Kontakt / Contact

DigiZeitschriften e.V.
Papendiek 14
37073 Goettingen
Email: info@digizeitschriften.de

Inventiones math. 2, 134—144 (1966)

Endomorphisms of Abelian Varieties over Finite Fields

JOHN TATE (Cambridge, USA)

§ 1. The Main Theorem

Almost all of the general facts about abelian varieties which we use without comment or refer to as "well known" are due to WEIL, and the references for them are [12] and [3]. Let k be a field, $\bar{k}$ its algebraic closure, and A an abelian variety defined over k, of dimension g. For each integer $m \geqq 1$, let A_m denote the group of elements $a \in A(\bar{k})$ such that $ma=0$. Let l be a prime number different from the characteristic of k, and let $T_l(A)$ denote the projective limit of the groups A_{l^n} with respect to the maps $A_{l^{n+1}} \to A_{l^n}$ which are induced by multiplication by l. It is well known that $T_l(A)$ is a free module of rank $2g$ over the ring $\boldsymbol{Z}_l$ of l-adic integers. The group $G=\mathrm{Gal}(\bar{k}/k)$ operates on $T_l(A)$.

Let A' and A'' be abelian varieties defined over k. The group $\mathrm{Hom}_k(A', A'')$ of homomorphisms of A' into A'' defined over k is $\boldsymbol{Z}$-free, and the canonical map

$$\boldsymbol{Z}_l \otimes \mathrm{Hom}_k(A', A'') \to \mathrm{Hom}_G\big(T_l(A'), T_l(A'')\big) \tag{1}$$

is injective. The aim of this paper is to prove the following result and give some applications of it.

Main Theorem. *If k is finite, the map* (1) *is bijective.*

In case A' and A'' are elliptic curves this theorem is an easy consequence of results of DEURING [2], as Mumford pointed out to me four years ago. The proof in the general case uses methods similar to those of DEURING, except that one must keep track of polarizations. I heartily thank S. LICHTENBAUM for having suggested to me that a proof might be based on the fact that a hypothesis like the one labelled $\mathrm{Hyp}(k, A, d, l)$ in § 2 below holds when k is finite.

One can hope [10] that the map (1) is bijective for fields k which are finitely generated over the prime field. SERRE [7] and [8] has proved this for elliptic curves over number fields in case either $A'=A''$, or the modular invariant of one of the curves is not an algebraic integer. Since the methods of this paper may possibly be of use over non-finite fields I have axiomatised them to some extent, postponing the assumption that k is finite until the end of the proof in § 2.

We conclude this introductory section with four easy lemmas which give rather trivial but useful variants of the statement that the map (1) is bijective. Let

$$V_l(A) = \boldsymbol{Q}_l \otimes_{\boldsymbol{Z}_l} T_l(A)$$

denote the vector space of dimension $2g$ over the field $\boldsymbol{Q}_l$ of l-adic numbers which is obtained by tensoring $T_l(A)$ with $\boldsymbol{Q}_l$ over $\boldsymbol{Z}_l$, and consider the map

$$\boldsymbol{Q}_l \otimes \mathrm{Hom}_k(A', A'') \to \mathrm{Hom}_G\big(V_l(A'), V_l(A'')\big). \tag{2}$$

Lemma 1. *The map* (2) *is injective, and the bijectivity of* (1) *is equivalent to that of* (2).

Indeed (2) is obtained by tensoring (1) with $\boldsymbol{Q}_l$ over $\boldsymbol{Z}_l$, and $\boldsymbol{Q}_l$ is flat over $\boldsymbol{Z}_l$. Hence the lemma follows from the fact that (1) is injective with torsion-free cokernel. This last-mentioned torsion-freeness comes from the fact that if a k-homomorphism $f\colon A' \to A''$ vanishes on $(A')_l$, then there is a k-homomorphism $g\colon A' \to A''$ such that $f = lg$.

Lemma 2. *The following statements are equivalent:*

(i) *The map* (2) *is bijective for every prime* $l \neq \mathrm{char}(k)$.

(ii) *The map* (2) *is bijective for one such* l, *and the dimension over* $\boldsymbol{Q}_l$ *of the right hand side of* (2) *is independent of* l.

This is clear because (2) is injective for all l, and the dimension of the left hand side of (2) is independent of l, being equal to the rank of $\mathrm{Hom}_k(A', A'')$.

Lemma 3. *To prove* (2) *bijective for all pairs of abelian varieties* A' *and* A'' *over a given field* k *it suffices to prove that the map*

$$\boldsymbol{Q}_l \otimes \mathrm{End}_k(A) \to \mathrm{End}_G\big(V_l(A)\big) \tag{3}$$

is bijective for every abelian variety A *defined over* k.

More precisely, the bijectivity of (2) for a given pair A' and A'' follows from that of (3) for $A = A' \times A''$. This follows immediately from the formula

$$\mathrm{End}_k(A' \times A'') = \mathrm{End}_k(A') \times \mathrm{Hom}_k(A', A'') \times \mathrm{Hom}_k(A'', A') \times \mathrm{End}_k(A'')$$

and the analogous formula for the ring of G-endomorphisms of

$$V_l(A' \times A'') \approx V_l(A') \times V_l(A'').$$

Consider now the two commuting subalgebras E_l and F_l of the $\boldsymbol{Q}_l$-algebra $\mathrm{End}(V_l(A))$ which are defined as follows:

E_l = the image of $\boldsymbol{Q}_l \otimes \mathrm{End}_k(A)$ by the map (3).

F_l=the subalgebra of $\mathrm{End}(V_l(A))$ generated by the automorphisms of $V_l(A)$ defined by elements of G.

Lemma 4. *If F_l is semisimple, the bijectivity of* (3) *is equivalent to the fact that F_l is the commutant of E_l in* $\mathrm{End}(V_l(A))$.

This follows from the semisimplicity of E_l and the theorem of bicommutation [1], because the bijectivity of (3) just means that E_l is the commutant of F_l in $\mathrm{End}(V_l(A))$.

§ 2. The Proof

Consider the following hypothesis concerning an abelian variety A defined over a field k, a prime l, and an integer $d \geqq 1$:

Hyp(k, A, d, l): *There exists (up to k-isomorphism) only a finite number of abelian varieties B defined over k such that:*

(a) *There exists a polarization ψ of B of degree d^2 defined over k.*

(b) *There exists a k-isogeny $B \to A$ of l-power degree.*

If k is finite, then Hyp(k, A, d, l) is satisfied, even if one replaces (b) by "dim $B=g$". This can be seen either by means of the moduli schemes [5], or simply because the polarization 3ψ gives a projective imbedding of B in $\boldsymbol{P}_{3^g d-1}$ of degree $3^g d(g!)$ defined over k; for this and more precise information about projective imbeddings of abelian varieties, see MUMFORD [6]. Whether or not Hyp(k, A, d, l) holds for number fields k, or for fields k finitely generated over the prime field seems to be an interesting diophantine question. The answer is yes when A is an elliptic curve, as follows from a result announced by SHAFARYEVITCH [9], the proof of which seems to depend on SIEGEL's theorem on integral points on affine curves and its generalizations.

Let $\hat{A}$ be the dual of A and let $(x, \hat{x}) \mapsto \langle x, \hat{x} \rangle$ denote the canonical pairing of $V_l(A)$ and $V_l(\hat{A})$ into $V_l(\boldsymbol{G}_m)$ which is induced by the "e_m-pairings" of A_m and $\hat{A}_m$ into the group of m-th roots of unity for $m=l^n$ and $n \to \infty$. Let ϑ: $A \to \hat{A}$ be a polarization of A defined over k, that is, a k-isogeny which, over $\bar{k}$, is of the form $\Lambda(L)$ for some ample invertible sheaf L on $A \times_k \bar{k}$, in the notation of [5]. Let $d^2 = \deg \vartheta$, and let

$$H_\vartheta(x, y) = \langle x, \vartheta\, y \rangle$$

be the non-degenerate alternating bilinear form on $V_l(A)$ with values in $V_l(\boldsymbol{G}_m)$ corresponding to ϑ.

Proposition 1. *Suppose that* Hyp(k, A, d, l) *is satisfied. Let W be a subspace of $V_l(A)$ which is maximal isotropic with respect to the form H_ϑ and stable under G. Then there exists an element $u \in E_l$ such that $u(V_l(A)) = W$.*

Let $T=T_l(A)$ and $V=V_l(A)$. For each integer $n\geqq 0$ put

$$X_n=(T\cap W)+l^n T.$$

Then X_n is a $\boldsymbol{Z}_l$-submodule of T of index l^{ng} and stable under G. It follows that there exists an abelian variety $B(n)$ and an isogeny $f_n\colon B\to A$ of degree l^{ng} defined over k such that $f_n(T_l(B(n)))=X_n$.

I claim that $B(n)$ has a polarization $\psi_n=l^{-n}f_n^*(\vartheta)$ defined over k. Indeed, $f_n^*(\vartheta)=\hat{f}\,\vartheta f$ is a polarization of $B(n)$ defined over k of degree $l^{2gn}d^2$. The corresponding alternating form is given by

$$H_{f_n^*(\vartheta)}(x,y)=\langle x,\hat{f}\,\vartheta f y\rangle=H_\vartheta(fx,fy).$$

The values taken by this form on $T_l(B(n))$ are therefore the same as the values taken by H_ϑ on $f(T_l(B(n)))=X_n=(T\cap W)+l^nT$. These latter are divisible by l^n because W is isotropic for H_ϑ, and H_ϑ takes integral values (i.e., values in $T_l(\boldsymbol{G}_m)$) on T. By the proposition on the last page of WEIL [*12*], we conclude that there exists a polarization ψ_n of $B(n)$ such that $l^n\psi_n=f^*(\vartheta)$. This ψ_n is defined over k because $f^*(\vartheta)$ is, and its degree is $l^{-2gn}\deg f^*(\vartheta)=d^2$.

By Hyp(k, A, d, l) it now follows that the number of k-isomorphism classes of the abelian varieties $B(n)$ is finite. Therefore there exists an infinite set I of positive integers such that for $i\in I$ the $B(i)$ are all isomorphic to each other over k. Let n be the smallest integer in I and for each $i\in I$ let $v_i\colon B(n)\to B(i)$ be a k-isomorphism. Put $u_i=f_i v_i f_n^{-1}$ which has meaning in $\boldsymbol{Q}\otimes\mathrm{End}_k(A)$ and therefore in E_l. We have $u_i(X_n)=X_i$, and in particular $u_i(X_n)\subset X_n$. Since $\mathrm{End}(X_n)$ is compact we can extract from $(u_i)_{i\in I}$ a subsequence $(u_j)_{j\in J}$ which converges to a limit u, and this limit is in E_l because E_l is closed. Since X_n is compact, $u(X_n)$ consists of the elements of the form $x=\lim x_j$, where $x_j\in u_j(X_n)=X_j$; and since the sets X_j are decreasing it follows that

$$u(X_n)=\bigcap_{j\in J}X_j=T\cap W.$$

Hence $u(V)=W$, which proves the proposition.

Proposition 2. *Suppose that* Hyp(k, A, d, l) *is satisfied and that the* $\boldsymbol{Q}_l$*-algebra* F_l *is isomorphic to a product of copies of* $\boldsymbol{Q}_l$. *Then the map* (3) *of Lemma* 3 *is bijective.*

Let D be the commutant of E_l in $\mathrm{End}(V_l(A))$. Let W be an isotropic subspace of $V=V_l(A)$ which is stable under F_l (i.e., under G). I claim that *W is also stable under D.* If W is maximal isotropic, i.e., if $\dim W=g$, then by Proposition 1 we have $W=uV$ for some $u\in E_l$, hence $DW=DuV=uDV\subset uV=W$ as claimed. Suppose now $\dim W<g$. The orthogonal complement W^0 of W is stable under G, hence under F_l, and in

virtue of our hypothesis on F_l we have a direct sum decomposition

$$W^0 = W \oplus \sum_{i=1}^{m} L_i$$

with each L_i of dimension 1 over $\boldsymbol{Q}_l$ and stable under F_l. Since $m = 2(g - \dim W) \geqq 2$, we have $W = W_1 \cap W_2$, with $W_i = W \oplus L_i$ isotropic, stable under F_l, and of dimension strictly greater than W. Since the intersection of stable subspaces is stable, our claim now follows by descending induction on dim W.

Applying this result with dim $W = 1$ we see that every eigenvector of F_l in V is an eigenvector of D. It follows that $D \subset F_l$ (the decomposition of V into factors V_i corresponding to the simple factors of F_l reduces this assertion to the evident statement that an endomorphism of V_i for which every element of V_i is an eigenvector is a scalar multiplication). Since $F_l \subset D$ trivially, we conclude that $F_l = D$, and by Lemma 4 the map (3) is bijective.

From now on we suppose k is finite. Then, as we have seen, Hyp(k, A, d, l) is satisfied, and Proposition 2 applies. Let π be the Frobenius endomorphism of A relative to k, and let $F = \boldsymbol{Q}(\pi)$ be the subalgebra of $E = \boldsymbol{Q} \otimes \mathrm{End}_k(A)$ generated by π. The effect of π on $A(\bar{k})$, and therefore on $V_l(A)$, is the same as that of the Frobenius automorphism of $\bar{k}/k$, which is a topological generator of G. This shows that F is in the center of the semisimple algebra E and is therefore itself semisimple, and it also shows that $F_l \approx \boldsymbol{Q}_l \otimes F$. By Proposition 2 we conclude that the map (3) is bijective for the prime numbers l which split completely in F. The existence of such l is well known. Therefore, by Lemma 2, we have only to show that the dimension of $\mathrm{End}_G(V_l(A))$ is independent of l, in order to complete the proof of the main theorem via Lemmas 1 and 3.

More generally, let B be another abelian variety over k and let f_A and f_B be the characteristic polynomials of the Frobenius endomorphisms π_A and π_B of A and B, respectively. Let K be an extension of $\boldsymbol{Q}$ and let

$$f_A = \prod P^{a(P)} \quad \text{and} \quad f_B = \prod P^{b(P)}$$

be the canonical factorization of f_A and f_B as products of powers of distinct irreducible polynomials P over K. Comparing these factorizations over K with the corresponding factorizations over $\boldsymbol{Q}$ one sees that the integer

$$r(f_A, f_B) = \sum_P a(P)\, b(P) \deg P \tag{4}$$

is independent of K. Taking $K = \boldsymbol{Q}_l$ and using the fact that π_A and π_B induce endomorphisms of $V_l(A)$ and $V_l(B)$ which are semisimple with

characteristic polynomials f_A and f_B one sees that

$$\dim \mathrm{Hom}_G(V_l(A), V_l(B)) = r(f_A, f_B). \tag{5}$$

Since the right hand side is independent of l, our main theorem is proved.

§ 3. Applications

In this section we list some immediate consequences of the main theorem.

Theorem 1. *Let A and B be abelian varieties over a finite field k, and let f_A and f_B be the characteristic polynomials of their Frobenius endomorphisms relative to k. Then*

(a) *With r defined as in* (4) *above we have*

$$\mathrm{rank}(\mathrm{Hom}_k(A, B)) = r(f_A, f_B).$$

(b) *The following statements are equivalent:*

(b1) *B is k-isogenous to an abelian subvariety of A defined over k.*

(b2) *$V_l(B)$ is G-isomorphic to a G-subspace of $V_l(A)$ for some l.*

(b3) *f_B divides f_A.*

(c) *The following statements are equivalent:*

(c1) *A and B are k-isogenous.*

(c2) *$f_A = f_B$.*

(c3) *The zeta functions of A and B are the same.*

(c4) *A and B have the same number of points in k' for every finite extension k' of k.*

The formula for the rank of $\mathrm{Hom}_k(A, B)$ follows from the bijectivity of the map (2) and formula (5).

If $\varphi: B \to A$ is a k-homomorphism, then the dimension of the kernel of $\varphi_l: V_l(B) \to V_l(A)$ is twice the dimension of Ker φ. Thus φ has a finite kernel if and only if φ_l is injective. This shows (b1) $\Rightarrow$ (b2). Conversely, if $u: V_l(B) \to V_l(A)$ is an injective G-homomorphism, then by our main theorem there exist elements $\varphi \in \boldsymbol{Q} \otimes \mathrm{Hom}_k(B, A)$ such that φ_l is arbitrarily close to u in $\mathrm{Hom}(V_l(B), V_l(A))$. A φ_l sufficiently close to u is injective, and a suitable multiple of the corresponding φ is in $\mathrm{Hom}_k(B, A)$ and has finite kernel. Hence (b2) $\Rightarrow$ (b1).

The implication (b2) $\Rightarrow$ (b3) is trivial, and the converse follows from the fact that the Frobenius endomorphisms π_A and π_B act semisimply on $V_l(A)$ and $V_l(B)$ with characteristic polynomials f_A and f_B.

The equivalence of (c1) and (c2) follows from that of (b1) and (b3). The equivalence of (c2), (c3), and (c4) is well known.

Theorem 2. *Let A be an abelian variety of dimension g over a finite field k. Let π be the Frobenius endomorphism of A relative to k and f its characteristic polynomial.*

(a) *The algebra $F=\boldsymbol{Q}[\pi]$ is the center of the semisimple algebra $E=\boldsymbol{Q}\otimes \mathrm{End}_k(A)$.*

(b) *We have*

$$2g\leqq[E:\boldsymbol{Q}]=r(f,f)\leqq(2g)^2.$$

(c) *The following statements are equivalent:*

(c1) $[E:\boldsymbol{Q}]=2g$.

(c2) *f has no multiple root.*

(c3) $E=F$.

(c4) *E is commutative.*

(d) *The following statements are equivalent:*

(d1) $[E:\boldsymbol{Q}]=(2g)^2$.

(d2) *f is a power of a linear polynomial.*

(d3) $F=\boldsymbol{Q}$.

(d4) *E is isomorphic to the algebra of g by g matrices over the quaternion algebra D_p over $\boldsymbol{Q}$ which is ramified only at p and ∞.*

(d5) *A is k-isogenous to the g-th power of a super-singular elliptic curve, all of whose endomorphisms are defined over k.*

(e) *A is k-isogenous to a power of a k-simple abelian variety if and only if f is a power of a $\boldsymbol{Q}$-irreducible polynomial P. When this is the case E is a central simple algebra over F which splits at all finite primes v of F not dividing $p=\mathrm{char}(k)$, but does not split at any real prime of F.*

By Lemma 4 and our main theorem we know that $F_l=\boldsymbol{Q}_l\otimes F$ is the center of $E_l=\boldsymbol{Q}_l\otimes E$. It follows that F is the center of E.

Let

$$f(T)=\prod_{i=1}^{s}(T-\pi_i)^{m_i}$$

with the π_i distinct and $m_i\geqq 1$. Then $\Sigma m_i=\deg f=2g$, and by theorem 1(a), we have $[E:\boldsymbol{Q}]=r(f,f)=\Sigma m_i^2$, so (b) follows from the obvious inequalities

$$(*)\qquad \sum m_i\leqq\sum m_i^2\leqq(\sum m_i)^2.$$

We have equality on the left of (*) if and only if $m_i=1$ for all i, $1\leqq i\leqq s$, and from this the equivalence of the four statements under (c) follows easily, once we note that, since F is semisimple, $[F:\boldsymbol{Q}]=s$, the number of distinct roots of f.

We have equality on the right of (*) if and only if $s=1$, and this shows the equivalence of (d1), (d2), and (d3). If $F=\boldsymbol{Q}$, then E is a simple algebra with center $\boldsymbol{Q}$ for which $E_l=\boldsymbol{Q}_l\otimes E$ is isomorphic to $\mathrm{End}(V_l(A))$ for all $l\neq p=\mathrm{char}(k)$. Thus the local invariants of E are 0 at all primes of $\boldsymbol{Q}$ except possibly at the archimedean prime ∞ and at the prime p. Since the invariant at ∞ is 0 or $\frac{1}{2}$ and the sum of the invariants is $\equiv 0 (\mathrm{mod}\ 1)$, the invariant at p is 0 or $\frac{1}{2}$, and we conclude that E is either the algebra $M_{2g}(\boldsymbol{Q})$ or $M_g(D_p)$. The first possibility is excluded, because an abelian variety of dimension g cannot be isogenous to the $2g$-th power of an abelian variety. Therefore $E\approx M_g(D_p)$, and there is a k-isogeny $A\sim B^g$, where B is an elliptic curve with $\boldsymbol{Q}\otimes \mathrm{End}_k(B)\approx D_p$. Conversely, if this last is true, then $E\approx M_g(D_p)$ and the center F of E is $\boldsymbol{Q}$. Thus (d3), (d4), and (d5) are equivalent.

As is well known, there is a unique factorization of A, up to k-isogeny, into a product of powers of non-k-isogenous k-simple abelian varieties A_j. This factorization corresponds to the decomposition of the semisimple algebra E into simple factors E_j, and therefore to the expression of its center F as a product of fields F_j. The F_j in turn correspond to the $\boldsymbol{Q}$-irreducible factors P_j of f. Thus A is isogenous to a power of a k-simple abelian variety if and only if f is the power of a $\boldsymbol{Q}$-irreducible polynomial P. Assume this is so. Then E is simple with center F. Let l be a rational prime number different from p. Then $V_l(A)$ is a free module of rank m over

$$F_l=\boldsymbol{Q}_l\otimes F=\prod_{v/l} F_v,$$

where m is the multiplicity of the roots of f. By our main theorem, the algebra $F_l\otimes_F E=\boldsymbol{Q}_l\otimes_{\boldsymbol{Q}} E=E_l$ is isomorphic to $\mathrm{End}_{F_l}(V_l(A))$, that is, to the algebra of m by m matrices over F_l. Hence E splits at all primes v dividing l.

Now suppose F has a real prime v. We may then view π as a real number, which, by the Riemann hypothesis, has absolute value $\sqrt{q}$, where $q=\mathrm{Card}\, k$. Consequently π is a root of the polynomial T^2-q. If q is a square in $\boldsymbol{Q}$, then π is rational, $F=\boldsymbol{Q}$, and we conclude from part (d) that E is a matrix algebra over the quaternion algebra D_p, which does not split at ∞. Suppose now that q is not a square in $\boldsymbol{Q}$. Then $F=\boldsymbol{Q}(\sqrt{p})$ is a real quadratic field. Using a superscript "prime" to denote the algebras attached to A relative to the quadratic extension k' of k we have

$$F'\subset F\subset E\subset E',$$

and E is the commutant of F in E'. Hence, in the Brauer group of F we have $E\sim E'\otimes_{F'} F$. Since $\pi'=\pi^2=q$, we have $F'=\boldsymbol{Q}$; hence by part (d), E' is a matrix algebra over the quaternion algebra D_p. And since D_p does

not split over R it follows that E does not split at either of the real primes of F.

This concludes the proof of Theorem 2, but raises the question of the local behavior of E at the primes v of F which divide p, in the situation just discussed when f is a power of a $\boldsymbol{Q}$-irreducible polynomial P. From Theorems 1 and 2 it follows easily that the class of E in the Brauer group of F depends only on P or, what is the same, on $F=\boldsymbol{Q}(\pi)$, *as abstract field furnished with the generator* π. Thus we see *a priori* that there must be a rule for computing the local invariants of E at the primes v of F in terms of π. In fact the rule is as follows:

For each prime v of F, including the archimedean primes, let $\|\pi\|_v$ denote the *normed* absolute value of π at v, and define i_v by

$$\|\pi\|_v = q^{-i_v}, \tag{6}$$

where q is the number of elements in k. Then

$$\mathrm{inv}_v(E) \equiv i_v \pmod{\boldsymbol{Z}} \qquad \text{for all primes } v \text{ of } F. \tag{7}$$

To see that this rule checks with part (e) of Theorem 2 for the primes v not dividing p, recall that π is an algebraic integer, all of whose conjugates have (ordinary) absolute value $\sqrt{q}$, and whose absolute norm is therefore a power of p. Consequently $i_v = -1$ for v complex, $i_v = -\frac{1}{2}$ for v real, and $i_v = 0$ for v finite not dividing p. We do not give the proof of (7) for primes v dividing p in this paper, because it involves the consideration of the formal group which plays the role of $T_p(A)$, its Dieudonné module, and its endomorphism ring, as in MANIN [4], and would lead us too far afield.

Note that, granting (7), the "product formula" $\Pi \|\pi\|_v = 1$ implies the "reciprocity law" $\Sigma i_v \equiv 0 \pmod{\boldsymbol{Z}}$ for the algebra E. Using (7) one can express the dimension g' of the k-simple constituent A' of A in terms of π. The result is $g' = \frac{1}{2} m \deg \pi$, where m is the least common denominator of the numbers i_v in (6). Indeed, by (7) this m is the period of E in the Brauer group of F, hence $m^2 = [E' : F]$, where E' is the division algebra corresponding to E, that is, the endomorphism algebra of A'.

We now consider schemes X, Y, ... projective and smooth over a finite field k, whose geometric fibres

$$\overline{X} = X \times_k \bar{k}, \ldots \tag{8}$$

are irreducible. Let $C(X)$ denote the following conjecture [10]: *The canonical map*

$$\boldsymbol{Q}_l \otimes NS_k(X) \to [H_l^2(\overline{X})(1)]^G \tag{9}$$

is bijective for all primes $l \neq \mathrm{char}(k)$, where $NS_k(X)$ denotes the Néron-Severi group of X over k, and where $H_l^2(\overline{X})(1)$ denotes the étale cohomology group of $\overline{X}$ with coefficients in $\boldsymbol{Q}_l$, twisted by $V_l(\boldsymbol{G}_m)$, as explained in [*10*].

Theorem 3. *$C(X)$ and $C(Y)$ imply $C(X \times Y)$.*

To see this one compares the decomposition

$$NS_k(X \times Y) = NS_k(X) \times NS_k(Y) \times DC_k(X, Y)$$

(DC denotes divisorial correspondences) with the Künneth decomposition

$$H_l^2(\overline{X} \times \overline{Y}) = H_l^2(\overline{X}) \times H_l^2(\overline{Y}) \times H_l^1(\overline{X}) \otimes H_l^1(\overline{Y}).$$

If we reinterpret the mixed terms in these decompositions in terms of the abelian varieties $A = \mathrm{Alb}(X)$ and $B = \mathrm{Pic}(Y)$ by means of the standard canonical isomorphisms

$$DC_k(X, Y) \approx \mathrm{Hom}_k(A, B)$$

and

$$H_l^1(\overline{X}) \otimes H_l^1(\overline{Y})(1) \approx \mathrm{Hom}\big(V_l(A), V_l(B)\big),$$

then we see by our main theorem that the map

$$\boldsymbol{Q}_l \otimes DC_k(X, Y) \to [H_l^1(\overline{X}) \otimes H_l^1(\overline{Y})(1)]^G \tag{10}$$

is bijective and this proves Theorem 3.

Theorem 4. *Suppose X is a product of curves and abelian varieties. Then $C(X)$ is true, and the rank of $NS_k(X)$ is equal to the order of the pole of the zeta function of X at the point $s = 1$.*

For an X of this type the statement about the rank of $NS_k(X)$ is equivalent to $C(X)$ being true, as explained in [*10*]. Since $C(X)$ is trivially true for curves, we are reduced by Theorem 3 to proving that $C(X)$ is true in case $X = A$ is an abelian variety. Consider the diagram

$$\begin{array}{ccc} \boldsymbol{Q}_l \otimes NS_k(A) & \underset{\beta}{\overset{\alpha}{\rightleftarrows}} & \boldsymbol{Q}_l \otimes DC_k(A, A) \\ \downarrow \gamma & & \downarrow \gamma \\ H_l^2(\bar{A})(1) & \underset{\beta}{\overset{\alpha}{\rightleftarrows}} & H_l^1(\bar{A}) \otimes H_l^1(\bar{A})(1) \end{array} \tag{11}$$

where γ is the map (9) attaching a cohomology class to a divisor class, where $\alpha = \mu^* - p_1^* - p_2^*$, the morphisms $\mu, p_1, p_2 \colon A \times A \to A$ being, respectively, the addition in A, and the projections on the first and second factors, and where $\beta = \Delta^*$, the morphism $\Delta \colon A \to A \times A$ being the diagonal

one. The diagram is commutative in the sense that $\alpha\gamma=\gamma\alpha$ and $\beta\gamma=\gamma\beta$, and we have

$$\beta\alpha=(\mu\Delta)^*-(p_1\Delta)^*-(p_2\Delta)^*=2^*-1^*-1^*=4-1-1=2,$$

because NS and H^2 are homogeneous quadratic functors of A. From this it follows that the left side of diagram (11) is a direct summand of the right side; thus the bijectivity of (10) for $X=Y=A$ implies that of (9) for $X=A$.

Corollary. *If X is a surface which is an abelian variety or the product of two curves, then the component prime to $p=\mathrm{char}(k)$ of the Brauer group of X is finite, and the product of its order with the determinant of the intersection matrix of a basis for $NS_k(X)$ can be computed from the zeta function of X.*

This follows from Theorem 5.2 of [*11*] because condition (iv) of that theorem is satisfied by such an X in virtue of Theorem 4 above.

References

[*1*] BOURBAKI, N.: Algèbre, Ch. 8, § 4, No. 2.

[*2*] DEURING, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Hamburg **14**, 197—272 (1941).

[*3*] LANG, S.: Abelian varieties. New York: Interscience 1959.

[*4*] MANIN, Y.: The theory of commutative formal groups over fields of finite characteristic. Russian math. surveys **18**, No. 6, 1—81 (1963).

[*5*] MUMFORD, D.: Geometric invariant theory. Ergebn. der Math., Bd. 34. Berlin-Heidelberg-New York: Springer 1965.

[*6*] — On the equations defining abelian varieties. I. Inventiones math. **1**, 287—354 (1966).

[*7*] SERRE, J.-P.: Groupes de Lie l-adiques attachés aux courbes elliptiques. Colloque Internat. du C.N.R.S. No. 143 a Clermont-Ferrand, Éditions du C.N.R.S., Paris 1966.

[*8*] — Courbes elliptiques et groupes formels, l'Annuaire du Collége de France, 1965/66.

[*9*] SHAFARYEVITCH, I.R.: Algebraic Number Fields. Proceedings of the Internat. Congr. of Math. in Stockholm, 1962, p. 163—176. (A.M.S. Translations, Ser. 2, vol. 31, p. 25—39.)

[*10*] TATE, J.: Algebraic cycles and poles of zeta functions. Arithmetical algebraic geometry, p. 93—110. New York: Harper & Row 1965.

[*11*] — On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. Seminaire Bourbaki, 1965/66, exposé 306.

[*12*] WEIL, A.: Variétés abéliennes et courbes algébriques. Act. No. 1064. Paris: Hermann 1948.

Institut des Hautes Études Scientifiques
Harvard University

(Received September 16, 1966)