1971a

ABELIAN VARIETIES OVER FINITE FIELDS[1]

W. C. WATERHOUSE and J. S. MILNE

I. Classification up to isogeny

1. We begin by fixing a field k, which will eventually be finite but need only be perfect until further notice. An *Abelian variety* is a subset of some projective n-space which

(i) is defined by polynomial equations on the coordinates (with coefficients in k),

(ii) is connected, and

(iii) has a group law which is algebraic (in the sense that the coordinates of the product of two points are rational functions of the coordinates of the factors).

The first theorem one proves is that Abelian varieties are commutative; this shows why we insist on connectedness, since otherwise we would be allowing all finite groups and the geometry would be of no help.

In the classical case $k = \mathbf{C}$ the structure of Abelian varieties is fairly well understood: they are all of the form $\mathbf{C}^g/\Lambda$ where Λ is a certain kind of lattice in $\mathbf{C}^g$. These lattices (sometimes disguised as homology groups) are basic to the classical treatment of the subject. They unfortunately disappear in characteristic $p > 0$, and part of our job will be developing substitutes for them. Nevertheless, $\mathbf{C}^g/\Lambda$ is a useful model to keep in mind when considering properties of Abelian varieties.

Let A be an Abelian variety of dimension g, for example, and n a nonzero integer. Multiplication by n is a homomorphism of the group A into itself, and in the classical case it obviously is surjective with finite kernel of cardinality n^{2g}. In general what one proves is that it is surjective (in a reasonable sense, though it need not be surjective on points with coordinates in k), and that its degree is n^{2g}. Here the degree of a map is a number, definable algebraically, which in good cases counts

[1]Preparation of the part by Waterhouse was supported by the contract NSF GP-9395.

the number of points with the same image; thus the degree of a homomorphism is the size of its kernel.

A homomorphism is called an *isogeny* if it is surjective with finite kernel; multiplication by n is a leading example. We say A and B are *isogenous* if there is an isogeny φ from A to B; this is reasonable terminology because there is then also an isogeny from B to A. Indeed, let $G = \ker \varphi$. If n is the degree of φ, then $G \subseteq A_n = \ker (A \xrightarrow{n} A)$. Hence $A \xrightarrow{n} A$ factors through $A/G = B$. The resulting map $\psi\colon B \to A$ is surjective (since $A \xrightarrow{n} A$ is) and has finite kernel (since φ is surjective and $\psi \circ \varphi$ has finite kernel).

Honesty compels me to confess that this proof is not so simple as it looks. It is not obvious that B has the reasonable properties of a quotient A/G; as we will see later, it is not even true without a rather fancy definition of $\ker \varphi$. But now that due warning has been given, I intend to ignore most such problems, and I urge you to do likewise. We therefore know that isogeny is an equivalence relation, and our main concern will be with the structure of Abelian varieties up to isogeny. This means formally that we are making multiplication by n invertible; in practice it means that instead of looking at objects like End A, we look mainly at objects like End $A \otimes_{\mathbf{Z}} \mathbf{Q}$.

THEOREM 1. *Let A be an Abelian variety. Then* End A *is finitely generated and torsion-free, and* End $A \otimes_{\mathbf{Z}} \mathbf{Q}$ *is a semisimple* $\mathbf{Q}$*-algebra.*

Freedom from torsion is simple: if $n\varphi = 0$, then $\varphi(A)$ is connected and lies in the finite set A_n, and so $\varphi(A) = 0$. The rest is not too hard, but we won't linger over it, because it is just the first indication of a better result ahead. Semisimple algebras have an attractive structure: the center is a product of fields, around each field is a division algebra, and around each division algebra is a matrix algebra. The hope is to find this reflected in the structure of A. Note that if $\varphi\colon A \to B$ is an isogeny, and $\psi\colon B \to A$ is the map constructed earlier, then $\alpha \mapsto \varphi \circ \alpha \circ \psi$ is an isomorphism of End $A \otimes \mathbf{Q}$ onto End $B \otimes \mathbf{Q}$; thus the structure of the algebra can at best give structure on A up to isogeny.

DEFINITION. An Abelian variety is *elementary* (or *simple*) if it has no nontrivial Abelian subvarieties. (It of course always has finite subgroups.)

If A and B are elementary, then clearly any nonzero homomorphism from A to B is surjective and has a finite kernel, i.e. is an isogeny. In particular, End $A \otimes \mathbf{Q}$ is a division algebra (Schur's lemma, as usual). We automatically have End $(A^m) =$ M_m (End A), the $m \times m$ matrices. Thus if $A_1, \ldots, A_n$ are nonisogenous elementary Abelian varieties, End $(\prod A_i^{m_i}) \otimes \mathbf{Q}$ is the semisimple algebra $\prod M_{m_i}$ (End $A_i \otimes \mathbf{Q}$). Our hope is then fulfilled by

THEOREM 2 (POINCARÉ-WEIL). *Every Abelian variety is isogenous to a product of powers of nonisogenous elementary Abelian varieties.*

2. We next turn to finding a replacement for the lattices; the idea is to grab hold of the only small, manageable things in sight. Let A be an Abelian variety of dimension g, and let l be a prime different from char (k). We know that

$$A_{l^n} = \ker (A \xrightarrow{l^n} A)$$

is a finite group of order $(l^n)^{2g}$; since it contains exactly l^{2g} elements killed by l, we must have $A_{l^n} \simeq (\mathbf{Z}/l^n\mathbf{Z})^{2g}$. The A_{l^n} form an inverse system under the maps l^m: $A_{l^n} \to A_{l^{n-m}}$, and we fit them together to form the *Tate module*

$$T_l A = \lim_{\leftarrow} A_{l^n}.$$

From what we have said about A_{l^n} it is clear that $T_l A \simeq (\mathbf{Z}_l)^{2g}$, where $\mathbf{Z}_l = \text{proj lim } \mathbf{Z}/l^n\mathbf{Z}$ is the l-adic integers. In the classical case there is a canonical isomorphism $\Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_l \simeq T_l A$, and you should think of $T_l A$ as capturing the nature of the lattice "locally at the prime l." If φ: $A \to B$ is a homomorphism, then clearly φ takes A_{l^n} to B_{l^n} and thus defines a map $T_l\varphi$: $T_l A \to T_l B$. This has the obvious reasonable properties (i.e., T_l is an additive functor).

It is time now to remember that k may not be algebraically closed. If for instance k is finite, then there are only finitely many points on A with coordinates in k, so there aren't enough points to make A_{l^n} as large as it should be. What we do, of course, is to take A_{l^n} consisting of points from the algebraic closure $\bar{k}$ of k; and then the statements are correct.

Once we notice this, we also pick up some additional structure. Let σ be an element of $\mathcal{G} = \text{Gal}(\bar{k}/k)$. If $x \in A_{l^n}$, then $\sigma x \in A_{l^n}$, because being in A_{l^n} is a condition defined by polynomials over k. Thus $T_l A$ is actually a $\mathcal{G}$-module. Furthermore, since by "homomorphisms" we mean group homomorphisms given by rational functions over k, the maps $T_l\varphi$ all commute with the $\mathcal{G}$-action. Finally, as evidence that $T_l A$ captures the local structure at l we have

THEOREM 3 (WEIL). *The map*

$$\text{Hom}(A, B) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \text{Hom}_{\mathcal{G}}(T_l A, T_l B)$$

is injective.

PROOF. Let $\{\varphi_i\}$ be a $\mathbf{Z}$-basis of Hom (A, B), and suppose $\sum \varphi_i \otimes \lambda_i$ goes to 0. Given n, choose integers b_i with $b_i \equiv \lambda_i \pmod{l^n}$. Then $\sum b_i\varphi_i$: $A \to B$ has image in l^n Hom $(T_l A, T_l B)$ and so vanishes on $A_{l^n} = \ker(l^n)$. This implies that there is a ψ: $A \to B$ such that $\sum b_i\varphi_i = \psi \circ l^n = l^n\psi$, and hence all $b_i \equiv 0 \pmod{l^n}$. Thus the λ_i are in $\bigcap l^n\mathbf{Z}_l = \{0\}$.

We have here assumed that Hom (A, B) is finitely generated; with a little further argument one can use this approach to prove it.

3. Our control over the local structure is now good except at $p = \text{char } k$ when this is nonzero. We can still define A_p to be the kernel of multiplication by p, but here there aren't enough points even in $\bar{k}$ (there are at most p^g, and perhaps only one). To understand what is happening, look at a simpler situation. The multiplicative group of $\bar{k}$ has of course an algebraic group law, and φ: $x \mapsto x^p$ is a homomorphism of the group onto itself. Obviously the polynomial map φ has degree p, but you can't tell this by looking at its kernel in $\bar{k}$, since that kernel would be the pth roots of unity and there aren't any except unity itself.

To provide sufficiently large kernels for maps like φ, then, we are forced to introduce objects that can look like "pth roots of unity in characteristic p". These are furnished by the theory of schemes; in a sense it allows us to look for pth roots of unity in rings that aren't fields, and there we can find them. After developing

the technique, one can then prove that A_{p^n} is a finite commutative group scheme of the right rank $(p^n)^{2g}$. The A_{p^n} fit together again in a reasonable way, forming what is called a *p-divisible group* (scheme).

At first sight it is probably not clear what has been gained by introducing these abstract-seeming objects. This will be clarified by the next theorem, for which we need to introduce a certain ring. Let W be the ring of Witt vectors over k. (If k is finite with p^a elements, then W is the ring of integers in the unramified extension of $\mathbf{Q}_p$ with degree a.) Let σ be the unique automorphism of W which reduces to the map $x \mapsto x^p$ on the residue field k. Let $\mathfrak{A} = W[F, V]$ where F and V are indeterminates subjected to the relations

(1) $FV = VF = p$, and

(2) $F\alpha = \alpha^\sigma F$ and $\alpha V = V\alpha^\sigma$ for $\alpha \in W$.

THEOREM 4 (DIEUDONNÉ-CARTIER-BARSOTTI-ODA). *There is a functor from*

$$\{\textit{finite commutative group schemes over } k \textit{ of } p\textit{-power rank}\}$$

to

$$\{\mathfrak{A}\textit{-modules of finite length}\};$$

it is an anti-equivalence of categories. If a group scheme G has rank p^s, then its Dieudonné module DG has length s.

It follows readily that p-divisible groups of co-rank $2g$ (like that coming from A) correspond to $\mathfrak{A}$-modules free of rank $2g$ over W. We write T_pA for the module thus associated with A. Any homomorphism $\varphi: A \to B$ induces an $\mathfrak{A}$-module map $T_p\varphi: T_pB \to T_pA$, and the same proof as before yields

THEOREM 5. *The map*

$$\operatorname{Hom}(A, B) \otimes \mathbf{Z}_p \to \operatorname{Hom}_{\mathfrak{A}}(T_pB, T_pA)$$

is injective.

4. In this section I will try to explain some of the ideas that go into the proof of the basic

THEOREM 6 (TATE). *Suppose that k is finite. Then the maps in Theorems 3 and 5 are bijective.*

From now on we assume that k is finite with $q = p^a$ elements. There is a natural decomposition

$$\operatorname{End}(A \times B) = \operatorname{End}(A) \times \operatorname{Hom}(A, B) \times \operatorname{Hom}(B, A) \times \operatorname{End}(B)$$

and a corresponding decomposition of $\operatorname{End} T_l(A \times B) = \operatorname{End}(T_lA \times T_lB)$; hence if we have an isomorphism on End $(A \times B)$ we have one on Hom (A, B). Thus we may restrict ourselves to endomorphism rings.

An argument like that in Theorem 3 shows that if φ lands in l (End T_lA) then

$\varphi = l\psi$ for some ψ; and thus the quotient of End (T_lA) by the image is torsion-free. Hence it will be enough to prove that

$$(*) \qquad E \otimes_{\mathbf{Q}} \mathbf{Q}_l \to \mathrm{End}_{\mathcal{G}}(V_lA)$$

is bijective, where $V_lA = T_lA \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ and E is the endomorphism algebra End $(A) \otimes \mathbf{Q}$.

Now the left-hand side of (*) has the same dimension for all l, and we know by Theorem 3 that the map is always injective. We will show that the right-hand sides all have the same dimension, so that it will then be enough to prove the isomorphism for a single l. At this point we need the fact that if $\varphi \in$ End A, then the function $n \mapsto$ [degree of $(\varphi - n)$] is a monic polynomial in n of degree 2 dim A with integer coefficients. One can prove that it equals the characteristic polynomial of $T_l\varphi$ on T_lA, and also equals the characteristic polynomial of $T_p\varphi$ acting W-linearly on T_pA.

We also need to recall that Gal $(\bar{k}/k)$ is generated (topologically) by $x \mapsto x^q$. This automorphism of course maps A (which is defined over k) into itself. But this map, since it is given simply by polynomials in the coordinates, actually corresponds to an element π_A in End A. We call π_A the *Frobenius endomorphism* of A, and write f_A for its characteristic polynomial. The elements of $\mathrm{End}_{\mathcal{G}} V_lA$ are now simply the $\mathbf{Q}_l$-linear maps on V_lA which commute with the specific map $T_l(\pi_A)$.

Since π_A is in the center of the semisimple algebra $E \otimes \mathbf{Q}_l$, it acts semisimply on V_l. Suppose its characteristic polynomial $f_A(X)$ factors as $\prod(X - \alpha_i)$ over some splitting field. Then by standard algebra the dimension of the commutant of $T_l(\pi_A)$ is the number of ordered pairs $\langle i, j\rangle$ (including $\langle i, i\rangle$) with $\alpha_i = \alpha_j$. This is obviously independent of l. A similar argument (complicated by the presence of the noncommutative ring $\mathfrak{a}$) works at $l = p$; see Part II.

It still must be shown that the map is bijective for some l. For this purpose one takes l to be a prime which splits completely in the algebra $\mathbf{Q}(\pi_A)$; this condition means that f_A splits into linear factors over $\mathbf{Q}_l$, and so the action of $T_l(\pi_A)$ is quite simple. The proof requires a clever use of a finiteness condition, however, and we will omit it.

I will instead end this section with an unsolved problem: does Theorem 6 hold when k is a number field? It has been proved (except for some cases) by Serre when A and B are elliptic curves. Here of course the Galois group $\mathcal{G}$ is much more complicated, and the representations of $\mathcal{G}$ on the T_lA seem to be quite interesting.

5. As a first consequence of Tate's Theorem we get

THEOREM 7. *Let A and B be Abelian varieties over a finite field k. The following are equivalent:*

(1) *A and B are isogenous.*

(2) *V_lA and V_lB are $\mathcal{G}$-isomorphic for some l.*

(3) *$f_A = f_B$.*

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

(5) *For each finite extension k' of k, the varieties A and B have the same number of points over k'.*

PROOF. We obviously have (1) $\Rightarrow$ (2) $\Rightarrow$ (3), and (3) $\Rightarrow$ (2) because a semi-simple representation is determined by its characteristic polynomial. Suppose now that $\mathrm{Hom}_{\mathcal{G}}(V_lA, V_lB) \simeq \mathrm{Hom}(A, B) \otimes \mathbf{Q}_l$ contains an isomorphism. We can approximate it by elements of $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$ which, if close enough, will also be isomorphisms. Multiplying by an integer we obtain a $\varphi \in \mathrm{Hom}(A, B)$ inducing an isomorphism $V_lA \to V_lB$. If $\ker \varphi$ contained any positive-dimensional Abelian variety C, then φ would annihilate the subspace V_lC of V_lA; hence $\ker \varphi$ is finite. Similarly $\varphi(A)$ cannot lie in any lower-dimensional subgroup of B, and φ is an isogeny.

By the definition of the zeta function, (4) $\Leftrightarrow$ (5). To connect these with (3), consider the map $\pi_A - 1: A \to A$. The points of its kernel are those fixed by $x \mapsto x^q$, i.e. the points with coordinates in k. After checking that the zeros are all separated (e.g. by looking on the tangent space), we can conclude that the number of points of A in k is

$$\text{degree}\,(\pi_A - 1) = f_A(1) = \prod (1 - \alpha_i),$$

where the α_i are the roots of f_A. Similarly, degree $(\pi_A^s - 1) = \prod(1 - \alpha_i^s)$ gives the number of points in the extension of degree s, and thus f_A determines the zeta function. To get the converse, you simply check that the values $\prod(1 - \alpha_i^s)$ (in fact, a finite number of them) are enough to determine the α_i and hence f_A.

6. We are now ready for the classification up to isogeny. We know from §1 that every Abelian variety is isogenous to a product of elementary ones, so those are all we need to discuss.

THEOREM 8. *Let A be an elementary Abelian variety over the field k with q elements. Then*

1. *$f_A = m_A^e$ for some integer e and some irreducible monic polynomial m_A with integer coefficients.*
2. *$E = \mathrm{End}(A) \otimes \mathbf{Q}$ is a division algebra whose center is $\Phi = \mathbf{Q}(\pi_A)$.*
3. *$|E: \mathbf{Q}| = e^2|\Phi: \mathbf{Q}|$, and $2 \dim A = e|\Phi: \mathbf{Q}|$.*
4. *Let v be a prime of Φ, and $\| \ \|_v$ the normalized absolute value. If $\|\pi_A\|_v = q^{-i}$, then i is the invariant of E at v. Explicitly, this is*

$$\begin{cases} \tfrac{1}{2} & \text{if } v \text{ is real,} \\ 0 & \text{if } v \text{ lies over a prime } l \neq p \text{ in } \mathbf{Q}, \\ \mathrm{ord}_v(\pi_A) \cdot |\Phi_v: \mathbf{Q}_p| / \mathrm{ord}_v(q) & \text{if } v \text{ lies over } p. \end{cases}$$

5. *Every embedding of Φ in $\mathbf{C}$ gives π_A the absolute value $q^{1/2}$. In other words, all roots of f_A have absolute value $q^{1/2}$.*

PROOF. We know that E is a division algebra, so its center is a field. That center is $\mathbf{Q}(\pi_A)$ because $E \otimes \mathbf{Q}_l$ is the commutant of $T_l\pi_A$ in $\mathrm{End}_{\mathbf{Q}_l}(V_lA)$. If f_A had two distinct irreducible factors, $\mathbf{Q}(\pi_A)$ could not be a field. The second statement in (3) is obvious from (1), and the first statement comes from the dimension computation in the proof of Theorem 6. The assertion in (5), which we will not prove, is an equivalent form of Weil's Riemann hypothesis for curves over finite fields. Suppose now we take a prime v. There are only a few cases where a real

prime exists (cf. §7), and (4) can be verified there directly. If v lies over $l \neq p$, we look at $V_l A$; by (1) we see that it is a free module of rank e over $\Phi \otimes \mathbf{Q}_l$. Hence $E \otimes \mathbf{Q}_l$, the commutant, is simply the $e \times e$ matrices over $\Phi \otimes \mathbf{Q}_l$. Thus E becomes a matrix algebra, i.e. has invariant 0, at all primes of Φ lying over l. A similar but messier computation lets us deduce the invariants at p from the structure of $T_p A$; see Part II.

COROLLARY. *A is determined up to isogeny by π_A, that is, by m_A.*

PROOF. Given a root π of m_A, we can by the above formulas compute the invariants of E at all primes of $\mathbf{Q}(\pi)$. There is a unique division algebra with center $\mathbf{Q}(\pi)$ and these invariants; its dimension gives us e and so determines $f_A = m_A^e$. For computational purposes we may note that e is the least common denominator of the invariants.

Let us say that an algebraic integer π is a *Weil number* (for q) if it satisfies statement (5) of Theorem 8. Every Abelian variety gives us a Weil number π_A determined up to conjugacy, and π_A determines A up to isogeny. The classification theory can now be summed up in

THEOREM 9 (TATE-HONDA). *Let k be finite. Then there is a one-to-one correspondence between*

$$\{\textit{isogeny classes of elementary Abelian varieties over } k\}$$

and

$$\{\textit{conjugacy classes of Weil numbers for } q = \operatorname{card}(k)\}.$$

To finish proving this, one just has to produce lots of Abelian varieties over k. The idea is to use the classical theory: construct Abelian varieties (with large endomorphism algebras) defined over a number field or a p-adic field, and reduce them mod p. A formula of Shimura and Taniyama describes the Weil numbers we get this way, and a few technical devices then produce enough varieties to give them all.

7. Let me conclude with a couple of remarks. First, it may not seem easy to produce algebraic integers π with all conjugates of absolute value $q^{1/2}$. In fact, however, they can be found quite simply as follows. If π is a Weil number, set $\beta = \pi + (q/\pi)$. Since $\bar{\pi} = |\pi|^2/\pi = q/\pi$ in every embedding, β is a totally real algebraic integer, and $|\beta| \leq 2q^{1/2}$ in every embedding. But now conversely, given any β satisfying these conditions, the roots of $X^2 - \beta X + q = 0$ will be Weil numbers. It is thus easy to write down a β, compute the root π, and read off properties of the corresponding isogeny class from Theorem 8. We may note that π can be real only for $\beta = \pm 2q^{1/2}$, that is, only in the special cases $\pi = \pm q^{1/2}$.

Finally, Tate's theorem is from one point of view an existence theorem for endomorphisms, and in this respect it has a converse. Let k be any field of characteristic p, let A be an elementary Abelian variety over k, let $E = \operatorname{End} A \otimes \mathbf{Q}$, and let Φ be the center of E. We say that A is of *CM-type* if $2 \dim A = |E\colon \Phi|^{1/2} |\Phi\colon \mathbf{Q}|$; this holds for k finite by Theorem 8. Grothendieck has recently proved that, conversely, any Abelian variety of *CM*-type is isogenous to a variety defined over a finite field.

II. Two Theorems of Tate

We here present proofs of two theorems stated in Part I:

THEOREM 1. *Let A and B be Abelian varieties over a finite field k with $q = p^a$ elements. Let T_pA and T_pB be the associated Dieudonné modules. Then*

$$\mathrm{Hom}_k(A, B) \otimes Z_p \xrightarrow{\sim} \mathrm{Hom}_{\mathfrak{a}}(T_pB, T_pA).$$

THEOREM 2. *Suppose that A is elementary over k with Weil number π. Let $E = \mathrm{End}\, A \otimes \mathbf{Q}$ with center $\Phi = \mathbf{Q}(\pi)$, and let v be a prime of Φ lying over p. Then the invariant of E at v is*

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} |\Phi_v\colon \mathbf{Q}_p|.$$

Tate announced these results in [13]; the proofs were presented to a seminar but have never been released to the public. Our proofs are basically the same, but rely more on [4].

PROOF OF THEOREM 1. We adopt the notation of Part I. In addition we write L for the fraction field $W \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, and V_pA for the L-module $T_pA \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then V_pA is actually a module over

$$L[F, V] = L[F, (1/p)F^{-1}] = L[F, F^{-1}],$$

or in other words an $L[F]$-module on which F is a bijection. As in Theorem 6 of Part I it is enough to prove that

$$E \otimes \mathbf{Q}_p \to \mathrm{End}_{L[F]}(V_pA)$$

is bijective for all A, and since injectivity is known it is enough to prove that the two algebras have the same dimension.

We recall from [4, Chapter 3] the structure of finite indecomposable modules V over $R = L[F]$. Such a V has the form $R/R\lambda$ for some λ in R, and there is a smallest r for which $V^r \simeq R/cR$ with c in the center of R. The center of R is $\mathbf{Q}_p[F^a]$, and in fact $c = m_V(F^a)$ with m_V a power of an irreducible polynomial; two indecomposables are isomorphic iff they have the same m_V. One can identify m_V as the minimal polynomial for F^a as a $\mathbf{Q}_p$-linear map on V. Clearly the $\mathbf{Q}_p$-characteristic polynomial for F^a on $R/m_V(F^a)R$ is $m_V^{a^2}$, and the L-characteristic polynomial is m_V^a; the L-characteristic polynomial on V is $m_V^{a/r}$.

Write V_pA now as a sum $\bigoplus V_i^{n_i}$ where the V_i are nonisomorphic indecomposables, and say $V_i^{r_i} \simeq R/m_i(F^a)R$. Let π be the Frobenius endomorphism of A, with characteristic polynomial f and minimal polynomial m. Then on V_pA we know that π acts as F^a and that f is its L-characteristic polynomial (cf. [6, p. 66]). We also know from Part I that m has no repeated roots. Since the $\mathbf{Q}_p$-minimal polynomial of F^a on $\bigoplus V_i^{n_i}$ is the least common multiple of the m_i, and this must divide m, we see that the m_i must all be without repeated roots. They are thus all irreducible, and being distinct have no roots in common. The characteristic

polynomial f is $\prod m_i^{an_i/r_i}$, so the formula in Part I shows that the dimension of E is

$$\sum (\deg m_i) a^2 n_i^2 / r_i^2.$$

But the endomorphisms of $V_i^{r_i} = R/m_i(F^a)R$ are just multiplications by elements of $R/m_i(F^a)R$, which gives $\mathbf{Q}_p$-dimension $a^2 \deg m_i$. Hence End $(V_i^{n_i})$ has dimension $(n_i^2/r_i^2)a^2 \deg m_i$, and

$$\dim \text{End } V_p A = \sum \dim \text{End } (V_i^{n_i}) = \sum (n_i^2/r_i^2) a^2 \deg m_i.$$

PROOF OF THEOREM 2. Suppose the prime v corresponds to the irreducible factor m_i of m over $\mathbf{Q}_p$. Then Φ_v is generated over $\mathbf{Q}_p$ by a root π of m_i. We note that V_i is a simple R-module, since any indecomposable submodule would correspond to a divisor of m_i. Hence $R/m_i(F^a)R$ is a simple algebra. Clearly it can be written as $L \otimes \Phi_v[F]$ with $F^a = \pi$ in Φ_v and $F(\alpha \otimes \varphi) = (\alpha^\sigma \otimes \varphi)F$, where σ is the Frobenius automorphism of L over $\mathbf{Q}_p$; the center is Φ_v.

Let f_v be the residue degree of Φ_v, and set $g = (f_v, a)$, so that $g = |L \cap \Phi_v\colon \mathbf{Q}_p|$ and $a/g = |L\Phi_v\colon \Phi_v|$. Let D be the algebra $L\Phi_v[F']$, where $(F')^{a/g} = \pi \in \Phi_v$ and $F'(\alpha\varphi) = (\alpha^{\sigma^0}\varphi)F'$. We define a map from $L \otimes \Phi_v[F]$ into the $g \times g$ matrices over D by sending

$$\alpha \otimes \varphi \mapsto \begin{pmatrix} \alpha\varphi & & & 0 \\ & \alpha^\sigma\varphi & & \\ & & \cdots & \\ 0 & & & \alpha^{\sigma^{g-1}}\varphi \end{pmatrix}$$

$$F \mapsto \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \cdots & & & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ F' & 0 & 0 & \cdots & 0 \end{pmatrix}$$

It is easy to check that this is a Φ_v-algebra homomorphism. Since $L \otimes \Phi_v[F]$ is simple, the map is injective; by dimension counting it is an isomorphism. Hence $L \otimes \Phi_v[F]$ has the same invariant as D.

Now D is in the standard form for a central simple algebra: $L\Phi_v$ is the unramified extension of degree a/g, and F' acts on it as a generator of the Galois group. Explicitly, it raises to the gth power on the residue field of Φ_v; the Frobenius of $L\Phi_v$ over Φ_v raises to the f_vth power and so is the (f_v/g)th power of our generator. Then it is well known (from explicit computation of the cocycle) that the invariant of D is $(f_v/g) \operatorname{ord}_v \pi/(a/g)$. If e_v is the ramification index of Φ_v over $\mathbf{Q}_p$, we have $e_v f_v = |\Phi_v\colon \mathbf{Q}_p|$ and $\operatorname{ord}_v q = a \cdot \operatorname{ord}_v p = a e_v$, so the number can also be written $(\operatorname{ord}_v \pi/\operatorname{ord}_v q) \cdot |\Phi_v\colon \mathbf{Q}_p|$.

This is the invariant of D, and hence of $R/m_i(F^a)R$. The ring $\text{End}_R(R/m_i(F^a)R)$ is the opposite ring, and so has the negative of that invariant; since it is End $(V_i^{r_i})$, both End (V_i) and End $(V_i^{n_i})$ have this negative invariant. But End $(V_i^{n_i})$ is the part of End $(V_p A)$ sitting over Φ_v, and so it gives the invariant at v. The map from $E \otimes \mathbf{Q}_p$ to End $(V_p A)$ is an anti-isomorphism, however, so the sign reverses again and gives us the invariant we want for E at v.

III. Further Topics

A. ENDOMORPHISM RINGS AND ISOMORPHISM CLASSES. In studying Abelian varieties over a finite field k, what we would like best is a description of the isomorphism classes; since we know a classification up to isogeny, we can restrict to a fixed isogeny class. One invariant obviously associated with A is the ring End (A), and as a first step we can ask which orders in the algebra E occur (up to isomorphism) as endomorphism rings. For any particular E one can answer this question by computation, constructing the spaces V_lA (and V_pA) and considering lattices in them. The problem is to formulate reasonable general theorems. One such involves a nice type of variety which we now define.

THEOREM. *Let A be an elementary Abelian variety over k. The following are equivalent*:

(1) $\pi_A + (q/\pi_A)$ *is a prime to* p,

(2) A_p *contains* $p^{\dim A}$ *points over* $\overline{k}$.

Such varieties are called *ordinary*. For them E is commutative and not changed by extending k.

THEOREM. *Let π be the Weil number of an elementary isogeny class, and E the endomorphism algebra. Then any endomorphism ring is an order containing π and q/π. The converse holds if the class is ordinary, or if $k = \mathbf{Z}/p\mathbf{Z}$ and $\pi \neq \pm p^{1/2}$. The converse does not hold in general, even when E is commutative and not changed by extending k.*

There is a reasonable classification theory for elementary Abelian varieties over $\mathbf{Z}/p\mathbf{Z}$, and a neat treatment of ordinary varieties has appeared in [1]. In general, however, the computation of the isomorphism classes seems to become quite unpleasant. Simplifications can be introduced by adding assumptions on End A, leading to results like the

THEOREM. *Let E be the algebra of an elementary isogeny class. Assume E is commutative, and let R be the ring of integers in E. Then the set of varieties in the class with* End $A = R$ *has the ideal class group of R acting freely on it. Two varieties are in the same orbit iff there is a separable isogeny between them, and one can give a formula for the number of orbits.*

The proof relies on passing from an ideal of End A to a variety isogenous to A; this process has interesting properties more generally. Details can be found in [17].

B. RELATION TO THE CONJECTURES OF BIRCH AND SWINNERTON-DYER. Tate's theorem (see I,§4) gives, in particular, the rank of the free abelian group $\mathrm{Hom}_k(A, B)$ in terms of the characteristic polynomials $f_A(X)$ and $f_B(X)$ of the Frobenius endomorphisms of A and B. It is possible to give similarly explicit descriptions of the higher extension groups of A and B, these groups being formed in the abelian category of all group schemes of finite type over k.

THEOREM 1. *Let A and B be abelian varieties over the finite field k.*

(a) $\mathrm{Hom}_k(A, B)$ *is a free abelian group of rank equal to* $r(f_A, f_B)$, *the number of ordered pairs* $\langle i, j\rangle$ *such that* $\alpha_i = \beta_j$ *where* $\alpha_1, \ldots, \alpha_{2g(A)}$ *are the roots of* $f_A(X)$ *and* $\beta_1, \ldots, \beta_{2g(B)}$ *the roots of* $f_B(X)$.

(b) $\mathrm{Ext}_k^1(A, B)$ *is finite, and its order* $[\mathrm{Ext}_k^1(A, B)]$ *is given by*

$$q^{g(A)g(B)} \prod_{\alpha_i \neq \beta_j} (1 - \alpha_i/\beta_j) = [\mathrm{Ext}_k^1(A, B)]|D|,$$

where D is the discriminant of the nondegenerate pairing

$$\mathrm{Hom}_k(A, B) \times \mathrm{Hom}_k(B, A) \to \mathbf{Z}$$

which takes two homomorphisms to the trace of their composite (as an endomorphism of A or B, indifferently).

(c) $\mathrm{Ext}_k^2(A, B)$ *is a divisible group of corank equal to* $r(f_A, f_B)$.

(d) $\mathrm{Ext}_k^i(A, B) = 0$, $i > 2$.

(a) is Tate's theorem (I, Theorem 6). (b) and (c) may be restated in terms of p-divisible group schemes and proved using their associated Galois modules of points ($p \neq$ char (k)) or Dieudonné modules ($p =$ char (k)) [6]. (d) follows from a much more general theorem on the vanishing of higher extension groups in categories of commutative group schemes over perfect fields [8].

Now let K be a function field in one variable over k. An abelian variety A over k can also be regarded as a "constant" abelian variety over K, and for any abelian variety over a global field there are the conjectures of Birch and Swinnerton-Dyer. For the constant abelian variety A, these take on an especially simple form. In fact, with the notations of [12, §1], S is empty and $\alpha_{i,v} = \alpha_i^{\deg(v)}$ where, as before, the α_i are the roots of $f_A(X)$. By comparing

$$L(s) = \prod_v \prod_i \frac{1}{1 - \alpha_i^{\deg(v)} Nv^{-s}} = \prod_i \prod_v \frac{1}{1 - (\alpha_i q^{-s})^{\deg(v)}}$$

with the known expressions for the zeta function of K

$$Z(K, T) = \frac{f_J(T)}{(1 - T)(1 - qT)} = \prod_v \frac{1}{1 - T^{\deg(v)}}$$

(J = Jacobian of the curve X associated to K/k) and with a little juggling, one reduces the conjectures to

(A) The rank of the group of K-rational points of A, $A(K)$, is $r(f_J, f_A)$.

(B) The order of the Tate-Šafarevič group Ш of A over K is given by

$$q^{g(J)g(A)} \prod_{\gamma_i \neq \alpha_j} \left(1 - \frac{\gamma_i}{\alpha_j}\right) = [Ш]|D'|$$

where the γ_i are the roots of $f_J(X)$ and D' is the discriminant of the canonical height pairing on the K-rational points of A and its dual (suitably normalized).

THEOREM 2. *In this special situation, conjectures* (A) *and* (B) *are true.*

(A) is due to Tate and follows directly from Theorem 1(a) by the obvious identification $A(K) = \mathrm{Hom}_k(J, A)$ (modulo torsion). (B) follows from Theorem 1(b) by identifying D' with D (with J for A, and A for B) and Ш with $\mathrm{Ext}^1_k(J, A)$. Ш can be interpreted as the first étale cohomology group of A over X, and the machinery of étale and flat cohomology used to reduce the identification to the statement, well known in the classical case, that a finite covering of X comes from an isogeny of its Jacobian J [7].

REFERENCES

1. P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.
2. A. Grothendieck and P. Deligne, *Séminaire de Géométrie Algébrique* 7, Exposé II, Inst. Hautes Etudes Sci., Paris (to appear).
3. T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR **37** #5216.
4. N. Jacobson, *The theory of rings*, Amer. Math. Soc. Math. Surveys, no. II, Amer. Math. Soc., Providence, R.I., 1943. MR **5**, 31.
5. S. Lang, *Abelian varieties*, Interscience Tracts in Pure and Appl. Math., no. 7, Interscience, New York, 1959. MR **21** #4959.
6. J. Milne, *Extensions of abelian varieties defined over a finite field*, Invent. Math. **5** (1968), 63–84. MR **37** #5226.
7. ———, *The Tate-Šafarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105. MR **39** #5581.
8. ———, *The homological dimension of commutative group schemes over a perfect field*, J. Algebra (to appear).
9. T. Oda, *The first deRham cohomology group and Dieudonné modules*, Ann. Sci. Ecole Norm. Sup. (4) **2** (1969), 63–135.
10. F. Oort, *Commutative group schemes*, Lecture Notes in Math., no. 15, Springer-Verlag, Berlin and New York, 1966. MR **35** #4229.
11. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.
12. J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analogue*, Séminaire Bourbaki 1965/66, Exposé 306, Benjamin, New York, 1966. MR **34** #5605.
13. ———, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR **34** #5829.
14. ———, *Endomorphisms of abelian varieties over finite fields.* II. (This paper, though cited in the literature, does not exist.)
15. ———, *p-divisible groups*, Proc. Conference on Local Fields, NUFFIC Summer School (Driebergen, Netherlands, 1966) Springer-Verlag, Berlin and New York, 1967. MR **37** #3885.
16. ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki 1968/69 Exposé 352, Benjamin, New York.
17. W. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) **2** (1969), 521–560.
18. A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Indust., no. 1064, Hermann, Paris, 1948. MR **10**, 621.

CORNELL UNIVERSITY
ITHACA, NEW YORK

UNIVERSITY OF MICHIGAN
ANN ARBOR, MICHIGAN 48104