ABELIAN VARIETIES

NIR ELBER

Contents

1. Introduction

The goal of this paper is to introduce some theory around abelian varieties for the purpose of stating Tate's conjecture and explain some applications. As such, abelian varieties and their Tate modules will be the main characters of our story.

Definition 1.1 (Abelian variety)**.** *Fix a field k. An abelian k-variety is a smooth, geometrically integral, projective group k-variety.*

Recall that a k-variety is a reduced, separated k-scheme of finite type, and a group k-variety is a k-variety which is a group object in the category of schemes.

Remark 1.2. *In practice, one can get away with only assuming that an abelian variety is proper and geometrically integral, and being smooth and projective follow. For example, see [SP, Section 0BF9].*

We could define Tate modules now, but we will wait until section 3 when we will be able to understand what we're looking at. For now, we say that each abelian variety A over k has attached to it an ℓ-adic Tate module $T_\ell A$ (which is a $\mathbb{Z}_\ell$-module), for each prime ℓ not divisible by the characteristic of k. Roughly speaking, the Tate module $T_\ell A$ is some algebraic gadget built from ℓ-power torsion of A.

It turns out that the T_ℓ construction is functorial. This allows us to state Tate's conjecture.

Conjecture 1.3 (Tate)**.** *Fix abelian varieties A and B over a field k. Then the map $\varphi \mapsto T_\ell\varphi$ induces an isomorphism*

$$\operatorname{Hom}_k(A,B)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \to \operatorname{Hom}_k(T_\ell A, T_\ell B).$$

Here, $\operatorname{Hom}_k(A,B)$ denotes the homomorphisms $A \to B$, and $\operatorname{Hom}_k(T_\ell A, T_\ell B)$ denotes the homomorphisms fixed by some Galois action to be defined later.

Anyway, Conjecture 1.3 is truly amazing: approximately speaking, we are able to intelligently discuss the geometry of abelian varieties (in the form of their homomorphisms) via the algebraic gadget of the Tate module. We will be able to see this in action later in Theorem 3.7.

Sadly, not much is known.

Theorem 1.4. *Conjecture 1.3 is known when k is a finite field [Tat66] and when k is a number field [Fal86].*

Date: 9 December 2022.

Both cases of Theorem 1.4 are beyond the scope of this paper. Instead, the main goal of the paper will be to show the following (much easier) result.

Theorem 1.5. *Fix abelian varieties A and B over a field k. Then the map $\varphi \mapsto T_\ell\varphi$ induces an injection*

$$\operatorname{Hom}_k(A,B)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \to \operatorname{Hom}_k(T_\ell A, T_\ell B).$$

1.1. **Layout.** The layout of this paper is as follows. In section 2, we establish some background on abelian varieties for the sake of being able to compute their torsion. The main result is that the n-torsion of an abelian variety A over a field k is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2\dim A}$ when and n is not divisible by $\operatorname{char} k$. Then in section 3 we will use the theory we have built to prove Theorem 1.5. As a bonus, we give an extra application of Theorem 1.4 in subsection 3.2.

1.2. **Notation.** Throughout, we work in Sch_k, where k is some field. We denote k-varieties by X, Y, Z and abelian k-varieties by A, B, C. We will allow $\operatorname{char} k \neq 0$ and to not be algebraically closed. All morphisms are k-morphisms. When needed, we denote the group law on A by $\mu_A\colon A\times A\to A$ or $+\colon A\times A\to A$, the identity by $0_A\colon \operatorname{Spec} k \to A$, and the inversion map by $\iota_A\colon A\to A$ or $[-1]\colon A\to A$.

2. Torsion of Abelian Varieties

The main goal of the present section is to show $A[n](k^{\mathrm{sep}}) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$ for $\operatorname{char} k \nmid n$. Along the way, we will discuss isogenies, which we will need to prove Theorem 1.5. Before going any further, we introduce the examples which will follow us throughout the paper.

Example 2.1. *Let k be a field with $\operatorname{char} k \neq 3$. Then $E := \operatorname{Proj} k[X,Y,Z]/\left(Y^2Z - X^3 - Z^3\right)$ is an elliptic curve. Indeed, the discriminant of the corresponding planar curve $y^2 = x^3+1$ is 3^3, which is not 0 because $\operatorname{char} k \neq 3$. Explicitly, the discriminant computation shows E is k-smooth, we see E is irreducible over any finite extension k'/k so that E is geometrically integral, and E embeds into $\mathbb{P}^2_k$ and is thus projective.*

Example 2.2. *Let Λ be a lattice of full rank in $\mathbb{C}^g$ for some $g\in\mathbb{Z}^+$. Then one can check that $\mathbb{C}/\Lambda$ defines abelian variety over $\mathbb{C}$.*

2.1. **Basic Properties.** We will permit arbitrary k-morphisms $\varphi\colon A\to B$ to be morphisms of abelian varieties over a field k, but we will shortly show that they must admit quite a bit of structure.

Remark 2.3. *For example, let $\varphi\colon A\to B$ be a morphism of abelian varieties over a field k. Because the structure morphism $\alpha\colon A\to\operatorname{Spec} k$ is proper, and similarly $\beta\colon B\to\operatorname{Spec} k$ is separated, it is a consequence of the Cancellation Theorem [Vak17, Theorem 11.2.1] that φ is proper. Namely, the diagonal morphism $\Delta\beta\colon B\times B\to\operatorname{Spec} k$ is a closed embedding and thus proper.*

Even though we permit all morphisms, some morphisms are still better than others.

Definition 2.4 (Homomorphism). *Fix a morphism $\varphi\colon A\to B$ of abelian varieties over a field k. Then φ is a homomorphism if and only if $\varphi\circ\mu_A = \mu_B\circ(\varphi,\varphi)$. Equivalently, for any k-scheme T, we require*

$$\varphi(t_1)+\varphi(t_2)=\varphi(t_1+t_2)$$

for all $t_1,t_2\in A(T)$. If $A=B$, then we call φ an endomorphism. The group of homomorphisms (with pointwise operation) is denoted $\operatorname{Hom}_k(A,B)$, and the ring of endomorphisms (with multiplication given by composition) is denoted $\operatorname{End}_k(A)$.

Definition 2.5 (Translation). *Fix an abelian variety A over a field k. Given $a\in A$, the morphism $\tau_a := \mu_A(\cdot,a)$ is the translation by a.*

We will shortly show that homomorphisms and translations can build all scheme morphisms. For this, we need the following result.

Theorem 2.6 (Rigidity). *Let X, Y, Z be proper irreducible varieties over a field k, and let $p\in X(k)$ and $q\in Y(k)$ be rational points. If a morphism $\varphi\colon X\times Y\to Z$ is constant on $X\times\{q\}$ and $\{p\}\times Y$, then φ is constant.*

Proof. We refer to [Vak17, Rigidity Lemma 11.5.12]. Note we have stated this result for varieties so as not to give the impression that this is a theorem about group schemes. ■

Corollary 2.7. *Let $\varphi\colon A\to B$ be a morphism of abelian k-varieties. Then φ is the composition of a homomorphism and a translation.*

Proof. We apply Theorem 2.6. Set $b \coloneqq \varphi(0_A) \in B(k)$. Letting $\tau \coloneqq \mu_B(\cdot, b)$ denote translation by b, it suffices to show $\psi \coloneqq \tau^{-1}\varphi$ is a homomorphism, where now $\psi(0_A) = 0_B$. (Here, $\tau^{-1} = \mu_B(\cdot, \iota_B(b))$.) For this, we need to show

$$\mu_B \circ (\psi, \psi) = \psi \circ \mu_A.$$

Equivalently, we need to show $\mu_B\big(\mu_B \circ (\psi, \psi), \iota_B \circ \psi \circ \mu_A\big)$ is constant, which we can check on $A \times \{0_A\}$ and $\{0_A\} \times A$. ■

Corollary 2.8. *Fix an abelian variety A over a field k. Then the group law on A is commutative.*

Proof. By Corollary 2.7, the inversion morphism $\iota_A \colon A \to A$ can be written as $\tau \circ \varphi$, where τ is a translation and φ a homomorphism. However, $\iota_A(0_A) = 0_A$, so $\tau(0_A) = 0_A$, so $\tau = \mathrm{id}_A$. Thus, ι_A is a homomorphism, so it follows A is commutative. (Formally, one could diagram chase with arrows by noting $A(T)$ is commutative for any test k-scheme T.) ■

Example 2.9. *The group law of the elliptic curve in Example 2.1 comes from* $\operatorname{Pic}^0(E)$ *and is therefore commutative. The group law of Example 2.2 is of course commutative.*

To define the Tate module, we will need a firm understanding of torsion, so we pick up the corresponding morphism.

Notation 2.10. *Given an abelian variety A over a field k and an integer $n \in \mathbb{Z}$, we define the morphism $[n] \colon A \to A$ by*

$$[n] \colon a \mapsto \underbrace{a + \cdots + a}_{n}.$$

Now that we know the group law is abelian (Corollary 2.8), we know $[n] \colon A \to A$ is a homomorphism.

2.2. **The Theorem of the Cube.** The following result will be useful.

Theorem 2.11 (Cube)**.** *Let X, Y, Z be proper irreducible varieties over a field k, and let $p \in X(k)$ and $q \in Y(k)$ and $r \in Z(k)$ be rational points. Then a line bundle $\mathcal{L}$ on $X \times Y \times Z$ is trivial if its restrictions to $\{p\} \times Y \times Z$ and $X \times \{q\} \times Z$ and $X \times Y \times \{r\}$ are all trivial.*

Proof. Proving this would take us a little too far afield, so we refer to [SP, Theorem 0BF4]. As with Theorem 2.6, we have stated this result for varieties so as not to give the impression that this is a result about group schemes. ■

We will be interested in using Theorem 2.11 to compute pullbacks of line bundles. The following two corollaries tell us how to use our theorem.

Corollary 2.12. *Fix an abelian variety A over a field k. Given integers $c_1, \ldots, c_n$, define the homomorphism $\mu_{c_1 \ldots c_n} \colon A^n \to A$ by*

$$\mu_{c_1 \ldots c_n}(a_1, \ldots, a_n) \coloneqq \sum_{i=1}^{n} c_i a_i.$$

Then, for any line bundle $\mathcal{L}$ on A, we have the isomorphism

$$\mu_{111}^*\mathcal{L} \otimes \mu_{100}^*\mathcal{L} \otimes \mu_{010}^*\mathcal{L} \otimes \mu_{001}^*\mathcal{L} \cong \mu_{110}^*\mathcal{L} \otimes \mu_{101}^*\mathcal{L} \otimes \mu_{011}^*\mathcal{L}$$

of line bundles on A^3.

Proof. We apply Theorem 2.11 to the difference

$$\mathcal{M} \coloneqq \mu_{111}^*\mathcal{L} \otimes \mu_{100}^*\mathcal{L} \otimes \mu_{010}^*\mathcal{L} \otimes \mu_{001}^*\mathcal{L} \otimes \left(\mu_{110}^*\mathcal{L}\right)^{\otimes -1} \otimes \left(\mu_{101}^*\mathcal{L}\right)^{\otimes -1} \otimes \left(\mu_{011}^*\mathcal{L}\right)^{\otimes -1}.$$

By symmetry, to apply Theorem 2.11, it suffices to show that $\mathcal{M}$ is trivial when restricted to $A \times A \times \{0_A\}$. Well, under the isomorphism $A \times A \times \{0_A\} \cong A \times A$, the restricted morphism $\mu_{c_1c_2c_3} \colon A \times A \times \{0_A\} \to A$ becomes $\mu_{c_1c_2} \colon A \times A \to A$, so $\mathcal{M}$ restricted to $A \times A \times \{0_A\}$ looks like

$$\mu_{11}^*\mathcal{L} \otimes \mu_{10}^*\mathcal{L} \otimes \mu_{01}^*\mathcal{L} \otimes \mu_{00}^*\mathcal{L} \otimes \left(\mu_{11}^*\mathcal{L}\right)^{\otimes -1} \otimes \left(\mu_{10}^*\mathcal{L}\right)^{\otimes -1} \otimes \left(\mu_{01}^*\mathcal{L}\right)^{\otimes -1}.$$

After cancellation, this is $\mu_{00}^*\mathcal{L}$, but μ_{00} is the composite morphism $A \to \{0_A\} \to A$ and therefore must be trivial. Explicitly, the only line bundle over $\{0_A\}$ is trivial, so its pullback to A will remain trivial. So indeed, $\mathcal{M}$ is trivial. ■

Corollary 2.13. *Fix an abelian variety A over a field k. For any k-scheme T and k-morphisms $\alpha,\beta,\gamma\colon T\to A$, we have*

$$(\alpha+\beta+\gamma)^*\mathcal{L}\otimes\alpha^*\mathcal{L}\otimes\beta^*\mathcal{L}\otimes\gamma^*\mathcal{L}\cong(\alpha+\beta)^*\mathcal{L}\otimes(\alpha+\gamma)^*\mathcal{L}\otimes(\beta+\gamma)^*\mathcal{L}.$$

Proof. This follows from pulling back the identity of Corollary 2.12 along the morphism $(\alpha,\beta,\gamma)\colon T\to A^3$. Indeed, for $c_1,c_2,c_3\in\mathbb{Z}$, we see $\mu_{c_1c_2c_3}\circ(\alpha,\beta,\gamma)=c_1\alpha+c_2\beta+c_3\gamma$. ■

We will always use Theorem 2.11 in its form as Corollary 2.13. For example, we have the following.

Corollary 2.14. *Fix an abelian variety A over a field k. For any integer $n\in\mathbb{Z}$ and line bundle $\mathcal{L}$ on A, we have*

$$[n]^*\mathcal{L}\cong\mathcal{L}^{\otimes n(n+1)/2}\otimes\left([-1]^*\mathcal{L}\right)^{\otimes n(n-1)/2}. \tag{2.1}$$

Proof. The point is to induct on n, using Corollary 2.13 for the induction; the precise statement will follow after some arithmetic.

To begin, we work out small cases. For $n=0$, we note $[0]\colon A\to A$ is the map $A\to\{0_A\}\to A$, so the pullback of $\mathcal{L}$ along $[0]$ trivializes at $\{0_A\}$ and is thus trivial. For $n=1$, there is again nothing to say.

We now induct. We show how to induct for $n\geq 0$, and a similar argument deals with $n\leq 0$. Suppose (2.1) holds for n and $n+1$ for some $n\geq -1$, so we show $n+2$. For this, we apply Corollary 2.13 to the morphisms $[1],[1],[n]\colon A\to A$ to get

$$[n+2]^*\mathcal{L}\otimes\mathcal{L}\otimes\mathcal{L}\otimes[n]^*\mathcal{L}\cong[2]^*\mathcal{L}\otimes[n+1]^*\mathcal{L}\otimes[n+1]^*\mathcal{L}.$$

Plugging in $n=-1$ and using the small cases shows $[2]^*\mathcal{L}\cong\mathcal{L}^{\otimes 3}\otimes[-1]\mathcal{L}$, as needed. Thus, we may rearrange the above relation to

$$\begin{aligned}[n+2]^*\mathcal{L}&\cong\mathcal{L}\otimes[-1]^*\mathcal{L}\otimes\left([n+1]^*\mathcal{L}\right)^{\otimes 2}\otimes\left([n]^*\mathcal{L}\right)^{\otimes -1}\\&\cong\mathcal{L}\otimes[-1]^*\mathcal{L}\otimes\mathcal{L}^{\otimes(n+1)(n+2)}\otimes\left([-1]^*\mathcal{L}\right)^{\otimes(n+1)n}\otimes\mathcal{L}^{\otimes -n(n+1)/2}\otimes\left([-1]^*\mathcal{L}\right)^{\otimes -n(n-1)/2}\\&\cong\mathcal{L}^{\otimes(n+2)(n+3)/2}\otimes\left([-1]^*\mathcal{L}\right)^{\otimes(n+2)(n+1)/2},\end{aligned}$$

which is what we wanted. ■

While we're here, we note that Corollary 2.13 produces a positive-definite bilinear form on $\operatorname{End}_k(A)$. This bilinear form will be a key ingredient in the proof of Theorem 1.5.

Proposition 2.15. *Fix an abelian variety A over a field k. Then there is a positive-definite symmetric $\mathbb{Z}$-bilinear form $\operatorname{End}_k(A)^2\to\mathbb{Z}$.*

Proof. This is surprisingly difficult and uses some theory of Chow groups, which we will not introduce. As such, we will be sketchy and refer to [EGM, Lemma 12.9] for details.[1] Fix a very ample line bundle $\mathcal{L}$ on A, which exists because A is projective. By replacing $\mathcal{L}$ with $\mathcal{L}\otimes[-1]^*\mathcal{L}$, we may assume $[-1]^*\mathcal{L}=\mathcal{L}$.

We begin by defining $\langle\cdot,\cdot\rangle_0\colon\operatorname{End}_k(A)^2\to\operatorname{Pic}A$ by

$$\langle\alpha,\beta\rangle_0\coloneqq(\alpha+\beta)^*\mathcal{L}\otimes\left(\alpha^*\mathcal{L}\right)^{\otimes -1}\otimes\left(\beta^*\mathcal{L}\right)^{\otimes -1}.$$

Note that $\langle\cdot,\cdot\rangle_0$ is symmetric by definition. To check bilinearity, we compute

$$\begin{aligned}\langle\alpha,\beta+\gamma\rangle_0&=(\alpha+\beta+\gamma)^*\mathcal{L}\otimes\left(\alpha^*\mathcal{L}\right)^{\otimes -1}\otimes\left((\beta+\gamma)^*\mathcal{L}\right)^{\otimes -1}\\&\overset{*}{=}(\alpha+\beta)^*\mathcal{L}\otimes(\alpha+\gamma)^*\mathcal{L}\otimes\left(\alpha^*\mathcal{L}\right)^{\otimes -2}\otimes\left(\beta^*\mathcal{L}\right)^{\otimes -1}\otimes\left(\gamma^*\mathcal{L}\right)^{\otimes -1}\\&=\langle\alpha,\beta\rangle_0\otimes\langle\alpha,\gamma\rangle_0,\end{aligned}$$

where we have used Corollary 2.13 at $\overset{*}{=}$.

To finish the definition of our bilinear form, we need some intersection theory. Map $\operatorname{Pic}A\to\mathbb{Z}$ by $\mathcal{M}\mapsto c_1(\mathcal{L})^{\dim A-1}\cap c_1(\mathcal{M})$, yielding

$$\langle f,g\rangle\coloneqq c_1(\mathcal{L})^{\dim A-1}\cap c_1(\langle f,g\rangle_0),$$

where $c_1\colon\operatorname{Pic}A\to\operatorname{CH}^1(A)$ denotes the first Chern class map, and $\cap$ denotes the cap product. The maps c_1 and $c_1(\mathcal{L})^{\dim A-1}\cap -$ are both linear, so $\langle\cdot,\cdot\rangle$ is automatically symmetric and bilinear.

[1] I also refer there in the likely event I make Chern-class-related mistakes in the following discussion.

Thus, the difficulty lies in showing that $\langle\cdot,\cdot\rangle$ is positive-definite. We will be quite sketchy. Suppose $\varphi\colon A\to A$ is nonzero so that we want to show $\langle\varphi,\varphi\rangle>0$. To begin, we use Corollary 2.14 to compute

$$\langle\varphi,\varphi\rangle=\varphi^*[2]^*\mathcal{L}\otimes\left(\varphi^*\mathcal{L}\right)^{\otimes-2}=\left(\varphi^*\mathcal{L}\right)^{\otimes 2},$$

so it suffices to show that $c_1\left(\varphi^*\mathcal{L}\right)$ is positive. On one hand, $B\coloneqq\operatorname{im}\varphi$ is a closed subvariety of A (because φ is proper), so we may think of φ as a dominant morphism $\varphi\colon A\to B$. On the other hand, $\mathcal{L}$ restricted to B remains very ample and therefore corresponds to an effective Weil divisor

$$D=\sum_{i=1}^N n_i[B_i].$$

Pulling back our divisor along $\varphi\colon A\to B$, we see $\varphi^*\mathcal{L}$ corresponds to the effective divisor

$$\varphi^*D=\sum_{i=1}^N n_i\left[\varphi^*B_i\right],$$

from which our positivity follows. ■

2.3. **Isogenies.** Isogenies provide a way of saying two abelian varieties are roughly the same (see Remark 2.21). Approximately speaking, they will be interesting to us because $[n]\colon A\to A$ is an isogeny. Now, for our definition, we need to define the kernel.

Definition 2.16 (Kernel)**.** *Fix a homomorphism $\varphi\colon A\to B$ of abelian varieties over a field k. The kernel $\ker\varphi$ is defined as the fiber of φ above 0_B. Note $\ker\varphi$ is an abelian subvariety of A. In the case of $[n]\colon A\to A$ for $n\in\mathbb{Z}$, we may write $A[n]\coloneqq\ker[n]$.*

Remark 2.17. *From the perspective of group theory, we expect all fibers of a homomorphism $\varphi\colon A\to B$ to look like $\ker\varphi$. This is the case. Explicitly, for any point $b\in B$, let $\tau\colon B\to B$ denote the isomorphism given by translation by $-b$. Then we see all squares in*

$$\begin{tikzcd}
(\ker\varphi)_{k(b)} \arrow[r, equal] \arrow[d, dashed, "\tau^{-1}\varphi"'] & (\ker\varphi)_{k(b)} \arrow[r] \arrow[d, "\varphi"] & \ker\varphi \arrow[r, hook] \arrow[d, "\varphi"] & B \arrow[d, "\varphi"] \\
\{b\} \arrow[r, "\tau"] & \{0_A\}_{k(b)} \arrow[r] & \{0_A\} \arrow[r, hook] & A
\end{tikzcd}$$

are pullback squares (here, the dashed arrow is induced), so it follows $\varphi^{-1}(\{b\})\cong(\ker\varphi)_{k(b)}$.

And here is our definition.

Definition 2.18 (Isogeny)**.** *Fix a field k. An isogeny is a homomorphism $\varphi\colon A\to B$ of abelian k-varieties that is dominant and has finite kernel.*

Note that being $\varphi\colon A\to B$ being dominant implies that $\varphi(A)$ is dense in B, but φ is proper by Remark 2.3, so $\varphi(A)\subseteq B$ is closed, so actually φ is surjective (on points).

Example 2.19. *We work in the context of Example 2.1. Set $E'\coloneqq\operatorname{Proj}k[X,Y,Z]/\left(Y^2Z-X^3+27Z^3\right)$, which has discriminant a power of 3 and is therefore also an elliptic curve over k. One can check that the map $\varphi\colon E\to E'$ given by*

$$\varphi([X:Y:Z])\coloneqq\begin{cases}\left[X^4+4XZ^3:X^3Y-8YZ^3:X^3Z\right] & X\neq 0,\\ [0:1:0] & X=0,\end{cases}$$

defines an isogeny where the kernel is $\{[0:1:0],[0:1:1],[0:-1:0]\}$. (This isogeny was found using Sage.)

Example 2.20. *We work in the context of Example 2.2, with $g=1$ for technical convenience. For any nonzero n, we see that $[n]\colon(\mathbb{C}/\Lambda)\to(\mathbb{C}/\Lambda)$ is an isogeny: on closed points, we see that the kernel is $\frac{1}{n}\Lambda/\Lambda$, which has n^2 elements. Additionally, $[n]$ sends the generic point to the generic point, so $[n]$ is dominant. It follows that $[n]$ is an isogeny. We will generalize this example in Proposition 2.24.*

Remark 2.21. *Intuitively, an isogeny is a "squishy isomorphism," as seen in Example 2.20. For example, one can show that an isogeny $\varphi\colon A\to B$ has an "inverse" isogeny $\psi\colon B\to A$ such that $\varphi\circ\psi=[n]$ and $\psi\circ\varphi=[n]$ for some positive integer n. (We will not show this here.) In particular, two abelian varieties being isogenous forms an equivalence relation.*

As with any good condition, there are many ways to say that a homomorphism is an isogeny.

Proposition 2.22. *Fix a homomorphism $\varphi\colon A \to B$ of abelian varieties over a field k. The following are equivalent.*

(a) φ is an isogeny. In other words, φ is dominant and has finite kernel.
(b) φ is dominant, and $\dim A = \dim B$.
(c) φ has finite kernel, and $\dim A = \dim B$.

Proof. We follow [Mil08, Proposition I.7.1]. The main point is that a spreading out argument shows that

$$\dim \varphi^{-1}(\{b\}) \geq \dim A - \dim \operatorname{im} \varphi, \tag{2.2}$$

for each $b \in B$, where equality holds on some nonempty open subscheme of B. (Here, $\operatorname{im} \varphi$ is topologically a closed subset of B because φ is proper, so we have given $\operatorname{im} \varphi$ the reduced closed scheme structure to make it a k-subvariety of B.) Proving this is somewhat technical, so we refer to [Mil08, Theorem 10.9].

However, once equality in (2.2) holds for a single $b \in B$, we note that Remark 2.17 says all fibers are isomorphic up to base-change by a field (which does not adjust dimension!), so we conclude

$$\dim \ker \varphi = \dim A - \dim \operatorname{im} \varphi.$$

Now, φ having finite kernel is equivalent to $\dim \ker \varphi = 0$, and φ being dominant is equivalent to $\operatorname{im} \varphi = B$, so the equivalence of (a), (b), and (c) follows. ■

Remark 2.23. *[Mil08, Proposition I.7.1] also shows that being an isogeny is equivalent to being finite, flat, and surjective, but we will not need this. However, we do need to know that isogenies are finite. By Zariski's Main Theorem (for example, see [Vak17, Theorem 30.6.2]), it suffices to show φ is quasifinite and proper. Well, φ is proper by Remark 2.3, and φ is quasifinite because it has finite kernel, and all fibers are isomorphic up to extension of scalars by Remark 2.17.*

And here is why we defined isogenies.

Proposition 2.24. *Fix an abelian variety A over a field k. Then the map $[n]\colon A \to A$ is an isogeny for all nonzero integers $n \in \mathbb{Z}$.*

Proof. The idea is to use Corollary 2.14. To show that $[n]\colon A \to A$ is an isogeny, it suffices by Proposition 2.22 to show that $A[n]$ has dimension 0. Because A is projective, there is a very ample line bundle $\mathcal{L}$ on A. By replacing $\mathcal{L}$ with $\mathcal{L} \otimes [-1]^*\mathcal{L}$, we may assume that $\mathcal{L} \cong [-1]^*\mathcal{L}$. Thus, Corollary 2.14 implies

$$[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n^2}.$$

Now, $[n]$ restricts to the zero map $A[n] \to \{0_A\} \to A[n]$ on $A[n]$, so $\mathcal{L}^{\otimes n^2}$ is trivial when restricted to $A[n]$. However, we see that $\mathcal{L}^{\otimes n^2}$ is very ample (recall $n \neq 0$) and will remain very ample when restricted to $A[n]$. Thus, $\dim A[n] = 0$,[2] so $[n]$ is an isogeny. ■

Here are a few quick corollaries.

Corollary 2.25. *Fix an abelian variety A over a field k. The group $A\left(\overline{k}\right)$ is divisible.*

Proof. All closed points on A are in $A\left(\overline{k}\right)$ because A is a k-variety. Thus, for nonzero n, we see $[n]\colon A \to A$ is an isogeny by Proposition 2.24, so $[n]$ is surjective on points and in particular on closed points, so $[n]\colon A\left(\overline{k}\right) \to A\left(\overline{k}\right)$ is surjective. ■

Example 2.26. *We work in the context of Example 2.1, where $k = \mathbb{F}_5$. Let $\varphi\colon E \to E$ denote the Frobenius automorphism given by $[X : Y : Z] \mapsto [X^p : Y^p : Z^p]$. One can compute (for example, using Sage) that $[5] = \varphi^{\circ 2}$; see also [Sil09, Exercise 5.16]. Thus, it follows that $[5]$ is surjective.*

Corollary 2.27. *Fix abelian varieties A and B over a field k. Then the group $\operatorname{Hom}_k(A, B)$ of homomorphisms $A \to B$ is torsion-free.*

[2] Making this explicit is somewhat annoying. Roughly speaking, if $\dim A[n] > 0$, one can replace $A[n]$ with a proper subcurve X, and then it is a consequence of the Riemann–Roch theorem (see [Har77, Corollary 3.3]) that the trivial line bundle is not ample.

Proof. Suppose $\varphi\colon A \to B$ has $\varphi \circ [n] = 0$ for some $n \in \mathbb{Z}^+$. However, $[n]$ is surjective on points by Proposition 2.24, so it follows that φ sends all points to 0_B. This forces φ to be the zero morphism. (One can see this conclusion directly on sheaves or base-change to the algebraic closure where a morphism of varieties is determined by the topological information.) ■

2.4. **Degrees of Isogenies.** We might be interested in the size of the kernel of an isogeny to know how much "squishing" it is doing, so we have the following definition.

Definition 2.28 (Degree)**.** *Fix an isogeny $\varphi\colon A \to B$ of abelian varieties over a field k. Then the degree of φ, denoted* $\deg\varphi$*, is defined as the degree of the field extension $\varphi^\sharp\colon K(B) \to K(A)$. This field extension is finite because isogenies are finite.*

By composing field extensions, we see that the degree is multiplicative. As mentioned above, the degree is (roughly speaking) the size of the kernel. Here is the precise statement.

Lemma 2.29. *Let $\varphi\colon X \to Y$ be a finite, dominant morphism of irreducible k-varieties such that the induced field extension $\varphi^\sharp\colon K(Y) \to K(X)$ is separable. Then there is a nonempty open subscheme $U \subseteq Y$ such that each $y \in Y$ has*

$$\#\varphi^{-1}(\{y\}) = [K(X) : K(Y)].$$

Proof. This is a spreading out argument—roughly speaking, we expect the Primitive element theorem to tell us that the fiber at the generic point has size $[K(X) : K(Y)]$.

The details are not terribly annoying, so we will include them. At any point, we may replace Y with a nonempty open subscheme $U \subseteq Y$ and X with $f^{-1}U$. For example, choosing an affine open subscheme of Y, we may assume that both X and Y are affine because φ is finite. Thus, φ is induced by a ring map $f\colon R \to S$, where $Y = \operatorname{Spec} R$ and $X = \operatorname{Spec} S$, and we may localize R as much as we please.

Note f is injective because φ is dominant, and S is a finite extension over R because f is finite. Further, set $K \coloneqq \operatorname{Frac} R$ and $L \coloneqq \operatorname{Frac} S$ so that L/K is a finite separable extension of fields. By the Primitive element theorem, we may find $\beta \in L$ such that $L = K[\beta]$. Now, by localizing R, we claim we may assume that β is integral over R and that

$$S = R[\beta].$$

We will be brief with this claim. By collecting denominators in the monic minimal polynomial for β in $L[x]$, we may assume that β is integral over R. Continuing, writing $S = R[s_1, \ldots, s_n]$ for some $s_1, \ldots, s_n \in S$, we note that each $s_i \in L$ can be written as a polynomial in β with coefficients in K. Collecting all these denominators and localizing R appropriately, we may assume that $s_i \in R[\beta]$ for each i and thus $S \subseteq R[\beta]$. Going in the other direction now, we see

$$K[\beta] = L = K[s_1, \ldots, s_n],$$

so we can write β as some polynomial in the s_i with coefficients in K. Again collecting these denominators and localizing R appropriately, we can force $\beta \in R[s_1, \ldots, s_n] = S$, so $R[\beta] \subseteq S$. It follows $R[\beta] = S$.

We are now ready to complete the proof. Let $\pi \in R[x]$ be a monic minimal polynomial for β so that $S \cong R[x]/(\pi)$. Because L/K is separable, π has nonzero discriminant $\operatorname{disc}\pi \in R$, so we localize at $\operatorname{disc}\pi$ to assume $\operatorname{disc}\pi \in R^\times$. To finish, we note that the fiber over some $\mathfrak{p} \in \operatorname{Spec} R$ is given by

$$\varphi^{-1}(\{\mathfrak{p}\}) = \operatorname{Spec}\left(S \otimes_R (R/\mathfrak{p})\right) \cong \operatorname{Spec} \frac{(R/\mathfrak{p})[x]}{(\pi)}.$$

However, $\operatorname{disc}\pi$ is a unit in $R/\mathfrak{p}$, so there are $\deg\pi = [L : K]$ distinct roots of π in $\overline{R/\mathfrak{p}}$, so there are $[L : K]$ distinct closed points in $\varphi^{-1}(\{\mathfrak{p}\})$. Note we only have to worry about closed points because $\varphi\colon \varphi^{-1}(\{\mathfrak{p}\}) \to \{\mathfrak{p}\}$ being finite implies that the fiber $\varphi^{-1}(\{\mathfrak{p}\})$ is zero-dimensional, so we are done. ■

Corollary 2.30. *Fix an isogeny $\varphi\colon A \to B$ of abelian varieties over a field k such that the field extension $\varphi^\sharp\colon K(B) \to K(A)$ is separable. Then $\#(\ker\varphi) = \deg\varphi$.*

Proof. By Lemma 2.29, there exists some $b \in B$ such that $\#\varphi^{-1}(\{b\}) = \deg\varphi$. However, Remark 2.17 tells us that $\varphi^{-1}(\{b\})$ is isomorphic to $\ker\varphi$ up to base-change by a field (which does not change the number of closed points), so the result follows. ■

Now, here is the degree computation for $[n]$.

Proposition 2.31. *Fix an abelian variety A over a field k. If n is a nonzero integer, then* $\deg[n] = n^{2\dim A}$.

Proof. For this, one uses intersection theory, which we will not introduce here. In brief, we use the very ample line bundle $\mathcal{L}$ with $\mathcal{L} \cong [-1]^*\mathcal{L}$ as defined in the proof of Proposition 2.24, and we write $\mathcal{L} = \mathcal{L}(D)$ for some divisor D. Then we can use the intersection product of divisors to compute

$$\deg[n] \cdot \underbrace{(D, \ldots, D)}_{\dim A} = \underbrace{([n]^*D, \ldots, [n]^*D)}_{\dim A} = \underbrace{\left(n^2D, \ldots, n^2D\right)}_{\dim A} = n^{2\dim A} \cdot \underbrace{(D, \ldots, D)}_{\dim A},$$

so we finish upon noting $(D, \ldots, D)$ is nonzero because D is very ample. We refer to [Mil08, Theorem I.7.2] or [Lom18, Proposition 5.17] for details. ■

Corollary 2.32. *Fix an abelian variety A over a field k. For $n \in \mathbb{Z}^+$ with $\operatorname{char} k \nmid n$, we have $A[n](k^{\text{sep}}) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$.*

Proof. By Proposition 2.31, the degree of $[n]$ is $n^{2\dim A}$. This implies the field extension $K(A) \to K(A)$ has degree $n^{2\dim A}$, which is not divisible by $\operatorname{char} k$, so the field extension is separable. Thus, the number of closed points in $A[n]$ is $n^{2\dim A}$ by Corollary 2.30, and all are defined over k^{sep}. (Technically, the fact that all points are defined over k^{sep} follows from their construction at the end of Lemma 2.29.)

Finishing the proof requires some group theory. We induct on n in steps.

(1) When $n = 1$, there is nothing to say. For primes ℓ not divisible by $\operatorname{char} k$, we see $A[\ell]\left(k^{\text{sep}}\right)$ has order $\ell^{2\dim A}$ while having exponent dividing ℓ, so the result follows.

(2) We now show the result for prime-powers by induction. Suppose that ℓ is not divisible by $\operatorname{char} k$ and that $A\left[\ell^v\right] \cong (\mathbb{Z}/\ell^v\mathbb{Z})^{2\dim A}$ for some $v \in \mathbb{Z}^+$. Then we have a short exact sequence

$$0 \to A[\ell]\left(k^{\text{sep}}\right) \to A\left[\ell^{v+1}\right]\left(k^{\text{sep}}\right) \xrightarrow{[\ell]} A\left[\ell^v\right]\left(k^{\text{sep}}\right) \to 0.$$

(This is exact on the right because $[\ell]$ is surjective on points.) Using the classification of finitely generated abelian groups again, we must have $A\left[\ell^{n+1}\right]\left(k^{\text{sep}}\right) \cong (\mathbb{Z}/\ell^{v+1}\mathbb{Z})^{2\dim A}$.

(3) We now show the general case by induction. If n is a prime-power, then we are done. Otherwise, we may write $n = n_1n_2$ where $\gcd(n_1, n_2) = 1$ where $n_1, n_2 < n$. Again, we have a short exact sequence

$$0 \to A[n_1]\left(k^{\text{sep}}\right) \to A[n]\left(k^{\text{sep}}\right) \xrightarrow{[n_1]} A[n_2]\left(k^{\text{sep}}\right) \to 0.$$

Thus, $A[n]\left(k^{\text{sep}}\right)$ has order $n^{2\dim A}$ and has a subgroup isomorphic to $\left(\mathbb{Z}/n_1\mathbb{Z}\right)^{2\dim A}$. By symmetry, we also have a subgroup isomorphic to $\left(\mathbb{Z}/n_2\mathbb{Z}\right)^{2\dim A}$, but because $\gcd(n_1, n_2) = 1$, we must have $A[n]\left(k^{\text{sep}}\right) \cong \left(\mathbb{Z}/n_1\mathbb{Z}\right)^{2\dim A} \oplus \left(\mathbb{Z}/n_2\mathbb{Z}\right)^{2\dim A}$, which is what we wanted. ■

Example 2.33. *We work in the context of Example 2.2. For any nonzero n, we saw that $[n] \colon (\mathbb{C}^g/\Lambda) \to (\mathbb{C}^g/\Lambda)$ has kernel $\frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. This is "how to remember" the 2 in Corollary 2.32.*

Non-Example 2.34. *We continue from Example 2.26. We saw $[5] = \varphi^{\circ 2}$, where $\varphi \colon E \to E$ was the Frobenius automorphism. It follows $[5]$ is injective on points, so $E[5]\left(\overline{k}\right) = 0$. In particular, $\operatorname{char} k \nmid n$ is necessary in Corollary 2.32.*

Remark 2.35. *In characteristic 0, we can see from Corollary 2.32 that the torsion subgroup of $A\left(k^{\text{sep}}\right)$ is isomorphic to $(\mathbb{Q}/\mathbb{Z})^{2\dim A}$ by taking a direct limit over all n. When defining the Tate module, we will take an inverse limit rather than a direct limit.*

3. The Tate Conjecture

The goal of the present section is to define the Tate module, explain why we should care about it, and prove Theorem 1.5.

3.1. **Tate Modules.**

At least, here is the definition of the Tate module.

Definition 3.1 (Tate module). *Fix an abelian variety A over a field k. For primes ℓ not divisible by $\operatorname{char} k$, we define the ℓ-adic Tate module by*

$$T_\ell A \coloneqq \varprojlim_{v \in \mathbb{Z}^+} A\left[\ell^v\right]\left(k^{\text{sep}}\right).$$

Here, the inverse limit is given by the "projection" maps $[\ell] \colon A\left[\ell^{v+1}\right]\left(k^{\text{sep}}\right) \to A\left[\ell^v\right]\left(k^{\text{sep}}\right)$. Occasionally, we might want to work with $V_\ell A \coloneqq T_\ell A \otimes_{\mathbb{Z}} \mathbb{Q}$.

We have the following quick remarks on this definition.

Remark 3.2. *Note that Corollary 2.32 gives us isomorphisms $A[\ell^v](k^{\mathrm{sep}}) \cong (\mathbb{Z}/\ell^v\mathbb{Z})^{2\dim A}$ which commute with the maps $[\ell]$, so we see*

$$T_\ell A \cong \varprojlim_{v\in\mathbb{Z}^+} (\mathbb{Z}/\ell^v\mathbb{Z})^{2\dim A} = \mathbb{Z}_\ell^{2\dim A}.$$

Thus, $T_\ell A$ is a free $\mathbb{Z}_\ell$-module, and $V_\ell A$ is a $\mathbb{Q}_\ell$-vector space of dimension $2\dim A$.

Remark 3.3. *Define $G := \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Then some $\sigma \in G$ acts on $A(k^{\mathrm{sep}})$ coordinate-wise (alternatively, one can pull back $\sigma\colon k^{\mathrm{sep}} \to k^{\mathrm{sep}}$ to a morphism $A_{k^{\mathrm{sep}}} \to A_{k^{\mathrm{sep}}}$) and commutes with the group law of A, so the action of σ descends to a morphism $A[n] \to A[n]$ for each $n \in \mathbb{Z}^+$. Thus, G acts on $T_\ell A$ and thus on $V_\ell A$ (by fixing $\mathbb{Q}$) and so defines a group representation*

$$G \to \mathrm{GL}(V_\ell A) \cong \mathrm{Gal}_{2\dim A}(\mathbb{Q}_\ell).$$

It is not too hard to see that this is a continuous homomorphism for the respective ℓ-adic topologies, so we see each abelian variety A over k has an attached Galois representation.

Quickly, we note the construction T_ℓ is functorial: given a homomorphism $\varphi\colon A \to B$, we note φ commutes with $[n]$ for any $n \in \mathbb{Z}^+$. As such, we induce a map $\varphi[n]\colon A[n] \to B[n]$, which gives a map

$$T_\ell A = \varprojlim_{v\in\mathbb{Z}^+} A[\ell^v](k^{\mathrm{sep}}) \xrightarrow{\varphi[\ell^v]} \varprojlim_{v\in\mathbb{Z}^+} B[\ell^v] = T_\ell B.$$

We call this composite $T_\ell\varphi$, and it is relatively clear that this construction is functorial. Intuitively, $T_\ell\varphi$ is "φ component-wise."

Already we can roughly see why the Tate module might be important: it provides some functor from geometric information in abelian varieties to more controlled algebraic information, in the form of a $\mathbb{Z}_\ell$-module. Arithmetically speaking, this algebraic information is desirable because there is an attached Galois representation, from Remark 3.3.

Anyway, we are now ready to prove Theorem 1.5. We quickly recall the statement.

Theorem 1.5. *Fix abelian varieties A and B over a field k. Then the map $\varphi \mapsto T_\ell\varphi$ induces an injection*

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

Proof. We roughly follow [EGM, Theorem 12.10] and [Sil09, Theorem III.7.4]. To begin, we reduce to the case where $A = B$. Define $C := A \times B$. Given a homomorphism $\varphi\colon A \to B$, we note $(0_A, \varphi)\colon (x, y) \mapsto (0_A, \varphi(x))$ defines a homomorphism $C \to C$ and makes the diagram

$$\begin{tikzcd}
\mathrm{Hom}_k(A,B)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \arrow[r, "T_\ell"] \arrow[d] & \mathrm{Hom}_k(T_\ell A, T_\ell B) \arrow[d] & \varphi\otimes z \arrow[r, mapsto] \arrow[d, mapsto] & z\cdot T_\ell\varphi \arrow[d, mapsto] \\
\mathrm{Hom}_k(C,C)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \arrow[r, "T_\ell"] & \mathrm{Hom}_k(T_\ell C, T_\ell C) & (0_A,\varphi)\otimes z \arrow[r, mapsto] & z\cdot(0, T_\ell\varphi)
\end{tikzcd}$$

commute. (We have silently used the fact that $T_\ell(A \times B) \cong T_\ell A \times T_\ell B$.) Now, the map $\varphi \mapsto (0 \times \varphi)$ is certainly injective (by projecting on the B-coordinate in the target), and $\mathbb{Z}_\ell$ is flat over $\mathbb{Z}$, so the left arrow above is injective. Thus, it suffices to show that the bottom arrow is injective, so we may replace A and B both with C.

Remark 3.4. *Note that we have increased the dimension of our abelian varieties here, so this reduction would not work if we wanted to only work with elliptic curves.*

Continuing, the input of the positive-definite symmetric bilinear form of Proposition 2.15 is in the following lemma.

Lemma 3.5. *Fix an abelian variety A over a field k. For any finitely generated submodule $M \subseteq \mathrm{End}_k(A)$, we claim the submodule*

$$M^{\mathrm{div}} := \left\{\varphi \in \mathrm{End}_k(A) : n\varphi \in M \text{ for some } n \in \mathbb{Z}^+\right\}$$

is also finitely generated.

Proof. Observe that this is not true if $\mathrm{Hom}_k(A, B)$ is replaced by $\mathbb{R}$ (for example, take $M = \mathbb{Z}$), so we will need to use something about the structure of abelian varieties. Additionally, note that Theorem 1.5 will be able to show that $\mathrm{Hom}_k(A, B)$ has finite $\mathbb{Z}$-rank, but we do not know this yet, which is why this lemma is necessary.

The idea is to view M as a lattice inside a real vector space and use the fact that the positive-definite symmetric bilinear form $\langle\cdot,\cdot\rangle$ of Proposition 2.15 is an integer for any $\varphi\in\operatorname{End}_k(A)$ to show that M^{div} is also a lattice. Indeed, set $V\coloneqq\operatorname{End}_k(A)\otimes_{\mathbb{Z}}\mathbb{R}$ to be an $\mathbb{R}$-vector space, and note $M_{\mathbb{R}}\coloneqq M\otimes_{\mathbb{Z}}\mathbb{R}$ is a finite-dimensional subspace because M is finitely generated. Because $\operatorname{End}_k(A)$ is torsion-free by Corollary 2.27, the natural map $\iota\colon\operatorname{End}_k(A)\hookrightarrow V$ is injective.

Thus, it suffices to show that the image $\iota\left(M^{\text{div}}\right)\subseteq V$ is finitely generated. For any $\varphi\in M^{\text{div}}$ with $n\in\mathbb{Z}^+$ such that $n\varphi\in M$, note

$$\iota(\varphi)=\varphi\otimes 1=n\varphi\otimes 1/n\in M_{\mathbb{R}},$$

so $\iota\left(M^{\text{div}}\right)$ lives in the finite-dimensional space $M_{\mathbb{R}}$. As such, we want to show $\iota\left(M^{\text{div}}\right)$ is a lattice in $M_{\mathbb{R}}$.

For this, we use a little topology. We can extend $\langle\cdot,\cdot\rangle\colon M^2\to\mathbb{Z}$ to a positive-definite symmetric bilinear form $\langle\cdot,\cdot\rangle_{\mathbb{R}}\colon M_{\mathbb{R}}^2\to\mathbb{R}$ by extending

$$\langle m\otimes r,m'\otimes r'\rangle_{\mathbb{R}}\coloneqq rr'\langle m,m'\rangle$$

linearly. (One can see $\langle\cdot,\cdot\rangle_{\mathbb{R}}$ is symmetric and $\mathbb{R}$-bilinear, and it is positive-definite because $\langle m\otimes r,m\otimes r\rangle_{\mathbb{R}}=r^2\langle m,m\rangle>0$.) Now, define the map $\|\cdot\|_{\mathbb{R}}:M_{\mathbb{R}}\to\mathbb{R}$ by $\|v\|_{\mathbb{R}}\coloneqq\langle v,v\rangle_{\mathbb{R}}$, which we see is a norm (it's a quadratic form) and thus gives $M_{\mathbb{R}}$ a topology as a normed vector space.

However, for $\varphi\in M^{\text{div}}$, we see $\|\iota(\varphi)\|_{\mathbb{R}}<1$ forces $\langle\varphi,\varphi\rangle<1$ and so $\langle\varphi,\varphi\rangle=0$ and so $\varphi=0$. Thus,

$$\iota\left(M^{\text{div}}\right)\cap\{v\in M_{\mathbb{R}}:\|v\|_{\mathbb{R}}<1\}=\{0\},$$

so $\iota\left(M^{\text{div}}\right)$ is a discrete subgroup of $M_{\mathbb{R}}$ and thus a lattice. ■

We are now ready to complete the proof of Theorem 1.5. Suppose $\varphi\in\operatorname{End}_k(A)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$ has $T_\ell\varphi=0$. We will show $\varphi=0$. The idea is to write φ in terms of some fixed $\mathbb{Z}_\ell$-basis and then show the coefficients must vanish because φ vanishes on $A\left[\ell^v\right]$ for arbitrarily large v.

To begin, we find a finitely generated submodule $M\subseteq\operatorname{End}_k(A)$ such that $\varphi\in M\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$. For example, we may write

$$\varphi=\sum_{i=1}^n\varphi_i\otimes z_i$$

for some φ_i and z_i and set $M\coloneqq(\varphi_1,\ldots,\varphi_n)$. Using Lemma 3.5, we may replace M with M^{div}, allowing us to assume that $n\psi\in M$ for some $n\in\mathbb{Z}^+$ and $\psi\in\operatorname{End}_k(A)$ forces $\psi\in M$.

Now, M is a $\mathbb{Z}$-torsion-free and finitely generated and thus $\mathbb{Z}$-free, so we may give M a basis. Rename the φ_i to be a basis for M, so the $\varphi_i\otimes 1$ remain a basis for the free $\mathbb{Z}_\ell$-module $M\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$, so we can write

$$\varphi=\sum_{i=1}^n\varphi_i\otimes z_i$$

for unique $z_i\in\mathbb{Z}_\ell$. We will show that $z_i=0$ for each i.

Well, we are given

$$\sum_{i=1}^n z_i\cdot T_\ell\varphi_i=0.$$

Fix some large exponent $v\in\mathbb{Z}^+$. Approximating, we may find $y_i\in\mathbb{Z}$ such that $z_i\equiv y_i\pmod{\ell^v}$, from which we define

$$\psi\coloneqq\sum_{i=1}^n y_i\varphi_i.$$

Now, for any $a\in A\left[\ell^v\right]$, we see

$$\psi(a)=\sum_{i=1}^n y_i\varphi_i(a)=\sum_{i=1}^n z_i\cdot T_\ell\varphi_i(a)=0$$

because a vanishes when multiplied by high enough powers of ℓ. Thus, ψ vanishes on $A\left[\ell^v\right]$, so viewing $\left[\ell^v\right]:A\to A$ as a quotient map,[3] we see ψ must factor through $\left[\ell^v\right]$. Namely, we can write $\psi=\ell^v\psi'$ for some $\psi'\in\operatorname{End}_k(A)$.

[3] We are using an fppf quotient here.

However, $\ell^v\psi' \in M$, so $\psi' \in M$ as well! Thus, because the φ_i are a basis for M, we see that each y_i must be divisible by ℓ^v, so each z_i is divisible by ℓ^v as well. Sending $v \to \infty$ shows $z_i = 0$ for each i, which completes the proof. ■

Here is a quick corollary we get even without the full power of Tate's conjecture.

Corollary 3.6. *Fix abelian varieties A and B over a field k. Then $\operatorname{Hom}_k(A, B)$ is $\mathbb{Z}$-free of rank at most $4(\dim A)(\dim B)$.*

Proof. Note $\operatorname{Hom}_k(A, B)$ is torsion-free already by Corollary 2.27. It might be tempting to apply Theorem 1.5 directly, but some care is required because $\operatorname{rank}_{\mathbb{Z}} M$ need not equal $\operatorname{rank}_{\mathbb{Z}_\ell}(M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$ for arbitrary $\mathbb{Z}$-modules M. Instead, we work with vector spaces: tensoring everything with $\mathbb{Q}_\ell$, we note we can embed

$$\operatorname{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow \operatorname{Hom}_k(T_\ell A, T_\ell B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \hookrightarrow \operatorname{Hom}_k(V_\ell A, V_\ell B), \tag{3.1}$$

where the last embedding is $\varphi \otimes r \mapsto r\varphi$. Now, for a $\mathbb{Q}$-vector space V, we do have $\dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}_\ell}(V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$, so $\operatorname{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-vector space of dimension at most $\dim_{\mathbb{Q}_\ell} \operatorname{Hom}_k(V_\ell A, V_\ell B) = 4(\dim A)(\dim B)$ from Remark 3.2.

Thus, we can find finitely many $\varphi_1, \ldots, \varphi_d \in \operatorname{Hom}_k(A, B)$ and $q_1, \ldots, q_d \in \mathbb{Q}$ such that the $\varphi_i \otimes q_i$ are a basis of $\operatorname{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$. In particular, for any $\varphi \in \operatorname{Hom}_k(A, B)$, there are rationals $q_1', \ldots, q_d'$ such that

$$\varphi \otimes 1 = \sum_{i=1}^{d} \varphi_i \otimes (q_i q_i'),$$

so clearing denominators and using the injectivity of $\operatorname{Hom}_k(A, B) \hookrightarrow \operatorname{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$ shows that $n\varphi \in (\varphi_1, \ldots, \varphi_d)$ for some $n \in \mathbb{Z}^+$. Applying Lemma 3.5 again, we conclude that $\operatorname{Hom}_k(A, B) = (\varphi_1, \ldots, \varphi_d)^{\operatorname{div}}$ is finitely generated over $\mathbb{Z}$, so using the embedding (3.1) one more time retrieves the claim. ■

3.2. **Application.** As a final note on why we might care about Conjecture 1.3, we show the following. We will be somewhat sketchy.

Theorem 3.7 ([Sil09, Exercise 5.4])**.** *Fix elliptic curves E_1 and E_2 over a finite field $\mathbb{F}_q$. The following are equivalent.*

(a) E_1 and E_2 are isogenous.
(b) $\#E_1(\mathbb{F}_{q^n}) = \#E_2(\mathbb{F}_{q^n})$ for all positive integers n.
(c) $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Proof. Quickly, let $\varphi_i \colon (E_i)_{\overline{\mathbb{F}_q}} \to (E_i)_{\overline{\mathbb{F}_q}}$ denote the Frobenius automorphism on E_i.

Showing (a) implies (b) does not require anything too serious. For a moment, work with a general elliptic curve E over $\mathbb{F}_q$, and let $\varphi \colon E \to E$ denote the Frobenius automorphisms. Now, a closed point $p \in E(\overline{k})$ is defined over $\mathbb{F}_{q^n}$ if and only if p is fixed by the action of $\varphi^{\circ n}$, so Corollary 2.30 implies

$$\#E(\mathbb{F}_{q^n}) = \#\ker(\operatorname{id}_E - \varphi^{\circ n}) = \deg(\operatorname{id}_E - \varphi^{\circ n}).$$

We now return to the proof. Let $\alpha \colon E_1 \to E_2$ be our isogeny. Because α is actually an isogeny defined over $\mathbb{F}_q$, we see α is fixed by the Galois action, so

$$\alpha \circ \varphi_1 = \varphi_2 \circ \alpha.$$

Thus, for any $n \in \mathbb{Z}^+$, we compute

$$\deg \alpha \cdot \#E_1(\mathbb{F}_{q^n}) = \deg(\alpha - \alpha \circ \varphi_1^{\circ n}) = \deg(\alpha - \varphi_2^{\circ n} \circ \alpha) = \deg \alpha \cdot \#E_2(\mathbb{F}_{q^n}),$$

from which the result follows.

Note (b) implies (c) with no work. Lastly, showing (c) implies (a) will use Theorem 1.4. Namely, fix some prime ℓ not dividing q, so it suffices to show that $\operatorname{Hom}_{\mathbb{F}_q}(V_\ell E_1, V_\ell E_2)$ is nonzero. Indeed, all nonzero homomorphisms $\alpha \colon E_1 \to E_2$ have closed (α is proper) and connected image, so α being nonconstant forces $\dim \operatorname{im} \alpha \geq 1$, which shows α is an isogeny by Proposition 2.22.

Well, we claim that $V_\ell E_1$ and $V_\ell E_2$ give isomorphic representations of G. In other words, we claim that the Galois representation $V_\ell E$ for an elliptic curve E depends only on $\#E(\mathbb{F}_q)$. As a vector space, $V_\ell E \cong \mathbb{Q}_\ell^2$, so we just have to make sure that the Galois action is forced. Well, G is topologically generated by the

Frobenius automorphism $\sigma\colon \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, and the image of σ in $V_\ell E$ is given $V_\ell \varphi$, where $\varphi\colon E_{\overline{\mathbb{F}_q}} \to E_{\overline{\mathbb{F}_q}}$ is the Frobenius automorphism. Now, [Sil09, Proposition III.8.6] tells us that

$$\det V_\ell \varphi = \deg \varphi = q \qquad \text{and} \qquad \operatorname{tr} V_\ell \varphi = 1 + \deg \varphi + \deg(1 - \varphi) = 1 + q - \#E\left(\mathbb{F}_q\right).$$

Thus, the characteristic polynomial of $V_\ell \varphi$ is uniquely determined by $\#E(\mathbb{F}_q)$. In fact, for any rational $a/b \in \mathbb{Q}$, we can compute the characteristic polynomial at a/b as

$$\det\left(\frac{a}{b} \operatorname{id}_{V_\ell E} - V_\ell \varphi\right) = \frac{\deg(a \operatorname{id}_E - b\varphi)}{b^2} \geq 0,$$

so the characteristic polynomial is nonnegative, meaning that $V_\ell \varphi$ is determined up to "conjugation" from its characteristic polynomial. So we have determined the action of G on $V_\ell E$, up to isomorphism, which completes the proof. ■

Example 3.8. *We continue Example 2.19. When k is a finite field, Theorem 3.7 tells us that we could actually see E and E' are isogenous purely by point-counting. Here is a table, computed using Sage.*

p	$\#E\left(\mathbb{F}_p\right)$	$\#E'\left(\mathbb{F}_p\right)$
5	6	6
7	12	12
11	12	12
13	12	12

Example 3.9. *We continue Example 2.19. Theorem 3.7 also tells us that $\#E\left(\mathbb{F}_p\right) = \#E'\left(\mathbb{F}_p\right)$ requires $\#E\left(\mathbb{F}_{p^n}\right) = \#E'\left(\mathbb{F}_{p^n}\right)$ for each $n \in \mathbb{Z}^+$. Here is another table, computed using Sage.*

n	$\#E\left(\mathbb{F}_{7^n}\right)$	$\#E'\left(\mathbb{F}_{7^n}\right)$
1	12	12
2	48	48
3	324	324
4	2496	2496

Remark 3.10. *We have stated Theorem 3.7 for elliptic curves, but more generally the following are equivalent for abelian varieties A and B over a finite field k.*

(a) A and B are isogenous.
(b) $\#A(k') = \#B(k')$ for any finite extension k' of k.

The main difficulty in extending the proof of Theorem 3.7 lies in the linear algebra at the end.

References

[Tat66] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Inventiones mathematicae* 2.2 (Apr. 1966), pp. 134–144. ISSN: 1432-1297. DOI: 10.1007/BF01404549. URL: https://doi.org/10.1007/BF01404549.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. New York: Springer-Verlag, 1977.

[Fal86] Gerd Faltings. *Arithmetic Geometry*. Ed. by Gary Cornell and Joseph H. Silverman. Springer New York, NY, 1986, pp. 9–26.

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics. Springer New York, NY, 2009. DOI: https://doi.org/10.1007/978-0-387-09494-6.

[Vak17] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. 2017. URL: http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf.

[Lom18] Davide Lombardo. *Abelian Varieties*. 2018. URL: https://people.dm.unipi.it/lombardo/Teaching/VarietaAbeliane1718/Notes.pdf.

[SP] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2022.

[EGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. *Abelian Varieties*. URL: http://van-der-geer.nl/~gerard/AV.pdf.