ABELIAN VARIETIES DEFINED OVER THEIR FIELDS OF MODULI, I
ABELIAN VARIETIES DEFINED OVER THEIR FIELDS OF MODULI, I

J. S. MILNE

Whenever we consider a triple \((A, \Phi, \theta)\) we will mean that \(A\) is an abelian variety of dimension \(d\), \(\Phi\) is a polarization of \(A\), \(\theta : F \to \text{End}^d(A) = \text{End} (A) \otimes_{\mathbb{Q}} \mathbb{Q}\) is a ring homomorphism where \(F\) is a field of degree \(2d\) over \(\mathbb{Q}\), \(\theta(F') = \theta(F)\) where \(\alpha \mapsto \alpha'\) is the involution of \(\text{End}^d(A)\) induced by \(\Phi\), and that \(A\), \(\Phi\), and \(\theta\) are all defined over some subfield of the complex numbers \(\mathbb{C}\). \(F\) is then necessarily a CM-field, and \((A, \Phi, \theta)\) is of type \((F, \Phi; a, \zeta)\) in the sense of [5, p. 128] for some lattice \(a\) in \(F\) and element \(\zeta\) of \(F\). We will assume that the reader is familiar with the definitions in [5].

Our main result is that \((A, \Phi, \theta)\) always has a model defined over its field of moduli \(k_0\), i.e. that there is an \((A_0, \Phi_0, \theta_0)\) defined over \(k_0\) which becomes isomorphic to \((A, \Phi, \theta)\) over \(\mathbb{C}\). As a consequence, one gets an alternative proof of a theorem of Casselman's [6, Theorem 6] characterizing those Grössen-characters which arise from abelian varieties. Also, one obtains a positive answer to a question of Shimura's concerning the existence of such Grössen-characters [6, p. 513].

In a second paper we intend to consider the question of, given \((A, \Phi, \theta)\), when is the pair \((A, \Phi)\) defined over its field of moduli.

We write \(k_{ab}\) for the maximal abelian extension of a field \(k\), and \(\bar{k}\) for its algebraic closure. \((F', \Phi')\) denotes the reflex of a CM-type \((F, \Phi)\).

**Theorem.** Let \((A, \Phi, \theta)\), as above, be of CM-type \((F, \Phi)\). Then there is a model \((A_0, \Phi_0, \theta_0)\) of \((A, \Phi, \theta)\) defined over the field of moduli \(k_0\) of \((A, \Phi, \theta)\) and such that all torsion points of \(A_0\) are rational over \(F'_{ab}\).

**Proof.** Let \(S\) be the (ordered) set of points of \(A\) of order 3, and let \(k_1\) be the field of moduli of \((A, \Phi, \theta, S)\).

(i) \(F' \subset k_1 \subset F_{ab}\)

This follows from [5, 5.16]

(ii) There is a model \((A_1, \Phi_1, \theta_1, S)\) for \((A, \Phi, \theta, S)\) defined over \(k_1\).

It is easy to see that there is a finite normal extension \(K\) of \(k_1\) such that \((A, \Phi, \theta, S)\) is defined over \(K\) and such that for every \(\sigma \in \text{Gal}(K/k_1)\) there is an isomorphism \(\lambda_\sigma : (A, \Phi, \theta, S) \to (A^\sigma, \Phi^\sigma, \theta^\sigma, S^\sigma)\) defined over \(K\). Let \(\lambda_{1, \sigma} = \lambda^\sigma_{-1}\) for \(\sigma, \tau \in \text{Gal}(K/k_1)\). From the fact that \(\text{Aut}(A, \Phi, \theta, S) = \{1\}[3, \S 21, \text{Thm 5}]\) it follows that

\[
\lambda^\sigma_{1, \rho} = \lambda_{\rho \tau, \rho \sigma}
\]

\[
\lambda_{1, \sigma} \lambda_{\rho, \rho} = \lambda_{1, \rho}
\]

Received 8 June, 1972.

†This paper was written while the author was a visitor at King's College, London and the University of Nottingham, and was supported by the Science Research Council.

[BULL. LONDON MATH. SOC., 4 (1972), 370–372]
for all \( \rho, \sigma, \tau \in \text{Gal}(K/k_1) \). Assertion (ii) now follows from [7].

(iii) \( A_1 \), as in (ii) above, has all of its torsion points rational over \( F_{\text{ab}}' \). This is [5, 7.8.8].

Regard now \( (A, \mathcal{C}, \theta) \) as being defined over \( k_1 \) and satisfying (iii). If \( k_1 = k_0 \) then the theorem is proved. If not, there is a field \( k_2 \), \( k_1 \supset k_2 \supset k_0 \supset F' \), such that \( k_1/k_2 \) is Galois of prime degree \( p \) (use (i)). Let \( \sigma \) generate \( \text{Gal}(k_1/k_2) \) and let \( \lambda : (A, C, \theta) \to (A^\sigma, C^\sigma, \theta^\sigma) \) be an isomorphism.

(iv) \( \lambda \) is defined over \( k_1 \).

This is a consequence of [6, Thm 5, Pptn 1]. Alternatively it may be proved as follows. \( a \mapsto a^\sigma \) is an isomorphism \( V_i A \to V_i A^\sigma \) which commutes with the actions of \( F \) and of \( \text{Gal}(k_1/k_1) \) (use (iii)). But it is clear from [4, Cor 2 to Thm 5] that any homomorphism \( V_i A \to V_i A \) which commutes with the action of \( F \) commutes with the action of \( \text{Gal}(k_1/k_1) \). Thus \( x^\tau = \lambda \) for all \( \tau \in \text{Gal}(k_1/k_1) \) which proves (iv).

Write \( v \) for the canonical isomorphism \( a^\sigma \mapsto a : (A^\sigma, \mathcal{C}^\sigma, \theta^\sigma) \to (A, \mathcal{C}, \theta) \). Then \( \Lambda = v \lambda^{\sigma^{-1}} \cdots \lambda^{\sigma} \) is an automorphism of \( (A, \mathcal{C}, \theta) \), and hence may be written as \( \theta(\alpha) \) with \( \alpha \in \mu(R) \) where \( R = \theta^{-1}(\text{End}_C(A)) \) and \( \mu(R) \) is the set of roots of unity in \( R \).

(v) \( \alpha \) is a \( p \)th power in \( R \).

If \( \mu \) is a homomorphism of abelian varieties we write \( \mu_i \) for the corresponding map on the Tate groups \( T_i \) (or \( V_i \)). The map \( a \mapsto \lambda_i^{-1}(a^\sigma) : T_i A \to T_i A \) is \( Z_i \)-linear and commutes with the action of \( \theta(R) \). By [4, Cor. 1 to Thm. 5] there exists an \( \alpha_i \in R_i = R \otimes Z_i \) such that \( \lambda_i^{-1}(a^\sigma) = \theta(\alpha_i^{-1})(a) \) all \( a \in T_i A \). It follows that \( \Lambda_i(a) = \theta(\alpha_i^\sigma)(a) \) all \( a \in T_i A \). Hence \( \theta(\alpha) = \theta(\alpha_i^\sigma) \), and so \( \alpha \) is a \( p \)th power in \( R_i \) for all primes \( l \). By class field theory, e.g. [1, X], this implies that \( \alpha \) is a \( p \)th power in \( F \), say \( \alpha = \beta^p \). By using that \( \alpha \in \mu(R) \) and is a \( p \)th power in \( R_i \) for all \( l \), one gets that \( \beta \in R_i \) for all \( l \). But \( R = \bigcap R_i \), and so \( \beta \in R \).

Replace \( \lambda \) by \( \lambda \theta(\beta^{-1}) \), so that now \( \Lambda = 1 \). Define \( \lambda_{j, i} : A^{\sigma^j} \to A^{\sigma^i} \) by

\[
\lambda_{j, i} = \lambda^{\sigma^{j-1}} \cdots \lambda^{\sigma^i},
\]

\( 0 \leq i \leq j \leq p-1 \), and \( \lambda_{j, i} = v^{\sigma^j} \lambda_{j+p, i} \), \( 0 \leq j \leq i \leq p-1 \). Then \( \lambda_{k,j} \lambda_{j, i} = \lambda_{k, i} \) and \( \lambda_{j, i} = \lambda_{j+1, i+1} \) and so [7] there is an \( (A_2, \mathcal{C}_2, \theta_2) \) defined over \( k_2 \) which is isomorphic to \( (A, \mathcal{C}, \theta) \) over \( k_1 \). Note that \( A_2 \) will therefore also satisfy (iii). If \( k_2 = k \) the proof is complete. If not, the above process may be used to find an \( (A_3, \mathcal{C}_3, \theta_3) \) over some \( k_3 \), \( k_2 \supset k_3 \supset k, k_2 \neq k_3 \). By continuing in this way, one eventually obtains the desired result.

In order to state the two corollaries, consider \( (A, \mathcal{C}, \theta) \) defined over some number field \( k \), and let it be of type \( (F, \Phi; \alpha, \zeta) \). Regard \( F \) as a subfield of \( C \), write \( \mathcal{I}_k \) for the idèle group of \( k \), put \( \mathcal{I}_k,_{\infty} = k \otimes Q R \subset \mathcal{I}_k \), and write \( \mathcal{I}_k,_{\infty} \) for the group of finite idèles of \( k \), i.e. those whose component at any infinite prime is 1. If \( x \in \mathcal{I}_F \), write \( x_1 \) for the component of \( x \) corresponding to the infinite prime defined by the given embedding of \( F \subset C \). Then \( \text{det} \Phi' \) defines a homomorphism \( F^{*} \to F^{*} \) and, since \( k \supset F' \), we
get a homomorphism $g = (\det \Phi') N_{k/k'} : k^* \to F^*$. This extends to a continuous homomorphism $I_k \to I_F$ which we also denote by $g$.

As explained in [6, p. 510], one obtains from $(A, \mathcal{C}, \theta)$ a Groessen-character $\psi : I_k \to \mathbb{C}^*$ such that,

1. for all $x \in I_{k, \infty}$, $\psi(x) = g(x)_1^{-1}$, and
2. for all $x \in I_{k, 0}$, $\psi(x) \in F^*$, $\psi(x) \overline{\psi(x)} = |x|_0$, and $\psi(x) a = g(x) a$, where $\overline{\psi(x)}$ is the complex conjugate of $\psi(x)$ and $|x|_0$ is the absolute norm of the ideal associated to $x$. Conversely, there is the following result.

**Corollary 1.** Let $k$ be a finite extension of $F'$. Any Groessen-character $\psi : I_k \to \mathbb{C}^*$ satisfying (1) and (2) arises from some $(A, \mathcal{C}, \theta)$ of type $(F, \Phi; a, \zeta)$ defined over $k$.

**Proof.** Let $(A, \mathcal{C}, \theta)$ be any structure of type $(F, \Phi; a, \zeta)$. It follows from [5, 5.16] that $k$ contains the field of moduli of $(A, \mathcal{C}, \theta)$ and so we may take $(A, \mathcal{C}, \theta)$ to be defined over $k$. Let $\psi'$ be the Groessen-character arising from $(A, \mathcal{C}, \theta)$ and put $\chi = \psi/\psi'$. By (1), $\chi$ is a Dirichlet character and so may be regarded as a character of $G = \text{Gal}(K/k)$ for some finite abelian extension $K$ of $k$. Let $R_\chi$ be $R$ regarded as a $G$-module by defining $\sigma \alpha = \chi(\sigma) \alpha$ for $\sigma \in G$, $\alpha \in R$. Then, in the notation of [2, §2], $(A', \mathcal{C}', \theta')$ with $A' = R_\chi \otimes_R A$ and obvious $\theta'$ and $\mathcal{C}'$ is of type $(F, \Phi; a, \zeta)$ and has Groessen-character $\chi \psi' = \psi$.

**Corollary 2.** Let $k$ be a finite extension of $Q$ and let $(F, \Phi; a, \zeta)$ be a possible type for a structure $(A, \mathcal{C}, \theta)$. Then there is a Groessen-character $\psi : I_k \to \mathbb{C}^*$ satisfying (1) and (2) if and only if $k$ contains the field of moduli of some $(A, \mathcal{C}, \theta)$ of type $(F, \Phi; a, \zeta)$.

**Proof.** The necessity follows from [5, 5.16] and the sufficiency from the theorem.

**Remarks 1.** In [6], Corollary 1 is proved directly and then, under certain hypotheses on $R$ ((5.2) loc. cit.), Shimura explicitly constructs a Groessen-character $\psi$ satisfying (1) and (2) and so deduces a weaker form of our Theorem 1.

2. Given $A$ and the map $\theta$ it is always possible to find a polarization $\mathcal{C}$ such that $\theta(F') = \theta(F)$ [5, p. 128]. Moreover [6, Ppnt 4] the field of moduli of $(A, \mathcal{C}, \theta)$ is independent of the $\mathcal{C}$ chosen. Thus it makes sense to speak of the field of moduli of $(A, \theta)$, and then Theorem 1 implies that this is also the smallest field of definition of $(A, \theta)$.

**References**

1. E. Artin and J. Tate, *Class field theory* (Harvard University, 1961).
**CORRECTION:** ABELIAN VARIETIES DEFINED OVER THEIR FIELDS OF MODULI, I

**J. S. MILNE**


The proof of the theorem contains an error. Before giving a correct proof, we state two lemmas.

**Lemma 1.** Let $K/k$ be a cyclic Galois extension of degree $m$, let $\sigma$ generate $\text{Gal}(K/k)$, and let $(A, \mathcal{C}, \theta)$ be defined over $K$. Suppose that there exists an isomorphism $\lambda : (A, \mathcal{C}, \theta) \to (A^\sigma, \mathcal{C}^\sigma, \theta^\sigma)$ over $K$ such that $\nu^\lambda_{\sigma^{-1}} \ldots \lambda^\sigma \lambda = 1$, where $\nu$ is the canonical isomorphism $(A'^m, \mathcal{C}^m, \theta'^m) \to (A, \mathcal{C}, \theta)$. Then $(A, \mathcal{C}, \theta)$ has a model over $k$, which becomes isomorphic to $(A, \mathcal{C}, 0)$ over $K$.

**Proof.** This follows easily from [7], as is essentially explained on p. 371.

**Lemma 2.** Let $G$ be an abelian pro-finite group and let $\phi : G \to \mathbb{Q}/\mathbb{Z}$ be a continuous character of $G$ whose image has order $p$. Then either:

(a) there exist subgroups $G'$ and $H$ of $G$ such that $H$ is cyclic of order $p^m$ for some $m$, $\phi(G') = 0$, and $G = G' \times H$, or

(b) for any $m > 0$ there exists a continuous character $\phi_m$ of $G$ such that $p^m \phi_m = \phi$.

**Proof.** If (b) is false for a given $m$, then there exists an element $\sigma \in G$, of order $p'$ for some $r \leq m$, such that $\phi(\sigma) \neq 0$. (Consider the sequence dual to $0 \to \text{Ker}(\phi(p^m)) \to G \to \mathbb{Q}/\mathbb{Z}$). There exists an open subgroup $G_0$ of $G$ such that $\phi(G_0) = 0$ and $\sigma$ has order $p'$ in $G/G_0$. Choose $H$ to be the subgroup of $G$ generated by $\sigma$, and then an easy application to $G/G_0$ of the theory of finite abelian groups shows the existence of $G'$ (note that $\phi(\sigma) \neq 0$ implies that $\sigma$ is not a $p$-th power in $G$).

We now prove the theorem. The proof is correct up to the statement (iv) (except that (i) should read: $F' \subset k_1 \subset F'_{\text{ab}}$). To remove a minor ambiguity in the proof of (iv), choose $\sigma$ to be an element of $\text{Gal}(F'_{\text{ab}}/k_2)$ whose image $\bar{\sigma}$ in $\text{Gal}(k_1/k_2)$ generates this last group. The error occurs in the statement that the canonical map $\nu : A'^p \to A$ acts on points by sending $a'^p \mapsto a$; it, of course, sends $a \mapsto a$.

The proof is correct, however, in the case that it is possible to choose $\sigma$ so that $\sigma^p = 1$ (in $\text{Gal}(F'_{\text{ab}}/k_2)$).

By applying Lemma 2 to $G = \text{Gal}(F'_{\text{ab}}/k_2)$ and the map $G \to \text{Gal}(k_1/k_2)$ one sees that only the following two cases have to be considered.

(a) It is possible to choose $\sigma$ so that $\sigma^p = 1$, for some $m$, and $G = G' \times H$ where $G'$ acts trivially on $k_1$ and $H$ is generated by $\sigma$.

(b) For any $m > 0$ there exists a field $K$, $F'_{\text{ab}} \supset K \supset k_1 \supset k_2$, such that $K/k_2$

Received 29 August, 1973.

is a cyclic Galois extension of degree $p^n$.

In the first case, we let $K \subset F'_{ab}$ be the fixed field of $G'$. Then $(A, \mathcal{C}, \theta)$, regarded as being defined over $K$, has a model over $k_2$. Indeed, if $m = 1$, then this was observed above, but when $m > 1$ the same argument applies.

In the second case, let $\lambda: (A, \mathcal{C}, \theta) \to (A^{\bar{g}}, \mathcal{C}^{\bar{g}}, \theta^{\bar{g}})$ be an isomorphism defined over $k_1$ and let $\nu \lambda^* \cdots \lambda^m = \alpha \in \mu(R).

If $\lambda$ is replaced by $\lambda \gamma$ for some $\gamma \in \text{Aut}_k((A, \mathcal{C}, \theta))$ then $\alpha$ is replaced by $\alpha \gamma^p$. Thus, as $\mu(R)$ is finite, we may assume that $\alpha^{p^{m-1}} = 1$ for some $m$. Choose $K$, as in (b), to be of degree $p^n$ over $k_2$. Let $\sigma_m$ be a generator of $\text{Gal}(K/k_2)$ whose restriction to $k_1$ is $\bar{\sigma}$. Then

$$\lambda: (A, \mathcal{C}, \theta) \to (A^{\bar{g}}, \mathcal{C}^{\bar{g}}, \theta^{\bar{g}}) = (A^{\sigma_m}, \mathcal{C}^{\sigma_m}, \theta^{\sigma_m})$$

is an isomorphism defined over $K$ and $\nu \lambda^{m=p^{m-1}}, \ldots \lambda^m \lambda = \alpha^{p^{m-1}} = 1$, and so, by Lemma 1, $(A, \mathcal{C}, \theta)$ has a model over $k_2$ which becomes isomorphic to $(A, \mathcal{C}, \theta)$ over $K$.

The proof may now be completed as before.

*Addendum:* Professor Shimura has pointed out to me that the claim on lines 25 and 26 of p. 371, viz that $\mu(R)$ is a pure subgroup of $\Pi^*_R$, does not hold for all rings $R$. Thus this condition, which appears to be essential for the validity of the theorem, should be included in the hypotheses. It holds, for example, if $\mu(R)$ is a direct summand of $\mu(F)$.

University of Michigan