity (8.1) shows that the product of the matrices representing $[\sigma]$ and $[\tau]$ is the matrix representing $[\sigma\tau]$. Hence $\mathcal{R} := \mathbf{Q}[\mathrm{Gal}(L/K)]$ operates on X.

An analogue of Proposition 6.5 shows that we have

$$X_L \approx \mathcal{R} \otimes_{\mathbf{Q}} A$$

in the category of abelian varieties over L up to isogeny. To see this explicitly, we let A_σ be a copy of A indexed by σ and consider the isomorphism of abelian varieties over L up to isogeny

$$\iota\colon \prod_\sigma A_\sigma \xrightarrow{\sim} \prod_\sigma {}^\sigma A = X_L$$

which takes A_σ to ${}^{\sigma^{-1}}A$ via the map ${}^{\sigma^{-1}}\mu_\sigma$. Via this isomorphism, the automorphism $[\sigma]$ of X is transported to the permutation which takes each factor A_g of $\prod_g A_g$ to the factor $A_{\sigma g}$, via the identity map $A \to A$.

Let B be the image of $\eta := \sum_\sigma [\sigma]$, so that B is an abelian subvariety of X which is defined over K. (The sum η need not be a literal endomorphism of X, so that, strictly speaking, one should consider the image of a suitable multiple of η.) The isomorphism ι makes B_L correspond to the diagonal image of A in $\prod A_\sigma = A \times \cdots \times A$. Hence B_L is isogenous to A. ∎

References

1. B. J. Birch and W. Kuyk, eds., *Modular functions of one variable IV*, Lecture Notes in Math., vol. 476, Spring-Verlag, Berlin and New York, 1975.
2. J. Buhler and B. H. Gross, *Arithmetic on elliptic curves with complex multiplication. II*, Invent. Math **79** (1985), 11–29.
3. W. Chi, *Twists of central simple algebras and endomorphism algebras of some abelian varieties*, Math. Ann. **276** (1987), 615–632.
4. P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proceedings of Symposia in Pure Mathematics **33** (1979), (2) 313–346.
5. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
6. G. Faltings, G. Wüstholz et. al., *Rational points*, F. Vieweg & Sohn, Braunschweig/Wiesbaden, 1984.
7. B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Math., vol. 776, Spring-Verlag, Berlin and New York, 1980.
8. A. Grothendieck, *SGA7 I, Exposé IX*, Lecture Notes in Math., vol. 288, Springer-Verlag, Berlin and New York, 1972, pp. 313–523.
9. H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Am. J. Math. **103** (1981), 727–776.
10. M. Koike, *On certain abelian varieties obtained from new forms of weight 2 on* $\Gamma_0(3^4)$ *and* $\Gamma_0(3^5)$, Nagoya Math. J. **62** (1976), 29–39.
11. D. J. Lorenzini, *On the jacobian of the modular curve* $X_0(N)$ (to appear).
12. B. Mazur, *Number theory as gadfly*, Am. Math. Monthly **98** (1991), 593–610.
13. J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.
14. D. Mumford, *Abelian varieties*, Second edition, Oxford University Press, London, 1974.
15. A. Ogg, *Elliptic curves and wild ramification*, Am. J. Math. **89** (1967), 1–21.
16. K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Annals of Math. **101** (1975), 555–562.

17. ______, *Galois action on division points on abelian varieties with many real multiplications*, Am. J. Math. **98** (1976), 751–804.

18. ______, *The ℓ-adic representations attached to an eigenform with Nebentypus: a survey*, Lecture Notes in Math., vol. 601, Springer-Verlag, Berlin and New York, 1977, pp. 17–52.

19. ______, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), 43–62.

20. ______, *Endomorphism algebras of Abelian varieties attached to newforms of weight 2*, Progress in Math. **12** (1981), 263–276.

21. J-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Addison-Wesley Publ. Co., Redding, Mass., 1989.

22. ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

23. ______, *Modular forms of weight one and Galois representations*, prepared in collaboration with C. J. Bushnell, Algebraic number fields (L-functions and Galois properties), A. Fröhlich, ed., Academic Press, London, New York and San Francisco, 1977, pp. 193–268.

24. ______, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.

25. G. Shimura, *Algebraic number fields and symplectic discontinuous groups*, Ann. of Math. **86** (1967), 503–592.

26. ______, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208.

27. ______, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, 1971.

28. ______, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. **95** (1972), 131–190.

29. ______, *On the factors of the Jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), 523–544.

30. ______, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

31. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Second printing corrected, Math. Society of Japan, Tokyo, 1975.

32. A. Weil, *The field of definition of a variety*, Am. J. Math **78** (1956), 509–524.

33. ______, *Adeles and algebraic groups*, Progress in Math., vol. 23, Birkhäuser, Boston and Basel, 1982.

UC Mathematics Department, Berkeley, CA 94720 USA

E-mail address: `ribet@math.berkeley.edu`