NOTES ON TATE CONJECTURES AND ARAKELOV THEORY

JAYCE GETZ

1. Abelian varieties and a conjecture of Tate

Before we begin, we write down for the record that most of these notes come verbatim out of Milne's online course notes [Mil].

Definition 1.1. Let k be a field. A complete, connected, group variety A/k is called an **abelian variety**.

Remark 1.2. As a note on terminology, according to Milne, an affine variety over a field k is a variety isomorphic to the spectrum of a finitely generated k-algebra R such that $R \otimes_k \overline{k}$ that has no nonzero nilpotents. A variety is a separated scheme admitting a covering by finitely many affine schemes [Mil, p. 5]. This is slightly different from Hartshorne's definition; he requires the base field to be algebraically closed.

It turns out that if A/k is an abelian variety and R is a k-algebra, then $A(R)$ is a commutative group [Mil, p. 9].

Definition 1.3. Let A, B be Abelian varieties. We say that a homomorphism $A \to B$ (a morphism of varieties and a homomorphism of groups) is an **isogeny** if it is surjective and has finite kernel.

Proposition 1.4. [Mil, p. 30] *For a homomorphism α of abelian varieties, the following are equivalent:*

1. *The homomorphism α is an isogeny.*
2. *We have $\dim A = \dim B$ and α is surjective.*
3. *We have $\dim A = \dim B$ and $\ker \alpha$ is finite.*
4. *The homomorphism α is finite, flat, and surjective.*

Thus our intuition of what an isogeny "is" from the elliptic curve case is still basically correct.

Definition 1.5. The **degree** of an isogeny $\alpha : A \to B$ is its degree as a regular map; that is,

$$\deg(\alpha) = [k(A) : k(\alpha^*(B)].$$

As in the elliptic curve case we have the multiplication-by-n isogeny $[n]$ with kernel $A[n]$. It satisfies the following:

Proposition 1.6. *Let A be an abelian variety of dimension g. Then*

$$[n] : A \longrightarrow A$$

is an isogeny of degree n^{2g}.

Proof. This is analogous to the elliptic curve case; one uses the existence of a very ample invertible sheaf $\mathcal{L}$ (a generalization of the canonical differential) to linearize the problem. The sheaf $\mathcal{L}$ behaves well with respect to a generalized Weil-pairing and corresponding dual abelian variety. See [Mil, p. 30]. □

Let ℓ be prime. As in the elliptic curve case we define the **Tate module** of A/k to be

$$T_\ell(A) := \varprojlim A[\ell^n].$$

One can prove [Mil, p. 42] that, provided $\ell \neq \mathrm{char}(k)$, we have

$$T_\ell(A) \approx \mathbb{Z}_\ell^{2g}.$$

as $\mathbb{Z}_\ell$-modules. Thus we obtain a Galois representation

$$\rho_A : G_{\overline{k}/k} \longrightarrow \mathrm{Aut}(T_\ell(A)) \approx \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

simply because ℓ^n-division points are sent to ℓ^n-division points under the action of Galois on A/k.

We now define, for two abelian varieties $A/k, B/k$,

$$\mathrm{Hom}(T_\ell(A), T_\ell(B)) := \{\mathbb{Z}_\ell\text{-linear maps } T_\ell(A) \to T_\ell(B)\}$$

and

$$\mathrm{Hom}_k(T_\ell(A), T_\ell(B)) \subseteq \mathrm{Hom}(T_\ell(A), T_\ell(B))$$

to be the $G_{\overline{k}/k}$-module of all $\mathbb{Z}_\ell$-linear maps equivariant under the Galois representation defined above. $\mathrm{End}(T_\ell(A))$ and $\mathrm{End}_k(T_\ell(A))$ are defined analogously in the obvious manner. Similarly, we define $\mathrm{Hom}_k(A, B)$ to be the $G_{\overline{k}/k}$-module of isogenies from A to B defined over k.

There is a natural map

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_k(T_\ell(A), T_\ell(B)).$$

That this map is an isomorphism was a conjecture of Tate, proven by Faltings in the number field case:

Theorem 1.7. [Fal86a] *Let k be a number field and $A/k, B/k$ be abelian varieties. The representation*

$$\rho_A : G_{\overline{k}/k} \longrightarrow Aut(T_\ell(A))$$

is semisimple, and the map

$$Hom_k(A, B) \otimes \mathbb{Z}_\ell \longrightarrow Hom_k(T_\ell(A), T_\ell(B))$$

is an isomorphism.

Remark 1.8. This theorem was first proven by Tate himself in the case that k is a finite field. Later J. G. Zarhin dealt with the case of a function field over a finite field and Faltings proved it in the number field case. See Faltings' historical account [Fal86b]. Theorem 1.7 is a crucial step in Faltings' proof of the Mordell conjecture.

Remark 1.9. Bijectivity of the map

$$\mathrm{Hom}_k(A, B) \longrightarrow \mathrm{Hom}_k(T_\ell(A), T_\ell(B)) \tag{1.1}$$

tells us that T_ℓ is a fully faithful functor from the category of g-dimensional abelian varieties with isogenies as morphisms to the category of $2g$-dimensional ℓ-adic Galois representations with $G_{\overline{k}/k}$-equivariant $\mathbb{Z}_\ell$-linear maps as morphisms. This description of the map (1.1) and the one in the next remark lead one to the interpretation of Theorem 1.7 as a special case of the Hodge-Tate conjectures.

Remark 1.10. If an abelian variety $A/\mathbb{C}$ has dimension g, then $A(\mathbb{C})$ is a g-dimensional complex Lie group. As such, its tangent space $\mathrm{Tgt}_0(A) \approx \mathbb{C}^g$ at the identity is defined, and one can show that we have an analytic isomorphism

$$A(\mathbb{C}) \cong \mathrm{Tgt}_0(A)/\Lambda \approx \mathbb{C}^g/\Lambda$$

for some lattice Λ (although the converse is not true for $g > 1$, that is, not every lattice in $\mathbb{C}^g$ defines an abelian variety). Thus, with respect to the usual topology we have that the first singular homology group satisfies

$$H_1(A(\mathbb{C}), \mathbb{Z}) \approx \mathbb{Z}^{2g}.$$

See [Mil, p. 10,11].

If A is defined over an arbitrary field k and one uses étale cohomology, it can be shown that

$$H_1^{\text{ét}}(A, \mathbb{Z}_\ell) \cong T_\ell(A).$$

Thus Theorem 1.7 can be interpreted as giving a description of when a map between homology groups corresponds to an algebro-geometric map.

2. The proof of Theorem 1.7

Our aim in this section is to sketch a proof of Theorem 1.7. We will require the following theorem of Faltings:

Theorem 2.1. *Let A/k be an abelian variety over a number field k. Up to isomorphism, there are only finitely many abelian varieties B/k isogenous to A by an isogeny of degree a power of ℓ.*

This is proven using Arakelov theory, and the author hopes to sketch a proof of it later. For the time being, we will assume it.

The first step of the proof of Theorem 1.7 is to prove injectivity of the map

$$\mathrm{Hom}_k(A, B) \longrightarrow \mathrm{Hom}(T_\ell(A), T_\ell(B)). \tag{2.1}$$

This is much easier than proving surjectivity; the proof follows the same lines as the proof in the elliptic curve case. The first step is the next proposition. Before we state it, we note that a simple abelian variety is just an abelian variety with no nontrivial abelian subvarieties.

Proposition 2.2. *For any abelian variety A/k, there are simple abelian varieties $A_1, ..., A_n \subset A$ such that the map*

$$\begin{array}{rcl} A_1 \times \cdots \times A_n & \longrightarrow & A \\ (a_1, \ldots, a_n) & \longmapsto & a_1 + \cdots + a_n \end{array}$$

is an isogeny.

Proof. See [Mil, p. 40]. The proof hinges on the fact that there exists an abelian variety dual to A. This allows one to define something analogous to an orthogonal complement to any abelian subvariety $A' \leq A$. □

Now we prove that the map (2.1) is an injection. Suppose α is a homomorphism such that the induced homomorphism on Tate modules, $T_\ell \alpha$, is identically zero. Then $\alpha(P) = 0$ for all $P \in A(\overline{k})$ such that $\ell^n P = 0$ for some n. Let $A' \subset A$ be a simple abelian variety, which we know exists by Proposition 2.2. Then the kernel of $\alpha|_{A'}$ is not finite because it contains $A'[\ell^n]$ for all n. Thus it is a nonzero abelian subvariety of A', which implies by simplicity that $\alpha|_{A'} = 0$. Thus α has every simple abelian subvariety of A in its kernel, which implies by Proposition 2.2 that α is identically zero.

Now note that, because $T_\ell(A)$ is torsion-free for any abelian variety A, the injectivity of (2.1) implies that the same is true of $\mathrm{Hom}_k(A, B)$. Thus for the proof of the second part of Theorem 1.7 it suffices to prove surjectivity of the map

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}_\ell \longrightarrow \mathrm{Hom}_k(T_\ell(A) \otimes \mathbb{Q}_\ell, T_\ell(B) \otimes \mathbb{Q}_\ell). \tag{2.2}$$

Before we can prove the surjectivity of (2.2), we must state a number of preliminary results. Throughout, A and B will denote abelian varieties defined over a field k.

Lemma 2.3. *If $\alpha : A \to B$ is an isogeny of degree prime to char k then* $\ker(\alpha)(\overline{k})$ *is a finite subgroup of $A(\overline{k})$ stable under that action of $G_{\overline{k}/k}$. Conversely, every such subgroup arises as the kernel of such an isogeny; that is, the quotient A/N is an abelian variety over k.*

Proof. See [Mil, p. 78]. This isn't terribly deep, especially in characteristic zero; it follows from a standard result dealing with the action of a finite group on a variety, see [Ser88, p.50]. □

Lemma 2.4. (1) *For any abelian variety A and $\ell \neq$ char k there is an exact sequence*

$$0 \longrightarrow T_\ell(A) \xrightarrow{\ell^n} T_\ell(A) \longrightarrow A[\ell^n] \longrightarrow 0\cdot$$

(2) *An isogeny $\alpha : A \to B$ of degree prime to chark defines an exact sequence*

$$0 \longrightarrow T_\ell(A) \longrightarrow T_\ell(A) \longrightarrow C \longrightarrow 0$$

with the order of C equal to the power of ℓ dividing $\deg(\alpha)$.

Proof. (1) That the multiplication by ℓ^n map has this property follows from the definition of the Tate module:

$$T_\ell(A) = \{(a_n)_{n \geq 1} : a_n \in A[\ell^n],\ \ell a_n = a_{n-1},\ \text{and } \ell a_1 = 0\}.$$

(2) We consider the following infinite diagram:

$$\begin{array}{ccccccccccc}
\downarrow & & \ell\downarrow & & \ell\downarrow & & \ell\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & K_{n+1} & \longrightarrow & B[\ell^{n+1}] & \xrightarrow{\alpha} & A[\ell^{n+1}] & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\
\downarrow & & \ell\downarrow & & \ell\downarrow & & \ell\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & K_n & \longrightarrow & B[\ell^n] & \xrightarrow{\alpha} & A[\ell^n] & \longrightarrow & C_n & \longrightarrow & 0 \\
\downarrow & & \ell\downarrow & & \ell\downarrow & & \ell\downarrow & & \downarrow & & \downarrow
\end{array}$$

The kernel of α is finite, so eventually $K_n = K_{n+1} = \cdots =: K$. The fact that $|K| < +\infty$ also implies that K contains no element divisible by all powers of ℓ; thus

$$\varprojlim K_n := \{(a_n)_{n\geq 1} : a_n \in K_n,\ \ell a_n = a_{n-1},\ \text{and } \ell a_1 = 0\}$$

is zero. Since $|B[\ell^n]| = \ell^{2gn} = |A[\ell^n]|$, we have $|K_n| = |C_n|$, so $|C_n|$ is constant for large n. The map $C_{n+1} \to C_n$ is surjective, and hence for large n it is a bijection. Thus $\varprojlim C_m \to C_n$ is a bijection for n sufficiently large. Passing to the inverse limit we obtain the desired short exact sequence.

□

We have one more "elementary" lemma to prove. Suppose $\alpha : B \to A$ is an isogeny. Then the image of $T_\ell\alpha : T_\ell B \to T_\ell A$ is a $G_{\overline{k}/k}$-stable $\mathbb{Z}_\ell$-module of finite index in T_ℓ. We now show that every such submodule arises from an isogeny α, which further has degree a power of ℓ.

Lemma 2.5. *Assume $\ell \neq$ char k. For any $G_{\overline{k}/k}$ submodule W of finite index in $T_\ell A$ there exists an abelian variety B and an isogeny $\alpha : B \to A$ of degree a power of ℓ such that $\alpha(T_\ell(B)) = W$.*

Proof. Because W is $G_{\overline{k}/k}$-stable, if it contains one point of order ℓ^n, it contains all points of order ℓ^n, for they are all zeros of the same polynomial in k. Because of this and the fact that W is of finite index, we can choose n large enough that $W \supset \ell^n T_\ell(A)$. Let N be the image of W in $T_\ell(A)/\ell^n T_\ell(A) = A[\ell^n]$. Then N is stable under the action of $G_{\overline{k}/k}$. Define $B := A/N$. Because $N \subset A[\ell^n]$ we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\ \ell^n\ } & A \\ {\scriptstyle\beta}\big\downarrow & & \big\uparrow{\scriptstyle\alpha} \\ A/N & =\!= & B \end{array}$$

Here β is just the quotient map. We now show that $\mathrm{im}(T_\ell\alpha : T_\ell(B) \to T_\ell(A)) = W$. From the diagram

$$\begin{array}{ccc} T_\ell(A) & \xrightarrow{\ \ell^n\ } & T_\ell(A) \\ {\scriptstyle T_\ell\beta}\big\downarrow & & \big\uparrow{\scriptstyle T_\ell\alpha} \\ T_\ell(B) & =\!= & T_\ell(B) \end{array}$$

we have that $\mathrm{im}(T_\ell\alpha) \supset \ell^n T_\ell(A)$, and so it suffices to show that the image of $\mathrm{im}(T_\ell\alpha)$ in $T_\ell(A)/\ell^n T_\ell(A) = A[\ell^n]$ (see Lemma 2.4.1) is N. We have

$$B[\ell^n] = \{a \in A(\overline{k}) : \ell^n a \in N\}/N,$$

and if $b \in B[\ell^n]$ is represented by $a \in A(\overline{k})$, then $\alpha(B) = \ell^n a$. Thus α maps $B(\overline{k})$ onto N. □

We now come to the preparatory lemma whose proof will use Theorem 2.1.

Lemma 2.6. *Let A/k be an abelian variety over a number field k. Then for any $W \subset T_\ell(A) \otimes \mathbb{Q}_\ell$ of finite index and stable under the action of $G_{\overline{k}/k}$, there is a $u \in End(A) \otimes \mathbb{Q}_\ell$ such that $uT_\ell(A) \otimes \mathbb{Q}_\ell = W$.*

Proof. To ease notation during the proof, set $T_\ell := T_\ell(A)$ and $V_\ell := T_\ell(A) \otimes \mathbb{Q}_\ell$. Let

$$X_n := (T_\ell \cap W) + \ell^n T_\ell.$$

This is a $\mathbb{Z}_\ell$-submodule of T_ℓ stable under the action of $G_{\overline{k}/k}$ and of finite index in T_ℓ. Therefore, by Lemma 2.5, there is an abelian variety $B(n)/k$ and an isogeny

$$f_n : B(n) \longrightarrow A$$

such that $f_n(T_\ell(B(n))) = X_n$.

According to Theorem 2.1, the $B(n)$ fall into only finitely many distinct isomorphism classes, and so at least one class has infinitely many $B(n)$'s, that is, there is an infinite set I of positive integers such that $B(i) \approx B(j)$ for $i, j \in I$. Let i_0 be the smallest element of I. For each $i \in I$, choose an isomorphism $v_i : B(i_0) \to B(i)$. Now consider the diagrams

$$\begin{array}{cccc} v_i: & B(i_0) & \longrightarrow & B(i) \\ & \downarrow f_{i_0} & & \downarrow f_i \\ & A & & A \end{array}$$

and

$$\begin{array}{cccc} T_\ell v_i: & T_\ell B(i_0) & \longrightarrow & T_\ell B(i) \\ & \downarrow f_{i_0} & & \downarrow f_i \\ & X_{i_0} & & X_i \end{array}$$

Now let $u_i := f_i v_i f_{i_0}^{-1}$, where $f_{i_0}^{-1}$ is the dual isogeny corresponding to f_{i_0}. We have $u_i \in \mathrm{End}(A) \otimes \mathbb{Q}$, and hence we can view u_i also as an element of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$. Further, by considering the lower diagram we have $u_i(X_{i_0}) = X_i$. Because $X_i \subset X_{i_0}$, we may view the u_i for $i \in I$ as elements of $\mathrm{End}(X_{i_0})$. Now, $\mathrm{End}(X_{i_0})$ is a submodule of a finitely generated free $\mathbb{Z}_\ell$-module, and hence is compact in the ℓ-adic topology. Thus, after replacing $(u_i)_{i \in I}$ with a subsequence, we may assume that $u_i \to u$ in $\mathrm{End}(X_{i_0}) \subset \mathrm{End}(T_\ell(A) \otimes \mathbb{Q}_\ell)$. We can view $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ as a subspace of $\mathrm{End}(T_\ell(A) \otimes \mathbb{Q}_\ell$, and hence it is closed. Since each $u_i \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$, their limit u is also in $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$.

For any $x \in X_{i_0}$, $u(x) := \lim u_i(x) \in \bigcap X_i$. Conversely, if $y \in \bigcap X_i$, then there exists for each $i \in I$, an element $x_i \in X_{i_0}$ such that $u(x_i) = y$. From the compactness of X_{i_0} (a submodule of a free $\mathbb{Z}_\ell$-module), we can, after replacing I with a subset if necessary, assume that the sequence (x_i) will converge to a limit $x \in X_{i_0}$. Collecting the observations of this paragraph, we have $u(x) = \lim u(x_i) = \lim u_i(x_i) = y$. Thus $u(X_{i_0}) = \cap X_j = T_\ell \cap W$, which in turn implies $u(T_\ell(A) \otimes \mathbb{Q}_\ell) = W$. □

Remark 2.7. Again, notice that this proof depended in a crucial way on Faltings' finiteness result Theorem 2.1.

We are now in a position to prove Tate's conjecture. Before we do, we recall the following facts about semisimple k-algebras (references are given on [Mil, p. 80]). By convention, we shall always assume k-algebras to be finite dimensional over k, and modules over a k-algebra R to be finite dimensional over R.

- Wedderburn's theorem states that every simple k-algebra is isomorphic to $M_n(D)$ for some division k-algebra D.
- Every right ideal in a semisimple k-algebra is generated by an idempotent (this follows upon applying Wedderburn's theorem and the straightforward characterization of right ideals in a matrix ring over a division algebra).

- Let $C_E(R)$ be the centralizer of a subalgebra R of a k-algebra E. If $E = \mathrm{End}_k(V)$ for some semisimple R-algebra V, then $C_E(C_E(R)) = R$.

Now let A is an abelian variety. Recall that we have a decomposition of A into simple abelian varieties via Proposition 2.2. Further, if A/k is a simple abelian variety, any nonzero element $\alpha \in \mathrm{End}(A)$ is an isogeny by simplicity, which implies that there exists $\beta \in \mathrm{End}(A)$ such that $\alpha \circ \beta = n \in \mathbb{Z}$ (see [Mil, Remark 7.12]). Thus $\mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra for any simple abelian variety A, because . From the injectivity of (2.1) we have for an arbitrary abelian variety A that $\mathrm{End}(A) \otimes \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-algebra, and combining this with the above remarks we see that it is semisimple. We will use this in the proof of the following theorem:

Theorem 2.8. *Let A be an abelian variety over a number field k and $\ell \neq$ char k be a prime. Then*

(1) *The $\mathbb{Q}_\ell[G_{\overline{k}/k}]$-module $T_\ell(A) \otimes \mathbb{Q}_\ell$ is semisimple.*
(2) *The map $End(A) \otimes \mathbb{Q}_\ell \widetilde{\longrightarrow} End_k(T_\ell(A) \otimes \mathbb{Q}_\ell)$ is an isomorphism.*

Proof. We use a subscript $_{\mathbb{Q}_\ell}$ as shorthand for $\otimes\mathbb{Q}_\ell$ below. As is only proper, we first prove (1). Let W be a $G_{\overline{k}/k}$-invariant subspace of $T_\ell(A) \otimes \mathbb{Q}_\ell$. It suffices to construct a complement W' to W that is also stable under $G_{\overline{k}/k}$. Let

$$\mathfrak{a} := \{u \in \mathrm{End}_k(A) \otimes \mathbb{Q}_\ell : u(T_\ell(A) \otimes \mathbb{Q}_\ell) \subset W\}$$

This is a right ideal in $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$. Further, an application of Lemma 2.6 implies that there exists $u \in \mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$ such that $uV_\ell A = W$, and hence $\mathfrak{a}(T_\ell(A) \otimes \mathbb{Q}_\ell) = W$. From the generalities on semisimple k-algebras above, we know that $\mathfrak{a}$ is generated by an idempotent e; further, by the last sentence, $eT_\ell(A) \otimes \mathbb{Q}_\ell = W$. We now have a decomposition

$$T_\ell(A)_{\mathbb{Q}_\ell} = eT_\ell(A)_{\mathbb{Q}_\ell} \oplus (1-e)T_\ell(A)_{\mathbb{Q}_\ell} = W \oplus W'.$$

Since the elements of $G_{\overline{k}/k}$ commute with the elements of $\mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$, $W' := (1-e)T_\ell(A)_{\mathbb{Q}_\ell}$ is stable under the action of $G_{\overline{k}/k}$.

Now we prove (2). Let C be the centralizer of $\mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$ in $\mathrm{End}(T_\ell(A)_{\mathbb{Q}_\ell})$ and let B be the centralizer of C. Because $\mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$ is semisimple, $B = \mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$.

Consider $\alpha \in \mathrm{End}_k(T_\ell(A) \oplus \mathbb{Q}_\ell)$; we have to show that $\alpha \in B$ (viewing the injection as an inclusion). The graph of α

$$W := \{(x, \alpha x) : x \in T_\ell(A) \otimes \mathbb{Q}_\ell\}$$

is a $G_{\overline{k}/k}$-invariant subspace of $T_\ell(A)_{\mathbb{Q}_\ell} \times T_\ell(A)_{\mathbb{Q}_\ell}$, and thus there is a $u \in \mathrm{End}_k(A \times A)_{\mathbb{Q}_\ell} = M_2(\mathrm{End}_k(A))_{\mathbb{Q}_\ell}$ such that $u(T_\ell(A \times A)_{\mathbb{Q}_\ell}) = W$. Let $c \in C$. Then $\left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) \in \mathrm{End}_k(T_\ell(A)_{\mathbb{Q}_\ell} \times T_\ell(A)_{\mathbb{Q}_\ell})$ commutes with $\mathrm{End}_k(A \times A) \otimes \mathbb{Q}_\ell$, and, in particular, with u. Thus

$$\left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) W = \left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) u(T_\ell(A)_{\mathbb{Q}_\ell}) = u \left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) (T_\ell(A)_{\mathbb{Q}_\ell}) \subset W.$$

This says that for any $x \in T_\ell(A)_{\mathbb{Q}_\ell}$, $(cx, c\alpha x) \in W$. Thus, by definition of W, $\alpha c x = c \alpha x$, and hence $c\alpha = \alpha c$. Because c was an arbitrary element of C, we have $\alpha \in B = \mathrm{End}_k(A) \otimes \mathbb{Q}_\ell$. □

Corollary 2.9. *Let A, B be abelian varieties over a number field k. Then the map*

$$Hom_k(A, B) \otimes \mathbb{Q}_\ell \longrightarrow Hom_k(T_\ell(A) \otimes \mathbb{Q}_\ell, T_\ell(B) \otimes \mathbb{Q}_\ell)$$

is an isomorphism.

Proof. We have the following "inclusions" (actually injections) of finite-dimensional $\mathbb{Q}_\ell$-vector spaces:

$$\begin{array}{cccc} \mathrm{End}_k(T_\ell(A)_{\mathbb{Q}_\ell}) & \times\mathrm{Hom}_k(T_\ell(A)_{\mathbb{Q}_\ell}, T_\ell(B)_{\mathbb{Q}_\ell}) & \times\mathrm{Hom}_k(T_\ell(B)_{\mathbb{Q}_\ell}, T_\ell(A)_{\mathbb{Q}_\ell}) & \times\mathrm{End}_k(T_\ell(A)_{\mathbb{Q}_\ell}) \\ \cup & \cup & \cup & \cup \\ \mathrm{End}_k(A)_{\mathbb{Q}_\ell} & \times\mathrm{Hom}_k(A, B)_{\mathbb{Q}_\ell} & \times\mathrm{Hom}_k(B, A)_{\mathbb{Q}_\ell} & \times\mathrm{End}(B)_{\mathbb{Q}_\ell} \end{array}$$

Again, the subscript ${}_{\mathbb{Q}_\ell}$ is shorthand for $\otimes\mathbb{Q}_\ell$. The top row is simply $\mathrm{End}_k(T_\ell(A \times B) \otimes \mathbb{Q}_\ell)$, and the bottom is just $\mathrm{End}_k(A \times B) \otimes \mathbb{Q}_\ell$. The fact that $\mathrm{End}_k(A \times B) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_k(T_\ell(A \times B) \otimes \mathbb{Q}_\ell)$ is an isomorphism then implies the result □

Remark 2.10. In the proof of Theorem 1.7, the only reason we needed to restrict to the number field case was in order to apply Faltings' finiteness result (Theorem 2.1). The analogous statement also holds for finite fields (see [Mil, §22]).

3. Heights and finiteness results

We begin by restating Theorem 2.1 in a slightly more general form:

Theorem 3.1. *Let A/k be an abelian variety over a number field. Then, up to isomorphism, there are only finitely many abelian varieties B over k that are isogenous to A.*

In this section, we give an indication of the proof of Theorem 3.1. Many of the tools that go into the proof are of at least as much interest as the result itself; we will simply use Theorem 3.1 as a means to motivate their introduction.

The (very) rough outline of the proof is as follows:

(1) Associate to each abelian variety a Faltings height h_F with the property that the set
$$\{h_F(B) : B/k \text{ is isogenous to } A/k\}$$
is finite (technically speaking, one has to require A to have "semistable reduction" over k for this to be true).

(2) Construct a projective variety V/k whose points correspond to "principally polarized" abelian varieties over k, and construct a modular height h_M on the points of V/k with respect to an embedding $v : V \hookrightarrow \mathbb{P}^n$. This height will have the property that
$$\{P \in V : h_M(P) < R\}$$
is finite for any given $R \in \mathbb{R}_{>0}$.

(3) Show that the two heights are related in the following sense:
$$h_F(A) = h_M(A, \lambda) + O(\log h_M(A, \lambda))$$
where (A, λ) is an abelian variety with a choice of "principal polarization" λ and the implied constant is dependent only on k.

If we ignore the "principal polarization" and "semistability" requirements, then we have a "proof." In the next few sections, we will describe the key tools used to make this outline into a valid proof.

4. Néron models

In the study of elliptic curves, it is crucial to understand whether or not a curve has good reduction at the maximal ideal of a local field. In order to understand this phenomenon in the case of an abelian variety, we will define the Néron model of a variety, which is (in some sense) a generalization of a minimal Weierstrass equation for an elliptic curve.

We now prepare to define Néron models. Let S be a Dedekind scheme, that is, a noetherian normal scheme of dimension ≤ 1 (e.g. the spectrum of a number field). Let K be the ring of rational functions of S. Suppose X_K is a K-scheme. Then an S**-model** of X_K is any S-scheme extending X_K, that is, the generic fiber of X_S is X_K (i.e. the fiber over the zero ideal of the map $X_S \to S$ is X_K). We make the following definition:

Definition 4.1. Let X_K be a smooth and separated K-scheme of finite type. A **Néron model** of X_K is an S-model X which is smooth, separated, of finite type, and which satisfies the following universal property, called the Néron mapping property:

For each smooth S-scheme Y and each K-morphism $u_K : Y_K \to X_K$ there is a unique S-morphism $Y \to X$ extending u_K.

In at least one setting of interest to us, Néron models always exist:

Theorem 4.2 (§1.3, [SBR90])**.** *Let A/K be an abelian variety over the field of fractions K of a discrete valuation ring R. Then A/K admits a Néron model over R.*

Now let k be the residue field of k. Recall that an *algebraic group* is a smooth group scheme over a field k. Theorem 4.2 tells us, in particular, that for K as in the theorem we have a means of associating to an abelian variety A/K an algebraic group A_0 over k, namely the special fiber of the Néron model, that is, the fiber over the prime ideal of K.

Using a theorem of Chevalley ([Che60], or see [Con] for a statement and proof in scheme-theoretic language), we obtain a filtration of A_0, namely

$$A_0 \supset (A_0)^0 \supset (A_0)^1 \supset 0$$

with $(A_0)^0$ the connected component of A_0 containing the identity element, $A_0/(A_0)^0$ a finite algebraic group, $(A_0)^0/(A_0)^1$ an abelian variety, and $(A_0)^1$ a commutative affine group scheme. Using this filtration, we define good reduction and semistable reduction. There are three possibilities to consider:

(1) The special fiber A_0 is itself an abelian variety. In this case we say that A has **good reduction**.
(2) The commutative affine group scheme $(A_0)^1$ is a torus (as a group scheme, not to be confused with the notion of a complex torus). That is, after a finite extension of k, $(A_0)^1$ becomes isomorphic to a product of copies of $\mathbb{A} - \{0\} = \mathbb{G}_m(k) = k^\times$.
(3) The commutative affine group scheme $(A_0)^1$ contains copies of $\mathbb{A} = \mathbb{G}_a(k) = k^+$.

Suppose as above that an abelian variety A has an associated Néron model with special fiber A_0. If A_0 satisfies (1) or (2), we say that A has semistable reduction. As in the elliptic curve case, by passing to a finite-dimensional field extension, we may assume that A has semistable reduction:

Theorem 4.3 (see [AW71] or [DM69]). *If A has good reduction, then the special fiber of the Néron model A_0 doesn't change under a finite field extension; if A has semistable reduction, then $(A_0)^0$ doesn't change under a finite field extension. Furthermore, A always acquires semistable reduction after a finite extension of the base field.*

Remark 4.4. The standard reference on Néron models is [SBR90]. See p. 246 of that book for a statement of a generalization of Theorem 4.3, but be forewarned that a proof is not given there.

5. The Faltings height of an abelian variety

Before we can define the Faltings height, we must first define the height of a normed module. Let K be a number field, and $\mathcal{O}_K$ the ring of integers of K. Let M be a projective $\mathcal{O}_K$ module of rank 1. We then have an isomorphism $M \otimes_{\mathcal{O}_K} K \approx K$, and a choice of such an isomorphism identifies M with a fractional ideal of K. Conversely, any fractional ideal is a projective $\mathcal{O}_K$ module of rank 1. Suppose that M is a fractional ideal of $\mathcal{O}_K$ (or, equivalently, a projective $\mathcal{O}_K$-module of rank 1, and we are given a norm $||\cdot||_v$ on $M \otimes_{\mathcal{O}_K} K_v$ for every infinite place $v\|\infty$. We define the *height* $H(M)$ of M by

$$H(M) := \frac{(M : \mathcal{O}_K m)}{\prod_{v\|\infty} ||m||_v^{\epsilon_v}}$$

for any nonzero $m \in M$, and

$$\epsilon_v := \begin{cases} 1 \text{ if } v \text{ is real} \\ 2 \text{ if } v \text{ is complex.} \end{cases}$$

Lemma 5.1. *This definition is independent of the choice of m.*

Proof. Recall that the normalized absolute value for a finite prime v corresponding to a prime ideal $\mathfrak{p}$ is defined by

$$|a|_v = (R : \mathfrak{p})^{-\mathrm{ord}_v(a)}$$

and for any infinite prime v

$$|a|_v = |a|^{\epsilon_v}$$

where $|\cdot|$ is the typical absolute value on $\mathbb{R} \subset \mathbb{C}$ or $\mathbb{C}$. The reason that these normalizations are typically taken is so that the product formula

$$\prod_v |a|_v = 1$$

is valid for $a \in K$. By the Chinese Remainder theorem, we have

$$M/\mathcal{O}_K m \approx \oplus_{v \text{ finite}} M_v/(\mathcal{O}_K)_v m$$

where $(\mathcal{O}_K)_v$ is the completion of $\mathcal{O}_K$ at v and $M_v = (\mathcal{O}_K)_v \otimes_{\mathcal{O}_K} M$ (notice that the direct sum has only finitely many nonzero terms). Now M_v is a projective module of rank 1 over $(\mathcal{O}_K)_v$ and hence is free of rank 1 because $(\mathcal{O}_K)_v$ is a principal ideal domain; say $M_v = (\mathcal{O}_K)_v m_v$. Thus

$$(M_v : (\mathcal{O}_K)_v m) = ((\mathcal{O}_K)_v m_v : (\mathcal{O}_K)_v m) = \left|\frac{m_v}{m}\right|_v.$$

Hence

$$H(M) = \frac{1}{\prod_{v \text{ finite}} \left|\frac{m_v}{m}\right|_v \cdot \prod_{v|\infty} ||m||_v^{\epsilon_v}}.$$

This clearly is independent of the choice of m by the product formula. □

We now define

$$h(M) := \frac{1}{[K:\mathbb{Q}]} \log H(M).$$

for any projective $\mathcal{O}_K$-module M of rank 1. This definition has the virtue that for any finite field extension L of K,

$$h(\mathcal{O}_L \otimes_{\mathcal{O}_K} M) = h(M).$$

We now give one of the two equivalent definitions of the height of an abelian variety over K given by Milne in [Mil, §26]. Choose a holomorphic g-form ω on the abelian variety A/K; it is well-defined up to multiplication by an element of $K^\times$. Note that for a finite prime v, we have a Néron model A_{K_v} of A/K, and a corresponding differential g-form ω_v (well-defined up to multiplication by a unit in $(\mathcal{O}_K)_v$). We define

$$H(A) := \frac{1}{\prod_{v\not|\infty} \left|\frac{\omega}{\omega_v}\right| \cdot \left((\frac{i}{2})^g \int_{A(\overline{K_v})} \omega \wedge \overline{\omega}\right)^{\epsilon_v/2}}.$$

and

$$h(A) := \frac{1}{[K:\mathbb{Q}]} \log H(A).$$

Provided that A is semistable, $h(A)$ will be invariant under field extension. We define the stable Faltings height of A

$$h_F(A) := h(A/L)$$

where L is a finite extension of K such that A_L has stable reduction at all primes of L.

This height is the first time we have touched on something that could be called Arakelov theory. The point is that one wants to consider metrics/norms that depended on all places, infinite or finite, of the field our variety is defined over simultaneously.

6. Moduli problems and Siegel modular varieties

The author is not planning on finishing this section. However, because it might be helpful before embarking on further reading, we make a few comments on both of topics in the section's title. First, we attempt to explain/motivate what people are talking about when they ask the question of whether or not a contravariant functor

$$\Phi : \mathbf{Sch}/S \longrightarrow \mathbf{Sets}$$

from schemes over a base scheme S to sets is representable. Such a functor is said to be **representable** if there is a scheme $T \to S$ and a natural isomorphism of functors

$$\mathrm{Mor}_S(R,T) \cong \Phi(R).$$

where $\mathrm{Mor}_S(R,T)$ is the set of S-morphisms from R to T. But what does this all mean? Really, what we want the representing scheme T to be is a machine that takes in a ring R and spits out the R-points of some object, say, an abelian variety. It turns out that the notion of a representing scheme and a "functor of points" (as $\mathrm{Mor}_S(R,T)$ is often called) is a useful scheme-theoretic formulation of the intuitive notion of "the set of R-points of a variety." To understand this, it might be helpful to consider the following simple example, taken from [J.H94, §IV.2.1.1]:

Example 6.1. Let K be a field, let $S = \mathrm{Spec}(K)$, and let X/K be an affine scheme, say given by equations

$$f_1 = f_2 = \cdots = f_r = 0$$

with $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. Then

$$\begin{aligned} \mathrm{Mor}_S(S,X) &= \{S\text{-morphisms } \mathrm{Spec}(K) \to X\} \\ &\cong \{K\text{-algebra homomorphisms } \frac{K[x_1,\ldots,x_n]}{(f_1,\ldots,f_r)} \to K\} \\ &\cong \{P \in K^n : f_1(P) = \cdots = f_r(P) = 0\}. \end{aligned}$$

The other comment we make is on Siegel modular varieties. Let

$$\mathcal{H}_d := \{M = (m_{ij}) \in M_{d\times d}(\mathbb{C}) : M = M^t \text{ and } (\mathrm{Im}(m_{ij})) \text{ is positive definite}\}$$

be the Siegel upper half space, and let

$$\mathrm{Sp}_{2d}(\mathbb{Z}) := \{M \in GL_2d(\mathbb{Z}) : MJM^t = J\}$$

(here $\mathrm{Im}(a+bi) = b$ for $a, b \in \mathbb{R}$, and $J := \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$).

The group $\mathrm{Sp}_{2d}(\mathbb{Z})$ acts on $\mathcal{H}_d$ by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \tau := (A\tau + B)(C\tau + D)^{-1}$$

for all $\tau \in \mathcal{H}_d$. It turns out that isomorphism classes of "principally polarized" abelian varieties over $\mathbb{C}$ are "parametrized" by

$$\mathrm{Sp}_{2d}(\mathbb{Z})\backslash\mathcal{H}_d.$$

See [Ros86] for references. This is a generalization of the familiar fact that isomorphism classes of elliptic curves over $\mathbb{C}$ are parametrized by

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$$

where $\mathcal{H}$ is the typical Poincaré complex upper half plane. This "parametrization" can be made more precise through the language of moduli problems. This language has the advantage that it allows one to discuss varieties that classify principally polarized abelian varieties over general fields.

We close with a final observation/question. Given that the space of abelian varieties has a moduli interpretation, one would expect the interpretation of modular forms as sections of a sheaf on the moduli space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ to generalize to the interpretation of Siegel modular forms as sections of sheaves on the higher-dimensional varieties $\mathrm{Sp}_{2d}(\mathbb{Z})\backslash\mathcal{H}_d$. Using the appropriate algebraic models of these varieties (which are known to exist, see [Mil, p. 103]), is it possible to construct a p-adic theory of Siegel modular forms similar to that of the Serre-Katz theory of p-adic elliptic modular forms? Perhaps this has already been done, but I doubt that all of the details have been worked out given that we still have incomplete knowledge of the theory of p-adic Hilbert modular forms (see [Gor02]).

References

[AW71] M. Artin and G. Winters. Degenerate fibres and stable reduction of curves. *Topology*, 10:373–383, 1971.

[Che60] C. Chevalley. Une démonstration d'un théorèm sur les groupes algébraiques. *J. Math. Pures Appl.*, 39:307–317, 1960.

[Con] B. Conrad. A modern proof of chevalley's theorem on algebraic groups. *unpublished, see http://www.math.lsa.umich.edu/ bdconrad/.*

[DM69] P. Deligne and D. Mumford. The irreducibility of the spaces of curves of given genus. *Publ. Math. IHES*, 36:75–110, 1969.

[Fal86a] G. Faltings. Finiteness theorems for abelian varieties over number fields. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 9–27. Springer-Verlag, 1986.

[Fal86b] G. Faltings. Some historical notes. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 1–8. Springer-Verlag, 1986.

[Gor02] E.Z. Goren. *Lectures on Hilbert Modular Varieties and Modular Forms*. Number 14 in CRM Monograph Series. AMS, 2002.

[J.H94] J.H.Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151. Springer-Verlag, 1994.

[Mil] J. Milne. *Abelian Varieties*. http://www.jmilne.org/math/.

[Ros86] M. Rosen. Abelian varieties over $\mathbb{C}$. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 79–101. Springer-Verlag, 1986.

[SBR90] W. Lütkebohmert S. Bosch and M. Raynaud. *Néron Models*. Number 3. Folge Band 21 in Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1990.

[Ser88] J-P. Serre. *Algebraic Groups and Class Fields*. Number 117. Springer-Verlag, 1988.

E-mail address: getz@math.wisc.edu