Inventiones math. 17, 177–190 (1972)

On the Arithmetic of Abelian Varieties*

J.S. Milne (London)

In § 1 we consider the situation: L/K is a finite separable field extension, A is an abelian variety over L, and A_* is the abelian variety over K obtained from A by restriction of scalars. We study the arithmetic properties of A_* relative to those of A, and in particular show that the conjectures of Birch and Swinnerton-Dyer hold for A if and only if they hold for A_*.

In § 2 we study certain twisted products of abelian varieties and use our results to show that the conjectures of Birch and Swinnerton-Dyer are true for a large class of twisted constant elliptic curves over function fields.

In § 3 we develop a method of handling abelian varieties over a number field K which are of CM-type but which do not have all their complex multiplications defined over K. In particular we compute under quite general conditions the conductors and zeta functions of such abelian varieties and so verify Serre's conjecture [12] on the form of the functional equation. Similar, but less complete, results have been obtained by Deuring [1] for elliptic curves and Shimura [15] for abelian varieties.

§ 1. The Arithmetic Invariants of the Norm

Let $T \to S$ be a morphism of schemes. We recall the definition and properties of the norm functor $N_{T/S}$ (in [19] this is denoted by $R_{T/S}$ and called restriction of field of definition, and in [3, Exp. 195] it is denoted by $\Pi_{T/S}$). If X is a T-scheme then $N_{T/S} X$ is uniquely determined as the S-scheme which represents the functor on S-schemes $Z \mapsto X(Z_T)$, where $Z_T = Z \times_S T$. There is a T-morphism $p: (N_{T/S} X)_T \to X$ such that any other T-morphism p': $Z_T \to X$ factors uniquely as $p' = p q_T$ with $q: Z \to N_{T/S} X$ an S-morphism. $N_{T/S} X$ always exists if X is quasi-projective and $T \to S$ is finite and faithfully flat [3, Exp. 221], and it is obvious from the definition that $N_{T/S}$ commutes with base change on S. If X is a group scheme then $N_{T/S} X$ acquires a unique group structure such that p is a morphism of group schemes. If X is smooth over T then it is obvious from the

* This research was supported by the Science Research Council of Great Britain.

functorial definition of smoothness [4, IV] that $N_{T/S}X$ is smooth. If X is an abelian scheme then $N_{T/S}X$ need not be an abelian scheme even (as Mumford has observed) if $T \to S$ corresponds to a finite field extension L/K. Indeed, if L/K is purely inseparable of degree m and A is an abelian variety of dimension d over L, then $L \otimes_K L = R$ is a local Artin ring with residue field L and $N_{R/L} A_R = (N_{L/K} A) \otimes_K L$ is an extension of A by a unipotent group scheme group scheme of dimension $(m-1)d$ [2, p. 263]. However if L/K is separable then $N_{L/K} A$ is an abelian variety because, for any Galois extensions $\bar{K}$ of K containing L, there is an isomorphism $P: (N_{L/K} A)_{\bar{K}} \to A_{\bar{K}}^{\sigma_1} \times \cdots \times A_{\bar{K}}^{\sigma_m}$ where $\sigma_1, \ldots, \sigma_m$ are the distinct embeddings of L in $\bar{K}$ over K [19, p. 5], and so $(N_{L/K} A)_{\bar{K}}$ is an abelian variety.

For the remainder of this section L/K will be a finite separable field extension of degree m, A an abelian variety over L of dimension d, $\bar{K}$ a Galois extension of K containing L (often equal to a separable algebraic closure K_s of K), $G = \mathrm{Gal}(\bar{K}/K)$, $H = \mathrm{Gal}(\bar{K}/L)$, and $\{\sigma_1, \ldots, \sigma_m\}$ a set of left coset representatives for H in G. We will compute the arithmetic invariants of $A_* = N_{L/K} A$.

(a) Points. $A_*(K) = A(L)$ and so their ranks (if finite) are equal. The morphism P above induces an isomorphism $A_*(\bar{K}) \to \mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} A(\bar{K})$ and this, with $\bar{K} = K_s$, induces canonical isomorphisms

$$T_l A_* \approx \mathbf{Z}_l[G] \otimes_{\mathbf{Z}_l[H]} T_l A \quad \text{and} \quad V_l A_* \approx \mathbf{Q}_l[G] \otimes_{\mathbf{Q}_l[H]} V_l A.$$

In other words, the l-adic representation of G on $T_l A_*$ (resp. $V_l A_*$) is the induced representation coming from the representation of H on $T_l A$ (resp. $V_l A$).

(b) Conductors. Let L be the field of fractions of a complete discrete valuation ring with finite residue field, and let V be a finite dimensional vector space over $\mathbf{Q}_l$ where l is not equal to the residue characteristic of L. Take $\bar{K} = K_s$ and let ρ be an l-adic representation of H on V. ρ automatically satisfies condition (H_ρ) of [12] and so the exponent of the tame conductor $\varepsilon(\rho)$ (resp. wild conductor $\delta(\rho)$, resp. conductor $f(\rho) = \varepsilon(\rho) + \delta(\rho)$) is defined. See [12] for the details.

Lemma. *Let ρ_* be the representation of $G = \mathrm{Gal}(K_s/K)$ induced by ρ. Then*

$$\varepsilon(\rho_*) = \varepsilon(\rho) + (m-1)\dim(V),$$
$$\delta(\rho_*) = \delta(\rho) + (\beta - m + 1)\dim(V),$$
$$f(\rho_*) = f(\rho) + \beta \dim(V)$$

where β is the exponent of the discriminant of L/K.

Proof. Straightforward using [11, VI Proposition 4].

When ρ_l is the representation of H defined by $V_l A$, Grothendieck [5] has shown that $\delta(\rho_l)$ is independent of l (different from the residue characteristic). $\varepsilon(\rho_l)$ is obviously independent of l because it equals $\mu(A)+2\lambda(A)$ where $\mu(A)$ and $\lambda(A)$ are the dimensions of the reductive and unipotent parts of the reduction of A. Thus, there are numbers $\varepsilon(A)$, $\delta(A)$, $f(A)$ depending only on A over L.

Now take L to be a global field i.e. a number field or function field in one variable over a finite field. In multiplicative notation, the conductor of A is the ideal or divisor $\mathfrak{f}(A)=\prod_w \mathfrak{p}_w^{f(w)}$ where w runs through the non-archimedean primes of L, L_w is the completion of L at w, and $f(w)=f(A_{L_w})$.

Proposition 1. *With the above notations,* $\mathfrak{f}(A_*)=N_{L/K}\left(\mathfrak{f}(A)\right) d_{L/K}^{2d}$, *where here* $N_{L/K}$ *refers to taking norms of ideals or divisors, and* $d_{L/K}$ *is the discriminant of* L *over* K. *In particular,* A_* *has good reduction at* v *if and only if* v *does not divide the discriminant of* L *over* K *and* A *has good reduction at all primes of* L *dividings* v.

Proof. Immediate from the lemma.

Remark. Let L/K be an extension of local fields with ramification index e, and let $\alpha(A)$ be the dimension of the part of the reduction of A which is an abelian variety.

Then

$$\alpha(A_*)=\frac{m}{e}\,\alpha(A),$$

$$\mu(A_*)=\frac{m}{e}\,\mu(A),$$

$$\lambda(A_*)=\frac{m}{e}\left(de-d+\lambda(A)\right).$$

Indeed, if $e=1$ this is obvious by looking at the norm of the Néron minimal model of A (see the next section (c)). If $e=m$ it follows from the formula $\varepsilon(A_*)=\varepsilon(A)+(m-1)\,2d$ and the obvious facts that $\alpha(A_*)\geqq\alpha(A)$, $\mu(A_*)\geqq\mu(A)$ (obvious, because $p\colon A_{*L}\to A$ is surjective). The general case follows by transitivity.

If L is a number field, write $d_L=|d_{L/\mathbf{Q}}|$, and if L is a function field in one variable over a finite field with q elements, write $d_L=q^{2g-2}$ where g is the genus of L. Define $N_L(\mathfrak{f}(A))=\prod_w N w^{f(w)}$ where w runs through the non-archimedean primes of L and Nw is the number of elements of the residue field $k(w)$ at w. Finally define $c(A)=N_L\left(\mathfrak{f}(A)\right) d_L^{2\dim(A)}$ [12, p. 12].

Corollary $c(A_*)=c(A)$.

Proof. Immediate from the theorem, the formula for the transitivity of norms, and the Hurwitz genus formula.

(c) Tamagawa Numbers. L is a global field. Let ω be a non-zero invariant exterior differential form of degree d on A. Define $\lambda_w=1$ if w is archimedean, and $\lambda_w=\frac{(Nw)^d}{n_w}$ where n_w is the order of $A^0_{w,0}(k(w))$, the group of points on the connected component of zero of the reduction of the Néron minimal model of A, if w is non-archimedean. By [19, 2.2.5] the λ_w form a set of convergence factors for A. We define $\tau(A)$ to be the measure of the adèle group of A relative to the Tamagawa measure $\Omega=(\omega,(\lambda_w))$ [19, p. 23].

Let ω_* be the invariant exterior differential form on A_* corresponding to ω as in [19, p. 24].

Proposition 2. (a) $\lambda_v=\prod_{w|v}\lambda_w$ *is equal to* $\frac{(Nv)^{\dim(A_*)}}{n_v}$ *for any non-archimedean prime* v *of* K.

(b) $\tau(A)=\tau(A_*)$.

Proof. (a) Let A_w be the Néron minimal model of A over R_w, the completion of the integers of L at w. A_w is quasi-projective and so $A_{w*}=N_{R_w/R_v}A_w$ exists. Clearly $A_{w*}\approx A_{*v}$, the Néron minimal model of A_*, because it is a smooth group scheme with the correct functorial property. Moreover the zero component A^0_{*v} of A_{*v} is isomorphic to $(A^0_w)_*$ because $(A^0_w)_*$ is an open subgroup scheme of A_{w*} with connected fibres.

If R_w is unramified over R_v, then $A^0_{*v}\otimes_{R_v}k(v)\approx N_{k(w)/k(v)}(A^0_w\otimes_{R_w}k(w))$ and so $n_w=n_v$, $Nw=Nv^{m'}$, and $\frac{Nw^d}{n_w}=\frac{Nv^{m'd}}{n_v}$, where $m'=[R_w:R_v]$.

If R_w is totally ramified over R_v, then $A^0_{*v}\otimes_{R_v}k(v)\approx N_{R_{w,m'}/k}(A^0_w\otimes_{R_w}R_{w,m'})$ where $R_{w,m'}$ is R_w modulo the m'th power of its maximal ideal. Thus $n_v=$ order of $A^0_w(R_{w,m'})=Nv^{(m'-1)d}n_w$ because A^0_w is smooth. $Nv=Nw$ and so $\frac{Nw^d}{n_w}=\frac{Nv^{m'd}}{n^v}$, and this suffices to complete the proof.

(b) Follows from (a) and [19, 2.3.2].

(d) Zeta Functions. L is again a global field. For any non-archimedean prime w of L we write I_w for an inertia group of w and π_w for a Frobenius element of H/I_w. Following [12] we define, for any prime $l\neq\mathrm{char}(k(w))$, a polynomial $P_{A,w}(T)=\det(1-T\pi_w)$ where π_w is regarded as acting on $(V_lA)^{I_w}=V_l(A^0_w\otimes_{R_w}k(w))$. Conjectures C_5, C_6, C_7 (*loc. cit.*) are known to be true in this case. Define

$$\zeta_A(s)=\prod_w P_{A,w}(Nw^{-s})^{-1}, \quad \zeta_A^*(s)=\frac{\zeta_A(s)}{\tau(A)}, \quad \xi_A(s)=c(A)^{s/2}\left(\frac{\Gamma(s)}{(2\pi)^{+s}}\right)^{nd}\zeta_A(s)$$

where $n=0$ if L is a function field and $n=[L:\mathbf{Q}]$ if L is number field.

Proposition 3. $\zeta_{A_*}(s)=\zeta_A(s)$, $\zeta^*_{A_*}(s)=\zeta^*_A(s)$, $\xi_{A_*}(s)=\xi_A(s)$.

Proof. After (b) and (c) it suffices to prove the first statement, and for this it suffices to show that $\prod_{w|v} P_{A,w}(Nw^{-s})=P_{A_*,v}(Nv^{-s})$. By passing to the completions, we may assume that w is the only prime of L lying over v. If L/K is unramified at v, then $(V_l A_*)^{I_v}=\mathbf{Q}_l[G/H]\otimes(V_l A)^{I_w}$, and G/H is a finite cyclic group of order m generated by the class of π_v. It follows that $P_{A_*,v}(T)=P_{A,w}(T^m)$, which gives the required equality. If L/K is totally ramified at v, then $(V_l A_*)^{I_v}=(V_l A)^{I_w}$, $\pi_v=\pi_w$, and the result is obvious.

Remark. Consider any projective smooth scheme V over L and let $V_*=N_{L/K}V$. Then it is possible to prove as above that

$$\zeta_{V_*}(s)=\zeta_V(s), \quad c(V_*)=c(V), \quad \xi_{V_*}(s)=\xi_V(s).$$

Indeed, $H^1(\bar{V}_*, \mathbf{Q}_l)\approx\mathbf{Q}_l[G]\otimes_{\mathbf{Q}_l[H]}H^1(\bar{V}, \mathbf{Q}_l)$, because

$$H^1(\bar{V}, \mathbf{Q}_l)\otimes_{\mathbf{Q}_l} V_l\mathbf{G}_m\approx V_l B,$$

where B is the Picard variety of V, and $\mathrm{Pic}^0(V_*)$ can be computed as in (e) below. (Note that $V_l A=\mathrm{Hom}_{\mathbf{Q}_l}(H^1(\bar{A}, \mathbf{Q}_l), \mathbf{Q}_l)$ so that we have actually been working with the dual of $H^1(\bar{A}, \mathbf{Q}_l)$ rather than with $H^1(\bar{A}, \mathbf{Q}_l)$ itself. However, this affects nothing.) The first two equalities follow immediately from the isomorphism as above. The only additional point for the last equality is to check that the Γ-factors agree, but this is easy.

(e) Pic^0. Let $b\in\mathrm{Pic}^0(A)$. The element $p^{\sigma_1 *}(b^{\sigma_1})+\dots+p^{\sigma_m *}(b^{\sigma_m})$ of $\mathrm{Pic}^0(A_{*K})$ is fixed under the action of G and so determines an element b_* of $\mathrm{Pic}^0(A_*)$.

Proposition 4. *The* map $b\mapsto b_*$ *is an isomorphism* $\mathrm{Pic}^0(A)\to\mathrm{Pic}^0(A_*)$.

Proof. This follows easily from the fact that $A\mapsto\mathrm{Pic}^0(A)$ is an additive functor on the category of abelian varieties over L [8, p. 75] and so commutes with products.

(f) Heights. L is a global field. We refer to [16, p. 5] for the definition of the logarithmic height pairing $\langle,\rangle_L$: $\mathrm{Pic}^0(A)\times A(L)\to\mathbf{R}$.

Proposition 5. *Let* $a\in A_*(K)$ *and* $b\in\mathrm{Pic}^0(A)$. *Then*

$$\langle b_*, a\rangle_K=\langle b, p(a)\rangle_L.$$

Proof. Choose $\bar{K}$ to be finite over K, of degree n say. Then, by using some obvious functorial properties of the height pairing, one gets that

$$\begin{aligned}\langle b_*, a\rangle_K = \frac{1}{n}\langle b_*, a\rangle_{\bar{K}} &= \frac{1}{n}\sum_{j=1}^{m}\langle p^{\sigma_j *}(b^{\sigma_j}), a\rangle_{\bar{K}}\\ &= \frac{1}{n}\sum_{j=1}^{m}\langle b^{\sigma_j}, p^{\sigma_j}(a)\rangle_{\bar{K}}\\ &= \frac{m}{n}\langle b, p(a)\rangle_{\bar{K}}\\ &= \langle b, p(a)\rangle_L.\end{aligned}$$

Corollary. *Let* $\{a_1, \dots, a_r\}$ (resp. $\{b_1, \dots, b_r\}$) *be a basis for* $A_*(K)$ (resp. $\mathrm{Pic}^0(A)$) *modulo torsion. Then* $\{p(a_1), \dots, p(a_r)\}$ (resp. $\{b_{1*}, \dots, b_{r*}\}$) *is a basis for* $A(L)$ (resp. $\mathrm{Pic}^0(A_*)$) *modulo torsion, and*

$$\det(\langle b_{j*}, a_i\rangle) = \det(\langle b_j, p(a_i)\rangle).$$

We now apply the above to the conjectures of Birch and Swinnerton-Dyer. These state that,

$$(B-S/D)\ \zeta_A^*(s) \sim \frac{[\text{Ш}]\,|\det(\langle b_i, a_j\rangle)|}{[A(K)_{\mathrm{tors}}]\,[A'(K)_{\mathrm{tors}}]}(s-1)^r, \qquad \text{as } s\to 1,$$

where the symbols are as defined above or as defined in [16, § 1]. For the sake of consistency, we must show that $\zeta_A^*(s)/L^*(s)\to 1$ as $s\to 1$, but this is a consequence of the following lemma.

Lemma. *Let M be a connected smooth commutative group scheme over a finite field k. If $P_M(T)=\det(1-\pi T)$ where π is the Frobenius endomorphism regarded as acting on $V_l M$, $l \neq \mathrm{char}(k)$, then $P_M(q^{-1}) = \frac{[M(k)]}{q^d}$ where $q=[k]$ and $d=$ dimension of M.*

Proof. If $0\to M'\to M\to M''\to 0$ is an exact sequence of group schemes then $P_M(T)=P_{M'}(T)\,P_{M''}(T)$ and $[M(k)]=[M'(k)]\,[M''(k)]$ (because $H^1(k, M')=0$). It follows that we need only prove the lemma for M equal to an abelian variety, a unipotent group, or a torus. The first case is well-known. If $M=\mathbf{G}_a$, then $P_M=1$ and $[M(k)]=q$. The result follows for any unipotent M because such a group has a composition series whose quotients are all isomorphic to $\mathbf{G}_a$.

Finally, let M be a torus. $P_M(T)=\det(1-T\hat{\pi})$ where $\hat{\pi}$ is π regarded as acting on the character group $\hat{M}$ of M. Then $P_M(q^{-1})=q^{-d}\det(q-\hat{\pi})=q^{-d}[M(k)]$ (see [9]).

Theorem 1. *$(B-S/D)$ is true for A if and only if it is true for A_*.*

Proof. After the above, we know that all corresponding factors, except the Tate-Šafarevič groups, are equal, but it is trivial to show that $Ш(A) \approx Ш(A_*)$ using (a).

Corollary. *Let L be a global field which is of degree m over the rational number field or a rational function field K_0. $(B-S/D)$ is true for all abelian varieties of dimension $\leqq d$ over L if it is true for all abelian varieties of dimension $\leqq md$ over K_0.*

§ 2. Forms of Products of Abelian Varieties

Throughout this section, $\bar{K}/K$ will be a Galois extension with Galois group G, and A an abelian variety of dimension d over K. A $\bar{K}/K$-form of A is a pair (A', ψ) where A' is an abelian variety over K and ψ is an isomorphism $A_{\bar{K}} \to A'_{\bar{K}}$. Then the map $\sigma \mapsto \psi^{-1}\psi^{\sigma}$: $G \to \mathrm{Aut}_{\bar{K}}(A)$ is a 1-cocycle for G with values in $\mathrm{Aut}_{\bar{K}}(A)$, and this correspondence sets up a bijection between the set of isomorphism classes of $\bar{K}/K$-forms of A and the elements of $H^1(G, \mathrm{Aut}_{\bar{K}}(A))$ (G acts on $A_{\bar{K}}$ through its action on $\bar{K}$, and it acts on $\mathrm{Aut}_{\bar{K}}(A)$ by $\phi \mapsto \phi^{\sigma} = \sigma\phi\sigma^{-1}$).

Let R be a commutative subring of $\mathrm{End}_K(A)$ and let M be an R-module, with a given isomorphism ψ: $R^n \to M$, on which G acts (through a finite quotient if $\bar{K}/K$ is infinite). Then $\sigma \mapsto s(\sigma) = \psi^{-1}\psi^{\sigma}$ is a homomorphism $G \to GL_n(R)$ which may be regarded as a 1-cocycle for G. If $GL_n(R)$ is regarded as a subgroup of $\mathrm{Aut}_{\bar{K}}(A^n)$ then we define $(M \otimes_R A, \psi_A)$ to be the $\bar{K}/K$-form of A^n corresponding s. $(M, \psi) \mapsto (M \otimes_R A, \psi_A)$ can be extended to an additive functor; given ϕ: $M \to M'$, ϕ_A: $M \otimes_R A \to M' \otimes_R A$ is the homomorphism such that $\psi_A^{-1}\,\phi_{A\bar{K}}\psi_A$ has the same matrix representation as $\psi^{-1}\phi\psi$.

If $\bar{K}/K$ is finite, then $R[G] \otimes_R A$ is isomorphic to $N_{\bar{K}/K} A$.

Proposition 6. (a) *If ϕ: $M \to M'$ has non-zero determinant* $\det_R(\phi)$ *with respect to the bases provided by ψ and ψ', then ϕ_A is an isogeny of degree $|N_{R/\mathbf{Z}}(\det_R(\phi))|^{2d/r}$ where $r = \mathrm{rank}_{\mathbf{Z}}(R)$.*

(b) *ψ_A induces isomorphisms of G-modules $M \otimes_R A(\bar{K}) \xrightarrow{\approx} (M \otimes_R A)(\bar{K})$, $M \otimes_R T_l A \xrightarrow{\approx} T_l(M \otimes_R A)$, $M \otimes_R V_l A \xrightarrow{\approx} V_l(M \otimes_R A)$.*

(c) *Let K be a global field. Then*

$$\mathfrak{f}(M \otimes_R A) = \mathfrak{f}(M)^{2d}\,\mathfrak{f}(A)^n,$$

$$c(M \otimes_R A) = c(M)^{2d}\,c(A)^n$$

where $\mathfrak{f}$ and c are the conductor and absolute conductor of A or the character of the representation of G on M [11, VI], *provided $\mathfrak{f}(M)$ and $\mathfrak{f}(A)$ (resp. $c(M)$ and $c(A)$) have disjoint supports.*

Proof. (a) Let F be the field of fractions of R. Since field extension does not change degrees or determinants we may assume that $K = \bar{K}$.

Then $M_n(F)$ is a simple **Q**-algebra and so, by [8, p. 179] it suffices to check that $\deg \phi_A = |N_{F/\mathbf{Q}} \det_R(\phi)|^{2d/r}$ for $\phi \in \mathbf{Z}$, but this is obvious.

(b) Follows directly from the definition of $M \otimes_R A$.

(c) Follows from (b) (cf. § 1).

Remark. 1. The first isomorphism in (b) can be used to give a more invariant definition of $M \otimes_R A$.

2. It is possible to deduce the zeta function of $M \otimes_R A$ from that of A and the representation of G on M.

Example. Let A be an abelian curve over K. Assume first that $j(A) \neq 0$, 1728 and that $\mathrm{char}(K) \neq 2$. Then $\mathrm{Aut}_{K_s}(A) = \mathrm{Aut}_K(A) = \{\pm 1\}$ and $H^1(\mathrm{Gal}(K_s/K), \mathrm{Aut}_{K_s}(A)) = K^*/K^{*2}$ by Kummer theory. Let A_d be the K_s/K-form of A corresponding to $d \in K^*$. If A has equation

$$Y^2 = X^3 + aX^2 + bX + c$$

then A_d has equation $dY^2 = X^3 + aX^2 + bX + c$ and ψ is the map $(x, y) \mapsto (x, \sqrt{d}\, y)$. If $\bar{K} = K(\sqrt{d})$, then $A_d = \mathbf{Z}_d \otimes_{\mathbf{Z}} A$ where $\mathbf{Z}_d$ is $\mathbf{Z}$ with $\sigma \in G$ acting as 1 or -1 according as σ is the identity or not. Thus if K is a global field and A has good reduction at a prime v then A_d has good reduction at v if and only if v is unramified in $\bar{K}/K$. Moreover

$$\zeta_{A_d}(s) = \prod_v \frac{1}{P_{A,v}((d/v)\, N v^{-s})}$$

(up to a finite number of factors) where (d/v) is the quadratic residue symbol for K.

If $j(A) \neq 0$ but $\mathrm{char}(K) = 2$, then $\mathrm{Aut}_{K_s}(A) = \mathrm{Aut}_K(A) = \{\pm 1\}$, $H^1(\mathrm{Gal}(K_s/K), \mathrm{Aut}_{K_s}(A)) = K/\wp K$, and if A_d corresponds to $d \in K$ and A has the equation $Y^2 + XY = X^3 + aX^2 + b$ then A_d has the equation $Y^2 + XY = X^3 + (a+d)X^2 + b$. If $\bar{K} = K(\wp^{-1}(d))$ then $A_d = \mathbf{Z}_d \otimes_{\mathbf{Z}} A$ with the obvious definition of $\mathbf{Z}_d$, and the same results hold as above.

If $j(A) = 0$ or 1728, then $\mathrm{Aut}_{K_s}(A)$ has order 4 ($j = 1728$, char $\neq 2, 3$), 6($j = 0$, char $\neq 2, 3$), 12($j = 0$, char $= 3$) or 24 ($j = 0$, char $= 2$) and there are many more cases to consider.

Proposition 7. *Assume that A is a simple abelian variety* (i.e. *simple over* K). *Let $s: G \to \mathrm{Aut}_K(A)$ be a homomorphism whose image is a finite subgroup contained in the centre R of* $\mathrm{End}(A)$. *Then $s(G)$ is cyclic, of order m say. Let R_i, $0 \leqq i \leqq m-1$, be R regarded as a G-module by $\sigma\, a = s(\sigma)^i\, a$ and let $A_i = R_i \otimes_R A$. Then, if L is the fixed field of $H = \ker(s)$, there is an isogeny of degree m^{md} $N_{L/K} A_L \to A_0 \times A_1 \times \cdots \times A_{m-1}$.*

Proof. Let σ_0 generate G/H and let $\zeta = s(\sigma_0)$. Then the homomorphism $\phi: R[G/H] \to \prod R_i$ with matrix $(\zeta^{ij})_{0 \leqq i, j \leqq m-1}$ relative to the obvious bases has determinant $\sqrt{m^m}$.

Example. 1. If A, A_d are abelian curves as in the example above, then the proposition shows there is an isogeny $N_{\bar{K}/K} A \to A \times A_d$ of degree 4.

2. In the situation of the proposition, $\zeta_{A_L}(s) = \zeta_{N_{L/K}A}(s) = \prod_{i=0}^{m} \zeta_{A_i}(s)$. For example, suppose that A has complex multiplication over K by $F = R \otimes_{\mathbf{Z}} \mathbf{Q}$ and let $\rho_\infty \colon I_K \to F_\infty^*$ be as defined in [13, p. 513]. Then

$$\zeta_{A_i}(s) = \prod_{\sigma} L(s, \chi_{i,\sigma}),$$

$$\zeta_{A_L}(s) = \prod_{i=0}^{m} \prod_{\sigma} L(s, \chi_{i,\sigma})$$

where σ runs through the embeddings $F \to \mathbf{C}$ and $\chi_{i,\sigma}$ is the composite $I_K \xrightarrow{s^i \cdot \rho_\infty} F_\infty^* \xrightarrow{1 \otimes \sigma} \mathbf{C}^*$ (s induces, in a canonical way, a map $I_K \to F \to F_\infty$, and we have used the same letter to denote this map).

Now let K be a global field of non-zero characteristic. An abelian curve A over K is said to be a twisted constant curve if $A \otimes_K K_s$ is constant i.e., of the form $A_0 \otimes_{k_s} K_s$ where k_s is the constant field of K_s. Equivalently, A is a twisted constant abelian curve if $j(A)$ is in the constant field of K, or if $\mathrm{End}_K(A) \neq \mathbf{Z}$.

Theorem 2. *Let A be a twisted constant abelian curve over K such that $j(A) \neq 0$, 1728 and $\mathrm{char}(K) \neq 2$. Then $(B-S/D)$ is true for A.*

Proof. Since $j(A)$ belongs to the constant field of K, there is a constant elliptic curve A_0 over K such that $j(A_0) = j(A)$ i.e. such that A is a K_s/K-form of A_0. In fact (see the above examples) there is a quadratic extension $\bar{K}$ of K such that A is a $\bar{K}/K$-form of A_0. By Proposition 7, there is an isogeny of degree 4, $N_{\bar{K}/K} A_{\bar{K}} \to A_0 \times A$. By [7], $(B-S/D)$ is true for A_0 and $A_{\bar{K}}$, and by Theorem 1 it is true for $N_{\bar{K}/K} A_{\bar{K}}$. Since $(B-S/D)$ is compatible with isogenies of degree prime to the characteristic of K [16] and with products, the theorem follows.

§ 3. Abelian Varieties with Complex Multiplication

K, $\bar{K}$, G, A will be as in § 2. We write $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$.

Theorem 3. *Let $\bar{K}/K$ be of finite degree m. Suppose that $\mathrm{End}^0_{\bar{K}}(A)$ contains a commutative subalgebra $E_{\bar{K}}$ such that $[E_{\bar{K}}: E_K] = m$ where $E_K = \mathrm{End}^0_K(A) \cap E_{\bar{K}}$. Assume that E_K is a field. Then $N_{\bar{K}/K} A_{\bar{K}}$ is isogenous to A^m.*

Proof. Let $\alpha_1, \ldots, \alpha_m$ be elements of $E_{\bar{K}} \cap \mathrm{End}_{\bar{K}}(A)$ which are linearly independent over $R = \mathrm{End}_K(A)$. Consider the homomorphism $\psi \colon A_{\bar{K}}^m \xrightarrow{\phi} A_{\bar{K}}^m \xrightarrow{P^{-1}} (N_{\bar{K}/K} A)_{\bar{K}}$ where ϕ has matrix $(\alpha_j^{\sigma_i})$ $(G = \{\sigma_1, \ldots, \sigma_m\})$ and P is as defined in § 1 (note that here $A_{\bar{K}}^{\sigma_i}$ is canonically isomorphic to $A_{\bar{K}}$). Obviously, $\psi^\sigma = \psi$, and so ψ defines a homomorphism $A^m \to N_{\bar{K}/K} A$.

Moreover the method of the proof of Proposition 6 may be used to show that $\deg(\psi)=|N_{R/\mathbf{Z}}(d_{S/R})|^{d/r}$ where $r=\operatorname{rank}_{\mathbf{Z}} R$, $S=R[\alpha_1,\dots,\alpha_m]$, and $d_{S/R}$ is the discriminant of S over R.

Corollary. *In the situation of the theorem.*

(a) $A(\bar{K})\otimes_{\mathbf{Z}}\mathbf{Q}\approx(A(K)\otimes_{\mathbf{Z}}\mathbf{Q})^m$ *and so* $\operatorname{rank}(A(\bar{K}))=m\operatorname{rank}A(K)$ (see also [6]).

Assume also that K is a global field.

(b) $\zeta_{A_{\bar{K}}}(s)=\zeta_A(s)^m$, $\xi_{A_{\bar{K}}}(s)=\xi_A(s)^m$,

$$N_{\bar{K}/K}(\mathfrak{f}(A_{\bar{K}}))\cdot d_{\bar{K}/K}^{2d}=\mathfrak{f}(A)^m.$$

(c) $(B-S/D)$ *is true for A over K if and only if it is true for $A_{\bar{K}}$ over $\bar{K}$.*

Proof. These all follow from the results in § 1.

Example. Let A be an abelian curve over $\mathbf{Q}$ which has complex multiplication by F. Then the conjecture $(B-S/D)$ is true for A over $\mathbf{Q}$ if and only if it is true for A over F.

Remark 1. The theorem has a partial converse. Let $\bar{K}/K$ be Galois of degree m and assume that A is simple and that $E_{\bar{K}}=\operatorname{End}^0_{\bar{K}}(A)$ is commutative. If $N_{\bar{K}/K}A$ is isogenous to A^m then $[\operatorname{End}^0_{\bar{K}}(A):\operatorname{End}^0_K(A)]=m$ and the isogeny is formed, as above, by taking elements of $\operatorname{End}_{\bar{K}}(A)$ which form a basis for $\operatorname{End}^0_{\bar{K}}(A)$ over $\operatorname{End}^0_K(A)$.

Indeed, if $\psi\colon A^m\to N_{\bar{K}/K}A_{\bar{K}}$ is the isogeny, then $\alpha=p\,\psi_{\bar{K}}\colon A^m_{\bar{K}}\to A_{\bar{K}}$ can be written $\alpha=(\alpha_1,\dots,\alpha_m)$ with $\alpha_i\in\operatorname{End}_{\bar{K}}(A)$. Since ψ is an isogeny, $p\,\psi_{\bar{K}}=(\alpha_j^{\sigma_i})\colon A^m_{\bar{K}}\to A^m_{\bar{K}}$ is an isogeny, and hence $\det(\alpha_j^{\sigma_i})\neq 0$. This implies that $\{\alpha_1,\dots,\alpha_m\}$ is a basis for $E_{\bar{K}}$ over E_K.

2. Assume that A is simple over K and let E be the centre of $\operatorname{End}^0_{K_s}(A)$. Let $\bar{K}$ be the smallest field containing K and such that $E\subset\operatorname{End}^0_{\bar{K}}(A)$. Then $\bar{K}$ is a finite Galois extension of K and $\bar{K}, K, A, E$ satisfy the conditions of the theorem.

Indeed, $\operatorname{Gal}(K_s/K)$ acts on $E\subset\operatorname{End}^0_{K_s}(A)$ and has fixed subfield $E_K=E\cap\operatorname{End}^0_K(A)$. Let H be the subgroup of $\operatorname{Gal}(K_s/K)$ of elements which act trivially on E. Then $\bar{K}$ is the fixed field of H, and so $[\bar{K}:K]=(\operatorname{Gal}(K_s/K):H)=[E:E_K]$.

We now apply the theorem to abelian varieties with complex multiplication. For the remainder of the paper, we let A be an abelian variety over a number field K which (over $\mathbf{C}$) is of CM-type (F,Φ) in the sense of [14]. We shall assume always that the image of F in $\operatorname{End}^0_{\mathbf{C}}(A)$ is stable under the action of $\operatorname{Gal}(K_s/K)$. This will be true when A is simple over $\mathbf{C}$ (for then $F=\operatorname{End}^0_{\mathbf{C}}(A)$), when $F_1=F\cap\operatorname{End}^0_K(A)$ is the maximal real subfield of F (for then $F=F_1E$ where E is the centre of $\operatorname{End}^0_{\mathbf{C}}(A)$, and E is stable under $\operatorname{Gal}(K_s/K)$), or, more generally, when A/K satisfies the conditions of Theorem 12 of [15]. Let $\bar{K}$ be the smallest field containing K such that $F \subset \mathrm{End}^0_{\bar{K}}(A)$. Then $G = \mathrm{Gal}(\bar{K}/K)$ acts on F and has fixed field $F_K = F \cap \mathrm{End}^0_K(A)$. $\bar{K}, K, A, F$ satisfy the conditions of the theorem.

Now let Σ be the set of embeddings $t\colon F \to \mathbf{C}$. G acts on Σ on the right. If $t \in \Sigma$ we write χ_t for the Grössen-character $\chi_t\colon I_{\bar{K}} \to \mathbf{C}^*$ defined in [13, p. 513] (note that we do not require a Grössen-character to take values in the unit circle).

Lemma. *$L(s, \chi_t) = L(s, \chi_{t\sigma})$ for all $\sigma \in G$, $t \in \Sigma$.*

Proof. It is easy to see that the homomorphism $\varepsilon\colon I_{\bar{K}} \to F^*$ defined in [13, Theorem 10] commutes with the action of G. Fix a prime v of K. If χ_t is unramified at the primes over v, then the factor of $L(s, \chi_t)$ (resp. $L(s, \chi_{t\sigma})$) corresponding to primes over v is

$$\prod_{w|v} \frac{1}{1 - \chi_t(i_w)\, N w^{-s}} \qquad \left(\text{resp. } \prod_{w|v} \frac{1}{1 - \chi_{t\sigma}(i_w)\, N w^{-s}}\right)$$

where i_w is the idèle whose component is 1 at primes $\neq w$ and a uniformizing parameter at w. By definition,

$$\chi_t(i_w) = t\, \varepsilon(i_w),$$
$$\chi_{t\sigma}(i_w) = t\, \sigma\, \varepsilon(i_w) = t\, \varepsilon(\sigma\, i_w) = t\, \varepsilon(i_{\sigma w}).$$

Since σ permutes the primes dividing v, this shows that the two factors are equal. If χ_t is ramified at one prime dividing v then it is ramified at all such primes and both factors are 1.

Theorem 4. *With the above notations,*

$$\zeta_A(s) = \prod_{t \in \Sigma/G} L(s, \chi_t).$$

Proof. Write

$$\zeta_A(s)_v = \frac{1}{P_{A,v}(N v^{-s})} \quad \text{and} \quad L(s, \chi)_v = \prod_{w|v} \frac{1}{1 - \chi(i_w)\, N w^{-s}}$$

(or 1) for the factors of $\zeta_A(s)$ and $L(s, \chi)$ corresponding to v.

Let $m = [\bar{K} : K]$. Then

$$\begin{aligned}
\zeta_A(s)_v^m &= \zeta_{N_{\bar{K}/K} A}(s)_v && \text{(Theorem 3)}\\
&= \prod_{w|v} \zeta_{A_{\bar{K}}}(s)_w && \text{(Proposition 3)}\\
&= \prod_{t \in \Sigma} L(s, \chi_t)_v && \text{([14], [13])}\\
&= \prod_{t \in \Sigma/G} (L(s, \chi_t)_v)^m.
\end{aligned}$$

Both $\zeta_A(s)_v$ and $\prod_{t\in\Sigma/G} L(s,\chi_t)_v$ are functions of the form $\prod \frac{1}{1-\alpha_i N v^{-s}}$ and it is easy to see from this that the above equation implies that $\zeta_A(s)_v = \prod_{t\in\Sigma/G} L(s,\chi_t)_v$.

Remark. 1. If we regard the χ_t as characters of the Weil group $\mathscr{G}_{\bar{K}}$ of $\bar{K}$ [18] then it is possible to define induced characters χ_{t*} on $\mathscr{G}_K$. Moreover (loc cit.) $L(s,\chi_{t*}) = L(s,\chi_t)$, $\mathfrak{f}(\chi_{t*}) = \mathfrak{f}(\chi_t)\, d_{\bar{K}/K}$. Thus, our results may be stated as follows: let A/K satisfy the conditions as above. Then, if $[F:F_K] = m$, there are $2d/m$ (quasi-) characters χ_i: $\mathscr{G}_K \to \mathbf{C}^*$ such that $\zeta_A(s) = \prod_i L(s,\chi_i)$, $\mathfrak{f}(A) = \mathfrak{f}(\chi_i)^{2d/m}$.

2. If for a Grössen-character χ of $\bar{K}$, $L(s,\chi)$ is multiplied by appropriate factors corresponding to the conductor of χ and to the infinite primes of $\bar{K}$, then the function $\Lambda(s,\chi)$ obtained satisfies the functional equation $\Lambda(2-s,\bar{\chi}) = w\,\Lambda(s,\chi)$ with $|w|=1$ (assuming that $\chi(i)=\chi_0(i)\,|i|^{\frac{1}{2}}$ where χ_0 is a Grössen-character which takes its values in the unit circle). Moreover, one checks that $\xi_{A_{\bar{K}}}(s) = \prod_{t\in\Sigma} \Lambda(s,\chi_t)$ (up to a trivial constant). Thus $A/\bar{K}$ satisfies Serre's conjecture [12, C_9], $\xi_{A_{\bar{K}}}(2-s) = w\,\xi_{A_{\bar{K}}}(s)$, with $w=1$.

After the above theorems, this result may be extended to A/K. In fact, one finds easily that $\xi_A(s) = \prod_{t\in\Sigma/G} \Lambda(s,\chi_t)$, from which it follows that $\xi_A(2-s) = w\,\xi_A(s)$, with $w=\pm 1$. ($w=\pm 1$ because $w(\chi)=w(\bar{\chi})^{-1}$, and so if $L(s,\chi)=L(s,\bar{\chi})$ then $w(\chi)=w(\bar{\chi})=\pm 1$.)

3. Theorem 4 (and the following discussion) is closely related to a result of Shimura [15, Thm. 12]. However, his conditions are apparently more complicated and he does not compute the factors of $\zeta_A(s)$ (and $\mathfrak{f}(A)$) corresponding to bad primes.

Perhaps it is worth clarifying the behaviour of A at bad primes. If A has complex multiplication defined over K then, for any prime v of K, A either has good reduction or totally unipotent reduction at v [13, p. 504] i.e. in the notation of § 1 either $\alpha_v(A)=d$ (and $\varepsilon_v(A)=0$) or $\lambda_v(A)=d$ (and $\varepsilon_v(A)=2d$). If, on the other hand, A, K, $\bar{K}$ are as above, and $[\bar{K}:K] = m > 1$ then

$$\alpha_v(A) = \frac{1}{m}\sum_{w|v} f(w|v)\,\alpha_w(A_{\bar{K}}),$$

$$\mu_v(A) = 0,$$

$$\lambda_v(A) = \frac{1}{m}\sum_{w|v} f(w|v)\big(d\,e(w|v) - d + \lambda_w(A)\big)$$

(see § 1) where $e(w|v)$ is the ramification index of w over v (in $\bar{K}/K$) and $f(w|v)$ is the residue class degree. Shimura [15, p. 536] gives an example where $\dim(A)=3$, $K=\mathbf{Q}$, $\bar{K}=\mathbf{Q}(\zeta+\zeta^{-1}, \sqrt{-11})$ with ζ a primitive 7th root of 1, $m=6$, and A has good reduction at the unique prime w of $\bar{K}$ dividing $v=7$. Then $f(w|v)=2$ (with $v=7$), and so $\alpha_v(A)=1$, $\lambda_v(A)=2$, and $\varepsilon_v(A)=4$. Thus A has bad reduction at 7 but the factor of $\zeta_A(s)$ corresponding to 7 is $\neq 1$.

We give two final applications of Theorem 3.

Theorem 5. *Let A/K, G, $\bar{K}$ be as in the discussion preceding the lemma above.*

(a) *For all primes l,* $\mathrm{End}_K(A)\otimes\mathbf{Q}_l\to\mathrm{End}_H(V_l A)$ *is an isomorphism, where* $H=\mathrm{Gal}(K_s/K)$.

(b) *Conjecture* 2 *of* [17, p. 104] *is true for A and* $i=1$ i.e. *the rank of the Néron-Severi group of A is equal to the order of the pole of the* 2-*part of the zeta function of A at* $s=2$.

Proof. (a) follows from the results in [14] if A has all of its complex multiplications defined over $\bar{K}$. Write $H_0=\mathrm{Gal}(K_s/\bar{K})\subset H$ and $A_*=N_{\bar{K}/K}A$. Then $M_m(\mathrm{End}^0_{\bar{K}}(A))\approx\mathrm{End}^0_{\bar{K}}(A_*)\approx\mathrm{End}^0_{\bar{K}}(A_*)^G$. But, $\mathrm{End}^0_{\bar{K}}(A_*)\otimes\mathbf{Q}_l\approx\mathrm{End}_{H_0}(\mathbf{Q}_l[H]\otimes_{\mathbf{Q}_l[H_0]}V_l(A_{\bar{K}}))$ as G-modules, and $M_m(\mathrm{End}_H(V_l A))\approx\mathrm{End}_{H_0}(\mathbf{Q}_l[H]\otimes_{\mathbf{Q}_l[H_0]}V_l(A_{\bar{K}}))^G$. (b) is proved in [10] when A has all of its complex multiplications defined over K, and the general case may be deduced similarly to the above.

References

1. Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins IV. Nachs. d. Akad. Wiss. p. 55–80. Göttingen, 1957.
2. Greenberg, M.: Schemata over local rings II. Ann. of Math. **78**, 256–266 (1963).
3. Grothendieck, A.: Fondements de la géométrie algébrique (extracts du Séminaire Bourbaki, 1957–62).
4. Grothendieck, A. (with J. Dieudonné): Eléments de géométrie algébrique. Publ. Math. I.H.E.S. (1960–1967).
5. Grothendieck, A.: Modèles de Néron et monodromie. Exposé IX of S.G.A. 7, I.H.E.S., 1967–68.
6. Honda, T.: Isogenies, rational points, and sections of group varieties. Jap. Jour. of Math. **31**, 84–101 (1960).
7. Milne, J.: The Tate-Šafarevič group of a constant abelian variety. Inventiones math. **6**, 91–105 (1968).
8. Mumford, D.: Abelian varieties. Oxford U.P., London (1970).
9. Ono, T.: On the Tamagawa number of algebraic tori. Ann. of Math. (2) **78**, 47–72 (1963).
10. Pohlmann, H.: Algebraic cycles on abelian varieties of complex multiplication type. Ann. of Math. **88**, 161–180 (1968).
11. Serre, J.-P.: Corps Locaux. Act. Sci. Ind. 1296. Paris: Hermann 1962.
12. Serre, J.-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange – Pisot – Poitou, 11e année, n° 19 (1969/70).
13. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. of Math. **88**, 492–517 (1968).
14. Shimura, G., Taniyama, Y.: Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan, n° 6. Tokyo, 1961.

15. Shimura, G.: On the zeta-function of an abelian variety with complex multiplication. Ann. of Math. **94**, 504–533 (1971).
16. Tate, J.: On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. Séminaire Bourbaki 1965/66, exposé 306.
17. Tate, J.: Algebraic cycles and poles of zeta functions. Arithmetical algebraic geometry, p. 93–110. New York: Harper and Row (1965).
18. Weil, A.: Sur la théorie du corps de classes. J. Math. Soc. Japan **3**, 1–35 (1951).
19. Weil, A.: Adeles and algebraic groups. Lecture notes. Princeton: Institute for Advanced Study 1961.

J.S. Milne
Department of Mathematics
University of Michigan
Ann Arbor, Mich. 48104
USA

(Received January 22, 1972 / May 31, 1972)