

TATE'S CONJECTURE ON THE ENDOMORPHISMS
OF ABELIAN VARIETIES

Norbert Schappacher

Contents:

§1	Statements
§2	Reductions
§3	Heights
§4	Variants

Following Faltings and using older arguments due to Tate and Zarhin, we shall deduce, from the diophantine result [F2], II 4.3, Tate's conjectural description of the endomorphisms of abelian varieties over number fields, in terms of ℓ -adic representations.

§ 1 Statements

Let K be a number field (of finite degree over \mathbb{Q}), and let A be an abelian variety defined over K . Put $g = \dim A$. For a prime number ℓ , and $n \geq 1$, denote by $A[\ell^n]$ the kernel of multiplication by ℓ^n on A , and write, as usual,

$$T_\ell(A) = \varprojlim_n A[\ell^n](\bar{K}); \quad V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

where \bar{K} is a fixed algebraic closure of K .

T_ℓ and V_ℓ actually define covariant functors in an obvious way. The absolute Galois group $\pi = \text{Gal}(\bar{K}/K)$ acts on $T_\ell(A)$, resp. $V_\ell(A)$, by \mathbb{Z}_ℓ -linear, resp. \mathbb{Q}_ℓ -linear, continuous transformations.

The object of this article is to prove the following theorem, known as Tate's conjecture on the endomorphisms $\text{End}_K A$ of A defined over K .

- 1.1 Theorem. (i) The action of π on $V_\ell(A)$ is *semi-simple*.
(ii) The natural map

$$\text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \text{End}_{\mathbb{Z}_\ell[\pi]}(T_\ell(A))$$

is an isomorphism.

Remark: The following facts can be found, e.g., in [Mu1]:

(i) Since K has characteristic 0 , $T_\ell(A)$ is a free \mathbb{Z}_ℓ -module of rank $2g$.

(ii) If B is another abelian variety over K , the homomorphisms $\text{Hom}_K(A, B)$ always form a free \mathbb{Z} -module of finite type, and the functor T_ℓ induces an injection

$$\text{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \text{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

whose image has to be in the submodule

$$\text{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))^\pi = \text{Hom}_{\mathbb{Z}_\ell}[\pi](T_\ell(A), T_\ell(B))$$

fixed by π , because $u(x)^g = u(x^g)$, for all $g \in \pi$, $x \in A[\ell^\infty]$, if $u \in \text{End } A$ is defined over K . So, the essential claim of 1.1(ii) is *surjectivity*.

1.2 Corollary. For A, B as above, the natural map

$$\text{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \text{Hom}_{\mathbb{Z}_\ell}[\pi](T_\ell(A), T_\ell(B))$$

is an isomorphism.

Proof: Apply 1.1 to the abelian variety $A \times B$. - See [F1], lemma 3.

The following corollary used to be known as the *isogeny conjecture* for abelian varieties over K .

1.3 Corollary. *The following statements are equivalent.*

- (i) *A and B are isogenous over K .*
- (ii) $V_\ell(A) \cong V_\ell(B)$, *as π -modules.*
- (iii) *For almost all primes v of K , $L_v(A,s) = L_v(B,s)$.*
- (iv) *For all v , $L_v(A,s) = L_v(B,s)$.*
- (v) *For almost all v , $\text{tr}(F_v | V_\ell(A)^{I_v}) = \text{tr}(F_v | V_\ell(B)^{I_v})$.*
- (vi) *For all v , $\text{tr}(F_v | V_\ell(A)^{I_v}) = \text{tr}(F_v | V_\ell(B)^{I_v})$.*

Here, $L_v(A,s)$ is the Euler factor at v of the Hasse-Weil L-function of A over K :

$$L(A/K,s) = \prod_v L_v(A,s) \quad (\text{for } \text{Re}(s) > \frac{3}{2}).$$

Let $I_v \subset \pi$ be an inertia subgroup at v , and $F_v \in \pi/I_v$ a Frobenius element at v . Then the action of F_v on $T_\ell(A)^{I_v}$ is well-defined, and we put

$$L_v(A,s) = \frac{1}{\det(1 - \text{Inv}^{-s} \cdot F_v | T_\ell(A)^{I_v})} ,$$

Inv being the cardinality of the residue class field at v . - This definition of L_v does not depend on the choice of the prime number $\ell \nmid \text{Inv}$, and I_v acts trivially on $T_\ell(A)$ for almost all v . Cf.[ST].

Corollary 1.3 asserts in particular that *the L-function $L(A/K,s)$ is a complete isogeny invariant of A/K .*

Proof of 1.3: (i) \iff (ii). $f \in \text{Hom}(A, B)$ is an isogeny if and only if $T_\ell(f)$ has full rank, i.e., $\det T_\ell(f) \neq 0$. This already implies (i) \implies (ii). On the other hand, suppose $\varphi: V_\ell(A) \rightarrow V_\ell(B)$ is an isomorphism of π -modules. Choose n such that $\ell^n \cdot \varphi \in \text{Hom}(T_\ell(A), T_\ell(B))$. This homomorphism comes from $\text{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, and can therefore be approximated by elements of $\text{Hom}(A, B)$. Since $\det(\ell^n \varphi) \neq 0$, the same will be true for good approximations. This way one finds the required isogeny.

Remark: Note that, for an isogeny $f: A \rightarrow B$, $T_\ell(f)$ is an isomorphism $T_\ell(A) \rightarrow T_\ell(B)$ if and only if $\ell \nmid \deg(f)$.

(v) \implies (ii) : A semi-simple representation of a \mathbb{Q}_ℓ -algebra in a finite-dimensional \mathbb{Q}_ℓ -vector space is determined by its character; [Bou], § 12, n°1. In our case, the character is continuous and therefore determined by its values on a dense subset of π . By Čebotarev's theorem (cf. [Se], chap. I), such a subset is provided by the Frobenius elements of a set of places of density 1.

The rest of the proof of 1.3 is logic. Note in particular that any quantifier may be used with ℓ in (ii).

1.4 Remark Since all higher étale cohomology groups

$$H_{\text{ét}}^n(A \times_{\overline{K}} \overline{K}, \mathbb{Q}_\ell)$$

of the abelian variety A are given by exterior powers of

$$H_{\text{ét}}^1(A \times_K \bar{K}, \mathbb{Q}_\ell) \cong \text{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), \mathbb{Q}_\ell)$$

the semi-simplicity asserted in 1.1 implies that:

For all $n \geq 0$, the action of π on $H_{\text{ét}}^n(A \times_K \bar{K}, \mathbb{Q}_\ell)$ is semi-simple.

In fact, since the representations of π in question are in finite dimensional vector spaces over a field of characteristic 0, this follows by passing to Lie-algebras: see [Hum], 13.2; [BoL], chap. I, § 6 n°5; cf. [BoL], chap. III, §9 n°8.

1.5 Tate's general conjecture

Let k be a field which is of finite type over its prime field, \bar{k} a fixed algebraic closure of k , $\pi = \text{Aut}_k(\bar{k})$ and ℓ a prime number different from the characteristic of k . Let X be a smooth projective geometrically connected variety over k , and write $\bar{X} = X \times_k \bar{k}$. Every closed irreducible subvariety \bar{Z} of \bar{X} of codimension r defines an ℓ -adic cohomology class

$$cl(\bar{Z}) \in H^{2r}(\bar{X}, \mathbb{Q}_\ell)(r) = \left\{ \varinjlim_n H_{\text{ét}}^{2r}(\bar{X}, (\mu_{\ell^n})^{\otimes r}) \right\}_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

namely the image of $1 \in \mathbb{Q}_\ell$ under the natural map from relative cohomology

$$\mathcal{O}_\ell \cong H_{\bar{Z}}^{2r}(\bar{X}, \mathcal{O}_\ell)(r) \longrightarrow H^{2r}(\bar{X}, \mathcal{O}_\ell)(r) .$$

Cf. [Mil], chap. VI.

Call $\mathcal{Z}^r(X)$ the free abelian group on subvarieties Z of X of codimension r defined over k , and

$$\mathcal{O}^r(X) = \mathcal{Z}^r(X) / \text{kernel } (Z \mapsto \text{cl}(\bar{Z})) .$$

Then the general form of Tate's conjecture related to our theorem is:

Conjecture: $\mathcal{O}^r(X) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \xrightarrow{\cong} H^{2r}(\bar{X}, \mathbb{Q}_\ell)(r)^\pi .$

Cf. [T3].

We shall now indicate how theorem 1.1(ii) can be seen to be a special case of this conjecture. In fact, things become more transparent when we deduce corollary 1.2 instead. So, suppose A and B are abelian varieties over k , and consider the diagram

$$\begin{array}{ccc}
 \text{Hom}(A, B) & \xrightarrow{(1)} & \text{Pic}^\circ(A \times B^*) \\
 \downarrow (6) & & \downarrow (2) \\
 & & H^2(A \times B^*, \mathbb{Q}_\ell)(1) \\
 & & \downarrow (3) \\
 & & H^1(A, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} H^1(B^*, \mathbb{Q}_\ell)(1) \\
 & & \downarrow (4) \\
 \text{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), V_\ell(B)) & \xleftarrow{(5)} & V_\ell(A) \otimes_{\mathbb{Q}_\ell} V_\ell(B)
 \end{array}$$

where B^*/k is the dual of B , and the maps are given as follows.

- (1) For $\varphi \in \text{Hom}(A, B)$, pullback of the Poincaré bundle $B \times B^*$ via $\varphi \times \text{id}: A \times B^* \rightarrow B \times B^*$.
- (2) First Chern class.
- (3) Projection onto the $(1, 1)$ - component in the Künneth-decomposition.
- (4) Use that $H^1(A, \mathcal{O}_\ell) = V_\ell(A)^*$ (dual), and that the Weil-pairing on $V_\ell(B)$ induces a duality

$$H^1(B, \mathcal{O}_\ell) \times H^1(B^*, \mathcal{O}_\ell) \longrightarrow \mathcal{O}_\ell(-1),$$

and thus an isomorphism

$$H^1(B^*, \mathcal{O}_\ell)(1) \cong H^1(B, \mathcal{O}_\ell)^* = V_\ell(B).$$

- (5) $\lambda \otimes b \mapsto (a \mapsto \lambda(a) \cdot b)$.
- (6) Our natural map, induced by the functor V_ℓ .

It is easy to see that this diagram commutes. All maps are π -equivariant, and from the definition of the Poincaré bundle, it is clear that the image of $\text{Hom}_k(A, B)$ under $(3) \circ (2) \circ (1)$ is precisely $\mathcal{O}^{1 \otimes 1}(A \times B^*) \subset [H^1(A) \otimes H^1(B)(1)]^\pi$, the $H^1 \otimes H^1$ -projection of $\mathcal{O}^1(A \times B^*)$. So, assuming Tate's conjecture, the surjectivity of (6) follows from the fact that (4) and (5) are isomorphisms.

1.6 A glance at the history

Elliptic curves over finite fields have lots of endomorphisms. This phenomenon was systematically perused by Deuring in [Deu], and, as Tate points out in [T1], Deuring's results allow one to deduce the analogue of Corollary 1.2 for A, B elliptic curves over a *finite* field K (of characteristic $\neq \ell$). In [T1], Tate generalized this to abelian varieties over finite fields. In this case, the semi-simplicity of the π -action can be shown directly, but the pattern of proof developed by Tate turned out to be adequate even for the number field case. In a sequence of papers - [Z1] through [Z5] - Zarhin proved the analogue of 1.1 for most function fields of finite transcendence degree over a finite field. For this, he had to refine Tate's way of reducing 1.1 to a diophantine statement, and some of our reduction steps are inspired by Zarhin's refinements.

There have been partial results in the number field case before Faltings' general proof of 1.1, of which we mention Serre's results on elliptic curves (see [Se]), the case of complex multiplication (see [Shim], cf. [ZZ]), and the Jacobian of modular curves ([Ri]).

§2 Reductions

In this section, theorem 1.1 will be seen to be a consequence of a diophantine result on abelian varieties over K . Using the finiteness theorem [F2], II 4.3, this diophantine statement is seen to result from the behaviour of the modular height under certain isogenies. These height calculations will be performed in § 3.

The notations are those of the beginning of § 1.

(2.1) *To prove 1.1(ii), it suffices to show that the natural injection*

$$\text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \longrightarrow \text{End}_{\mathbb{Q}_\ell}[\pi](V_\ell(A))$$

is an isomorphism.

In fact, this map is still injective since \mathbb{Q}_ℓ is flat over \mathbb{Z}_ℓ . Furthermore, the cokernel of the \mathbb{Z}_ℓ -linear map is torsion-free: an endomorphism of A vanishing on $A[\ell]$ is divisible by ℓ .

(2.2) *Let $K' \supset K$ be a finite extension. If 1.1 is true for $A \times_K K'$ over K' , then it holds also over K .*

Let $\pi' = \text{Gal}(\bar{K}/K')$, $\pi'' = \text{Gal}(\bar{K}/K'')$, where K'' is a finite Galois extension of K containing K' . Since π'' is normal in π' , the semi-simplicity of $V_\ell(A \times_K K') = V_\ell(A)$ as a π' -module implies that of the π'' -module $V_\ell(A)$. π acts on

the decomposition of this π'' -module into simple factors, and adding up these π -orbits decomposes $V_\ell(A)$ as a π -module.

Any $\varphi \in \text{End}(T_\ell(A))$ fixed by π is also fixed by π' ; therefore comes from an $f \in \text{End}_K(A \times_K K') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. But f is again fixed under π , and thus lies in $\text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.

(2.3) In proving 1.1, we may assume that A has semi-stable reduction over the ring of integers \mathcal{O} of K .

This is a consequence of 2.2 and Grothendieck's semi-stable reduction theorem - [Groth], thm. 3.6 - which asserts that there is a finite (separable) extension K' of K such that $A \times_K K'$ acquires semi-stable reduction over $\mathcal{O}_{K'}$. We shall recall the definition and various properties of abelian varieties with semi-stable reduction in § 3.

(2.4) To prove 1.1, it suffices to show the following:

(*) $\left\{ \begin{array}{l} \text{For every } \pi \text{-invariant subspace } W \subset V_\ell(A), \text{ there is} \\ u \in \text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \text{ such that } u \cdot V_\ell(A) = W. \end{array} \right.$

A reduction step of this kind is already essential in Tate [T1]. Cf. also [Z4], lemma 3.1. First note that the right ideal

$$\{v \in \text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \mid v \cdot V_\ell(A) \subset W\},$$

like any right ideal in a semi-simple algebra, is generated

by some projector u_0 , i.e., $u_0^2 = u_0$. If u exists as in (*), it follows that $u_0 \cdot V_\ell(A) = W$. So every π -invariant subspace of $V_\ell(A)$ is a direct factor, which implies the semi-simplicity of the π -action.

Let C be the commutant of $\text{End}_K A \otimes \mathbb{Q}_\ell$ in $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. The commutant C° of C equals $\text{End}_K A \otimes \mathbb{Q}_\ell$, by the theorem of bicommutation - [Bou], § 5, n°4 -, again because $\text{End}_K A \otimes \mathbb{Q}_\ell$ is a semi-simple algebra.

Assume we know (*) for all abelian varieties over K , in particular for $A \times A$. Then the graph

$$W = \{(x, \varphi(x)) \mid x \in V_\ell(A)\} \subset V_\ell(A)^2 = V_\ell(A \times A)$$

of any $\varphi \in \text{End}_{\mathbb{Q}_\ell}[\pi](V_\ell(A))$ is a π -invariant subspace, so there is $u \in \text{End}_K A^2 \otimes \mathbb{Q}_\ell$ such that $u \cdot V_\ell(A \times A) = W$.

It will be enough to show that $\varphi \in C^\circ$. So take $\alpha \in C$. Then

$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in \text{End}(V_\ell(A)^2)$ commutes with $\text{End}_K A^2 \otimes \mathbb{Q}_\ell$, in particular with u . Consequently $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} W \subset W$, which means that $\alpha\varphi = \varphi\alpha$, i.e., $\varphi \in C^\circ$.

2.5 Subspaces and ℓ -divisible groups.

Given a \mathbb{Q}_ℓ -linear subspace $W \subset V_\ell(A)$, put $U = W \cap T_\ell(A)$.

Then, for $n \geq 1$,

$$\ell^{-n} U/U \hookrightarrow \ell^{-n} T_\ell(A)/T_\ell(A) = A[\ell^n](\bar{K})$$

defines the levels of an ℓ -divisible subgroup G of $A(\ell)/\bar{K}$ with $\text{height}(G) = \dim_{\mathbb{Q}_\ell} W$. (Cf. [Grun].) If W is π -invariant, G is defined over K .

Over K , we can divide A by G_n (for $n \geq 1$), obtaining abelian varieties A/G_n over K , together with isogenies

$$A \begin{array}{c} \xrightarrow{P_n} \\ \xleftarrow{f_n} \end{array} A/G_n$$

of degree $\ell^{n \cdot \dim W}$, such that

$$\begin{aligned} T_\ell(P_n)^{-1} (T_\ell(A/G_n)) &= \ell^{-n} U + T_\ell(A), \\ T_\ell(f_n) (T_\ell(A/G_n)) &= U + \ell^n T_\ell(A) =: T_n. \end{aligned}$$

(2.6) Given a π -invariant subspace $W \subset V_\ell(A)$, condition (*) of (2.4) is satisfied, if infinitely many of the abelian varieties A/G_n ($n \geq 0$) are isomorphic to each other over K .

The proof of 2.6 is the essential step which enabled Tate to prove the analogue of 1.1 for abelian varieties over finite fields; see [T1], Proposition 1.

To prove 2.6, let I be an infinite subset of \mathbb{N} , with smallest element i_0 , such that, for all $i \in I$, there are isomorphisms defined over K ,

$$v_i : A/G_{i_0} \xrightarrow{\sim} A/G_i.$$

In $\text{End}_K A \otimes \mathbb{Q}_\ell$, consider the element u_i composed of

$$A \xrightarrow{f_{i_0}^{-1}} A/G_{i_0} \xrightarrow{v_i} A/G_i \xrightarrow{f_i} A .$$

Viewed in $\text{End } V_\ell(A)$, u_i maps T_{i_0} onto $T_i \subset T_{i_0}$, in the notations of 2.5. But $\text{End } T_{i_0}$ is compact. So, selecting a smaller I if necessary, we may assume that the sequence $(u_i)_{i \in I}$ converges to a limit u which still comes from $\text{End}_K A \otimes \mathbb{Q}_\ell$ since this set is closed in $\text{End } V_\ell(A)$.

Consider $U = \bigcap_{i \in I} T_i$. Since $u_i(T_{i_0}) = T_i$, every $x \in U$ is a limit $\lim_{i \in I} u_i(y_i)$, for certain $y_i \in T_{i_0}$. Passing to an accumulation point y of the y_i 's we see that $U = u(T_{i_0})$. Thus, $u \cdot V_\ell(A) = W$, as required.

Taking into account (2.3), it is now obvious that we will be done with the proof of Theorem 1.1, once we have obtained the following two results.

2.7 Proposition: *In the notation of (2.5), assuming A , and therefore all the A/G_n , to have semi-stable reduction, the modular height $h(A/G_n)$ is independent of n , for n sufficiently large.*

2.8. Theorem: *Given g and c , there exist, up to isomorphism, only finitely many abelian varieties A with semi-stable reduction over K such that $\dim A = g$ and $h(A) \leq c$.*

The proof of (2.7) and the reduction of (2.8) to the analogous statement for principally polarized abelian varieties which was proved in [F2] will be the subject of the next section.

§ 3 Heights

Before turning to the proofs proper of (2.7) and (2.8), let us recall some basic facts about abelian varieties with semi-stable reduction. The reference for this is [Groth].

Given an abelian variety A_K over the number field K , recall that there exists the *Néron-model* A of A_K which is a smooth group scheme over the ring of integers R of K , and is uniquely characterized by the fact that

$$\text{Hom}_R(S, A) \cong \text{Hom}_K(S_K, A_K) ,$$

for every smooth group scheme S over R with generic fibre S_K . From now on, we will always denote by A the connected component of A , with fibres the connected components of 0 of the fibres of A .

A_K is said to have *semi-stable reduction* over K , if for every $s \in \text{Spec } R$, the fibre A_s sits in an exact sequence

$$1 \longrightarrow T_s \longrightarrow A_s \longrightarrow B_s \longrightarrow 0 ,$$

with an abelian variety B_s and a torus T_s over $k(s)$. Equivalently, [Groth], 3.2, A_K has semi-stable reduction, if there exists some smooth separated group scheme G of finite type over $\text{Spec } R$ whose fibres are all extensions of an abelian variety by a torus as above, and whose generic fibre is A_K .

Assume now that A_K and B_K are abelian varieties with semi-stable reduction over K . Suppose an isogeny

$$\varphi : A_K \longrightarrow B_K$$

over K is given. By the universal property of the (connected) Néron model, φ certainly extends to a morphism over $\text{Spec } R$:

$$\varphi : A \longrightarrow B .$$

Semi-stability implies furthermore that this morphism is *faithfully flat*, and that the kernel

$$G = \ker (A \xrightarrow{\varphi} B)$$

is a quasi-finite, flat group scheme over $\text{Spec } R$. (Cf. [Groth], 2.2.1, or [Mu2], lemma 6.12 : the typical bad case ruled out by semi-stability is multiplication by $p : \mathbb{G}_a \longrightarrow \mathbb{G}_a$, over a field of characteristic p .) Note that G is *not necessarily a finite group scheme* over $\text{Spec } R$ (unless A and B have good reduction everywhere) : its fibres will have varying orders in general.

At any rate, one obtains the exact sequence

$$0 \longrightarrow s^*(\Omega_{B/R}^1) \xrightarrow{\varphi^*} s^*(\Omega_{A/R}^1) \longrightarrow s^*(\Omega_{G/R}^1) \longrightarrow 0.$$

Here, s denotes the zero-sections of the group schemes in question. The exactness at the centre follows from that of the well-known sequence of relative differentials,

$$\varphi^*(\Omega_{B/R}^1) \longrightarrow \Omega_{A/R}^1 \longrightarrow \Omega_{A/B}^1 \longrightarrow 0 .$$

Now, the order of the finite group $s^*(\Omega_{G/R}^1)$ equals

$$\# (s^* \Omega_{G/R}^1) = \# \operatorname{coker}(\wedge^g \varphi^* : \omega_{B/R} \longrightarrow \omega_{A/R}),$$

where $\omega_{X/R}$ denotes the maximal exterior power of $s^*(\Omega_{X/R}^1)$.

This is shown by localizing and applying a well-known corollary of the theorem of elementary divisors.

Recall the definition of the *modular height* of a (semi-)abelian variety:

$$h(A) = \frac{1}{[K:\mathbb{Q}]} \operatorname{deg}(\omega_{A/R}),$$

with:

$$\operatorname{deg}(\omega_{A/R}) = \log \#(\omega_{A/R}/p.R) - \sum_{v|\infty} \varepsilon_v \cdot \log \|p\|_v ,$$

p being a non-zero element of $\omega_{A/R}$, and $\varepsilon_v = 1$ or 2 , according as v is real or complex.

As φ changes the volume by $\sqrt{\operatorname{deg} \varphi}$ at every infinite place of K , we see that we have the

(3.1) Isogeny Formula: *Under the above assumptions,*

$$h(B) - h(A) = \frac{1}{2} \log(\operatorname{deg} \varphi) - \frac{1}{[K:\mathbb{Q}]} \log \#(s^* \Omega_{G/R}^1) .$$

(3.2) For the application of this isogeny formula in the proof of (2.7) we shall need the theory of the *fixed and torus parts* of $T_{\mathcal{X}}(A_K)$, for an abelian variety A_K with semi-stable

reduction. See [Groth], esp. § 5. Let us recall the basics of this theory in the situation we shall encounter.

Let v be a place of K dividing ℓ , and R_v the completion of R at v . As over the spectrum of any Henselian local ring, every quasi-finite scheme X over $\text{Spec } R_v$ decomposes as

$$X = \tilde{X} \amalg Y,$$

where \tilde{X} is *finite* over R_v , and Y has no special fibre, cf. [EGA II]6.2.6. Given A_K with semi-stable reduction as before, we can apply this to the quasi-finite group scheme $A[\ell^v]$, the kernel of multiplication by ℓ^v on the connected Néron model of A_K , considered over the completion R_v , thus obtaining its *finite part* $\widetilde{A}[\ell^v]$ over R_v . These finite parts make up a strict (i.e., $\ell: A \rightarrow A$ is surjective) projective system which then defines what is called the *fixed part* of the Tate-module of A :

$$T_\ell(A)^f \subset T_\ell(A).$$

We shall make use of this submodule *in the generic fibre* (i.e., the only Tate-module we ever considered in §§ 1 and 2) which may be written all explicitly

$$T_\ell(A_K)^f(\overline{K}_v) \subset T_\ell(A_K)(\overline{K}_v).$$

Henceforth, we shall simply write

$$T_\ell(A_{K_v})^f \subset T_\ell(A_{K_v}),$$

even if we think only of the ℓ -adic Galois-representation given by the \overline{K}_V -rational points.

Let \hat{A} over $\text{Spf}(R_V)$ be the formal completion of A/R_V along its special fibre A_0 . Now, in the decomposition above

$$A[\ell^v] = \widetilde{A[\ell^v]} \amalg C_v \quad (v \geq 0)$$

we have

$$\hat{A}[\ell^v] = \widehat{A[\ell^v]} \quad ,$$

because C_v has no special fibre. Therefore,

$$T_\ell(\hat{A}) = T_\ell(A)^f \quad ,$$

if we agree to identify finite schemes over $\text{Spec } R_V$ with finite formal schemes over $\text{Spf}(R_V)$. (Cf. [EGA III], 4.8.)

Furthermore, by semi-stability, the special fibre A_0 sits in an exact sequence

$$1 \longrightarrow T_0 \longrightarrow A_0 \longrightarrow B_0 \longrightarrow 0 \quad ,$$

for some abelian variety B_0 and torus T_0 over $k_V = R_V/\mathfrak{m}_V$.

For every $n \geq 1$, there is a unique torus T_n over $R_V/\mathfrak{m}_V^{(n+1)}$ with special fibre T_0 . ([Gro], 3.6 bis). Being unique, the T_n fit together to define a formal torus \hat{T}/R_V which injects into \hat{A} . This torus gives us a submodule

$$T_\ell(A)^t := T_\ell(\hat{T}) \subset T_\ell(\hat{A}) = T_\ell(A)^f \quad .$$

Here too, we can consider the generic fibre. So we have a two-step filtration

$$T_{\ell}(A_{K_V})^t \subset T_{\ell}(A_{K_V})^f \subset T_{\ell}(A_{K_V})$$

of the Tate-module of the semi-stable abelian variety A_K over K .

Likewise, for the dual abelian variety A_K^* over K , we get submodules

$$T_{\ell}(A_{K_V}^*)^t \subset T_{\ell}(A_{K_V}^*)^f \subset T_{\ell}(A_{K_V}^*) \quad .$$

The Weil pairing provides an alternating duality

$$T_{\ell}(A_K) \times T_{\ell}(A_K^*) \longrightarrow \mathbb{Z}_{\ell}(1) \quad .$$

The *Orthogonality Theorem* - [Groth], 5.2 - asserts that, with respect to this pairing,

$$T_{\ell}(A_{K_V})^t = (T_{\ell}(A_{K_V}^*)^f)^{\perp} \quad ,$$

and, of course, the other way around:

$$T_{\ell}(A_{K_V}^*)^t = (T_{\ell}(A_{K_V})^f)^{\perp} \quad .$$

As a first consequence of this, let us note right away the

3.3 Lemma: Call $D_v = \text{Gal}(\overline{K_v}/K_v) \subset \pi$ the decomposition group and $I_v \subset D_v$ the inertia subgroup of v . Then I_v acts trivially on $T_\ell(A_{K_v})/T_\ell(A_{K_v})^f$, and D_v acts via a finite quotient.

Proof: By the orthogonality theorem,

$$T_\ell(A_{K_v})/T_\ell(A_{K_v})^f \cong \text{Hom}(T_\ell(\hat{T}), T_\ell(G_m)) .$$

So, the lemma follows from the fact that \hat{T} is split by a finite unramified extension of K_v (in fact, T_0 is split by the algebraic closure of the residue field k_v).

(3.4) We can now return to the situation envisaged in (2.5), with a view to proving (2.7). Rewriting (2.5) in our present notation, we are given an abelian variety A_K with semi-stable reduction over K , an ℓ -divisible group $(G_{nK})_{n \geq 0}$, and the quotients

$$A_K \xrightarrow{P_n} (A_K/G_{nK}) = A_{nK} .$$

Passing to connected Néron models, call G_n now the kernel of the isogeny of connected Néron models

$$p_n: A \longrightarrow A_n \quad \text{over } R .$$

Fixing a place $v|\ell$, decompose, as in (3.2) above,

$$G_n = G_n \overset{\sim}{\perp} H_n \quad \text{over } R_v .$$

with \tilde{G}_n finite over $\text{Spec } R_V$, and H_n without special fibre. - Thus,

$$\tilde{G}_n = \hat{A}[\ell^n] \cap G_n .$$

Now, our problem is that $\bigcup_{n \geq 0} \tilde{G}_n$ need not be an ℓ -divisible group over R_V .

In fact, consider first the Galois representation in the generic fibre : $\bigcup_{n \geq 0} \tilde{G}_n(\overline{K}_V)$. Being an intersection of two ℓ -divisible groups over K_V , this is of the form:

$$\left(\begin{array}{l} \overline{K}_V\text{-rational points of an} \\ \ell\text{-divisible group over } K_V \end{array} \right) \oplus \left(\begin{array}{l} \text{finite abelian} \\ \text{group} \end{array} \right) .$$

The finite group is contained in some $\tilde{G}_{n_0}(\overline{K}_V)$, so for $\Gamma_n = \tilde{G}_{n_0+n}/\tilde{G}_{n_0}$ ($n \geq 0$), we find that $\bigcup_{n \geq 0} \Gamma_n(\overline{K}_V)$ is ℓ -divisible over K_V .

But $\bigcup_{n \geq 0} \Gamma_n$ need not be an ℓ -divisible group over R_V . In fact, the sequences

$$0 \longrightarrow \Gamma_n \longrightarrow \Gamma_{n+m} \xrightarrow{\ell^n} \Gamma_m \longrightarrow 0$$

may not be exact over R_V . This problem is discussed on the last page of [T2], and we are going to apply Tate's trick to get around it: Look at the maps induced by multiplication by ℓ

$$(*)_n : \Gamma_{n+2}/\Gamma_{n+1} \xrightarrow{\ell} \Gamma_{n+1}/\Gamma_n \quad (n \geq 0) .$$

Let E_n be the affine algebra of Γ_{n+1}/Γ_n . Since $\bigcup_{n \geq 0} \Gamma_n$ is an ℓ -divisible group over K_V , $F := E_n \otimes_{R_V} K_V$ is a finite-dimensional K_V -algebra which does not depend on n . So, the E_n form an increasing sequence of orders in F . Such a sequence has to become stationary. In other words, the maps $(*)_n$ are isomorphisms for, say, $n \geq n_1$. We claim that the

$$\tilde{\Gamma} := \Gamma_{n_1+n}/\Gamma_{n_1} \cong \tilde{G}_{n_0+n_1+n}/\tilde{G}_{n_0+n_1} \quad (n \geq 0)$$

constitute an ℓ -divisible group over R_V . - We have to show that the long rows of the following commutative diagram are exact, for all n .

$$\begin{array}{ccccccc}
 & & & & & & (*)_{n_1+n} \\
 & & & & & & \Gamma_{n_1+n+1}/\Gamma_{n_1+n} \\
 & & 0 & \longrightarrow & \Gamma_{n_1+n+2}/\Gamma_{n_1+n+1} & \xrightarrow{\cong} & \\
 & & & & \uparrow & & \uparrow \\
 0 & \longrightarrow & \tilde{\Gamma}_1 & \longrightarrow & \tilde{\Gamma}_{n+2} & \xrightarrow{\ell} & \tilde{\Gamma}_{n+1} \longrightarrow 0 \\
 & & \parallel & & \uparrow & & \uparrow \\
 0 & \longrightarrow & \tilde{\Gamma}_1 & \longrightarrow & \tilde{\Gamma}_{n+1} & \xrightarrow{\ell} & \tilde{\Gamma}_n \longrightarrow 0
 \end{array}$$

This follows from this very diagram by induction.

(3.5) We can now begin to show that

$$h(A_{n_0+n_1}) = h(A_{n_0+n_1+n})$$

for all $n \geq 0$, which gives (2.7).

To simplify notations, let us pretend that $n_0=n_1=0$, so that

$\tilde{\Gamma}_n = \tilde{G}_n$. Recall that $A_n = A/G_n$ (connected semi-abelian scheme over R). From 3.1, we get:

$$h(A_n) - h(A) = \frac{1}{2} \log (\deg p_n) - \frac{1}{[K:\mathbb{Q}]} \log \#(s^*\Omega_{G_n}^1/R).$$

Recall (3.2) that, for all places v of K dividing ℓ ,

$$G_n = \tilde{G}_n \amalg H_n \quad \text{over } R_v,$$

where H_n is concentrated in the generic fibre, and \tilde{G}_n is finite over R_v . Completing along the special fibre, one finds $\hat{G}_n = \hat{G}_n^\Delta$, over R_v . - Taking differentials commutes with completion, so we get successively:

$$\#(s^*\Omega_{G_n}^1/R) = \prod_{v|\ell} \#(s^*\Omega_{G_n/R_v}^1) = \prod_{v|\ell} \#(s^*\Omega_{\hat{G}_n/R_v}^1) = \prod_{v|\ell} \#(s^*\Omega_{\tilde{G}_n/R_v}^1).$$

By [Grun], 3.4, we have

$$\#(s^*\Omega_{\tilde{G}_n/R_v}^1) = \#(R_v/\ell^n R_v)^{d_v},$$

where d_v is the dimension of the ℓ -divisible group $\bigcup_{n \geq 0} \tilde{G}_n$ over R_v (we have assumed for simplicity that this is ℓ -divisible).

Call $h = \dim_{\mathbb{Q}_\ell}(W) = \text{rank}_{\mathbb{Z}_\ell}(U)$ (see 2.5) the height of the ℓ -divisible group $\bigcup_{n \geq 0} G_{nK}$ over K .

We find:

$$h(A_n) - h(A) = n \cdot \log(\ell) \cdot \left\{ \frac{h}{2} - \sum_{v|\ell} \frac{[K_v : \mathbb{Q}_\ell]}{[K : \mathbb{Q}]} d_v \right\}$$

We have to show that the expression in curly brackets is zero!

(3.6) Put $\tilde{\pi} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and consider the induced Galois-representations (recall that $U = T_\ell(\bigcup_n G_{nK})$, see 2.5)

$$\tilde{U} = \text{Ind}_\pi^{\tilde{\pi}} U \subset \text{Ind}_\pi^{\tilde{\pi}} T_\ell(A_K) = T_\ell(B_\mathbb{Q}) ,$$

where $B_\mathbb{Q} = \text{Res}_{K/\mathbb{Q}}(A_K)$ is the abelian variety over \mathbb{Q} obtained from A_K by Weil-restriction from K to \mathbb{Q} . We are going to more or less evaluate the character

$$\det \tilde{U} : \tilde{\pi} \longrightarrow \mathbb{Z}_\ell^*$$

in two different ways!

First, it is well-known (cf., e.g., [Mar], 3.2, which is easily generalized to our situation) that

$$\det \tilde{U} = \varepsilon^h \cdot (\det U \circ \text{Ver}_\pi^{\tilde{\pi}}) ,$$

where $\varepsilon : \tilde{\pi} \longrightarrow \{\pm 1\}$ is the signature of the permutations induced by $\tilde{\pi}$ on the homogeneous space $\tilde{\pi}/\pi$, and $\text{Ver}_\pi^{\tilde{\pi}}$ is the transfer map : $\tilde{\pi}^{ab} \longrightarrow \pi^{ab}$. To compute $\det U$ at a place v of K dividing ℓ , up to an unramified character of finite order, we may replace $\bigcup_n G_{nK_v}$ by $\bigcup_n \tilde{G}_{nK_v}$ - this follows from (3.3) since

$$T_\ell(\text{UG}_{\mathbb{N}}^{\sim} / T_\ell(\text{UG}_{\mathbb{N}K_V}^{\sim})) \hookrightarrow T_\ell(A_{K_V}) / T_\ell(A_{K_V})^f .$$

Now, by [Grun], 5.2, we have

$$\wedge^{\tilde{h}} T_\ell(\text{UG}_{\mathbb{N}K_V}^{\sim}) \otimes_{\mathbb{Z}_\ell} C_V \cong C_V(d_V) ,$$

where \tilde{h} is the height of the ℓ -divisible group $\text{UG}_{\mathbb{N}}^{\sim}$ over R_V , and $C_V(d_V)$ is the completion of $\overline{K_V}$ with Galois-action given by the restriction to $\text{Gal}(C_V/K_V) \hookrightarrow \pi \subset \tilde{\pi}$ of the character $\chi_\ell^{d_V}$, with $\chi_\ell: \tilde{\pi} \rightarrow \mathbb{Z}_\ell^*$ the cyclotomic character giving the action of $\tilde{\pi}$ on $T_\ell(\mathbb{G}_m)$. Composing with $\text{Ver}_{\tilde{\pi}}$, and adding up the results for all $v|\ell$, we see that

$$(\det U \circ \text{Ver}_{\tilde{\pi}}) \cdot \chi_\ell^{-\sum_{v|\ell} [K_V:\mathbb{Q}_\ell] d_V}$$

is unramified at ℓ . (The transfer map does not introduce any new ramification because it corresponds to the natural map of ideles $\mathbb{Q}_A^* \rightarrow K_A^*$, via class field theory.) On the other hand, at each finite place w of K not dividing ℓ , the inertia I_w acts unipotently on U since A_K has semi-stable reduction: [Groth], 3.8. As unipotent matrices have determinant 1, we conclude that the character

$$\varphi = \det \tilde{U} \cdot \epsilon^{-h} \cdot \chi_\ell^{-\sum_{v|\ell} [K_V:\mathbb{Q}_\ell] d_V} : \tilde{\pi} \rightarrow \mathbb{Z}_\ell^*$$

is unramified at every rational prime.

But \mathbb{Q} has no (abelian) extensions that are unramified at all finite places (use Minkowski or class field theory). So, by

class field theory, φ has to be the *trivial character*.

Thus for any rational prime $p \neq \ell$ where $B_{\mathbb{Q}}$ has good reduction, if $F_p \in \tilde{\pi}^{\text{ab}}$ is a Frobenius element at p , then, on the one hand, we certainly have $\varphi(p) = 1$. On the other hand, by the part of the "Weil-conjectures" proved by Weil himself, the eigenvalues of F_p on \tilde{U} are algebraic numbers purely of absolute value $p^{1/2}$, since $\tilde{U} \subset T_{\ell}(B_{\mathbb{Q}})$. So, $\det \tilde{U}(F_p)$ is an algebraic number purely of absolute value $p^{h[K:\mathbb{Q}]/2}$ (recall that $h = \text{rank}_{\mathbb{Z}_{\ell}}(U)$!). As $\chi_{\ell}(F_p) = p \in \mathbb{Z}_{\ell}^*$ we conclude that

$$\frac{h[K:\mathbb{Q}]}{2} = \sum_{v|\ell} [K_v:\mathbb{Q}_{\ell}] d_v .$$

This proves (3.5), and therefore (2.7).

We still have to deduce the diophantine result 2.8 from the corresponding assertion, proved in [F2], about *principally polarized* abelian varieties. We claim it will be enough to establish the following two results:

3.7 Proposition: For any abelian variety A_K over K with semi-stable reduction, calling A_K^* its dual abelian variety, we have

$$h(A_K^*) = h(A_K) .$$

3.8 Lemma [Zarhin]: For any abelian variety A_K over K , calling A_K^* its dual, $A_K^4 \times A_K^*$ carries a principal polarization.

In fact, given 3.7 and 3.8, we find

$$h(A_K^4 \times A_K^{*4}) = 8 \cdot h(A_K) ,$$

and of course,

$$\dim (A_K^4 \times A_K^{*4}) = 8 \dim (A_K) .$$

So, the number of K -isomorphism classes of $A_K^4 \times A_K^{*4}$ (even equipped with a principal polarization) is finite. But the ring $\mathcal{E} = \text{End}_K(A_K^4 \times A_K^{*4})$ is finitely generated over \mathbb{Z} , and $\mathcal{E} \otimes \mathbb{Q}$ is a semi-simple algebra. Therefore there are, up to conjugation by \mathcal{E}^* , only finitely many idempotents in \mathcal{E} . (In fact: e and e' are conjugate if and only if $\mathcal{E}e \cong \mathcal{E}e'$ and $\mathcal{E}(1-e) \cong \mathcal{E}(1-e')$. But the number of subspaces $(\mathcal{E} \otimes \mathbb{Q}) \cdot e$ and $(\mathcal{E} \otimes \mathbb{Q})(1-e)$ is finite, and the theorem of Jordan and Zassenhaus implies there are only finitely many choices of a lattice in each of these spaces.) Thus, 2.8 follows from 3.7 and 3.8.

Proof of 3.7 : In computing h , we are free to make finite extensions of the base field. Also, the proposition is trivial if A_K is principally polarizable, because then $A \cong A^*$. Now, over a suitable extension field, A is isogenous to a principally polarized abelian variety. So, it is enough to show that $h(A^*) - h(A)$ is an isogeny invariant. Since every isogeny can be factored (over an extension field) into steps of prime degree, we are reduced to showing that

$$h(A^*) - h(B^*) + h(B) - h(A) = 0 ,$$

Provided there is an isogeny $\varphi: A \rightarrow B$ of degree ℓ .

By our isogeny formula 3.1, applied to φ and to the dual isogeny

$$\varphi^* : B^* \longrightarrow A^* \quad (\text{also of degree } \ell) ,$$

with respective kernels $G \hookrightarrow A$ and $G^* \hookrightarrow B^*$, we have to prove that

$$[K:\mathbb{Q}] \cdot \log(\ell) = \log(\#(s^*\Omega_{G/R}^1) \cdot \#(s^*\Omega_{G^*/R}^1)) .$$

Using the localisation and completion process as in (3.5), it suffices to show that, for every place v of K dividing ℓ ,

$$(3.9) \quad \#(s^*\Omega_{\hat{G}/R_v}^1) \cdot \#(s^*\Omega_{\hat{G}^*/R_v}^1) = \#(R_v/\ell R_v) .$$

To prove 3.9, we shall break up φ and φ^* according to the two-step filtrations of T_ℓ discussed in 3.2. - $T_\ell(\varphi)$ and its dual $T_\ell(\varphi^*)$ induce three pairs of dual maps (the duality following from the orthogonality theorem quoted in 3.2) :

$$T_\ell(A)^t \longrightarrow T_\ell(B)^t$$

(I)

$$T_\ell(A^*)/T_\ell(A^*)^f \longleftarrow T_\ell(B^*)/T_\ell(B^*)^f$$

$$T_\ell(A)^f/T_\ell(A)^t \longrightarrow T_\ell(B)^f/T_\ell(B)^t$$

(II)

$$T_\ell(A^*)^f/T_\ell(A^*)^t \longleftarrow T_\ell(B^*)^f/T_\ell(B^*)^t$$

$$(III) \quad \begin{array}{ccc} T_{\ell}(A)/T_{\ell}(A)^f & \longrightarrow & T_{\ell}(B)/T_{\ell}(B)^f \\ T_{\ell}(A^*)^t & \longleftarrow & T_{\ell}(B^*)^t \end{array}$$

Considering the decompositions of the formal completions of our semi-stable abelian varieties over R_V :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \hat{T}(A) & \longrightarrow & \hat{A} & \longrightarrow & \hat{Ab}(A) & \longrightarrow & 0 \\ & & \downarrow \hat{T}(\varphi) & & \downarrow \hat{\varphi} & & \downarrow \hat{Ab}(\varphi) & & \\ 1 & \longrightarrow & \hat{T}(B) & \longrightarrow & \hat{B} & \longrightarrow & \hat{Ab}(B) & \longrightarrow & 0 \end{array} \quad ,$$

the maps between the torus parts of the Tate-modules in (I) and (III) are induced by the map $\hat{T}(\varphi)$ between the completed tori (resp. by $\hat{T}(\varphi^*)$), and the maps in (II) are derived from the pair of dual mappings $\hat{Ab}(\varphi), \hat{Ab}(\varphi^*)$ between formal abelian schemes over $\text{Spf}(R_V)$.

\hat{G} and \hat{G}^* have order 1 or ℓ , so *precisely one* of the three pairs of dual maps will have non-trivial kernels. More precisely: Suppose a kernel sits in (I). Then $\hat{G} \subset \hat{T}(A)$, and forcibly $\hat{G}^* = 0$. As \hat{G} is of multiplicative type,

$$\#(s^* \Omega_{\hat{G}/R_V}^1) = \#(R_V/\ell R_V)$$

- just as for μ_{ℓ} , see [Grun], 2.5. Next, suppose $\hat{G} \not\subset \hat{T}(A)$, and $\hat{G}^* \neq 0$. Then $\hat{T}(\varphi)$ and $\hat{T}(\varphi^*)$ are isomorphisms, whereas $\hat{Ab}(\varphi)$ and $\hat{Ab}(\varphi^*)$ are dual isogenies of

degree l , with kernels \hat{G} and \hat{G}^* , respectively. Applying the functor $\text{Hom}(\cdot, \hat{\mathbb{C}}_m)$ to the short exact sequence

$$0 \longrightarrow \hat{G} \longrightarrow \hat{\text{Ab}}(A) \longrightarrow \hat{\text{Ab}}(B) \longrightarrow 0,$$

we obtain the exact sequence (of fppf-sheaves)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(\hat{G}, \hat{\mathbb{C}}_m) & \longrightarrow & \text{Ext}^1(\hat{\text{Ab}}(B), \hat{\mathbb{C}}_m) & \longrightarrow & \text{Ext}^1(\hat{\text{Ab}}(A), \hat{\mathbb{C}}_m) \\ & & & & \parallel & & \parallel \\ & & & & \hat{\text{Ab}}(B^*) & & \hat{\text{Ab}}(A^*) \end{array} .$$

This shows that \hat{G} and \hat{G}^* are dual to each other, and consequently (see [Grun], 2.4) :

$$\#(s^*\Omega_{\hat{G}/R_V}^1) \#(s^*\Omega_{\hat{G}^*/R_V}^1) = \#(R_V/\mathfrak{l}R_V),$$

as required.

Finally, if the maps in (I) and (II) are all bijective, then we must have $\hat{G} = 0$ and $\hat{G}^* \subset \hat{T}(B^*)$. This case is exactly dual to the first one we treated.

q.e.d.

To complete this section, we still have to do the

Proof of lemma 3.8:

There is always some polarization on A_K over K , so let \mathcal{L} be an ample line bundle on A_K defined over K , giving rise to the symplectic form

$$\langle , \rangle : T_\ell(A_K) \times T_\ell(A_K) \longrightarrow \mathbb{Z}_\ell(1) ,$$

for any prime ℓ . Choose an integer $N > 0$ such that, for all ℓ ,

$$T_\ell(A_K)^* \subset \frac{1}{N} T_\ell(A_K) \subset T_\ell(A_K) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell ,$$

where $T_\ell(A_K)^*$ is the dual lattice of $T_\ell(A_K)$ with respect to \langle , \rangle . (E.g., $N = \deg(\mathcal{L})$.) There are $a, b, c, d \in \mathbb{Z}$ with

$$a^2 + b^2 + c^2 + d^2 \equiv -1 \pmod{N} .$$

(In fact, $2^2 + 1^2 + 1^2 + 1^2 \equiv -1 \pmod{8}$, and if $-1 \notin (\mathbb{F}_p^*)^2$, then $1 \notin -(\mathbb{F}_p^*)^2 \cup 1 + (\mathbb{F}_p^*)^2$, so that $-(\mathbb{F}_p^*)^2 \cap 1 + (\mathbb{F}_p^*)^2 \neq \emptyset$. From there, one goes with Newton.) Put

$$\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} \in M_4(\mathbb{Z}) ,$$

so that ${}^t \alpha \cdot \alpha \equiv -1 \pmod{N}$. For each ℓ , consider the lattice

$$\begin{pmatrix} I_4 & \alpha \\ 0 & I_4 \end{pmatrix} (T_\ell(A_K)^4 \oplus T_\ell(A_K)^{*4}) \subset V_\ell(A_K)^8 .$$

It is easily checked that, by its very construction, this lattice is selfdual and integral-valued with respect to the form \langle , \rangle^8 on $V_\ell(A_K)^8$. (Note that, as α has rational-integral entries, the Rosati involution of \langle , \rangle^4 on α is simply the transpose.) As the lattice is clearly Galois-invariant, there is a quotient B_K of A_K over K , such that $T_\ell(B_K)$ is the above lattice. B_K is obviously isomorphic to $A_K^4 \times A_K^{*4}$, and from the properties of $T_\ell(B_K)$ we see that it admits a principal polarization.

q.e.d.

This completes the proof of the Tate conjecture.

§ 4 Variants

In this section, we collect some variants of Theorem 1.1 , and indicate a possible variation of its proof.

Let us start with the following obvious consequence of Theorem 1.1 and Corollary 1.2. The notations are those of the beginning of § 1.

4.1 Variant Let T be a finite set of rational primes. Then:

- (i) The action of π on $\bigoplus_{\ell \in T} V_{\ell}(A)$ is semi-simple.
- (ii) The natural map

$$\text{Hom}_K(A, B) \otimes_{\mathbb{Z}} \left(\prod_{\ell \in T} \mathbb{Z}_{\ell} \right) \longrightarrow \prod_{\ell \in T} \text{Hom}_{\pi}(T_{\ell}(A), T_{\ell}(B))$$

is an isomorphism.

There is a less trivial and more interesting way to pass from one \mathbb{Z}_{ℓ} to $\hat{\mathbb{Z}} = \lim_{\substack{\longleftarrow \\ n \in \mathbb{N}}} (\mathbb{Z}/n\mathbb{Z}) = \prod_{\text{all } \ell} \mathbb{Z}_{\ell}$:

4.2 Theorem (See last remark of [F1]; cf. [De], 2.7) Let

$$T(A) = \prod_{\text{all } \ell} T_{\ell}(A) , \quad \text{and}$$

$$\rho : \hat{\mathbb{Z}}[\pi] \longrightarrow \text{End}_{\hat{\mathbb{Z}}} (T(A))$$

be the homomorphism given by the action of π on $T(A)$. Then the subalgebra $\rho(\hat{\mathbb{Z}}[\pi])$ of $\text{End}_{\hat{\mathbb{Z}}} (T(A))$ is of finite index in the commutant of

$$\text{End}_K(A) \hookrightarrow \text{End}_{\mathbb{Z}} \hat{\mathbb{Z}}(T(A))$$

in $\text{End}_{\mathbb{Z}} \hat{\mathbb{Z}}(T(A))$.

Note that 4.2 implies 1.1. In fact, 4.2 implies that, for all primes ℓ , the image of

$$\rho_{\ell}^{\otimes \mathbb{Q}_{\ell}} : \mathbb{Q}_{\ell}[\pi] \longrightarrow \text{End}_{\mathbb{Q}_{\ell}}(V_{\ell}(A))$$

is the commutant of the semi-simple \mathbb{Q}_{ℓ} -algebra $\text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell}$. So, this image is itself a semi-simple \mathbb{Q}_{ℓ} -algebra, whence (i) of 1.1. Furthermore, by the theorem of bicommutation, $\text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell}$ is the commutant of $\rho_{\ell}(\mathbb{Q}_{\ell}[\pi])$ in $\text{End}_{\mathbb{Q}_{\ell}} V_{\ell}(A)$, which implies (ii) of 1.1 - cf. 2.4 above.

But 4.2 is much more precise: It says that, for almost all ℓ , $\rho_{\ell}(\mathbb{Z}_{\ell}[\pi])$ is exactly the commutant of $\text{End}_K(A)$ in $\text{End}_{\mathbb{Z}_{\ell}}(T_{\ell}(A))$!

Proof of 4.2: All we have to show is the last-mentioned equality of $\rho_{\ell}(\mathbb{Z}_{\ell}[\pi])$ and $\text{End}_K(A)^{\circ}$, for almost all ℓ . We proceed by a reduction very much reminiscent of 2.4.

(4.3) *It suffices to show that, for almost all prime numbers ℓ , if W is a π -invariant subspace of the \mathbb{F}_{ℓ} -vector space $A[\ell](\bar{\mathbb{K}})$, then there is $u \in \text{End}_K A$ such that $W = A[\ell](\bar{\mathbb{K}}) \cap \ker(u)$.*

In fact, assuming the condition of 4.3, one immediately gets the semi-simplicity of the π -action on the \mathbb{F}_{ℓ} -vector space $A[\ell](\bar{\mathbb{K}})$. So, the algebra \mathbb{F}_{ℓ} generated by the elements of

π in $\text{End}_{\mathbb{F}_\ell} (A[\ell](\bar{K}))$ is a semi-simple \mathbb{F}_ℓ -algebra. Thus, letting

$$E_\ell = \text{End}_K A \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z} \subset \text{End}_{\mathbb{F}_\ell} (A[\ell](\bar{K})) \quad ,$$

and denoting commutants by $^\circ$, the theorem of bicommutation tells us that $\mathbb{F}_\ell = E_\ell^\circ$ if and only if $\mathbb{F}_\ell^\circ = E_\ell$. But the condition of 4.3 for $A \times A$ implies $\mathbb{F}_\ell^\circ = E_\ell$, by exactly the same argument as in 2.4. So, we have $\mathbb{F}_\ell = E_\ell^\circ$, for almost all primes ℓ . Finally, calling $\text{End}_K A^\circ$ the commutant of $\text{End}_K A$ in $\text{End}_{\mathbb{Z}, \ell} (T_\ell(A))$, we have mappings

$$\mathbb{F}_\ell \xrightarrow{\rho_\ell \otimes \mathbb{Z}/\ell\mathbb{Z}} \text{End}_K A^\circ / \ell \cdot \text{End}_K A^\circ \hookrightarrow E_\ell^\circ \quad .$$

So, by Nakayama's lemma, $\mathbb{F}_\ell = E_\ell^\circ$ implies $\rho_\ell(\mathbb{Z}_\ell[\pi]) = \text{End}_K A^\circ$. This proves 4.3.

In order to prove 4.2, we have to use a result which will only be established in the following article:

4.4 Theorem (see [Wüst], 3.5). For A with semi-stable reduction over K , there is a finite set of primes T such that, for any isogeny $A \rightarrow B$ over K of degree prime to all $\ell \in T$, one has

$$h(A) = h(B) \quad .$$

Like in 2.2, 2.3, we have to prove 4.2 only for semi-stable A . Suppose then that the condition of 4.3 fails to be true. Then there is an infinite set M of prime numbers such that for all $\ell \in M$ there is a π -invariant subspace $W_\ell \subset A[\ell](\bar{K})$ which does not come from an endomorphism u as required in

4.3. Then 4.4 and 2.8 imply that there is an infinite subset $M_0 \subset M$ such that for all $\ell, \ell' \in M_0$, $A/W_\ell \cong A/W_{\ell'}$. Taking $\ell \neq \ell'$ in M_0 , call f the composite map

$$A \longrightarrow A/W_\ell \xrightarrow{\cong} A/W_{\ell'} \longrightarrow A.$$

Since the degree of the last map is a power of ℓ' , the endomorphism $f \in \text{End}_K A$ satisfies indeed

$$W_\ell = A[\ell](\bar{K}) \cap \ker(f),$$

contradicting our initial assumption on M . This proves 4.2.

(4.5) To conclude, let us recall (cf. [T1] and [F1]) that we could have used the weaker diophantine result on *principally polarized* abelian varieties, [F2], II 4.3, instead of 2.8, in the proof of Theorem 1.1, at the expense of working a little harder on the reduction steps of § 2. Refining 2.4, we would have had to reduce to showing that any *maximal isotropic* subspace $W \subset V_\ell(A)$ - with respect to the ℓ -adic Riemann form of some fixed principal polarization on A - is the image of some global endomorphism. This is done by an argument quite similar to the one we had to use here in the proof of 3.8 in order to get 2.8. See [Z4], 2.6, for this reduction. Incidentally, in this approach, it is legal to assume A *principally polarized* because, over a field extension (see 2.2) A is isogenous to some *principally polarized* abelian variety B ; and 1.1 is invariant under isogeny, thanks to 2.1, because isogenous varieties have isomorphic π -representations V_ℓ .

References

- [Bou] N. Bourbaki, Algèbre, chap. 8; Paris 1958.
- [BoL] N. Bourbaki, Groupes et algèbres de Lie, chap. 1 and chap. 2 et 3 ; Paris 1971/72.
- [Deu] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper; Abh. Math. Sem. Han-sische Univ. 14 (1941), 197-272.
- [F1] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern; Inventiones Math. 73 (1983), 349-366.
- [F2] G. Faltings, contribution to this volume (chap. I,II,VI).
- [De] P. Deligne, Preuves des conjectures de Tate et de Shafarevitch; Sém. Bourbaki n°616 (1983/84).
- [EGA II] A. Grothendieck, Éléments de Géométrie Algébrique, II; Publ. Math. I.H.E.S. 8 (1961).
- [EGA III] A. Grothendieck, Éléments de Géométrie Algébrique, III; Publ. Math. I.H.E.S. 11 (1961).
- [Gro] A. Grothendieck, Groupes de type multiplicatif: Homomorphismes dans un schéma en groupes; in: SGA 3/Schémas en groupes II, Springer Lect. Notes Math. 152 (1970).
- [Groth] A. Grothendieck, Modèles de Néron et Monodromie; exp. IX in: SGA 7 I, Springer Lect. Notes Math. 288 (1972).
- [Grun] F. Grunewald, contribution to this volume (chap. III).
- [Hum] J.E. Humphreys, Linear algebraic groups; Springer GTM 21, 1975.

- [Mar] J. Martinet, Character Theory and Artin L-functions; in: Algebraic Number fields (A. Fröhlich, ed.), Proc. LMS Symp. Durham; Acad. Press 1977.
- [Mil] J.S. Milne, Etale Cohomology; Princeton U Press, 1980.
- [Mu1] D. Mumford, Abelian Varieties; Oxford U Press, 1974.
- [Mu2] D. Mumford and J. Fogarty, Geometric Invariant Theory (2nd enlarged edition); Springer Ergebnisse 34 (1982).
- [Ri] K.A. Ribet, Twists of Modular Forms and Endomorphisms of Abelian Varieties; Math. Ann. 253 (1980), 43-62.
- [Se] J.P. Serre, Abelian ℓ -adic representations and elliptic curves ; Benjamin 1968.
- [Shim] G. Shimura, On the zeta-function of an abelian variety with complex multiplication; Ann. Math. 94 (1971), 504-533.
- [ST] J.P. Serre and J. Tate, Good reduction of abelian varieties; Ann. Math. 88 (1968), 492-517.
- [T1] J. Tate, Endomorphisms of abelian varieties over finite fields; Inventiones Math. 2 (1966), 134-144.
- [T2] J. Tate, p -divisible groups; in : Proc. of a conference on *Local Fields* (Driebergen), Springer 1967.
- [T3] J. Tate, Algebraic cycles and poles of zeta functions; in: Arithmetical algebraic geometry, New York (Harper & Row) 1966.
- [Wüst] G. Wüstholz, contribution to this volume (chap. V).
- [Z1] Ju.G. Zarhin, Isogenies of abelian varieties over fields of finite characteristic, Mat. Sb. 95(137) (1974), 461-470 = Math. USSR Sb. 24 (1974), 451-461.

- [Z2] Ju.G. Zarhin, A finiteness theorem for isogenies of abelian varieties over function fields of finite characteristic; *Funct. Anal. i ego Prilozh.* 8 (1974), 31-34.
- [Z3] Ju.G. Zarhin, A remark on endomorphisms of abelian varieties over function fields of finite characteristic; *Izv. Akad. Nauk SSR, Ser. Mat.* 38 (1974) = *Math. USSR Izvest.* 8 (1974), n°3, 477-480.
- [Z4] Ju.G. Zarhin, Endomorphisms of abelian varieties over fields of finite characteristic; *Izv. Akad. Nauk SSR, Ser. Mat.* 39 (1975) = *Math. USSR Izvest.* 9 (1975), n°2, 255-260.
- [Z5] Ju.G. Zarhin, Abelian varieties in characteristic p ; *Mat. Zametki* 19, 3 (1976), 393-400 = *Math. Notes* 19 (1976), 240-244.
- [ZZ] H. Pohlmann, Algebraic cycles on abelian varieties of complex multiplication type; *Annals of Math.* 88(1968), 161-180.