Abelian varieties

Caleb Ji

Feburary 7, 2024

These are supplementary notes to a talk on abelian varieties. We cover two distinct topics: Tate's isogeny theorem and the moduli space of principally polarized abelian varieties. This material is all standard and mostly taken from [1] and [2].

1 Tate's isogeny theorem

Let A and B be abelian varieties over a field k. Let l be a prime different from $\operatorname{char} k$ and let $G = G_k$ be the Galois group of k, which acts on $T_l(A), T_l(B)$. Consider the morphism

$$\operatorname{Hom}_k(A, B) \otimes \mathbb{Z}_l \to \operatorname{Hom}_G(T_l(A), T_l(B)). \tag{1}$$

In [2], Tate showed that this morphism is an isomorphism when k is a finite field.

1.1 Reductions

Recall that last time, we saw that $\phi \in \operatorname{Hom}(A, B)$ is divisible by l^n if $T_l(\phi)\colon T_l(A) \to T_l(B)$ is. This implies the cokernel of eq. (1) is torsion-free.

We can also show that eq. (1) is injective. But first, note that $\operatorname{Hom}(A, B) \to \operatorname{Hom}_{\mathbb{Z}_l}(T_l(A)T_l(B))$ is injective by the following argument. If $\phi \in \operatorname{Hom}(A, B)$ is 0 on $T_l(A)$, then $\phi(A_{l^n}(\overline{k})) = 0$ for all n. Restricting to any simple abelian subvariety $A' \hookrightarrow A$, we see that the kernel of ϕ restricted to A' is not finite, and is thus equal to A'. Then because A is isogenous to a product of simple subvarieties (Poincaré reducibility theorem), we see that $\phi = 0$.

Lemma 1.1. *If A is simple, then $\operatorname{End}_k(A)$ is finitely generated.*

Proof. Since A is simple all endomorphisms are isogenies, and have integer degrees. Take $\{e_i\}_i$ linearly independent over $\mathbb{Z}$ in $\operatorname{End}(A)$ and let M be the $\mathbb{Z}$-submodule of $\operatorname{End}(T_l(A))$ generated by the $T_l(e_i)$. Then $\mathbb{Q}M \cap \operatorname{End}(A)$ is discrete in $\mathbb{Q}M$ (because by taking degrees, its intersection with a neighborhood of 0 is just 0), and is therefore a finitely generated $\mathbb{Z}$-module. Choosing the e_i to be a $\mathbb{Q}$-basis of $\operatorname{End}^0(A)$, we have $\operatorname{End}(A) = \mathbb{Q}M \cap \operatorname{End}(A)$ which is finitely generated. □

Remark. The proof above relies on knowing that $\operatorname{End}^0(A)$ is a finite $\mathbb{Q}$-vector space. If we do not assume this, then we can still prove the next proposition by assuming there is a relation between $e_1, \ldots, e_r$ and applying the argument to the submodule they generate.

Proposition 1.2. *The morphism*

$$\operatorname{Hom}_k(A, B) \otimes \mathbb{Z}_l \to \operatorname{Hom}_G(T_l(A), T_l(B))$$

is injective with torsion-free cokernel.

Proof. We already know the second statement. For the first, we will show that $\mathrm{End}(A, B)$ is a finitely generated $\mathbb{Z}$-module. Indeed, choosing isogenies $\prod A_i \to A$ and $B \to \prod B_j$ with the A_i and B_j simple, we see that $\mathrm{Hom}(A, B)$ injects into $\prod \mathrm{Hom}(A_i, B_j)$, and each factor injects into $\mathrm{End}(A_i)$ which is finite-dimensional.

Now choose a $\mathbb{Z}$-basis $e_1, \dots, e_r$ for $\mathrm{Hom}(A, B)$ and assume that $\sum a_i T_l(e_i) = 0$ for $a_i \in \mathbb{Z}_l$. Then we can find integers $n_i(r)$ (approximating a_i by taking the first r digits) such that $\sum n_i(r) T_l(e_i) \neq 0$ is divisible by an arbitrarily large power of l in $\mathrm{End}(T_l(A))$ for sufficiently large r. But then the same is true in $\mathrm{End}(A)$, and thus each of the $n_i(r)$ is also divisible by an arbitrarily large power of l, which cannot occur unless they go to 0. □

Next, we tensor by $\mathbb{Q}_l$. Let $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$.

Lemma 1.3. *The map*

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}_l \to \mathrm{Hom}_G(V_l(A), V_l(B)) \tag{2}$$

is injective, and is bijective if and only if eq. (1) is. In fact, eq. (1) is bijective if and only if

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

is.

Proof. Because $\mathbb{Q}_l$ is flat over $\mathbb{Z}_l$, the injectivity follows from proposition 1.2. Surjectivity follows because the cokernel of eq. (1) is torsion-free. Finally, we can reduce to the case $A = B$ because $\mathrm{End}(A \times B) = \mathrm{End}_k(A) \oplus \mathrm{Hom}(A, B) \oplus \mathrm{Hom}(B, A) \oplus \mathrm{End}(B)$. □

1.2 A key lemma coming from a finiteness result

Consider the following finiteness condition.

Condition 1.4. *Given an abelian variety A/k, there are only finitely many abelian varieties B, up to k-isomorphism, which are isogenous to A with degree a power of l (where $l \neq \mathrm{char}\, k$ is a prime).*

In fact, a much stronger condition is true when k is finite; in that case there are only finitely many abelian varieties up to k-isomorphism of dimension g. For this, one can invoke the existence of Hilbert schemes or construct a parameterization directly. We sketch the idea.

First one shows there are finitely many such abelian varieties with a polarization ψ of degree d^2. Such a polarization arises from an ample line bundle $\mathcal{L}$, and by the theorem of the square $\mathcal{L}^3$ is very ample. (This can be used to prove that abelian varieties are projective.) One has that $\chi(\mathcal{L}) = \sqrt{\deg \phi_{\mathcal{L}}} = d$. Furthermore, Hirzebruch-Riemann-Roch gives $\chi(\mathcal{L}) = (D^g)/g!$, so we have $\chi(3\mathcal{L}) = 3^g d$. This realizes B as a degree $3^g d(g!)$ subvariety of $\mathbb{P}^{3^g d - 1}$, and if the ground field are finite then there are finitely any of these up to isomorphism. Then it can be shown (Zarhin's trick) that $(B \times B^\vee)^4$ has a principal polarization, and an abelian variety has only finitely many direct factors up to isomorphism.

Now we prove a lemma about constructing isogenies from the Tate module.

Lemma 1.5. *Let W be a G-stable submodule of $T_l(A)$ of finite index. Then there is an abelian variety B and an l-power isogeny $B \to A$ whose image on Tate modules is W.*

Sketch. Pick n such that $l^n T_l(A) \subset W$, and let N be the image of W in $T_l(A)/l^n T_l(A)$. Then we take $B = A/N$, and $[l^n]\colon A \to A$ factors through B to give the desired isogeny. □

The key lemma is the following.

Lemma 1.6. *Suppose condition 1.4 is satisfied. Then given any G-stable subspace $W \subset V_l(A)$, there is some $u \in \mathrm{End}(A) \otimes \mathbb{Q}_l$ such that $u(V_l(A)) = W$.*

Proof. Let
$$X_n = (T_l(A) \cap W) + l^n T_l(A).$$
Then X_n is stable under the action of G, and is a finite-index $\mathbb{Z}_l$-submodule of T_l. Then by the previous lemma, there is an abelian variety B_n with an isogeny $f_n \colon B_n \to A$ such that $f_n(T_l(B_n)) = X_n$. Since there are finitely many isomorphism classes of abelian varieties for B_n, we will take an infinite set I of B_i which are all isomorphic. Say j is the smallest such index, so X_j is the biggest of the X_i. We have isomorphisms $v_i \colon B_j \to B_i$.

$$\begin{array}{ccc} B_j & \xrightarrow{v_j} & B_i \\ & {\scriptstyle f_j}\searrow & \downarrow{\scriptstyle f_i} \\ & & A \end{array}$$

Note that $u_i := f_i v_i f_j^{-1} \in \mathrm{End}(A) \otimes \mathbb{Q}_l$. Then $u_i(X_j) = X_i \subset X_j$. Since $\mathrm{End}(X_j)$ is compact we can extract a subsequence I' of the u_i that converges to some u which gives an element of $\mathrm{End}(A) \otimes \mathbb{Q}_l$ with $u(X_j) = \cap_{i \in I'} X_i = T_l(A) \cap W$. This implies that $u(V_l(A)) = W$, as desired. □

1.3 Finishing the proof

The fact that $V_l(A)$ is a semisimple G-representation is generally included in the statement of Tate's isogeny theorem. Thus, we need to prove the following.

Theorem 1.7. *Let A be an abelian variety over a finite field k and let $l \neq \mathrm{char}\, k$ be a prime. Then:*
(a) $V_l(A)$ is a semisimple G-representation.
(b) $\mathrm{End}_k(A) \otimes \mathbb{Q}_l \to \mathrm{End}_G(V_l(A))$.

Before proving this, we review some noncommutative algebra. By Wedderburn's theorems, every semisimple k-algebra is a finite product of square matrices of division algebras $M_n(D)$. The right ideals in $M_n(D)$ are obtained by requiring that a certain subset of the columns be 0, and are thus are each generated by an idempotent given by an appropriate diagonal matrix.

Let $R \subset E$ be k-algebras and let $E = \mathrm{End}_k(V)$ for some faithful semisimple R-module V. The double centralizer theorem states that $C_E(C_E(R)) = R$. By the previous results, we know that $\mathrm{End}(A) \otimes \mathbb{Q}_l$ is a semisimple $\mathbb{Q}_l$-algebra.

Proof of theorem 1.7. (a) Given W a G-stable subspace of $V_l(A)$, we need to construct a complementary G-stable subspace. Let $\mathfrak{a} \subset \mathrm{End}_k(A) \otimes \mathbb{Q}_l$ be the right ideal of elements which preserve W; by lemma 1.6 we know that $\mathfrak{a} V_l(A) = W$. Thus $\dashv$ is generated by an idempotent e, and we have $eV_l(A) = W$. Then $(1 - e)V_l(A)$ is a G-invariant complementary subspace to W.

(b) Take $\alpha \in \mathrm{End}_G(V_l(A))$. To show α comes from $\mathrm{End}_k(A) \otimes \mathbb{Q}_l$, we let $C = C_{\mathrm{End}_G(V_l(A))}(\mathrm{End}_k(A) \otimes \mathbb{Q}_l)$; then $\mathrm{End}_k(A) \otimes \mathbb{Q}_l$ is the centralizer of C because it is semisimple. So we have to show that for every $c \in C$, we have $c\alpha = \alpha c$.

The graph of α is a G-invariant subspace $W \subset V_l(A) \times V_l(A)$, because α is G-invariant. Thus there is some $u \in \mathrm{End}_k(A \times A) \otimes \mathbb{Q}_l$ such that $u(V_l(A) \times V_l(A)) = W$. Note that $cI_2 \in \mathrm{End}(V_l(A) \times V_l(A))$ commutes with u, so
$$cI_2 W = cI_2 uW = ucI_2 W \subset W,$$
which means that $(cx, c\alpha x) = (cx, \alpha cx)$ for all $x \in V_l(A)$. This implies that $c\alpha = \alpha c$ as desired. □

Corollary 1.8. *Let R be the image of $\mathbb{Q}_l[G]$ in $\mathrm{End}(V_l(A))$. Then R is semisimple and $C(R) = \mathrm{End}(A) \otimes \mathbb{Q}_l$. R is the centralizer of $\mathrm{End}(A) \otimes \mathbb{Q}_l$ in $\mathrm{End}(V_l(A))$.*

1.4 Faltings's theorem and the Tate conjecture

Tate's isogeny theorem is part of a larger, important story in arithmetic geometry. First, its validity for number fields was an important part of the proof of Faltings's theorem. We give a quick sketch.

Recall that we used a finiteness theorem for abelian varieties to prove the Tate conjecture. This is a version of the Shafarevich conjecture, and is much harder to prove over number fields. However, Faltings proved a version of finiteness up to isogeny, using the Faltings height. This allowed him to prove the Tate conjecture for number fields, which allowed him to deduce the Shafarevich conjecture, from which the Mordell conjecture follows.

1. (Finiteness I) There are finitely many abelian varieties B which are isogenous to A.
2. (Tate conjecture I) a) The representation of G_K on $V_l(A)$ is semisimple.
   b) The natural map $\operatorname{Hom}_K(A,B)\otimes_{\mathbb{Z}}\mathbb{Z}_l \to \operatorname{Hom}_{G_K}(T_l(A),T_l(B))$ is an isomorphism.
3. (Shafarevich conjecture for AV) Let S be a finite set of places of K and fix a positive integer g. Then there are only finitely many isomorphism classes of abelian varieties A/K of dimension g with good reduction outside S.
4. (Shafarevich conjecture) With the notation above, there are only finitely many isomorphism classes of smooth projective curves C of genus g with good reduction outside S.
5. (Mordell's conjecture) If $g \geq 2$, then $C(K)$ is finite.

1.5 The Tate conjecture

There is another direction in which the Tate isogeny theorem can be generalized, namely the Tate conjecture on algebraic cycles. This puts the Tate isogeny theorem into a much richer perspective. The Tate conjecture is an enormously important question in arithmetic geometry and we will hardly scratch the surface here, not even saying anything about (e.g.) the deep connection with the BSD conjecture.

Let X be a smooth geometrically irreducible projective variety over a field k, and let $\overline{X} = X \times_k \operatorname{Spec}\overline{k}$. Recall the cycle class map, sending subvarieties to étale cohomology. This is a homomorphism

$$c^r(Z(\overline{X})) \to H^{2r}(\overline{X}, \mathbb{Q}_l(r)).$$

In the case of divisors, this can be seen through the first Chern class. Indeed, the Kummer sequence gives an injection

$$\operatorname{Pic}(\overline{X})/l^n \operatorname{Pic}(\overline{X}) \hookrightarrow H^2(\overline{X}, \mu_n),$$

and taking the inverse limit gives an injection

$$\operatorname{Pic}(\overline{X}) \otimes \mathbb{Q}_l \hookrightarrow H^2(\overline{X}, \mu_n).$$

We define $A(\overline{X})$ to be the left hand side, or more generally, the quotient of the Chow group by the classes which map to 0 under the cycle class map. This equivalence relation is known as *homological equivalence*, and sits between rational/algebraic equivalence and numerical equivalence. In the case of divisors, we can say more. Recall we have the surjections

$$\operatorname{Pic}(\overline{X}) \twoheadrightarrow \operatorname{NS}(\overline{X}) \twoheadrightarrow \operatorname{Num}(\overline{X})$$

corresponding to rational, algebraic, and numerical equivalence. The kernel of the second surjection is torsion, so in this case homological and numerical equivalence coincide.

We now state the Tate conjecture. Note that the image of $Z(X)$ in $Z(\overline{X})$ is fixed by G_k, and thus its cycle class is as well. The Tate conjecture states a converse.

Conjecture 1.9 (Tate)**.** *Let X be a smooth projective variety over a field k which is finitely generated over its prime field. Then the map*

$$A^r(X) \otimes \mathbb{Q}_l \to H^{2r}(\overline{X}, \mathbb{Q}_l(2r))^{G_K}$$

is an isomorphism.

Let us now relate this with the version we saw for abelian varieties. The idea is that, first the Tate module of an abelian variety is dual to its l-adic cohomology, and second, homomorphisms between abelian varieties and their cohomology can be described by cycles or cohomology classes of the product, which is a very classical motivic idea.

First, let us say we know the Tate conjecture. We will apply it to a product of abelian varieties $A \times B$. First, note that by identifying B with its double dual and using the fact that the dual represents Pic^0, we have that

$$\mathrm{Hom}_k(A, B) = \ker(A^1(A \times \hat{B}) \to A^1(A) \times A^1(\hat{B})).$$

On the other hand, by Künneth we have

$$H^1(A, \mathbb{Q}_l) \times H^1(\hat{B}, \mathbb{Q}_l) \cong \ker(H^2(A \times \hat{B}) \to H^2(A, \mathbb{Q}_l) \times H^2(\hat{B}, \mathbb{Q}_l)).$$

Applying the cycle class map, given the Tate conjecture we can identify $\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}_l$ with the Galois invariants of $H^1(A, \mathbb{Q}_l) \times H^1(\hat{B}, \mathbb{Q}_l)$, which are identified with the G_K maps on Tate modules.

In the other direction, fix a polarization λ, and recall the Rosati involution $\alpha^\dagger$ on $\mathrm{End}(A) \otimes \mathbb{Q}$ defined by $\lambda^{-1} \circ \alpha^\vee \circ \lambda$. Over an algebraically closed field, the map sending $\mathcal{L} \mapsto \lambda^{-1} \circ \lambda_{\mathcal{L}}$ identifies $\mathrm{NS}(A) \otimes \mathbb{Q}_l$ with the subgroup of $\mathrm{End}(A) \otimes \mathbb{Q}$ fixed by $\dagger$. Similarly, $H^2(\overline{A}, \mathbb{Q}_l) = \wedge^2 H^1(\overline{A}, \mathbb{Q}_l)$ can be identified with the subgroup of $\mathrm{End}(V_l(A))$ fixed under the Rosati involution. Making these identifications, we see that the Tate isogeny theorem implies the Tate conjecture in the case of divisors on abelian varieties.

The semisimplicity of the Galois representation on étale cohomology and numerical equivalence coinciding with homological equivalence are also generally bunched together with the Tate conjecture. Among other things, these would imply most of Grothendieck's standard conjectures, as well as the BSD conjecture for function fields.

2 The moduli space of abelian varieties

We will now give a brief introduction to the classical story of moduli of abelian varieties over $\mathbb{C}$. However this moduli space exists over $\mathbb{Z}$, and many of the AWS projects are about understanding its various stratifications in characteristic p.

2.1 The Riemann bilinear relations

Working over $\mathbb{C}$, it can be shown that any connected compact complex Lie group (including complex abelian varieties) is a torus, i.e. of the form $\mathbb{C}^g/\Lambda$ for some lattice Λ. Then the period matrix Π is a $g \times 2g$ matrix where the $2g$ columns correspond to the coordinates of the lattice vectors. One can check that Π indeed defines a period matrix if and only if $\begin{bmatrix} \Pi \\ \overline{\Pi} \end{bmatrix}$ is invertible. By taking a change of basis, one can make Π look like $\begin{bmatrix} I_g & \Omega \end{bmatrix}$. Then the previous condition amounts to $\Im(\Omega)$ being invertible.

Now a fundamental question is: when does Π determine an abelian variety? This is answered by the Riemann bilinear relations.

Theorem 2.1. *The period matrix Π determines an abelian variety if and only if there exists a skew symmetric matrix E such that*
i) $\Pi E^{-1}\Pi^T = 0$
ii) $i\Pi E^{-1}\overline{\Pi}^T$ is positive-definite.

The matrix E can be interpreted as the imaginary part of a Riemann form or a polarization H. A polarization H with respect to Λ is a positive-definite Hermitian form with $\Im H$ integer-valued on Λ. We recover H from E by

$$H(u, v) = E(iu, v) + iE(u, v).$$

Using linear algebra, Riemann's bilinear relations are equivalent to there existing a polarization.

Why does a polarization, or Riemann's bilinear relations give a complex torus the structure of an abelian variety? In other words, how are they related to projectivity?

First, assume we have an embedding $A = \mathbb{C}^g/\Lambda \subset \mathbb{P}^n$. Recall that $H^k(A, \mathbb{Z}) \cong \bigwedge^k(\Lambda^*)$. Then one can take the pullback of the generator of $H^2(\mathbb{P}^n, \mathbb{Z})$ to $H^2(A, \mathbb{Z})$, or equivalently the first Chern class of the line bundle defining the embedding, which gives a skew-symmetric integer-valued form on Γ. This turns out to be the matrix A defining the (imaginary part of) the polarization. Furthermore, this cohomology class is the restriction of the Kähler form on $\mathbb{P}^n$, which has an explicit representative giving the positive-definite Hermitian condition.

On the other hand, given a polarization, one can construct a projective embedding using theta functions arising from the polarization. This is more analytically involved, and gives a concrete realization of the abstract proof of projectivity over arbitrary fields in [1]. Finally, we remark that in the case of Jacobians, Riemann's bilinear relations can be understood very concretely, with properties of the intersection pairing on the homology of a Riemann surface give rise to a natural polarization.

2.2 $\mathcal{A}_g(\mathbb{C})$

Given a polarization H with imaginary part E, we can write $E = \left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)$ where D is diagonal. If D can be taken to be I_g, then we call this a principal polarization. Recall that such that polarizations are associated to period lattices $\begin{bmatrix} I_g & \Omega \end{bmatrix}$. Writing a principal polarization in the standard symplectic form, the Riemann bilinear relations say that Ω is symmetric and has positive-definite imaginary part. The set of such matrices is known as $\mathfrak{h}$, the Siegel upper half-space.

Any point in the Siegel upper half-space determines a principally polarized abelian variety, and one can check that two are isomorphic if they are related by the action of the symplectic group. Recall $\mathrm{Sp}_{2g}(\mathbb{C})$ consists of the invertible matrices which preserve the symplectic form (i.e. $M^T JM = J$). The action of $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ on $\Omega \in \mathfrak{h}_g$ is given by $\Omega \mapsto (A\Omega + B)(C\Omega + D)^{-1}$. Then we can define the moduli space of principally polarized abelian varieties by

$$\mathcal{A}_g = \mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathfrak{h}_\mathfrak{g}.$$

This is the classical complex construction, but Mumford was able to give an algebraic construction of $\mathcal{A}_g$ over an arbitrary base. There are of course also stacky versions.

References

[1] J. S. Milne. "Abelian Varieties". In: *Arithmetic Geometry*. Ed. by Gary Cornell and Joseph H. Silverman. New York, NY: Springer New York, 1986, pp. 103–150. ISBN: 978-1-4613-8655-1. DOI: 10.1007/978-1-4613-8655-1_5. URL: https://doi.org/10.1007/978-1-4613-8655-1_5.

[2] J. TATE. "Endomorphisms of Abelian Varieties over Finite Fields." In: *Inventiones mathematicae* 2 (1966), pp. 134–144. URL: http://eudml.org/doc/141848.