MATH 254B: ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION

Instructor: Prof. Yunqing Tang
Notes written by CJ Dowd
Spring 2024

Contents

Part I

Analytic theory of CM abelian varieties

1 Introduction (01/17/2024)

This course is about abelian varieties with complex multiplication (abbreviated as CMAVs). Major results we will prove include definability of CMAVs over $\overline{\mathbb{Q}}$, the Shimura-Taniyama formula, and the Main Theorem of Complex Multiplication. Additionally, a substantial portion of the course will be devoted to developing the general theory of abelian varieties. We will have roughly biweekly homeworks (5 total).

Prerequisites:

- A graduate course in algebraic number theory. We will review some of the main statements of class field theory near the end of the course when we state and prove the Main Theorem of Complex Multiplication, but we will not have time to prove any results from CFT—see the references, especially [Mil20] and [Ked21], if you would like to learn more. We will not need group cohomology.
- A graduate course in scheme theory, especially comfort working with line bundles. We will review some results from sheaf cohomology.
- We will cite results from noncommutative algebra without proof, which will be relevant when studying the endomorphism ring of an abelian variety. Good sources for these results are [Mil20, §IV] and [Mil10].
- Near the beginning of the course we use some basic Lie theory, although not nearly enough to make Lie theory a strict prerequisite.
- Familiarity with complex manifolds is largely unnecessary, although we will cite the Hodge decomposition when discussing the CM type associated to a CMAV.

We attempt to give examples where possible. Keep in mind that many basic examples of abelian varieties are supplied by elliptic curves. Unfortunately, it is generally difficult to write down explicit polynomial equations cutting out an abelian variety inside projective space, even starting in dimension 2. Explicit descriptions are much easier in the complex analytic setting, where abelian varieties are of the form $\mathbb{C}^n/\Lambda$ for a suitable lattice Λ. Moreover, in the analytic setting is especially simple to write down a CM abelian variety with a prescribed CM type.

In the first couple weeks, we will be stating a lot of results without necessarily fully explaining them. Do not worry; we will eventually see more rigorous proofs, especially for the general theory of abelian varieties from the perspective of algebraic geometry. One major result whose proof we unfortunately omit is the algebraizibility of tori with a Riemann form (Theorem 1.1), which implies the equivalence of the algebraic and analytic categories of abelian varieties over $\mathbb{C}$. Despite this, we will freely switch between the analytic and algebraic categories as best suits our needs.

CJ's note: These are an edited version of my course notes for Yunqing Tang's Math 254B in the Spring 2024 semester at UC Berkeley. I worked to revise and polish these notes during the semester and the following summer. In some areas these notes are substantially expanded versions of original lectures, mainly where I felt more detailed explanations were needed. I learned the majority of the content of these notes during the course. Since I am not an expert, these notes may contain silly mistakes that I missed. If you see any errors in these notes, or if you can offer details in places where they seem to be missing, please let me or Prof. Tang know.

1.1 Abelian varieties over $\mathbb{C}$

Definition 1.1. An *elliptic curve* over a field k is a pair (E, e), where E is a smooth proper curve of genus 1 over k and $e \in E(k)$.

If $k = \mathbb{C}$, then $E(\mathbb{C})$ may be given the structure of a compact genus 1 Riemann surface isomorphic to $\mathbb{C}/\Lambda$ for some lattice[1] $\Lambda \subset \mathbb{C}$. The identity e corresponds to the coset Λ in this interpretation.

More generally:

Theorem 1.1. [Mum08, Cor on p.33] Consider $X = V/\Lambda$, where $V \simeq \mathbb{C}^n$ and $\Lambda \subset V$ is a lattice. The following are equivalent:

1. X can be holomorphically embedded into $\mathbb{CP}^n$.
2. X is the analytification of some algebraic variety.[a]
3. There exists a positive definite Hermitian form $H : V \times V \to \mathbb{C}$ such that $\operatorname{Im} H(\Lambda \times \Lambda) \subseteq \mathbb{Z}$.

[a] Our definition of a variety is a reduced separated scheme of finite type over a field. In particular, we do not assume projectivity or quasiprojectivity.

The main idea for (3) $\implies$ (1) in Theorem 1.1 is to associate a certain line bundle $\mathscr{L}$ to the positive definite form H. One then shows that this line bundle is ample—in fact, that $\mathscr{L}^{\otimes 3}$ is very ample—by studying the so-called theta functions associated to the pair (Λ, H). These theta functions form the space of global sections of $\mathscr{L}$. One of the key ingredients is Fourier analysis. Unfortunately, we will not say any more about these things in this course; read [Mum08, §I.3] if you are interested in the full proof.

Definition 1.2. An *abelian variety* over $\mathbb{C}$ is the algebraic variety associated to a complex torus V/Λ satisfying one of the equivalent conditions of Theorem 1.1.

[1] In this course, whenever we say a discrete subgroup Λ is a lattice of some real vector space V, we mean full rank, i.e. $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \simeq V$ as real vector spaces. Such lattices are always cocompact.

Lemma 1.2. Suppose $V \simeq \mathbb{C}^n$. We have a bijection between:

1. Hermitian forms H on V;
2. Skew-symmetric forms on $V_{\mathbb{R}}$ (V viewed as an $\mathbb{R}$-vector space) such that $\psi(iv, iw) = \psi(v, w)$.

The skew-symmetric form associated to a Hermitian form H is $\operatorname{Im} H$, and the Hermitian form associated to a skew-symmetric form is $H(v, w) = \psi(iv, w) + i\psi(v, w)$.

Definition 1.3. A skew-symmetric form $\psi : \Lambda \times \Lambda \to \mathbb{Z}$ is said to be a *Riemann form* if $\psi_{\mathbb{R}} : V \times V \to \mathbb{R}$ satisfies

1. $\psi(iv, iw) = \psi(v, w)$; and
2. The associated Hermitian form H from Lemma 1.2 is positive definite.

Hence condition 3 in Theorem 1.1 is equivalent to existence of a Riemann form.

1.2 CM fields

Lemma 1.3. [Mil10, Prop. 1.4] For a number field[a] E, the following are equivalent:

1. There exists a field $E^+ \subset E$ such that $E^+/\mathbb{Q}$ is totally real and E/E^+ is an imaginary quadratic extension.
2. There exists a nontrivial $c \in \operatorname{Aut}(E)$ such that for all embeddings $\tau : E \hookrightarrow \mathbb{C}$, we have $c' \circ \tau = \tau \circ c$, where c' denotes complex conjugation in $\mathbb{C}$.
3. There exists a field $E^+ \subset E$ with $E^+/\mathbb{Q}$ totally real such that $E = E^+[\alpha]$, where $\alpha^2 \in E^+$ is *totally negative*, i.e. under every embedding $\tau : E^+ \to \mathbb{R}$ we have $\tau(\alpha^2) < 0$.

[a] A finite field extension of $\mathbb{Q}$.

The automorphism c in condition 2 is uniquely determined, since under any given embedding $E \hookrightarrow \mathbb{C}$, at most one automorphism of E corresponds to complex conjugation. We must have $E^+ = \operatorname{Fix}(c) \subset E$, so the totally real subfield E^+ is also uniquely determined.

Definition 1.4. A number field E satisfying one of the conditions in Lemma 1.3 is said to be a *CM field*. More generally, a CM algebra is a finite product of CM fields: $E = E_1 \times \cdots \times E_n$ for CM fields $E_1, \ldots, E_n$.

Remark 1.4. Some authors additionally define totally real fields to be CM by taking criterion (2) above without the assumption that c is nontrivial. For us, the term "CM field" will be reserved exclusively for a quadratic imaginary extension of a totally real field.

The symbol E will typically be reserved for CM fields or algebras in these notes.[2]

[2] Although we will occasionally also use E to denote an elliptic curve when no confusion is possible.

Example 1.5. All quadratic imaginary fields are CM with totally real subfield $\mathbb{Q}$. All cyclotomic fields $\mathbb{Q}(\zeta_n)$ for $n \geq 3$ are CM with totally real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Example 1.6. A CM field need not be Galois. For example, let E^+ be any non-Galois totally real field, e.g. $\mathbb{Q}[\alpha]$ where α is a root of a generic irreducible cubic with real roots. Then $E := E^+(i)$ is a CM field which is non-Galois; otherwise, $\mathrm{Gal}(E/E^+)$ would have index 2 in $\mathrm{Gal}(E/\mathbb{Q})$, hence a normal subgroup, so that E^+ would be Galois.

Corollary 1.7. If $E_1, \ldots, E_n \subseteq \overline{\mathbb{Q}}$ are CM fields, then their compositum $E_1 \cdots E_n$ is also CM. In particular, the Galois closure of $E \subset \overline{\mathbb{Q}}$ is CM.

Proof. We use condition 3 from Lemma 1.3. It suffices to prove this fact for the compositum of two CM fields E_1, E_2 with respective totally real subfields E_1^+, E_2^+. Let α_1, α_2 be elements in E_1, E_2, respectively, with totally negative squares such that $E_i^+[\alpha_i] = E_i$. Then $\alpha_1\alpha_2$ has totally positive square, so $\alpha_1\alpha_2$ is totally real. We conclude that $E^+ := E_1^+E_2^+[\alpha_1\alpha_2]$ is totally real, and we have $E^+[\alpha_1] = E^+[\alpha_2] = E_1E_2$, so condition 3 is again satisfied.

The remark about the Galois closure follows from the fact that the Galois closure of E is the compositum of the images of the finitely many embeddings $E \hookrightarrow \overline{\mathbb{Q}}$. ∎

Definition 1.5. Let E be a CM algebra. A *CM type* on E is a subset $\Phi \subseteq \mathrm{Hom}(E, \mathbb{C})$ such that $\mathrm{Hom}(E, \mathbb{C}) = \Phi \coprod c\Phi$, where c is complex conjugation. We may also denote complex conjugation with a bar when there are no ambiguities.

Remark 1.8. If $E = E_1 \times \cdots \times E_n$ is a CM algebra, then choosing a CM type on E is not equivalent to choosing a CM type on each of the E_j individually. If $\Phi_1, \ldots, \Phi_n$ are respective CM types on $E_1, \ldots, E_n$, then $\Phi_1 \times \cdots \times \Phi_n \subset \prod_{j=1}^n \mathrm{Hom}(E_j, \mathbb{C}) \simeq \mathrm{Hom}(E, \mathbb{C})$ is too small to be a CM type on E if $n > 1$.

Example 1.9. *(Construction of CM abelian varieties.)* Given a CM type (E, Φ) with $n = \frac{1}{2}[E : \mathbb{Q}] = |\Phi|$, consider the embedding $\Phi : \mathcal{O}_E \hookrightarrow \mathbb{C}^n$ given by $\alpha \mapsto (\varphi(\alpha))_{\varphi \in \Phi}$. Then $\mathbb{C}^n/\mathcal{O}_E$ is a complex torus, and indeed an abelian variety.
To prove this, by Theorem 1.1 we need to exhibit a Riemann form on $\mathcal{O}_E$. Fact: by weak approximation, we can find a totally imaginary $\xi \in \mathcal{O}_E$ such that $\mathrm{Im}(\varphi(\xi)) > 0$ for all $\varphi \in \Phi$. Given such ξ, we define $\psi : \mathcal{O}_E \times \mathcal{O}_E \to \mathbb{Z}$ by $(x, y) \mapsto \mathrm{tr}_{E/\mathbb{Q}}(\xi c(x)y)$. On the homework, you will verify that this is indeed a Riemann form.

Example 1.10. The case $n = 1$ of the previous example corresponds to the case of a CM elliptic curve. Let $E/\mathbb{Q}$ be an imaginary quadratic extension and let Φ be a choice of embedding $E \hookrightarrow \mathbb{C}$ (out of only two possibilities). Let $\tau \in \mathcal{O}_E$ be any element such that $\mathcal{O}_E = \mathbb{Z} + \tau\mathbb{Z}$, and let ξ be as in the previous example. We compute $\mathrm{tr}_{E/\mathbb{Q}}(\xi c(x)y) = \xi\overline{x}y + \overline{\xi}x\overline{y} = \xi(\overline{x}y - x\overline{y})$. The associated Riemann form ψ has matrix

$$\begin{pmatrix} 0 & \xi(\tau - \overline{\tau}) \\ \xi(\overline{\tau} - \tau) & 0 \end{pmatrix}$$

with respect to the basis $\{1, \tau\}$. (Note that the entries of this matrix are real—in fact integers—since both $\overline{\tau} - \tau$ and ξ are pure imaginary.)

We have essentially constructed all CM abelian varieties in this way, though we have not defined what this means yet. However, there is a slight generalization we can make: instead of using the ring of integers $\mathcal{O}_E$, we can more generally use a fractional ideal of this ring and make some adjustments.

2 Basic properties of abelian varieties (01/19/2024)

2.1 Group objects

Definition 2.1. Let S be a base scheme. A *group scheme* over S is a group object in the category of S-schemes.

A *group variety* over a field k is a group object in the category of k-varieties.

A *complex analytic Lie group* over $\mathbb{C}$ is a group object in the category of complex manifolds.

What is a group object in a category $\mathcal{C}$? This is an object $G \in \mathcal{C}$ endowed with morphisms $m : G \times G \to G$, $i : G \to G$, and $e : \{*\} \to G$ corresponding to multiplication, inversion, and an identity section. Here, the product is the product in the category $\mathcal{C}$—in the category of S-schemes or k-varieties, this is the fiber product over S or k—and $\{*\}$ denotes the final object in the category, which is $S, \mathrm{Spec}\, k$, or a point in each of the three cases listed previously.

We require these morphisms to satisfy commutative diagrams encoding the usual group axioms:

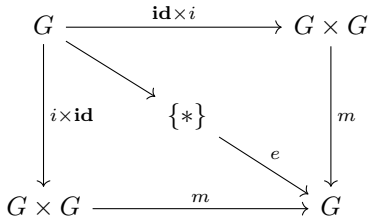
- Associativity:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathbf{id} \times m} & G \times G \\ \downarrow{\scriptstyle m \times \mathbf{id}} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

- Identity:

$$\begin{array}{ccccc} G \times \{*\} \simeq G \simeq \{*\} \times G & & \xrightarrow{\mathbf{id} \times G} & & G \times G \\ \downarrow{\scriptstyle G \times \mathbf{id}} & \searrow^{\mathbf{id}} & & & \downarrow{\scriptstyle m} \\ G \times G & & \xrightarrow{m} & & G \end{array}$$

- Inverse:



2.2 Abelian varieties

Definition 2.2. An *abelian variety* over a field k is a smooth connected proper group scheme over $\operatorname{Spec} k$.

Remark 2.1. These properties allow us to deduce quite a bit more—for example, we can use connectedness and the existence of a k-valued point to deduce that abelian varieties are geometrically connected, hence geometrically irreducible. Smoothness is equivalent to geometric reducedness for group schemes over a field, so we even get geometric integrality. In particular, even though our definition specifies that an abelian variety is a group *scheme* over k, it is in fact also a group *variety* over k. We will eventually prove that every abelian variety is projective, not just proper, but we need to develop the theory of line bundles on abelian varieties first. There are many equivalent definitions of an abelian variety; the Stacks Project gives 16 of them [Sta24, Tag 0H2U].
These remarks are largely unimportant in the context of this course, but if you are interested in the details, see [EvdGM24], especially Theorem 2.25 and Section 3.2, or [Sta24, Tag 0BF9]. If you would prefer to work through facts like these on your own, see instead the exercises in the first few chapters of Brian Conrad's notes [Con15].

Note that we don't actually include commutativity of the group law here. A general, non-proper group variety is not commutative, e.g. the algebraic variety GL_n for $n \geq 2$. However, it turns out that properness guarantees commutativity.

Definition 2.3. An *abelian scheme* A over S is a group scheme A/S such that the structure morphism $\pi : A \to S$ is proper and smooth with geometrically connected fibers.

Again, we will not worry about the technical scheme-theoretical details of these requirements. Our use case for a general abelian scheme will be over an arithmetic base such as $\operatorname{Spec} \mathbb{Z}_p$. If $\overline{s} = \operatorname{Spec} \overline{k} \to S$ is a geometric point of S, then the fiber $A_{\overline{s}}$ is connected, so in particular $A_{\overline{s}}$ is an abelian variety over $\overline{k}$.

It is often more intuitive to view abelian varieties from the perspective of the functor of points. For example, to check or define the group law, it suffices to work with $A(\overline{k})$.

Theorem 2.2. Let A/k be an abelian variety. Then A is commutative.

We will prove this in full generality once we start developing the algebraic theory of abelian varieties, but for now we prove commutativity in the analytic setting. Given an

abelian variety $A/\mathbb{C}$, the set of $\mathbb{C}$-points $A(\mathbb{C})$ can be endowed with the structure of a smooth compact connected complex analytic Lie group.

Proposition 2.3. [Mum08, pp.1-2] A connected compact complex Lie group is isomorphic to V/Λ for some vector space $V \simeq \mathbb{C}^n$ and lattice $\Lambda \subset V$.

Proof. (Sketch.) Consider the Lie algebra $\operatorname{Lie} A(\mathbb{C}) := T_e(A(\mathbb{C}))$. You can think of this either as the algebraic tangent space or the complex analytic tangent space. For every $x \in A(\mathbb{C})$, we obtain a conjugation morphism $c_x : A(\mathbb{C}) \to A(\mathbb{C})$ defined by $y \mapsto xyx^{-1}$. Taking the derivative yields, for each $x \in A(\mathbb{C})$, a linear map $dc_x : \operatorname{Lie} A(\mathbb{C}) \to \operatorname{Lie} A(\mathbb{C})$. The map $x \mapsto dc_x$ defines a holomorphic homomorphism $A(\mathbb{C}) \to \mathrm{GL}(\operatorname{Lie} A(\mathbb{C}))$. But $A(\mathbb{C})$ is compact and connected and $\mathrm{GL}(\operatorname{Lie} A(\mathbb{C}))$ may be viewed as an open subset of $\mathbb{C}^n$, so we conclude that $x \mapsto dc_x$ is constant, hence $dc_x = \mathbf{id}_{\operatorname{Lie} A(\mathbb{C})}$ for all x. This implies that $c_x(y) = y$ for all $x \in A(\mathbb{C})$ and all y in some neighborhood of the identity. Such neighborhoods generate all of $A(\mathbb{C})$, so we conclude $c_x = \mathbf{id}_G$ for all $x \in A(\mathbb{C})$, i.e. the group law is commutative.

Since the group law is commutative, the exponential map $\exp_A : \operatorname{Lie} A(\mathbb{C}) \to A(\mathbb{C})$ is a group homomorphism, hence a Lie group covering map, so we conclude that $A(\mathbb{C}) \simeq \operatorname{Lie} A(\mathbb{C})/\ker \exp_A$ as complex Lie groups. Since $\exp_A$ is a local homeomorphism near the origin and $A(\mathbb{C})$ is compact, this kernel must be a lattice in the Lie algebra. ∎

Corollary 2.4. Let $A/\mathbb{C}$ be an abelian variety of dimension g.

1. $[n] : A \to A$ is surjective with kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$. Here, $[n]$ denotes the map $x \mapsto \underbrace{x + x + \cdots + x}_{n \text{ times}}$.
2. $\pi_1(A(\mathbb{C})) \simeq H_1(A(\mathbb{C}), \mathbb{Z}) \simeq \Lambda \simeq \mathbb{Z}^{2g}$.

Proof. Both of these are clear from the description of $A \simeq V/\Lambda$ from the previous proposition. Note that the universal covering space of A is V, which gives part 2. ∎

Definition 2.4. Let A, B be abelian varieties over k. A morphism $f : A \to B$ is called an *isogeny* if f is a surjective homomorphism with finite kernel.

Example 2.5. Multiplication by n is an isogeny $[n] : A \to A$ for any abelian variety A.

Proposition 2.6. [Mil86, 1.2] Given complex tori V/Λ, V'/Λ', holomorphic maps $V/\Lambda \to V'/\Lambda'$ sending $0 \mapsto 0$ are in bijection with $\mathbb{C}$-linear maps $\alpha : V \to V'$ such that $\alpha(\Lambda) \subseteq \Lambda'$.

Corollary 2.7. Any holomorphic map between abelian varieties preserving the identity is *automatically a group homomorphism.*

This is also true more generally for abelian schemes.

3 Structure theory, definition of CM abelian varieties (01/22/2024)

3.1 Structure of the category of abelian varieties

Remark 3.1. Given abelian varieties $A, B/k$, we say A is isogenous to B if there exists an isogeny $A \to B$, and write $A \sim B$. Perhaps surprisingly, $A \sim B$ is an equivalence relation in the category of abelian varieties. Reflexivity and transitivity are obvious. For symmetry, it is true that given any isogeny $f : A \to B$ there exists an isogeny $g : B \to A$ such that $g \circ f = [n]$, for some $n \in \mathbb{Z}$, although we won't prove this yet.

Theorem 3.2. *(Poincaré reducibility.)* Let A/k be an abelian variety and let $B \subseteq A$ be an abelian subvariety (i.e. a closed subvariety over k that is closed under the group operations and inherits the structure of an abelian variety). Then there exists another abelian subvariety $B' \subseteq A/k$ such that $B \cap B'$ is a finite set and $B + B' = A$, or equivalently $A \sim B \times B'$.

Proof. Exercise/read [Mum08, p.160], or [Mil10, Thm 2.12] for the case over $\mathbb{C}$. ■

Remark 3.3. Any reduced connected closed subgroup variety of an abelian variety is automatically abelian, since closed immersions are proper. In characteristic 0, all group varieties are automatically reduced, so the only requirement is connectedness in this case.

On the homework, you will also be asked to give an example of $B \subseteq A$ such that any complement B' as in the theorem necessarily has $B \cap B'$ nontrivial.

Definition 3.1. An abelian variety A/k is called *simple* if the only abelian subvarieties are $\{e\}$ or A itself.

Remark 3.4. The definition of simplicity depends on the field of definition k. Abelian varieties that are simple over a given field might not be simple after base change to a field extension.

Corollary 3.5. For any abelian variety A/k, we can write

$$A \sim \prod_{i=1}^{n} A_i^{r_i},$$

where each A_i/k is simple, $r_i \in \mathbb{Z}_{>0}$, and the A_i are pairwise nonisogenous.

Proof. Apply Poincaré reducibility inductively. ■

Definition 3.2. Let $A, B/k$ be abelian varieties. We write $\mathrm{Hom}(A,B)$ for the abelian group (equivalently, $\mathbb{Z}$-module) of homomorphisms from A to B; we do not require these to be isogenies. We write $\mathrm{Hom}^0(A,B) := \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Likewise, we write $\mathrm{End}(A) = \mathrm{Hom}(A,A)$ and $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Remark 3.6. We are implicitly working in the category of abelian varieties over some given field k, so when we refer to a homomorphism $A \to B$, we mean one defined over k. Therefore these Hom groups and endomorphism rings may get larger after base change. If we really want to emphasize that the homomorphisms must be defined over the base field, we will write $\mathrm{Hom}_k(A,B)$, or for endomorphisms $\mathrm{End}^0(A/k)$.

Remark 3.7. You can think of $\mathrm{End}^0(A)$ as the group obtained from $\mathrm{End}(A)$ by formally inverting all of the multiplication by n maps.

Remark 3.8. $\mathrm{Hom}^0(A,B)$ and $\mathrm{End}^0(A)$ depend only on the isogeny classes of A and B, since isogenies become isomorphisms after tensoring with $\mathbb{Q}$.

Corollary 3.9. If A/k is simple, then $\mathrm{End}^0(A)$ is a division algebra. More generally, with A decomposed as in Corollary 3.5, we have

$$\mathrm{End}^0(A) = \prod_{i=1}^{n} M_{r_i}(\mathrm{End}^0(A_i)).$$

Proof. The first part follows from the fact that for a simple abelian variety, the only endomorphisms are 0 and isogenies, and for any isogeny f on A, there exists g such that $g \circ f = [n]$ for some $n \in \mathbb{Z}$; then the inverse of f in $\mathrm{End}^0(A)$ is $[n]^{-1} \circ g$. The general decomposition follows from the fact that there are no nontrivial homomorphisms between the distinct simple factors A_i. ■

3.2 Definition of CM abelian varieties

Definition 3.3. An abelian variety A/k is said to have *complex multiplication* over k if $\mathrm{End}^0(A)$ contains a CM algebra E such that $[E : \mathbb{Q}] = 2 \dim A$. (A CM algebra is a finite product of CM fields.)

Remark 3.10. The main idea is that CM abelian varieties have unusually large endomorphism rings, which gives them special properties. Chief among these properties, as we will see over and over again later in these notes, is that the Tate modules $T_\ell(A)$ are rank 1 free E-modules. This fact alone will be responsible for a substantial portion of the CM theory.

A CM abelian variety has the "largest endomorphism ring possible," in the following sense:

Lemma 3.11. If A is a simple abelian variety over a field $k \subseteq \mathbb{C}$, then $[\mathrm{End}^0(A) : \mathbb{Q}] \leq 2 \dim A$.

Proof. Over $k \subseteq \mathbb{C}$, we identify a simple abelian variety A with a torus V/Λ. Then $\mathrm{End}^0(A)$ acts faithfully on $H_1(A(\mathbb{C}), \mathbb{Q}) \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^{2 \dim A}$, giving an embedding $\mathrm{End}^0(A) \hookrightarrow \mathrm{End}(\mathbb{Q}^{2 \dim A})$.

We show in general that if V is an n-dimensional vector space, then any subspace $W \subseteq \mathrm{End}(V)$ of dimension at least $n+1$ contains nonzero noninvertible elements. This proves the claim since $\mathrm{End}^0(A)$ is a division algebra. Choose any nonzero $v \in V$ and independent elements $\varphi_1, \dots, \varphi_{n+1} \in W$. Then the vectors $\varphi_1(v), \dots, \varphi_{n+1}(v)$ satisfy a nontrivial linear dependence, which pulls back to some nontrivial linear combination φ of the φ_i such that $\varphi(v) = 0$, so φ is not invertible. ∎

Remark 3.12. This lemma is false in positive characteristic, since, for example, supersingular elliptic curves have endomorphism rings of degree 4.

Example 3.13. Being CM and simple over $k \subseteq \mathbb{C}$ is equivalent to saying $\mathrm{End}^0(A)$ is a CM field of degree $2 \dim A$. If A is simple and CM, then an embedding $E \hookrightarrow \mathrm{End}^0(A)$ with $[E : \mathbb{Q}] = 2 \dim A$ forces $E = \mathrm{End}^0(A)$ by the previous lemma, and the CM algebra E must be a field since the only CM algebras that are division algebras are fields.

Conversely, suppose A is an abelian variety with $\mathrm{End}^0(A)$ a CM field of degree $2 \dim A$. Then A is automatically CM, and A is simple by Corollary 3.9, since otherwise we see explicitly that $\mathrm{End}^0(A)$ has zerodivisors.

Remark 3.14. We are not claiming if A has CM by a field (of degree $2 \dim A$), then it is simple—it's important that we've identified $E = \mathrm{End}^0(A)$ in the above example, since generally $\mathrm{End}^0(A)$ can be larger than E. A condition for simplicity that is determined solely by the CM field, without reference to $\mathrm{End}^0(A)$, is discussed later in Proposition 4.8.

For more general k, we can instead work with the Tate module $T_\ell(A)$ to mimic the first homology group; we have a similar faithful action $\mathrm{End}(A) \curvearrowright T_\ell(A) := \varprojlim A[\ell^n]$.

Example 3.15. Let E_1, E_2 be any nonisomorphic imaginary quadratic fields. We have embeddings $\mathcal{O}_{E_i} \hookrightarrow \mathbb{C}$ as lattices. Then

$$\mathrm{End}^0(\mathbb{C}/\mathcal{O}_{E_1} \times \mathbb{C}/\mathcal{O}_{E_2}) = E_1 \times E_2.$$

This is a CM algebra that is not a field, and it is degree 4 over $\mathbb{Q}$.

Example 3.16. Instead of taking two different fields, instead consider

$$\mathrm{End}^0((\mathbb{C}/\mathcal{O}_{E_1})^2) = M_2(E_1).$$

This contains many degree 4 CM fields; for example, given any $D \in \mathbb{Z}_{\neq 0}$, we have

$$\begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}^2 = DI,$$

so we realize $\mathbb{Q}(\sqrt{D}) \cdot E_1$ as a degree 4 CM subfield of $M_2(E_1)$. This illustrates that the CM algebra of an abelian variety might not be unique, not even abstractly up to isomorphism.

The ambiguity demonstrated by the previous example necessitates some rigidification of the data.

Definition 3.4. Let E be a CM field. An *abelian variety with CM by E* is a tuple (A, i), where A is an abelian variety of dimension $\frac{1}{2}[E : \mathbb{Q}]$ and $i : E \hookrightarrow \mathrm{End}^0(A)$ is an embedding of E as a subfield of $\mathrm{End}^0(A)$.

We will very often abbreviate "abelian variety with CM" to just CMAV. Don't forget that these objects include the data of the embedding $i : E \hookrightarrow \mathrm{End}^0$.

More generally, let $\mathcal{O}$ be an order in a CM field E. Then an abelian variety with CM by $\mathcal{O}$ is the data of a tuple (A, i) where A is an abelian variety of dimension $\frac{1}{2}[E : \mathbb{Q}]$ and $i : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is a choice of embedding of $\mathcal{O}$ into the endomorphism ring $\mathrm{End}(A)$.

The tuple (A, i) determines a CM type $\Phi \subseteq \mathrm{Hom}(E, \mathbb{C})$ on E associated to (A, i), via the following recipe.

Let (A, i) have CM by E. The choice of $i : E \hookrightarrow \mathrm{End}^0(A)$ determines a faithful representation $E \curvearrowright H_1(A(\mathbb{C}), \mathbb{Q})$, which gives $H_1(A(\mathbb{C}), \mathbb{Q}))$ the structure of a 1-dimensional E-vector space. By Hodge theory we have a canonical decomposition

$$H^1(A(\mathbb{C}), \mathbb{C}) = H^{0,1} \oplus H^{1,0}$$

where $H^{1,0} = \overline{H^{0,1}}$. We have

$$H^{0,1} = H^0(A(\mathbb{C}), \Omega^1) = \bigoplus \mathbb{C} \cdot dz_i,$$

where Ω^1 is the sheaf of holomorphic 1-forms and the z_i are the coordinate functions of $A \simeq \mathbb{C}^n/\Lambda$ near the identity. There is a natural identification $H^0(A(\mathbb{C}), \Omega^1) = T_e(A)^*$, so dualizing gives a canonical decomposition $H_1(A(\mathbb{C}), \mathbb{C}) = \mathrm{Lie}\, A(\mathbb{C}) \oplus \overline{\mathrm{Lie}\, A(\mathbb{C})}$. Since $H_1(A(\mathbb{C}), \mathbb{C}) \simeq H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ by the universal coefficient theorem, $H_1(A(\mathbb{C}), \mathbb{C})$ inherits the structure of an $2 \dim A$-dimensional E-module over $\mathbb{C}$. By standard algebraic number theory we have

$$H_1(A(\mathbb{C}), \mathbb{C}) \simeq E \otimes_{\mathbb{Q}} \mathbb{C} \simeq \bigoplus_{\varphi \in \mathrm{Hom}(E, \mathbb{C})} \mathbb{C}_\varphi$$

as E-modules, where $\mathbb{C}_\varphi$ denotes the space $\mathbb{C}$ treated as an E-module via multiplication

under a given embedding $\varphi : E \hookrightarrow \mathbb{C}$. In the decomposition $H_1(A(\mathbb{C}), \mathbb{C}) = \operatorname{Lie} A(\mathbb{C}) \oplus \overline{\operatorname{Lie} A(\mathbb{C})}$, the two factors are E-invariant—(anti)holomorphic vector fields certainly push forward to (anti)holomorphic vector fields under any automorphism—but swapped by complex conjugation c, so we conclude that our decomposition restricts to a decomposition

$$\operatorname{Lie} A(\mathbb{C}) = \bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi,$$

where $\Phi \subseteq \operatorname{Hom}(E, \mathbb{C})$ is a CM type of E. Except for the choice of embedding $i : E \hookrightarrow \operatorname{End}^0(A)$, all the identifications we have made are canonical, so Φ is uniquely determined by the tuple (A, i).

Definition 3.5. We say that the pair (E, Φ) is the *CM type* of (A, i).

If we want to define the CM type of an abelian variety over some $k \subseteq \mathbb{C}$, we should also specify the embedding $k \hookrightarrow \mathbb{C}$.

4 Classification of CMAVs (01/24/2024)

A recap: Given $A/\mathbb{C}$ and $i : E \hookrightarrow \operatorname{End}^0(A)$ for a CM field E, E acts on $\operatorname{Lie}(A(\mathbb{C}))$, and we may decompose this representation as $\bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$, where Φ is the CM type of (A, i).

4.1 Classification of CM abelian varieties by CM type

Remark 4.1. Given a CM field E with CM type Φ, recall that we defined an abelian variety $A(\mathbb{C}) = \mathbb{C}^\Phi/\mathcal{O}_E \simeq \operatorname{Lie} A(\mathbb{C})/\Lambda$ in Example 1.9. Then the CM type of this A is (E, Φ), where the embedding $i : E \hookrightarrow \operatorname{End}^0(A)$ is the obvious one induced by isomorphism $A(\mathbb{C}) = \mathbb{C}^\Phi/\mathcal{O}_E$.

Definition 4.1. An *isomorphism of CM types* $(E, \Phi) \to (E', \Phi')$ is a field isomorphism $\alpha : E \to E'$ such that $\varphi' \circ \alpha \in \Phi$ for all $\varphi' \in \Phi'$.

Proposition 4.2. Given a CM algebra E, we have a bijection between:

1. Abelian varieties (A, i) with CM by E, modulo E-equivariant isogenies; and
2. CM types (E, Φ) on E up to isomorphism.

The bijection is given by sending a CM type (E, Φ) to the class of abelian variety $\mathbb{C}^\Phi/\mathcal{O}_E$, and in the other direction sending a CM abelian variety to its CM type.

Proof. We first check that the map (2) $\to$ (1) defined by $(E, \Phi) \to \mathbb{C}^\Phi/\mathcal{O}_E$ is well-defined, i.e. if we have an isomorphism of CM types $\alpha : (E, \Phi) \to (E, \Phi')$, then we get an E-invariant isogeny (in fact, isomorphism) $\mathbb{C}^\Phi/\mathcal{O}_E \to \mathbb{C}^{\Phi'}/\mathcal{O}_E$. Since α induces a bijection $\alpha_* : \Phi \to \Phi'$, we have a commutative diagram

$$\begin{array}{ccccccc} \mathbb{C}^\Phi & & \xrightarrow{\quad\alpha_*\quad} & & & & \mathbb{C}^{\Phi'} \\ \uparrow & & & & & & \uparrow \\ \mathcal{O}_E & \hookrightarrow & E & \xrightarrow{\alpha} & E & \hookleftarrow & \mathcal{O}_E, \end{array}$$

which shows that we get an isomorphism $\mathbb{C}^\Phi/\mathcal{O}_E \simeq \mathbb{C}^{\Phi'}/\mathcal{O}_E$ where the respective $\mathcal{O}_E$-actions are identified, as desired.

Next, we must describe all possible (A, i). An arbitrary CMAV, say with with CM type (E, Φ), is of the form $A = \mathrm{Lie}(A)/\Lambda = \mathbb{C}^\Phi/\Lambda$, where Λ is some lattice, and we are given some embedding $E \hookrightarrow \mathrm{End}^0(A)$. Here, E acts on $\mathbb{C}^\Phi = \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$ appropriately, and Φ is the given CM type by definition (we defined it using the Lie algebra). The main idea is to embed an order of E into Λ, compatibly with the E-action. We also know that $\mathrm{End}^0(A)$, hence E, acts faithfully on $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$.

We claim that there exists $v \in \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ with trivial stabilizer in E. If E is a field, then any nonzero v works, and more generally:

Lemma 4.3. Let $E = E_1 \times \cdots \times E_n$ be a product of division algebras with an embedding $E \hookrightarrow \mathrm{End}(k^n)$ for an infinite field k. Then there exists $v \in k^n$ such that $x \cdot v = 0$ with $x \in E$ implies $x = 0$.

Proof. Let e_i be the i-th idempotent in the algebra E, i.e. the element whose i-th coordinate is 1 and all other coordinates are 0 in the coordinates $E = E_1 \times \cdots \times E_n$. Since E acts faithfully, $\ker(e_i) \subsetneq k^n$ is a proper subspace, so since k is infinite, $\bigcup_{i=1}^n \ker(e_i)$ is a proper subset of k^n (standard important linear algebra fact).

Choose any v in the complement of this set, and suppose $e = (a_i)_{i=1}^n$ satisfies $e \cdot v = 0$. If the i-th coordinate a_i is nonzero for some i, then $(a_i^{-1} e_i)(e) \cdot v = e_i \cdot v = 0$, which contradicts the choice of v. Hence $e = 0$, so E acts freely on the orbit of v. ■

Since $[E : \mathbb{Q}] = \dim_{\mathbb{Q}} \Lambda \otimes \mathbb{Q}$, we conclude any such choice of v yields an isomorphism $E \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ as E-modules, hence an embedding $\Lambda \subseteq E$ as a lattice that is commensurate with the ring of integers $\mathcal{O}_E$. This commensurability induces an E-equivariant isogeny $\mathbb{C}^\Phi/\Lambda \to \mathbb{C}^\Phi/\mathcal{O}_E$, so indeed the map (2) → (1) is surjective.

The composition (2) → (1) → (2) is the identity by Remark 4.1 (though we neglect to prove this remark), so we conclude that these maps are actually all bijections. ■

Remark 4.4. (Very vague, don't worry about this.) If A is an abelian variety, and we have $E' \hookrightarrow \mathrm{End}^0(A)$ with E' CM but $[E' : \mathbb{Q}] < 2 \dim A$, then in the moduli space of principally polarized abelian varieties $\mathscr{A}_g$, we get something positive dimensional, and the CM type is related to signatures on PEL type Shimura varieties. In contrast, the CM case gives a finite set of points.

If $\mathcal{O}$ is an order in a CM field E, recall that we can more generally refer to abelian varieties with CM by $\mathcal{O}$, which is the data of a tuple (A, i), where $i : \mathcal{O} \hookrightarrow \mathrm{End}(A)$. This also specifies CM by E if we tensor with $\mathbb{Q}$.

Corollary 4.5. Let $\mathcal{O} \subset E$ be an order in a CM algebra. There is a bijection between

- Abelian varieties (A, i) with CM by $\mathcal{O}$, where $i : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ for an order $\mathcal{O}$ of E, modulo $\mathcal{O}$-invariant *isomorphisms*; and
- Equivalence classes of tuples $(E, \Phi, \mathfrak{a})$, where (E, Φ) is a CM type, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$, and we define $(E, \Phi, \mathfrak{a}) \sim (E', \Phi', \mathfrak{a}')$ if we have an isomorphism of CM types $\alpha : (E, \Phi) \to (E', \Phi')$ such that $\alpha(\mathfrak{a}) = k\mathfrak{a}'$ for some $k \in (E')^\times$.

Corollary 4.6. For a given CM type (E, Φ), isomorphism classes of abelian varieties with CM by $\mathcal{O}_E$ are in natural bijection with the class group of E.

4.2 Primitive CM types

Definition 4.2. Let $E_0 \subseteq E$ be CM algebras.

1. Given a CM type (E_0, Φ_0), its *extension* (E, Φ) is given by setting
$$\Phi := \{\varphi : E \hookrightarrow \mathbb{C} : \varphi|_{E_0} \in \Phi_0\}.$$
This is always another CM type.
2. Conversely, given a CM type (E, Φ), its *restriction* is (E_0, Φ_0), where
$$\Phi|_{E_0} := \{\varphi|_{E_0} : \varphi \in \Phi\}.$$
However, (E_0, Φ_0) is not always a CM type; in fact, it is a CM type if and only if (E, Φ) is already an extension of a CM type on E_0.

Definition 4.3. We say a CM type (E, Φ) is *primitive* if there exist no proper sub-CM types (E_0, Φ_0) that extend to Φ (equivalently, such that $\Phi|_{E_0}$ is a CM type).

Proposition 4.7. Let E be a CM field. For any CM type (E, Φ), there exists a unique primitive CM type (E_0, Φ_0) such that $E_0 \subseteq E$ and $\Phi|_{E_0} = \Phi_0$.

Proof. [Mil10, Prop. 1.9]. ■

Proposition 4.8. There is a bijection between:

1. Simple CMAVs/$\mathbb{C}$ up to isogeny; and
2. Primitive CM types (E, Φ) up to isomorphism.

The bijection is given by sending (A, i) to $(\mathrm{End}^0 A, \Phi)$, where Φ is the CM type of (A, i).

Corollary 4.9. A CMAV is simple if and only if its CM is by a field with primitive CM type.

Example 4.10. Let (E, Φ) be an extension of (E_0, Φ_0). Then $\mathbb{C}^\Phi/\mathcal{O}_E$ is isogenous to $(\mathbb{C}^{\Phi_0}/\mathcal{O}_{E_0})^{[E:E_0]} \simeq (\mathbb{C}^{\Phi_0}/\mathcal{O}_{E_0}) \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E$.

5 Jacobian of the Fermat curves (01/26/24)

5.1 Wrapping up yesterday

A clarification from last time: whenever we are talking about isogeny or isomorphisms of CMAVs $(A, i), (A', i')$ with CM by E, E', we mean a pair (f, α), where $\alpha : E \to E'$ is an isomorphism and $f : A \to A'$ is an isogeny/isomorphism such that the following diagram commutes:

$$\begin{array}{ccc} E & \xhookrightarrow{i} & \mathrm{End}^0(A) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle f_*} \\ E & \xhookrightarrow{i'} & \mathrm{End}^0(A') \end{array}$$

(Note that f also induces an isomorphism $f_* : \mathrm{End}^0(A) \to \mathrm{End}^0(A')$ even if f is only an isogeny, since isogenies become isomorphisms after tensoring with $\mathbb{Q}$.) We will usually fix a single CM type (E, Φ), in which case the only ambiguity is the embedding $i : E \hookrightarrow \mathrm{End}^0(A)$. This is usually what we have in mind for the bijections in Proposition 4.2 and Corollaries 4.5 and 4.6.

We now prove Proposition 4.8 from last time.

Proof. We already have a general correspondence from Proposition 4.2, so we need only show that it restricts in the desired case.

If (E, Φ) is an extension of (E_0, Φ_0) with $E_0 \subsetneq E$, then A is not simple, since (proper nonzero) subset of A fixed by $E_0 \hookrightarrow \mathrm{End}^0(A)$ is also an abelian variety.

Conversely, suppose (E, Φ) is primitive. We want to show that $\mathbb{C}^\Phi/\mathcal{O}_E$ is simple. We sketch this; see [Mil10, Proposition 3.6]. Suppose $\mathbb{C}^\Phi/\mathcal{O}_E$ is not simple. Then:

1. Show that $A \simeq A_0^r$ for some simple A_0.[3] This follows from the fact that E is a field: if there were distinct factors in the decomposition, then we would not be able to find a CM *field* of degree $2 \dim A$ in $\mathrm{End}^0(A)$.

2. Show that if $r > 1$, then (E, Φ) is not primitive.

■

[3] An abelian variety whose Poincaré decomposition into simple factors only has one isogeny class is called *isotypic*.

5.2 Jacobians

We introduce Jacobians via an example. Let $C \subseteq \mathbb{P}^2_{\mathbb{C}}$ be the *Fermat curve* $C = V(X^p + Y^p = Z^p)$, described in homogeneous coordinates with p prime. This is smooth with genus $\frac{(p-1)(p-2)}{2}$. Its *Jacobian* $J(C)$ is the group variety whose functor of points parametrizes degree 0 divisor classes (equivalently, line bundles) on C. It is not obvious that this functor is representable, but in the complex case there is a nice explicit analytic construction.

For an arbitrary smooth curve C, we construct

$$J(C) = H^0(C, \Omega^1)^\vee / H_1(C, \mathbb{Z}).$$

Here, a class in $H_1(C, \mathbb{Z})$, represented by a loop γ, is identified with the functional on $H^0(C, \Omega^1)$ given by $\omega \mapsto \oint_\gamma \omega$, and the integral is independent of representative of the homology class.

How exactly does this parametrize line bundles? Let an element of $\mathrm{Pic}^0(C)$ be represented by some divisor of the form $\sum_i [p_i] - [q_i]$. Then to this divisor we associate the functional $\omega \mapsto \sum_i \int_{p_i}^{q_i} \omega$. This integral *is not* well defined *a priori*, since it depends on the choice of path, but the only ambiguities occur from integrating around loops. So it *is* a well-defined functional modulo integration around loops, i.e. as an element of $H^0(C, \Omega^1)^\vee / H_1(C, \mathbb{Z})$. Moreover, this element is independent of the choice of representative divisor.

Theorem 5.1. $J(C)$ is a CM abelian variety, where C is the Fermat curve above.

In general, if C is a smooth curve, then $J(C)$ is an abelian variety—clear from its description as a torus once we know that this construction is actually algebraic—but it might not be CM.

We momentarily specialize to the case $p = 3$. The curve $X^3 + Y^3 = Z^3$ is a genus 1 elliptic curve, choosing identity element $(0 : 0 : 1)$. The group of third roots of unity μ_3 acts on this curve by $(X : Y : Z) \mapsto (\zeta_3^i X : Y : Z)$, and this preserves the identity element, so we conclude that we have CM by $\mathbb{Q}(\zeta_3)$. (An elliptic curve is naturally its own Jacobian.)

5.3 Constructing CMAVs for cyclotomic fields via the Fermat curve

For concreteness, we set $\zeta_p = e^{2\pi i/p}$ to give a fixed embedding of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$. In the case of a general Fermat curve $C = V(X^p + Y^p = Z^p)$, $\mu_p \times \mu_p$ acts on C by

$$(X : Y : Z) \mapsto (\zeta_p^i X : \zeta_p^j Y : Z)$$

so we conclude we have an embedding $\mu_p \times \mu_p \hookrightarrow \mathrm{End}(J(C))$. Fact: working in the affine coordinate chart with $x = \frac{X}{Z}, y = \frac{Y}{Z}$, the 1-forms

$$\omega_{r,s} := \frac{1}{p} x^r y^s \frac{dx^p}{x^p y^p} = x^{r-1} y^{s-1} \frac{dx}{y^{p-1}} = -x^{r-1} y^{s-1} \frac{dy}{x^{p-1}}$$

where $1 < r, s \leq p-1$ are integers with $r + s \leq p - 1$, form a $\mathbb{C}$-basis of $H^0(C, \Omega^1)$. This condition on a pair of integers (r, s) will show up a lot in the remainder of this section, so for brevity we define:

Definition 5.1. We say that a pair of integers (r, s) is *admissible* if $1 \leq r, s \leq p-1$ and $r + s \leq p - 1$.

The $\mu_p \times \mu_p$ action sends

$$(\zeta_p^i, \zeta_p^j) : \omega_{r,s} \mapsto \zeta_p^{ir+js}\omega_{r,s}.$$

(no restrictions on the pair $(i, j) \in \mathbb{Z}/p\mathbb{Z}$). That is, these basis elements are eigenforms for the $\mu_p \times \mu_p$-action. Since $\mu_p \times \mu_p$ acts on each form $\omega_{r,s}$ by a different character, this shows that these forms are linearly independent, which gives a proof that these forms do indeed constitute a basis of $H^0(C, \Omega^1_C) \simeq \mathbb{C}^{(p-1)(p-2)/2}$ once we know:

Lemma 5.2. There are exactly $p - 2$ equivalence classes of admissible pairs (r, s), each of size $(p - 1)/2$, defined by the relation $(r, s) \simeq (r', s')$ iff there exists $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $mr \equiv r' \bmod p$ and $ms \equiv s' \bmod p$. Hence there are $(p - 1)(p - 2)/2$ different admissible pairs in total.

Proof. Every equivalence class of admissible pairs has a unique representative of the form $(1, s)$ with $1 \leq s \leq p - 2$. For such a representative, there are exactly $(p - 1)/2$ values of $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ for which (m, ms) is congruent to an admissible pair mod p. In fact, m satisfies this property if and only if $-m$ does not satisfy it, i.e. such m constitute a full set of coset representatives for $\{\pm 1\} \bmod p$. ■

Example 5.3. Let $p = 5$. The three equivalence classes of admissible pairs in Lemma 5.2 are

$$\{(1, 1), (2, 2)\}$$
$$\{(1, 2), (3, 1)\}$$
$$\{(1, 3), (2, 1)\}.$$

Corollary 5.4. The equivalence classes of admissible pairs $[(r, s)]$ yield CM types on $\mathbb{Q}(\zeta_p)$: identifying $\mathrm{Hom}(\mathbb{Q}(\zeta_p), \mathbb{C}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ via $(\zeta_p \mapsto \zeta_p^n) \mapsto n \bmod p$, the class $[(r, s)]$ corresponds to the CM type $\Phi = \{r' : (r', s') \in [(r, s)]\}$.

Proof. WLOG take $(r, s) = (1, s)$. Complex conjugation sends $n \mapsto -n$ under the identification $\mathrm{Hom}(\mathbb{Q}(\zeta_p), \mathbb{C}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, so a set Φ is a CM type if it corresponds to a complete set of coset representatives for $\{\pm 1\}$. But we've already observed that $\{m : (m, ms) \in [(1, s)]\}$ satisfies this property. ■

Remark 5.5. We are not claiming that this construction yields *all* CM types on $\mathbb{Q}(\zeta_p)$. In fact, we miss most of them: there are $2^{(p-1)/2}$ CM types on $\mathbb{Q}(\zeta_p)$, but the construction only gives $p - 2$ of them.

Let (r, s) be an admissible pair. We can construct a curve $C_{r,s}$ equipped with a map $C \to C_{r,s} : (x, y) \mapsto (x^p, x^r y^s)$. More specifically, this is the unique smooth curve with

function field $\mathbb{C}(u,v)/(v^p - u^r(1-u)^s)$. The map $C \to C_{r,s}$ induces a map $J(C_{r,s}) \to J(C)$.

Proposition 5.6. $C_{r,s}$ is a curve of genus $(p-1)/2$. Moreover, $C_{r,s} \simeq C_{r',s'}$ if and only if $(r,s) \simeq (r',s')$ as admissible types. In particular, $C_{r,s}$ is isomorphic to a unique curve of the form $C_{1,s'}$.

Since we have a concrete description of $J(C_{r,s}) = H^0(C_{r,s}, \Omega_{C_{r,s}})^\vee / H_1(C_{r,s}, \mathbb{Z})$, hence a natural identification $H^0(C_{r,s}, \Omega_{C_{r,s}})^\vee \simeq \mathrm{Lie}(J(C_{r,s}))$, we can explicitly determine the CM type on this abelian variety via the action on differentials described previously. Let μ_p act on C via $\zeta_p \cdot (X : Y : Z) = (\zeta_p X : Y : Z)$ (only using half of the $\mu_p \times \mu_p$-action). We also have action of μ_p on $C_{r,s}$ via $\zeta_p \cdot (u,v) = (u, \zeta_p^r v)$, which is compatible with the map $C \to C_{r,s}$. These actions descend to compatible actions by $\mathbb{Z}[\zeta_p]$ on the respective Jacobians, hence CM by $\mathbb{Q}(\zeta_p)$ on $J(C_{r,s})$ since the dimensions are correct.

By our computation of the action on differentials, the eigenvalues of ζ_p on $H^0(C, \Omega^1_C)$ are $\{\zeta_p^r : 1 \le r \le p-2\}$, and each eigenvalue has multiplicity $(p-1)/2$. Note that $\dim_{\mathbb{C}} H^0(C, \Omega^1_C) = (p-1)(p-2)/2$, but $\dim_{\mathbb{C}} H^0(C_{r,s}, \Omega^1_{C_{r,s}})$ is only $(p-1)/2$, so the image of the pullback map $H^0(C_{r,s}, \Omega^1_{C_{r,s}}) \hookrightarrow H^0(C, \Omega^1_C)$ is a proper $\mathbb{Q}(\zeta_p)$-subrepresentation. (This map is injective because it is induced by a finite separable morphism of curves.) To determine the CM type of $J(C_{r,s})$, we therefore must determine precisely what this subrepresentation is.

Proposition 5.7. As a subspace of $H^0(C, \Omega^1_C)$, $H^0(C_{r,s}, \Omega^1_{C_{r,s}})$ has basis given by $\{\omega_{r',s'} : (r',s') \sim (r,s)\}$, ranging over all admissible pairs (r',s') equivalent to (r,s).

Proof. See [Lan83, Theorem 7.2]. ∎

Corollary 5.8. $J(C_{r,s})$ has CM by $\mathbb{Q}(\zeta_p)$ with CM type $\Phi = \{r' : (r',s') \simeq (r,s)\} \subset (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathrm{Hom}(\mathbb{Q}(\zeta_p), \mathbb{C})$, with notation as in Corollary 5.4.

Proof. The eigenvalue of the action of ζ_p on $\omega_{r,s}$ is ζ_p^r, so by Proposition 5.7, the spectrum of this operator on $H^0(C_{r,s}, \Omega^1_{C_{r,s}})$, hence also on $H^0(C_{r,s}, \Omega^1_{C_{r,s}})^\vee$, is $\{\zeta_p^{r'} : (r',s') \simeq (r,s)\}$. This precisely determines the CM type to be $\Phi = \{r' : (r',s') \simeq (r,s)\}$. ∎

This also shows how to find the CM type on $J(C)$ as well, since Proposition 5.7 implies that $H^0(C, \Omega^1_C)$ is the direct sum of the various $H^0(C_{r,s}, \Omega^1_{C_{r,s}})$ ranging over admissible equivalence classes $[(r,s)]$. In particular, $\prod_{[(r,s)]} J(C_{r,s}) \to J(C)$ is an isogeny, since the images of differentials of the $J(C_{r,s})$ form a direct sum decomposition of $\mathrm{Lie}(J(C))$.

Remark 5.9. The $J(C_{r,s})$ might not be simple. On Homework 1, you should find a case where the CM type of $J(C_{r,s})$ is non-primitive.

For more details and discussion of this construction, see [Lan83], especially §1.6 and §1.7. This includes discussion of the case of the Fermat curve $X^N + Y^N = Z^N$ and CM by $\mathbb{Q}(\zeta_N)$ when N is not necessarily prime. However, Lang's discussion of the Jacobian at the end of §1.7 is very brief.

6 Rosati involution (01/29/2024)

6.1 Rosati involution

Let $A/\mathbb{C} = V/\Lambda$ with Riemann form $\psi : \Lambda \times \Lambda \to \mathbb{Z}$.

Definition 6.1. The *Rosati involution* is the unique involution on $\mathrm{End}^0(A)$, usually denoted by a superscript †, satisfying

$$\psi(\alpha x, y) = \psi(x, \alpha^\dagger y)$$

for all $\alpha \in \mathrm{End}^0(A)$ and all $x, y \in \Lambda$.

Remark 6.1. A Riemann form gives a map $\psi : \Lambda \to \Lambda^\vee$, which becomes an isomorphism after tensoring with $\mathbb{Q}$. The Rosati involution yields, for any $\alpha \in \mathrm{End}^0(\alpha)$, a commutative diagram

$$\begin{array}{ccc} \Lambda \otimes \mathbb{Q} & \xrightarrow{\psi} & \Lambda^\vee \otimes \mathbb{Q} \\ \downarrow{\scriptstyle \alpha^\dagger} & & \downarrow{\scriptstyle \alpha^\vee} \\ \Lambda \otimes \mathbb{Q} & \xrightarrow{\psi} & \Lambda^\vee \otimes \mathbb{Q} \end{array}$$

This gives a direct formula for the Rosati involution as

$$\alpha^\dagger = \psi^{-1} \circ \alpha^\vee \circ \psi$$

and shows that it exists and is unique.
In a more general algebraic setting over an arbitrary field k, we will have a similar description of the Rosati involution based on a *polarization* $\psi : A \to A^\vee$.

Lemma 6.2. Let $V = T_e(A(\mathbb{C}))$, and let H be the positive definite Hermitian form on V induced by a Riemann form $\psi : \Lambda \times \Lambda \to \mathbb{Z}$; note that $\mathrm{End}^0(A(\mathbb{C}))$ acts faithfully on V. Then the Rosati involution associated to ψ also defines an adjoint involution on $\mathrm{End}^0(A(\mathbb{C}))$. with respect to H.

Proof. There isn't really much to do here besides recall definitions: H is defined by $H(v, w) = \psi(iv, w) + i\psi(v, w)$, where ψ is extended to $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \simeq V_{\mathbb{R}}$ as real vector spaces. Then for $\alpha \in \mathrm{End}^0(A)$, we have

$$\begin{aligned} H(\alpha v, w) &= \psi(\alpha(iv), w) + i\psi(v, w) \\ &= \psi(iv, \alpha^\dagger w) + i\psi(v, \alpha^\dagger w) \\ &= H(v, \alpha^\dagger w). \end{aligned}$$

■

Proposition 6.3. Let $\mathrm{Tr} : \mathrm{End}^0(A) \to \mathbb{Q}$ be the trace map, treating elements of $\mathrm{End}^0(A)$ as $\mathbb{Q}$-linear endomorphisms on $H_1(A, \mathbb{Q})$. Then $\mathrm{Tr}(\alpha^\dagger \circ \alpha) > 0$ for all nonzero $\alpha \, \mathrm{End}^0(A)$.

Proof. See also the first few pages of [Lan83].

Let $V = T_e(A(\mathbb{C}))$ and let $H : V \times V \to \mathbb{C}$ be the positive definite Hermitian form associated to ψ. The trace of an element of $\mathrm{End}^0(A)$ on V as an $\mathbb{R}$-endomorphism is the same as its trace as an operator on $H_1(A, \mathbb{Q})$ as a $\mathbb{Q}$-endomorphism, so it suffices to show that that $\mathrm{Tr}(\alpha^\dagger \circ \alpha) > 0$ treating $\alpha^\dagger \circ \alpha$ as an endomorphism of V.

Note that any $\alpha \in \mathrm{End}^0(A)$ is in fact $\mathbb{C}$-linear on $V = \mathbb{C}^g$, since by definition endomorphisms of A must respect the complex structure. Hence it makes sense to say that $\alpha^\dagger \circ \alpha$ is a self-adjoint operator on V with respect to the Hermitian form H. By the spectral theorem, we conclude that $\alpha^\dagger \circ \alpha$, treated as a complex endomorphism, is diagonalizable with real eigenvalues. Moreover, if v is a λ-eigenvector of $\alpha^\dagger \circ \alpha$, then

$$0 \leq H(\alpha v, \alpha v) = H((\alpha^\dagger \circ \alpha)v, v) = \lambda H(v, v),$$

so $\lambda \geq 0$, and if $\alpha \neq 0$ at least one eigenvalue is positive.

This tells us that $\alpha^\dagger \circ \alpha$ has positive trace as a $\mathbb{C}$-linear operator. If we instead treat $\alpha^\dagger \circ \alpha$ as an $\mathbb{R}$-linear operator on $V_\mathbb{R} \simeq \mathbb{R}^{2g}$, by restricting scalars, the trace gets multiplied by 2.[4] Therefore the trace is also positive as an $\mathbb{R}$-linear operator. ■

Fact: on a CM algebra E, there exists a unique positive involution, given by complex conjugation on each factor. Therefore, for any simple CMAV A, we may identify $\mathrm{End}^0(A)$ with a CM algebra with Rosati involution given by conjugation. Then we have

$$\psi(\alpha x, y) = \psi(x, c(\alpha) y).$$

If A is not necessarily simple, then for any given Riemann form ψ there exists a CM algebra $E \subseteq \mathrm{End}^0(A)$ with $[E : \mathbb{Q}] = 2 \dim A$ such that $E^+ = E$.

Lemma 6.4. Let $A = V/\Lambda$ be simple,

$$\psi : \Lambda \otimes_\mathbb{Z} \mathbb{Q} \times \Lambda \otimes_\mathbb{Z} \mathbb{Q} \to \mathbb{Q}$$

be a nondegenerate skew-symmetric form such that $\psi(\alpha x, y) = \psi(x, c(\alpha) y)$ for all $\alpha \in E \simeq \mathrm{End}^0(A)$. Then $\psi(x, y) = \mathrm{tr}_{E/\mathbb{Q}}(\xi c(x) y)$ for all $x, y \in E \simeq \Lambda\mathbb{Q}$, where $\xi \in E$ is a totally imaginary element, i.e. $c(\xi) = -\xi$.

6.2 Data of CMAVs with polarizations

Definition 6.2. Let (A, i, ψ) be a tuple consisting of the data of an abelian variety A, an embedding $E \hookrightarrow \mathrm{End}^0(A)$ for a CM algebra E, and a Riemann form ψ such that $E^\dagger = E$

[4] In general, let L/K be a finite field extension, let V be an L-vector space, say of dimension n, and let $\alpha \in \mathrm{End}_L(V)$. Denote by $\mathrm{Tr}_L(\alpha)$ the usual trace of α as an L-linear endomorphism on V, and denote by $\mathrm{Tr}_K(\alpha)$ the trace we get by instead treating α as a K-linear endomorphism on $V \simeq K^{n[L:K]}$. Then $\mathrm{Tr}_K(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_L(\alpha))$, where $\mathrm{Tr}_{L/K} : L \to K$ is the field-theoretic trace map.

with respect to the Rosati involution induced by ψ. We define $(A, i, \psi) \sim (A', i', \psi')$ if there exists an isomorphism $f : A \to A, \alpha : E \to E'$ making all diagrams relevant to these data commute.

To such a tuple (A, i, ψ), we associate a tuple $(E, \Phi, \mathfrak{a}, \xi)$ consisting of a CM type (E, Φ), a fractional ideal $\mathfrak{a} \subseteq E$, and a totally imaginary element $\xi \in E$. We already know how to get a CM type from (A, i). Pick some $v \in H_1(A, \mathbb{Q})$ such that $E \to H_1(A, \mathbb{Q}) : a \mapsto a \cdot v$ is an isomorphism (see the proof of Theorem 4.2). Let $\mathfrak{a} \subset E$ be the lattice identified with Λ under this isomorphism, and let $\xi \in E^\times$ such that $c(\xi) = -\xi$. The choice of v ambiguous up to multiplication by $E^\times$, and a different choice sends $v \mapsto a^{-1}v$ for some $a \in E^\times$, yielding an isomorphism

$$(E, \Phi, \mathfrak{a}, \xi) \simeq (X, \Phi, a\mathfrak{a}, \xi/a(ca)).$$

6.3 Every CMAV is defined over $\overline{\mathbb{Q}}$

Proposition 6.5. Let $k = \overline{k} \hookrightarrow \mathbb{C}$. The functor

$$\begin{aligned} \mathsf{AV}_k &\to \mathsf{AV}_{\mathbb{C}} \\ A &\mapsto A_{\mathbb{C}} \end{aligned}$$

(from the category of abelian varieties over k to the category of abelian varieties over $\mathbb{C}$) is fully faithful, and its essential image contains all CMAVs over $\mathbb{C}$. In particular, taking $k = \overline{\mathbb{Q}}$, all CMAVs are defined over $\overline{\mathbb{Q}}$.

This allows us to port a lot of the theory we have developed over $\mathbb{C}$ to $\overline{\mathbb{Q}}$.

Proof. The key observation is that we get a map $A(k) \hookrightarrow A(\mathbb{C})$ such that $A(k)_{\text{tors}} \simeq A(\mathbb{C})$, since the equations cutting out torsion elements (of any given order n) are algebraic with coefficients in k.

Faithfulness: Suppose we have two homomorphisms $f, g : A \to A'$ such that $f_{\mathbb{C}} = g_{\mathbb{C}}$. Hence in particular $f_{\mathbb{C}}|_{A(\mathbb{C})_{\text{tors}}} = g_{\mathbb{C}}|_{A(\mathbb{C})_{\text{tors}}}$. By the previous observation, this implies $f|_{A(k)_{\text{tors}}} = g|_{A(k)_{\text{tors}}}$. Then the claim that $f = g$ follows if we can show that $A(k)_{\text{tors}}$ is Zariski dense in A, which we can do by applying the following lemma for any prime number ℓ.

Lemma 6.6. Let A be an abelian variety over an algebraically closed field k. Then for any prime $\ell \neq \text{char}(k)$, $A[\ell^\infty]$ is Zariski dense in A. (This should be read as "the only closed subscheme of A containing all of the closed subschemes $A[\ell^m], m \in \mathbb{Z}$, is A itself.")

We state this in the general algebraic setting since it is not much harder to prove there—however, we will use the fact that $A[\ell^m] \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^{2\dim A}$. We will get to this later, but this fact is clear when working in the analytic setting over $\mathbb{C}$, so we still obtain a complete proof of Proposition 6.5.

Proof. Let B be the Zariski closure of $A[\ell^\infty]$ with its reduced induced structure. Then B is proper and reduced. Moreover, we claim B is a subgroup variety of A. To show this, we need to show that the group operations factor through B, e.g. $m|_{B\times B} : B \times B \to A$ factors through $B \hookrightarrow A$. Let $g, h \in B(k)$; then any open neighborhoods $U_1 \ni g$, $U_2 \ni h$ in A intersect $A[\ell^\infty](k)$ since B is the closure of this set. Let V be an open neighborhood of $g + h \in A(k)$; then the preimage $m^{-1}(V)$ is open and therefore contains a product of neighborhoods $U_1 \times U_2$ as above. Choosing any two ℓ^∞-torsion points $z_1, z_2 \in U_1, U_2$ we conclude that $z_1 + z_2$ is an ℓ^∞-torsion point in V. But this shows that any neighborhood of $g + h$ contains an ℓ^∞-torsion points, hence by definition $g + h \in B(k)$. A similar argument shows that B is preserved by inversion, and the fact that the unit map factors through B is clear.

Hence B is a proper reduced subgroup variety of A, so the connected component of its identity B^0 is an abelian subvariety. We claim that $A[\ell^\infty] \subseteq B^0$. Since B is finite type, it has a finite number n of connected components. Suppose $e = v_\ell(n)$ is the maximum power of ℓ dividing n; then $\ell^e A[\ell^\infty]$ is contained in B^0, since the only ℓ^∞-torsion elements of the finite group B/B^0 have order dividing ℓ^e. But $A[\ell^\infty]$ is an ℓ-divisible group, so in fact $A[\ell^\infty] = \ell^e A[\ell^\infty] \subseteq B^0$ too.

For $\ell \neq \mathrm{char}(k)$ and any abelian variety A', we have $A'[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2\dim A'}$. Therefore the fact that $B^0 \supseteq A[\ell]$ implies that $\dim B^0 \geq \dim A$. But A is connected and B^0 is a subvariety of A, whence $B^0 = B = A$. ∎

Remark 6.7. This proof can be easily modified to prove Lemma 6.6 for $\ell = \mathrm{char}(k)$ if A is assumed to be an ordinary abelian variety.

Fullness: We apply descent theory. We can write[5] $k = \mathbb{C}^{\mathrm{Aut}(\mathbb{C}/k)}$. Let $f : A_\mathbb{C} \to A'_\mathbb{C}$ be any homomorphism over $\mathbb{C}$; we wish to show that this actually comes from a homomorphism over k. For $\tau \in \mathrm{Aut}(\mathbb{C}/k)$ we consider the map ${}^\tau f : A_\mathbb{C} \to A'_\mathbb{C}$ given by the map $\tau \circ f \circ \tau^{-1}$. By descent theory, f comes from a morphism over k if and only if ${}^\tau f = f$ for all τ. This is again true if and only if ${}^\tau f$ and f agree on the dense subset $(A_\mathbb{C})_{\mathrm{tors}}$, but again all points of these subgroups are defined over $k = \overline{k}$, so these maps are the same.

We'll finish the claim about CMAVs next time. ∎

7 Fields of definition (01/31/2024)

7.1 CMAVs in the essential image

Suppose A is a (not necessarily abelian) variety over $\mathbb{C}$. Then there exists a ring R, with $\mathbb{Q} \supseteq R \supsetneq \mathbb{C}$ and R finitely generated $\mathbb{Q}$-algebra, such that A is defined over R as a scheme, i.e. there exists an R-scheme $\mathscr{A}$ such that $\mathscr{A}_\mathbb{C} \simeq A$. This is not very mysterious: A is finite type over $\mathbb{C}$, so there are finitely coefficients involved in the polynomials cutting it out. We can take R to be generated by these polynomials and then use the same equations as before for $\mathscr{A}$. We say that $\mathscr{A}$ is obtained from A by "spreading out."

[5] If $\alpha, \beta \in \mathbb{C}$ are two transcendental elements over k, then a Zorn's lemma argument shows that the automorphism on $k[\alpha, \beta]$ swapping the two elements extends to $\mathbb{C}$.

Proposition 7.1. With notation as above, suppose that A is an abelian variety over $\mathbb{C}$. Then there exists a finitely generated $R/\mathbb{Q}$, a proper group scheme $\mathscr{A}/R$, and nonempty open $U \subseteq \operatorname{Spec} R$ such that $\mathscr{A}_U/U$ is an abelian scheme.

Proof. The morphisms defining the group laws again involve only finitely many coefficients, and we can take R large enough to include all of them. Therefore we can spread out to find $\mathscr{A}/R$ with the structure of a group scheme such that $\mathscr{A}_{\mathbb{C}} \simeq A$.

Since we can originally write $A/\mathbb{C}$ as a closed subvariety of $\mathbb{P}^N_{\mathbb{C}}$ for some N, we can use the same equations to write $\mathscr{A}$ as a closed subscheme of $\mathbb{P}^N_R$. In particular, $\mathscr{A}/R$ is projective, hence proper. Since properness is stable under base change, this will remain true if we later restrict to some open $U \subseteq \operatorname{Spec} R$.

For connectedness on geometric fibers, we have a morphism $\mathcal{O}_{\operatorname{Spec} R} \to \pi_* \mathcal{O}_{\mathscr{A}}$. A fiber over a geometric point $\overline{s} \hookrightarrow \operatorname{Spec} R$ is connected if and only if this morphism is an isomorphism on the stalk at $\overline{s}$. But $\overline{s} = \operatorname{Spec} k'$ for some algebraically closed $k' \subseteq \mathbb{C}$, and a k'-scheme is (geometrically) connected if and only if it is (geometrically) connected over $\mathbb{C}$: one definition of geometric connectedness is that the scheme is connected after base change to any field extension, not necessarily an algebraic field extension.

Note that if $\mathscr{A}$ is an R-group, then $\mathscr{A}_U$ is a U-group for any open $U \subseteq \operatorname{Spec} R$. Since $\mathscr{A}$ is smooth on the generic fiber, and smoothness is an open condition, we may choose some $U \subseteq \operatorname{Spec} R$ so that $\mathscr{A}_U$ is smooth over U, and $\mathscr{A}_U/U$ still satisfies all of the other criteria for being an abelian scheme.

See also [Mil86, Remark 20.9]. ∎

We finish the proof of Proposition 6.5.

Essential image: Let $A/\mathbb{C}$ be an arbitrary CM abelian variety defined over $\mathbb{C}$. Spread out A to an abelian variety over some open $U \subseteq \operatorname{Spec} R$, with $k \subseteq R \subset \mathbb{C}$ and R finitely generated over k. We may assume $k = \overline{k}$. Letting $\mathcal{O} := \operatorname{End}(A/\mathbb{C})$, we may enlarge R and shrink U sufficiently to have $\mathcal{O} \subseteq \operatorname{End}(\mathscr{A}_U/U)$ too, since $\operatorname{End}(\mathscr{A}_s)$ is always finitely generated[6] over $\mathbb{Z}$. Pick a geometric point $s : \operatorname{Spec} k \to U$; then $B := \mathscr{A}_s$ is an abelian variety over k that base changes to A, so we have $B(k)_{\text{tors}} = A(\mathbb{C})_{\text{tors}}$.

B/k is CM with the same CM type as A; its endomorphism ring is large enough since we took U appropriately, and we have an isomorphism $\operatorname{Lie}(B_{\mathbb{C}}) \simeq \operatorname{Lie}(A)$. By Proposition 4.2, this means that $B_{\mathbb{C}}$ is isogenous to A. Therefore, there exists a finite subvariety $G \subset B_{\mathbb{C}}$ such that $B_{\mathbb{C}}/G = A$. But such G is torsion, so $B(k)_{\text{tors}} = A(\mathbb{C})_{\text{tors}}$ implies that G is defined over k, too, so we may descend $B_{\mathbb{C}}/G$ to a quotient[7] of B defined over k.

[6] We will eventually prove this in full detail in Theorem 24.1, but it is easy to show finite generation in the analytic category by using the fact that morphisms between abelian varieties are in correspondence with maps between lattices.

[7] We have not defined how to take a quotient of a group scheme. In general, quotients of group schemes are subtle and do not always work (instead requiring algebraic spaces), but the case of quotienting an abelian variety by a finite subgroup behaves as it should. We'll discuss this in more detail after we learn about fpqc descent.

7.2 Reflex fields

Remark 7.2. We can alternatively define a CM type as a subset of $\mathrm{Hom}(E, \overline{\mathbb{Q}})$ rather than $\mathrm{Hom}(E, \mathbb{C})$—it does not matter which complex conjugation we choose on $\overline{\mathbb{Q}}$, since all choices become the same on E if E is a CM algebra.

Definition 7.1. Given a CM type (E, Φ), its reflex field $E^* \subseteq \overline{\mathbb{Q}} \subset \mathbb{C}$ is the fixed field of the subgroup

$$\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \sigma\Phi = \Phi\}$$

.

Fact: if E is a field, then E^* is contained in the Galois closure of E in $\overline{\mathbb{Q}}$. By definition, E^* is a field even if E is not a field.

Lemma 7.3. [Mil10, Propositions 1.16, 1.18] Let (E, Φ) be a CM type with reflex field E^*.

1. E^* is the subfield of $\overline{\mathbb{Q}}$ generated by $\sum_{\varphi\in\Phi} \varphi(a)$, ranging over all $a \in E$.
2. E^* is a CM field.
3. If $(E, \Phi) = \prod_{1\le i\le m}(E_i, \Phi_i)$, then E^* is the compositum $E_1^* \cdots E_m^*$.
4. If (E_1, Φ_1) is an extension of (E, Φ), then $E_1^* = E^*$.

Proof. Omitted; read Milne. ∎

Since E^* is a CM field, you may ask whether there is a natural CM type on it arising from the CM type (E, Φ). We'll talk about this later.

Proposition 7.4. Let A/k with $k \hookrightarrow \mathbb{C}$. Assume $A_{\overline{k}}$ is a CMAV with CM type (E, Φ) and reflex field E^*.

1. If $E \subseteq \mathrm{End}^0(A/k)$, then $E^* \subseteq k$.
2. If $E^* \subseteq k$ and $A_{\overline{k}}$ is simple, then $E \subseteq \mathrm{End}^0(A/k)$.

Proof. 1. E acts on $\mathrm{Lie}\, A$, which is a k-vector space. By the definition of the CM type on A, we have $\mathrm{Lie}\, A_{\mathbb{C}} \simeq \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$ as E-representations. Given $a \in E$, we can compute the trace of its action on $\mathrm{Lie}\, A$ after base changing to $\mathbb{C}$, so we conclude that

$$\mathrm{Tr}(a|\,\mathrm{Lie}\, A_{\mathbb{C}}) = \sum_{\varphi\in\Phi} \varphi(a).$$

But this trace comes from a k-vector space endomorphism, so it must lie in k. Such traces generate E^* by part 1 of Lemma 7.3, so $E^* \subseteq k$.

2. By Example 3.13, simplicity of $A_{\overline{k}}$implies that E is a field and that $E = \mathrm{End}^0(A_{\overline{k}})$. The group $\mathrm{Gal}(\overline{k}/k)$ acts on $\mathrm{End}^0(A_{\overline{k}})$, so we must show this action is trivial, so that $\mathrm{End}^0(A_{\overline{k}}) = \mathrm{End}^0(A/k)$.

   Any $\sigma \in \mathrm{Gal}(\overline{k}/k)$ fixes k, so it also fixes E^*; by the definition of the reflex field, this means that $\sigma \circ \Phi = \Phi$.

   We know $\mathrm{Lie}\, A_{\overline{k}} \simeq \bigoplus_{\varphi\in\Phi} \overline{k}_\varphi$ as E-representations. Therefore, given $\sigma \in \mathrm{Gal}(\overline{k}/k)$, the isomorphism $\sigma : \mathrm{Lie}\, A_{\overline{k}} \to \mathrm{Lie}\, A_{\overline{k}}$ induced by σ corresponds to an isomorphism $\sigma : \bigoplus_{\varphi\in\Phi} \overline{k}_\varphi \to \bigoplus_{\varphi\in\Phi} \overline{k}_\varphi$. Hence σ induces an automorphism of the CM type (E, Φ), so there exists $\alpha \in \mathrm{Aut}(E)$ such that $\Phi = \sigma\circ\Phi = \Phi\circ\alpha$. Letting E_0 be the fixed subfield of α, it follows that the restriction $(E_0, \Phi|_{E_0})$ is a CM type; see [Mil10, Proposition 1.9]. But (E, Φ) is primitive, so we must have $\alpha = \mathbf{id}_E$.

■

Corollary 7.5. There are no CMAVs defined over $\mathbb{Q}$.

Remark 7.6. When we say that a CMAV A is defined over $\mathbb{Q}$, we specifically mean that $\mathrm{End}^0_{\mathbb{Q}}(A)$ is already large enough to admit an embedding $E \hookrightarrow \mathrm{End}^0_{\mathbb{Q}}(A)$ with E CM and $[E : \mathbb{Q}] = 2\dim A$, without needing to take a field extension to get more endomorphisms. There are plenty of CMAVs that are defined *as abelian varieties* over $\mathbb{Q}$, but we do not get enough endomorphisms that are defined over $\mathbb{Q}$. For example, the elliptic curve $A : y^2 = x^3 + x$ has $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}[i]$, generated by the endomorphism $(x, y) \mapsto (-x, iy)$, but this endomorphism is not defined over $\mathbb{Q}$.

Proof. If A has CM by E and is defined (as a CMAV) over $\mathbb{Q}$, then by definition this means that $E \hookrightarrow \mathrm{End}^0_{\mathbb{Q}}(A)$. By Proposition 7.4, we conclude that $E^* \subseteq \mathbb{Q}$. This is impossible since E^* is itself CM by Lemma 7.3 Part 2, hence a nontrivial extension of $\mathbb{Q}$. ■

8 Shimura-Taniyama formula (02/02/2024)

8.1 Statements

Let A/K be an abelian variety over a number field K.

Definition 8.1. For a prime $\mathfrak{p}$ of K, we say that A has *good reduction* as $\mathfrak{p}$ if there exists an abelian scheme $\mathscr{A}/\mathcal{O}_{\mathrm{Spec}\, K_\mathfrak{p}}$ such that $\mathscr{A}_K = A$.

In particular, good reduction means that $\mathscr{A}$ must be smooth over $\mathcal{O}_{\mathrm{Spec}\, K_\mathfrak{p}}$. The spectrum of this DVR only has two points, and we already know that the generic fiber is an abelian variety A, so really this is equivalent to the special fiber being an abelian variety.

Now let $X/\mathbb{F}_q$ be a variety. There exists a map $F_X : X(\overline{\mathbb{F}}_q) \to X(\overline{\mathbb{F}}_q)$ defined in coordinates by sending $a \mapsto a^q$; this is the (q-th power) Frobenius map on X.

Definition 8.2. If X is an abelian variety, the (ℓ-adic) *Tate module* is $T_\ell = \varprojlim_n A(\overline{\mathbb{F}}_q)[\ell^n]$. Then Frobenius also descends to an action on the Tate module.

Theorem 8.1. *(Shimura-Taniyama formula.)* Let A/K be a CMAV with CM type (E, Φ) such that K contains all Galois conjugates of E (hence also the reflex field E^*) and $E \subseteq \mathrm{End}^0(A/K)$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime of good reduction, with $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$. Assume further:

1. $K_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified;
2. $\mathrm{End}(A) \cap E = \mathcal{O}_E$.

Then:

(a) There exists $\pi \in \mathcal{O}_E$ such that π induces the Frobenius action on $A \bmod \mathfrak{p}$.

(b) The ideal $(\pi) \subseteq \mathcal{O}_E$ is given by $\prod_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{K/\varphi E}\, \mathfrak{p})$.

The assumptions (1) and (2) are unnecessary but make the proof easier. There is another version that we will also consider:

Theorem 8.2. *(Shimura-Taniyama formula v2, Tate's paper.)* Let A/K have CM type (E, Φ) (with $E \subseteq \mathrm{End}^0(A/K)$, and suppose $\mathfrak{p}$ is a prime of good reduction lying over $(p) \subset \mathbb{Z}$, with $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$. Then:

(a) There exists $\pi \in E$ that induces $F_A \bmod \mathfrak{p}$.

(b) For all places of E dividing p, we have

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \frac{\#(\Phi \cap H_v)}{\#H_v},$$

where $H_v = \mathrm{Hom}(E_v, \overline{\mathbb{Q}}_p)$.

Remark 8.3. The Shimura-Taniyama formula is not to be confused with the Shimura-Taniyama conjecture, aka the modularity theorem.

8.2 Eigenvalues of Frobenius

Here are some corollaries that will make these results more concrete and actually allow you to compute things on the homework.

Suppose $\mathcal{O}_E \subseteq \mathrm{End}(A/K)$. By the theory of Néron models, we can take $\mathscr{A}$ so that $\mathrm{End}(A/K) = \mathrm{End}(\mathscr{A}/\mathcal{O}_{K_{\mathfrak{p}}})$. The latter injects into $\mathrm{End}(A \bmod \mathfrak{p})$ by the theory of Tate modules, which we will discuss later.

Corollary 8.4. Let A/K be CMAV with hypotheses as in the Shimura-Taniyama theorem.

(a) The characteristic polynomial of $F_{A \bmod \mathfrak{p}}$ is an integer polynomial.

(b) The q-adic valuations (i.e. the p-adic valuation renormalized so that $v(q) = 1$) of the eigenvalues of the characteristic polynomial of $F_{A \bmod \mathfrak{p}}$ are

$$\left\{ \frac{\#(\Phi \cap H_v)}{\#H_v} \right\}_{v|p}$$

each with multiplicity $\#H_v$.

Here, we take the characteristic polynomial of Frobenius to be the one via its action on the Tate module $V_\ell = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ over $\mathbb{Q}_\ell$. This is also the same as the characteristic polynomial of the lift of π to $H_1(A(\mathbb{C}), \mathbb{Q})$. Part (a) is true for non-CM AVs via the Weil conjectures, but part (b) seems to be a lot harder to approach in general.

The eigenvalues of Frobenius are one of the Great Mysteries of number theory. For example, they control whether an abelian variety is ordinary or otherwise how non-ordinary it is; if the valuations are all 0 or 1, then the AV is ordinary, and if all of them are $1/2$, it is supersingular. We know basically everything in the CM case by the above theorem, but more generally less is known. For example, we don't even know if a given abelian surface over K reduces to a supersingular abelian surface over $\mathbb{F}_q$ for infinitely many q.

We first prove the corollary from the Shimura-Taniyama formula:

Proof. (a) The characteristic polynomial of Frobenius is the same as the characteristic polynomial of π as a $\mathbb{Q}$-linear transformation on E—we consider π to act on $H_1(A, \mathbb{Q})$—so it is an integer polynomial. Explicitly, this polynomial is

$$\prod_{\sigma \in \mathrm{Hom}(E, \overline{\mathbb{Q}})} (x - \sigma(\pi)) \in \mathbb{Z}[x].$$

(b) Over $\mathbb{Q}_p$, we can rewrite the above polynomial as

$$\prod_{v|p} \prod_{\sigma \in \mathrm{Hom}(E_v, \overline{\mathbb{Q}}_p)} (x - \sigma(\pi)),$$

and the $\sigma(\pi)$ in the inner product all have the same valuation $\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)}$, which is equal to $\frac{\#(\Phi \cap H_v)}{\#H_v}$ by Theorem 8.2.

■

Example 8.5. Let A be an elliptic curve with CM by an imaginary quadratic field E. There are two cases for a prime $p \in \mathbb{Z}$:

- If p splits in $E/\mathbb{Q}$ into two places v_1, v_2, then $\#H_v = \#H_{v_2} = 1$. Since the CM type Φ has only one element, we conclude that the Frobenius eigenvalues have q-adic valuation 0 and 1, each with multiplicity 1. This is the case of an ordinary reduction.
- Otherwise, if p is inert or ramified, then $\#H_v = 2$, and we get the eigenvalue of valuation $1/2$ with multiplicity 2. This is the case of a supersingular reduction.

By the Chebotarev density theorem, this tells us that exactly half of the reductions of A will be ordinary and half will be supersingular (in the natural density of primes). In particular, any CM elliptic curve reduces to a supersingular curve for infinitely many p.

Example 8.6. Now let $\dim A = 2$ (an abelian surface), and suppose $E = \mathbb{Q}(\zeta_5)$.

1. If p splits completely in $E/\mathbb{Q}$, then we similarly get eigenvalues of valuation $0, 0, 1, 1$, yielding an ordinary abelian variety.
2. If $p \neq 5$ is inert in $E/\mathbb{Q}(\sqrt{5})$, then for any place v lying above p (there are either 1 or 2) we have $c(H_v) = H_v$, i.e. $\Phi \cap H_v$ consists of exactly half of the elements of H_v. Hence the q-valuation of all eigenvalues are $1/2$.

On the homework, you will compute the q-valuation of the Frobenius eigenvalues for the Jacobians of some Fermat curves. You will also give an example of an CMAV A of dimension 2 with Frobenius eigenvalues of valuation $0, 1/2, 1/2, 1$.

We will not be able to prove the Shimura-Taniyama formula for a while because we have not yet built the algebraic theory of abelian varieties and schemes. The proof will be given in Lecture 30.

Part II

Algebraic theory of abelian varieties

9 General theory of AVs (02/05/2024)

I was absent this day; this section is reconstructed from Prof. Tang's outline, Nir Elber's notes, and the accounts of these facts in [Con15].

9.1 The Rigidity Lemma and applications

We now work in the algebro-geometric setting over an arbitrary field k. Recall from Lecture 2:

Definition 9.1. An abelian variety over a field k is a group variety that is smooth, connected, and proper (among many other equivalent definitions).

We claimed early on that it is the properness that ensures abelian varieties are commutative group schemes. In the complex analytic setting, we used a compactness argument to conclude that the adjoint action is trivial. In the algebraic setting, the key is the following result:

Theorem 9.1. *(Rigidity lemma.)* Let X, Y be geometrically integral varieties over a field k and Z a separated k-scheme. Let $f : X \times_k Y \to Z$ be a k-morphism. Suppose:

- X/k is proper and $X(k)$ is nonempty, say $x_0 \in X(k)$;
- There exists $y_0 \in Y(k)$ such that $f|_{X \times \{y\}}$ is constant, mapping everything to a point $z_0 \in Z(k)$.

Then there exists a morphism $g : Y \to Z$ such that the following diagram commutes:

$$\begin{array}{ccc} X \times Y & & \\ \downarrow{\scriptstyle \mathrm{pr}_Y} & \searrow^{f} & \\ Y & \xrightarrow{g} & Z \end{array}$$

That is, the morphism f is independent of its first coordinate.

Proof. Define $g(y) := f(x_0, y)$; more rigorously, g is the composition

$$Y \simeq \operatorname{Spec} k \times Y \xrightarrow{x_0 \times \mathbf{id}_Y} X \times Y \xrightarrow{f} Z.$$

To show that $f = g \circ \mathrm{pr}_Y$, it is enough to show that this is true on an open dense subset of $X \times Y$, since the source is reduced and the target is separated (see [Har77, Exercise II.4.2] or [Vak, Theorem 11.4.2] for the "Reduced-to-separated theorem"). Since X and Y are both geometrically integral, $X \times Y$ is irreducible, so any nonempty open subset is dense.

Let $U \ni z_0$ is any open affine neighborhood of z_0 in Z. By continuity, $f^{-1}(Z \setminus U)$ is closed in $X \times Y$, and since X is proper, the projection $\mathrm{pr}_Y(f^{-1}(Z \setminus U))$ is again closed. (Recall that proper schemes are universally closed by definition, so in the Cartesian diagram

$$\begin{array}{ccc} X \times Y & \xrightarrow{\mathrm{pr}_Y} & Y \\ \downarrow & & \downarrow \\ X & \longrightarrow & \operatorname{Spec} k \end{array}$$

the top arrow is a closed map because the bottom arrow is.) Define $V := \mathrm{pr}_Y(f^{-1}(Z \setminus U))$, which we know is *open* and *nonempty*: it at least contains y_0, since $f(x_0, y_0) \in U$.

The open set $X \times_k V \subseteq X \times_k Y$ is the open set we will use to test the equality of f and $g \circ \mathrm{proj}_Y$. It is even enough to check equality on $\overline{k}$-points, since these are dense in any k-variety. (The maximal locus of agreement of any two morphisms $\varphi, \psi : S \to T$ is locally closed in general and closed if T is separated, in the sense that in the Cartesian diagram

$$\begin{array}{ccc} V & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle \varphi \times \psi} \\ T & \xrightarrow{\Delta} & T \times T \end{array}$$

the map $V \to S$ is locally closed, and closed if S is separated.

So let $y \in V(\overline{k})$. Then $f(X_{\overline{k}} \times_{\overline{k}} \{y\})$ maps inside U_k, but $X_{\overline{k}} \times_{\overline{k}} \{y\}$ is proper over $\operatorname{Spec} \overline{k}$ and $U_{\overline{k}}$ is affine, so f is constant (the image of a proper morphism is proper, and the only proper subschemes of an affine scheme are the finite). Hence for any $x \in X(\overline{k})$, we must have $f(x, y) = f(x_0, y) = g(x, y)$, as desired. ■

Remark 9.2. The hypotheses in the Rigidity Lemma can be slightly weakened; see the version in [Con15, Theorem 1.7.1].

Some immediate applications:

Corollary 9.3. Let A and B be abelian varieties, and let $f : A \to B$ be an arbitrary morphism of k-varieties (not necessarily a homomorphism). Then there exists a homomorphism $h \in \operatorname{Hom}_k(A, B)$ and a point $b \in B(k)$ such that $f = t_b \circ h$, where $t_b : B \to B$ is the translation by b. In particular, if $f(e_A) = e_B$, then f is automatically a homomorphism, where the e's are the identity elements.

Proof. We reduce to the case $f(e_A) = e_B$ by post-composing with translation by $b = -f(e_A)$. Writing the group law multiplicatively for the moment, without yet knowing that this law is commutative, define $\alpha : A \times A \to B$ by

$$\alpha(x_1, x_2) = f(x_1 x_2) f(x_2)^{-1} f(x_1)^{-1}.$$

Then $\alpha(x_1, e_A) = f(x_1) f(e_A)^{-1} f(x_1)^{-1} = e_B$, and likewise $\alpha(e_A, x_2) = e_B$. By the Rigidity Lemma, $\alpha : A \times A \to B$ factors through *both* projections $A \times A \to A$, so α must be constant with $\alpha(A \times A) = \{e_B\}$. But this means $f(x_1 x_2) = f(x_1) f(x_2)$, i.e. f is a homomorphism. ■

Corollary 9.4. The group law on an abelian variety is commutative.

Proof. The inverse morphism $i : A \to A$ preserves e_A, so by Corollary 9.3, i is automatically a homomorphism. But a group is commutative if and only if the inverse map defines a automorphism. ■

Remark 9.5. Since the group law on A is commutative, multiplication by n is a homomorphism. We denote the multiplication by n morphism as $[n] : A \to A$.

Remark 9.6. From now on, we will notate the group law on an abelian variety additively.

9.2 Theorem of the Cube statement and corollaries

Theorem 9.7. *(Theorem of the Cube.)* Let X, Y, Z be geometrically integral k-varieties with X and Y proper. Let $x_0 \in X(k), y_0 \in Y(k), z_0 \in Z(k)$. Suppose a line bundle $\mathscr{L}$ on $X \times Y \times Z$ becomes trivial under the three restrictions

$$\mathscr{L}|_{X\times Y\times\{z_0\}}, \mathscr{L}|_{X\times\{y_0\}\times Z}, \mathscr{L}|_{\{x_0\}\times Y\times Z}.$$

Then $\mathscr{L}$ itself is trivial.

It will take quite a bit of work to prove this; we'll start next lecture. For now, we give some consequences.

Theorem 9.8. *(Cubical structure of line bundles.)* Let A be an abelian variety and X any variety over k. Given three morphisms $f, g, h : X \to A$ and a line bundle $\mathscr{L}$ on A, we have an isomorphism

$$(f+g+h)^*\mathscr{L} \otimes f^*\mathscr{L} \otimes g^*\mathscr{L} \otimes h^*\mathscr{L} = (f+g)^*\mathscr{L} \otimes (g+h)^*\mathscr{L} \otimes (h+f)^*\mathscr{L}. \tag{1}$$

In particular, take $X = A \times A \times A$ and let $\mathrm{m}_\bullet : X \to A$ denote the projection onto the indices $\bullet$ followed by addition in the group law. Then

$$\mathrm{m}_{123}^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L} \simeq \mathrm{m}_{12}^*\mathscr{L} \otimes \mathrm{m}_{23}^*\mathscr{L} \otimes \mathrm{m}_{13}^*\mathscr{L}. \tag{2}$$

Proof. The isomorphism 2 is the *universal* case: the general case 1 can be obtained from 2 by pulling back along the morphism $(f, g, h) : X \to A \times A \times A$. Therefore, we need only prove 2.

Equivalently, we must show that

$$\mathscr{K} := \mathrm{m}_{123}^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L} \otimes \mathrm{m}_{12}^*\mathscr{L}^{-1} \otimes \mathrm{m}_{23}^*\mathscr{L}^{-1} \otimes \mathrm{m}_{13}^*\mathscr{L}^{-1}$$

is trivial. This follows from Theorem 9.7 if we can show that $\mathscr{K}|_{\{e_A\}\times A\times A}, \mathscr{K}|_{A\times\{e_A\}\times A}$, and $\mathscr{K}|_{A\times A\times\{e_A\}}$ are all trivial, so by symmetry we need only show that $\mathscr{K}|_{\{e_A\}\times A\times A}$ is trivial. But

$$\mathscr{K}|_{\{e_A\}\times A\times A} = \mathrm{m}_{23}^*\mathscr{L} \otimes \mathcal{O} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1} \otimes \mathrm{m}_{23}^*\mathscr{L}^{-1} \otimes \mathrm{pr}_3^*\mathscr{L}^{-1}$$

and the factors cancel. ∎

Remark 9.9. As currently stated, the isomorphism appearing in Theorem 9.8 is not canonical. Moreover, when considering abelian schemes over a more general base S, it might not be true that $e^*\mathscr{L}$ is trivial, where $e : S \to A$ is the unit morphism. The "correct" version of Theorem 9.8 is

$$\mathrm{m}_{123}^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L} \simeq \mathrm{m}_{12}^*\mathscr{L} \otimes \mathrm{m}_{23}^*\mathscr{L} \otimes \mathrm{m}_{13}^*\mathscr{L} \otimes e_X^*\mathscr{L}$$

where $e_X : X \to A$ is the base change of the unit morphism; the extra term cancels the factor that was trivial in our original computation. Naturality of this version of the isomorphism is the content of one of the exercises in Homework 2.

Corollary 9.10. *(Quadratic structure of line bundles.)* Let $\mathscr{L}$ be a line bundle on an abelian variety A. Then for any $n \in \mathbb{Z}$,

$$[n]^*\mathscr{L} = \mathscr{L}^{\otimes n(n+1)/2} \otimes [-1]^*\mathscr{L}^{\otimes n(n-1)/2}.$$

In particular, if $\mathscr{L} = [-1]^*\mathscr{L}$ (we say such $\mathscr{L}$ is *symmetric*), then $[n]^*\mathscr{L} = \mathscr{L}^{\otimes n^2}$, and if $\mathscr{L}^{-1} = [-1]^*\mathscr{L}$ (we say such $\mathscr{L}$ is *antisymmetric*), then $[n]^*\mathscr{L} = \mathscr{L}^{\otimes n}$.

Proof. The statement is trivial for $n \in \{-1, 0, 1\}$. Suppose we know the statement for n and $n-1$. Then

$$[n]^*\mathscr{L} \otimes [n]^*\mathscr{L} \otimes [1]^*\mathscr{L} \otimes [-1]^*\mathscr{L} \simeq [n+1]^*\mathscr{L} \otimes [n-1]^*\mathscr{L} \otimes [0]^*\mathscr{L}$$

by Theorem 9.8, taking $X = A$ and $f = [n], g = [1], h = [-1]$. By inductive hypothesis, the above simplifies to

$$\begin{aligned}&(\mathscr{L}^{\otimes n(n+1)/2} \otimes [-1]^*\mathscr{L}^{n(n-1)/2})^{\otimes 2} \otimes \mathscr{L} \otimes [-1]^*\mathscr{L} \\ &\simeq [n+1]^*\mathscr{L} \otimes \mathscr{L}^{\otimes (n-1)n/2} \otimes [-1]^*\mathscr{L}^{(n-1)(n-2)/2}\end{aligned}$$

and gathering like factors gives the formula for $[n+1]^*\mathscr{L}$. Likewise, this same argument gives the formula for $n-1$ if it is known for n and $n+1$. Therefore we win by upwards and downwards induction. ∎

10 Theorem of the Cube proof part I (02/07/2024)

The proof of the Theorem of the Cube (Theorem 9.7) will occupy us for the next two lectures. We will need to cite other well-known theorems in algebraic geometry and apply some cohomology theory.

The proof is much simpler if one blackboxes the existence of the Picard variety. This is how [Con15] does it; the proof is a straightforward application of the Seesaw Principle and the Rigidity Lemma. Instead we will follow the proof in [Mum08], which avoids the Picard variety but unfortunately is rather technical and unintuitive.

10.1 Theorem of the square

We first give one last crucial application of the Theorem of the Cube.

Corollary 10.1. *(Theorem of the square.)* Let A/k be an abelian variety. For all $x, y \in A(k)$ and line bundle $\mathscr{L}$ on A, we have

$$t_{x+y}^*\mathscr{L} \otimes \mathscr{L} \simeq t_x^*\mathscr{L} \otimes t_y^*\mathscr{L},$$

where t_z denotes translation by z.

Proof. Apply the Theorem of the Cube with $X = A, f : A \to \{x\}$, $g : A \to \{y\}$, and $h = \mathbf{id}_A$. ■

Remark 10.2. Suppose k'/k is a field extension, and pick any line bundle $\mathscr{L}$ on A. Then the theorem of the square shows that $\phi_{\mathscr{L}} : A(k') \to \mathrm{Pic}(A_{k'})$ defined by $x \mapsto t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ is a group homomorphism, since by tensoring the isomorphism in the theorem of the square by $\mathscr{L}^{-2}$ we obtain

$$t_{x+y}^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq (t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}) \otimes (t_y^*\mathscr{L} \otimes \mathscr{L}^{-1}).$$

The homomorphism $\phi_{\mathscr{L}}$ is vitally important in the theory of abelian varieties, especially when $\mathscr{L}$ is ample. If you've studied elliptic curves, this is the generalization of the isomorphism $E \to \mathrm{Pic}^0(E)$ given by $P \mapsto \mathcal{O}(P) - \mathcal{O}(e)$. These are the homomorphisms that yield polarizations when $\mathscr{L}$ is ample.

10.2 Review of cohomology

Let $f : X \to Y$ be a morphism of noetherian schemes. We have higher pushforward functors $R^n f_* : \mathbf{QCoh}(X) \to \mathbf{QCoh}(Y)$ on the categories of quasicoherent sheaves on X and Y. If f is proper, then these higher pushforwards send coherent sheaves to coherent sheaves.

We know the following properties of these functors:

1. $R^0 f_* = f_*$ is the usual pushforward map.
2. A short exact sequence of sheaves induces a long exact sequence in cohomology.
3. If $Y = \operatorname{Spec} R$, then $R^n f_* \mathscr{F}$ is the sheaf associated to the R-module $H^n(X, \mathscr{F})$.
4. If $Y = \operatorname{Spec} R$ and X is separated, then $H^n(X, \mathscr{F})$ can be computed using Čech cohomology. Let $\mathcal{U} = \{U_i\}_{i \in I}$ be a finite cover of X by affine opens, and fix an ordering of I. The Čech complex $C^\bullet(\mathcal{U}, \mathscr{F})$ is a complex of R-modules with

$$C^n(\mathcal{U}, \mathscr{F}) = \prod_{i_0 < \cdots < i_n} \Gamma(U_{i_0} \cap \cdots \cap U_{i_n}, \mathscr{F})$$

with coboundary maps $d^n : C^n(\mathcal{U}, \mathscr{F}) \to C^{n+1}(\mathcal{U}, \mathscr{F})$ given by

$$(d\sigma)_{i_0<\cdots<i_{n+1}} := \sum_{j=0}^{n+1} (-1)^j \sigma_{i_0<\cdots<\hat{i}_j<\cdots<i_{n+1}}|_{U_{i_0}\cap\cdots\cap U_{n+1}}.$$

Then we define Čech cohomology to be the cohomology of this complex. For example, $\check{H}^0(\mathcal{U}, \mathscr{F}) = \Gamma(X, \mathscr{F})$.

Theorem 10.3. *(Semicontinuity theorem.)* [Mum08, II.5, Cor. 1], [Vak, 28.1.1] Let $X \to Y$ be a proper morphism of noetherian schemes, and let $\mathscr{F}$ be a coherent sheaf on X that is flat over Y. Then for all integers $n \geq 0$, the function $Y \to \mathbb{Z}$ defined by

$$y \mapsto \dim_{k(y)} H^n(X_y, \mathscr{F}|_{X_y})$$

is *upper-semicontinuous*, which means that the preimage of $[m, \infty)$ is closed for any $m \geq 0$.

Grauert's theorem gives a criterion to check whether a higher pushforward is locally free and determine its rank.

Theorem 10.4. *(Grauert's theorem.)* [Mum08, II.5, Cor. 2] [Vak, 25.1.5] Let hypotheses be as in the semicontinuity theorem, and assume also that Y is reduced and connected. Then the following are equivalent:

1. $\dim_{k(y)} H^n(X_y, \mathscr{F}|_{X_y})$ is constant for all $y \in Y$.
2. $R^n f_* \mathscr{F}$ is locally free of finite rank and $R^n f_* \mathscr{F} \otimes k(y) \to H^n(X_y, \mathscr{F}|_{X_y})$ is an isomorphism for all $y \in Y$.

10.3 Seesaw principle

We can reduce proof of the Theorem of the Cube to the case $k = \overline{k}$, since we have:

Lemma 10.5. Let V/k be a proper and geometrically integral scheme.

1. $\Gamma(V, \mathcal{O}_V) = k$.
2. Let $\mathscr{L}/V$ be a line bundle. If $\mathscr{L}_{\overline{k}}$ is trivial, then $\mathscr{L}$ is also trivial.

Proof. 1. See [Sta24, Tag 0BUG].

2. If $\Gamma(V^{\pm 1}_{\overline{k}, \mathscr{L}_{\overline{k}}}) \simeq \Gamma(V, \mathscr{L}^{\pm 1}) \otimes \overline{k}$ are nonzero, then so are $\Gamma(V, \mathscr{L}^{\pm 1})$. By Lemma 10.6, these conditions are equivalent to triviality.

■

Lemma 10.6. Let V/k be again as in the previous lemma, and $\mathscr{L}$ a line bundle on V. Then $\mathscr{L} \simeq \mathcal{O}_V$ if and only if $\mathscr{L}$ and $\mathscr{L}^{-1}$ both have nonzero global sections.

Proof. If $\mathscr{L}$ is trivial, the claim is immediate from part (1) of Lemma 10.5. For the other direction, use a global section $s \in \Gamma(V, \mathscr{L})$ to define a morphism $s : \mathcal{O}_V \to \mathscr{L}$, and use a global section $t \in \Gamma(V, \mathscr{L}^{-1})$ to define a morphism $\mathcal{O}_V \to \mathscr{L}^{-1}$. Tensoring the latter by $\mathscr{L}$ yields a morphism $t : \mathscr{L} \to \mathcal{O}_V$. The composition $t \circ s : \mathcal{O}_V \to \mathcal{O}_V$ is a nonzero morphism, but the only automorphisms of $\mathcal{O}_V$ are scalar multiplication by k, so we conclude that t and s are isomorphisms. ∎

The main reason we need all of these results from cohomology is for the following very helpful result:

Theorem 10.7. *(Seesaw Principle.)* Let X/k be proper and geometrically integral, let T/k be a variety, and let $\mathscr{L}$ be a line bundle on $X \times_k T$. Then:

1. The set $T_1 = \{t \in T \text{ closed: } \mathscr{L}_{X \times \{t\}} \text{ trivial}\}$ is closed.
2. There exists some line bundle $\mathscr{M}$ on T_1 such that $\mathscr{L}|_{X \times T_1} \simeq \mathrm{pr}_{T_1}^* \mathscr{M}$.

Proof. We have

$$\begin{aligned} T_1 &= \{t \in T : \Gamma(X \times \{t\}, \mathscr{L}^{\pm}|_{X \times \{t\}} \neq 0\} \\ &= \{t \in T : \dim \Gamma(X \times \{t\}, \mathscr{L}^{\pm}|_{X \times \{t\}} > 0\}. \end{aligned}$$

This set is closed by the semicontinuity theorem, proving part (1) of the theorem. For part (2), on $X \times T_1$, we have

$$\dim_{k(t)} H^0(X \times \{t\}, \mathscr{L}|_{X \times \{t\}}) = 1,$$

since by definition $\mathscr{L}|_{X \times \{t\}}$ is trivial on this locus. By Grauert's theorem, we conclude $\mathrm{pr}_{T_1,*} \mathscr{L}$ is locally free of rank 1, i.e. a line bundle $\mathscr{M}$. By adjunction, we have a natural map

$$\mathrm{pr}_{T_1}^* \mathscr{M} = \mathrm{pr}_{T_1}^* \mathrm{pr}_{T_1,*} \mathscr{L}|_{X \times T_1} \to \mathscr{L}_{X \times T_1}$$

which we can check on fibers to be an isomorphism. ∎

We will often use Seesaw Principle in the guise of the following corollary.

Corollary 10.8. Let $X, T, \mathscr{L}$ be as in Theorem 10.7. If there exists a point $x_0 \in X(k)$ such that $\mathscr{L}|_{\{x_0\} \times T}$ is trivial, and if $\mathscr{L}|_{X \times \{t\}}$ is trivial for *all* $t \in T$, then $\mathscr{L}$ is trivial.

Proof. By the Seesaw Principle, everywhere triviality of $\mathscr{L}|_{X \times \{t\}}$ tells us that $\mathscr{L} = \mathrm{pr}_2^* \mathscr{M}$ for some line bundle $\mathscr{M}$ on T. But for any $x_0 \in X(k)$, the composition

$$T \xrightarrow{\sim} \{x_0\} \times T \hookrightarrow X \times T \xrightarrow{\mathrm{pr}_2} T$$

is the identity on T. This means that $\mathcal{O}_T \simeq \mathscr{L}|_{\{x_0\} \times T} \simeq \mathbf{id}_T^* \mathscr{M} \simeq \mathscr{M}$, so $\mathscr{M}$, hence also $\mathscr{L} = \mathrm{pr}_2^* \mathscr{M}$, is trivial. ∎

Remark 10.9. (See also [Mum08, pp. 52-53].) We ended lecture by discussing the Theorem of the Cube in the complex analytic case. Let $W = X \times Y \times Z$ be a complex-analytic variety. We have the exponential exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_W \xrightarrow{\exp} \mathcal{O}_W^\times \longrightarrow 1$$

inducing an exact sequence

$$H^1(W, \mathcal{O}_W) \to H^1(W, \mathcal{O}_W^\times) \longrightarrow H^2(W, \mathbb{Z}).$$

The middle term is $\mathrm{Pic}(W)$.
The Theorem of the Cube may be rephrased as the assertion that

$$\mathrm{Pic}(X \times Y \times Z) \to \mathrm{Pic}(X \times Y) \times \mathrm{Pic}(X \times Z) \times \mathrm{Pic}(Y \times Z)$$

is injective, where the the pullback maps are defined with respect to some arbitrary base points x_0, y_0, z_0. In general, given a contravariant functor T from the category of proper varieties to the category of abelian groups, we say that T is of order n if

$$T(X_0 \times \cdots \times X_n) \to \prod_{i=0}^{n} T(X_0 \times \cdots \times \hat{X}_i \times \cdots \times X_n)$$

is always injective, where the maps on each factor are induced by the maps $X_0 \times \cdots \times \{x_i\} \times \cdots \times X_n \to X_0 \times \cdots \times X_n$ for some collection of base points x_i. In this sense, the functor $H^1(W, \mathcal{O}_W)$ is order 1 (linear) and $H^2(W, \mathbb{Z})$ is order 2 (quadratic) by the Künneth formulas.[a] If a functor T is order n, then it is also order m for any $m \geq n$, so we know that Pic is sandwiched in an exact sequence between two quadratic functors. Hence it, too, must be quadratic, since the middle arrow of the following commutative diagram must also be injective:

$$\begin{array}{ccccc} H^1(X_0 \times X_1 \times X_2, \mathcal{O}) & \hookrightarrow & \mathrm{Pic}(X_0 \times X_1 \times X_2) & \twoheadrightarrow & H^2(X_0 \times X_1 \times X_2, \mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{i=0}^2 H^1(\dots, \mathcal{O}) & \hookrightarrow & \prod_{i=0}^2 \mathrm{Pic}(\dots) & \twoheadrightarrow & \prod_{i=0}^2 H^2(\dots, \mathbb{Z}) \end{array}$$

[a] See [Sta24, Tag 0BEC] for the Künneth formula for sheaf cohomology, which basically works as we expect it to in the case of trivial sheaves.

11 Theorem of the Cube proof part II (02/09/2024)

11.1 Reduction to the case of a smooth curve

Today we finish the proof of the Theorem of the Cube 9.7. We want to reduce our proof to the case of X being a smooth projective curve.

Lemma 11.1. Let X be a proper geometrically integral variety over a field k. For any $x_0, x_1 \in X$, there exists a geometrically irreducible curve $C \subseteq X$ containing x_0 and x_1.

Proof. Our main steps will be to apply Chow's lemma to reduce to the case that X is projective, and then apply a theorem of Bertini to supply a curve with the desired properties.

Theorem 11.2. *(Chow's lemma.)* [Vak, 19.9.2] Let $\pi : X \to \operatorname{Spec} A$ be a proper map, with A a noetherian ring. Then there exists a surjective proper morphism $\mu : X' \to X$ such that $\pi \circ \mu : X' \to \operatorname{Spec} A$ is projective and such that there exists an open dense $U \subseteq X$ with $\mu^{-1}(U) \to U$ an isomorphism.

Theorem 11.3. *(Bertini irreducibility theorem.)* [Jou83], [Ben11] Let k be an infinite field, and suppose $X \hookrightarrow \mathbb{P}^N_k$ is a geometrically integral projective variety over k. Then there exists a hyperplane $H \subseteq \mathbb{P}^N_k$ such that $H \cap X$ is geometrically integral. Moreover, the set of hyperplanes H for which this is true forms a Zariski open dense subset in the family of all hyperplanes of $\mathbb{P}^N$.

Remark 11.4. The lemma still holds for finite fields if we replace "hyperplane" by "hypersurface"; see [CP16, Theorem 1.1.1.8]. It usually also still works if we require other properties of $H \cap X$, such as smoothness.

Given a proper variety X and a surjective morphism $\mu : X' \to X$ as in Chow's lemma, one way to produce a geometrically irreducible curve containing given points $x_0, x_1 \in X$ are to take points $x_0' \in \mu^{-1}(x_0), x_1' \in \mu^{-1}(x_1)$, find a geometrically irreducible curve in X' through x_0' and x_1', and then take the image of this curve under μ. The image of a geometrically irreducible variety is again geometrically irreducible, and the image of an irreducible (complete) curve is either a point or another (complete) curve, but our image contains x_0 and x_1. Since X' must be geometrically irreducible if X is, we reduce to the case that X is projective.

We induct on the dimension of $\dim_k X$. If $\dim X = 1$, we are done. Otherwise, take the blowup $\operatorname{Bl}_{\{x_0,x_1\}} X$ along the two points, which is also projective. The two exceptional divisors have codimension 1, so applying Bertini's irreducibility theorem we get a geometrically irreducible subvariety of $\operatorname{Bl}_{\{x_0,x_1\}} X$ that intersects both of these. Projecting back down onto X yields a geometrically integral subvariety containing x_0, x_1 of strictly lesser dimension, so we conclude by induction. ∎

We return to proving the Theorem of the Cube. Given any closed $x \in X$, use Lemma 11.1 to produce a geometrically integral curve $C \subseteq X$ containing x and the base point x_0. Let its normalization be C'. We have an induced map $\pi_x : C' \times Y \times Z \to X \times Y \times Z$. The pullback $\pi^*\mathscr{L}$ on $C' \times Y \times Z$ satisfies the hypotheses of the Theorem of the Cube, except with X replaced by C' and x_0 replaced by some point in C' lying over $x_0 \in C$. If $\pi^*\mathscr{L}$ is trivial, then $\mathscr{L}|_{\{x\}\times Y\times\{z\}}$ is trivial for all $x \in X, z \in Z$, as

$$\pi^*\mathscr{L}|_{\{x'\}\times Y\times\{z\}} = \mathcal{O}|_{\{x'\}\times Y\times\{z\}}$$

for any $x' \in C'$ lying over x and $\pi|_{\{x'\}\times Y\times\{z\}} : \{x'\} \times Y \times \{z\} \to \{x\} \times Y \times \{z\}$ is an isomorphism. If $\mathscr{L}|_{\{x\}\times Y\times\{z\}}$ is trivial for all $x \in X, z \in Z$, then since we also know that $\mathscr{L}|_{X\times\{y_0\}\times Z}$ is trivial, the Seesaw Principle via Corollary 10.8 tells us that $\mathscr{L}$ is also trivial,

where $X \times Z$ takes the role of T and Y takes the role of X in the corollary (this is permissible since Y is assumed proper).

Since we have shown that $\mathscr{L}$ is trivial if $\pi^*\mathscr{L}$ is trivial, it suffices to prove the theorem in the case that X is a geometrically integral smooth curve.

11.2 End of proof

It suffices to prove the theorem after replacing Z by a dense open subset $Z' \subseteq Z$, since if $\mathscr{L}|_{X\times Y\times\{z\}}$ is trivial for all $z \in Z'$, then by part (1) of the Seesaw Principle 10.7, $\mathscr{L}|_{X\times Y\times\{z\}}$ is trivial for all $z \in Z$. Then another application of the Seesaw Principle shows that $\mathscr{L}$ is trivial. (We will select the appropriate Z' shortly.)

As justified in the previous section, we assume X is a smooth projective curve, say of genus g. Then a generic divisor $E \subset X$ of degree g has $H^0(X, \Omega_X(-E)) = 0$. Choose one such divisor and define $\mathscr{M} := \mathrm{pr}_1^*\,\mathcal{O}(E) \otimes \mathscr{L}$—a line bundle on $X \times Y \times Z$—and let W be the support of $R^1\,\mathrm{pr}_{23,*}\,\mathscr{M}$, which is a closed subset $W \hookrightarrow Y \times Z$. The assumptions $\mathscr{L}|_{X\times Y\times\{z_0\}} \simeq \mathcal{O}_{X\times Y}$ and $\mathscr{L}|_{X\times\{y_0\}\times Z} \simeq \mathcal{O}_{X\times Z}$ imply

$$\mathscr{M}|_{X\times\{y\}\times\{z_0\}} \simeq \mathscr{M}|_{X\times\{y_0\}\times\{z\}} \simeq \mathcal{O}(E) \tag{3}$$

for all $y \in Y, z \in Z$. Therefore, by Serre duality,

$$\begin{aligned} H^1(X \times \{y\} \times \{z_0\}, \mathscr{M}|_{X\times\{y\}\times\{z_0\}}) &= H^1(X, \mathcal{O}(E)) \\ &= H^0(X, \Omega_X(-E)) \\ &= 0. \end{aligned}$$

Since Y is proper, $\mathrm{pr}_Z(W) \subseteq Z$ is closed. Since $H^1(X \times \{y\} \times \{z_0\}, \mathscr{M}|_{X\times\{y\}\times\{z_0\}}) = 0$ for all $y \in Y$, by Grauert's theorem we conclude $R^1\,\mathrm{pr}_{23,*}\,\mathscr{M}|_{Y\times\{z_0\}} = 0$, hence $R^1\,\mathrm{pr}_{23,*}\,\mathscr{M}$ is not supported anywhere above z_0. This means $z_0 \notin \mathrm{pr}_Z(W)$. Therefore there exists an open neighborhood $Z' \ni z_0$ such that $W \cap (Y \times Z')$ is empty. Since Z is connected, Z' is dense, so by our previous remarks it suffices to prove the theorem over $X \times Y \times Z'$.

On $Y \times Z'$, we have $R^1\,\mathrm{pr}_{23,*}\,\mathscr{M} = 0$. We conclude that, for any $y \in Y, z \in Z'$,

$$H^0(X, \mathscr{M}|_{X\times\{y\}\times\{z\}}) = \chi(\mathscr{M}|_{X\times\{y\}\times\{z\}}) = \chi(\mathscr{M}|_{X\times\{y\}\times\{z_0\}}) = \chi(\mathcal{O}(E)) = 1$$

where the last equality is given by the Riemann-Roch formula

$$\chi(\mathcal{O}(E)) = 1 - g + \deg(\mathcal{O}(E)) = 1.$$

Hence one more application of Grauert's theorem shows that $\mathscr{N} := \mathrm{pr}_{23,*}\,\mathscr{M}$ is a locally free rank 1 module on $Y \times Z'$, i.e. an invertible sheaf.

We construct a divisor $D \subseteq X \times Y \times Z'$. Pick an open cover $\{U_i\}$ of $Y \times Z'$ such that $\mathscr{N}|_{U_i}$ is trivial, fixing specific isomorphisms $\alpha_i : \mathcal{O}_{U_i} \to \mathscr{N}|_{U_i}$. Then

$$\alpha_i(1) \in \Gamma(U_i, \mathscr{N}) = \Gamma(X \times U_i, \mathscr{M}).$$

Define D_i to be the zero locus of $\alpha_i(1)$ on $X \times U_i$. Such D_i glue to a divisor $D \subset X \times Y \times Z'$,

because on overlaps $U_i \cap U_k$ the functions α_i, α_j differ by a unit. Then

$$\mathcal{O}(D)|_{X\times\{y\}\times\{z\}} \simeq \mathscr{M}|_{X\times\{y\}\times\{z\}} \tag{4}$$

for all $y, z \in Y \times Z'$ since for each y, z there is a neighborhood $U_i \ni \{y\} \times \{z\}$ on which $D \cap U_i$ is cut out by a section of $\mathscr{M}|_{U_i}$.

We claim that $D = E \times Y \times Z'$. The isomorphisms (3) and (4) show that

$$\mathcal{O}(D)|_{X\times\{y_0\}\times\{z\}} = \mathcal{O}(D)|_{X\times\{y\}\times\{z_0\}} = \mathcal{O}(E). \tag{5}$$

for any $y \in Y, z \in Z'$. Therefore, if $p \in X$ is not contained in the support of E, we have

$$D \cap (\{p\} \times Y \times \{z_0\}) = D \cap (\{p\} \times \{y_0\} \times Z') = \emptyset,$$

so the closed subset

$$T := \mathrm{pr}_Z(D|_{\{p\}\times Y\times Z'}) \subseteq Z'$$

does not contain z_0. The set $D|_{\{p\}\times Y\times Z'}$ on $Y \times Z'$ is the divisor associated to the line bundle $\mathscr{N}$, so this has pure codimension 1 in $\{p\} \times Y \times Z'$, and therefore its projection to Z' has component all of codimension at most 1. But $T \subsetneq Z'$, ruling out the possibility of codimension 0, so we conclude T also has pure of codimension 1 in Z'. We clearly have

$$D \cap (\{p\} \times Y \times Z') \subseteq \{p\} \times Y \times T. \tag{6}$$

Any irreducible component of $\{p\}\times Y\times T$ must either equal a component of $D\cap(\{p\}\times Y\times Z')$ or not intersect, since components of both sides all have codimension 1. But it is impossible for this intersection to be trivial since, by definition, any point of T must have some point of $D \cap (\{p\} \times Y \times Z')$ in its preimage. We conclude that the inclusion in (6) is an equality. Yet we also know that D does not meet $\{p\} \times \{y_0\} \times Z'$, so the only possibility is $T = \emptyset$.

We conclude that D is supported only over E. Conversely, Equation (5) shows that D is supported everywhere on $E \times X \times Y$, so we conclude that the support of D is precisely $E \times X \times Y$. Hence we can write these Weil divisors as

$$D = \sum_i n_i(\{p_i\} \times Y \times Z)$$
$$E = \sum_i m_i(\{p_i\} \times Y \times Z)$$

for positive integers m_i. But then restricting to $X \times \{y_0\} \times \{z\}$ and applying Equation 5 shows that we must have all $m_i = n_i$, hence $D = E$ as divisors. This equality, in conjunction with Equation (4), finally lets us conclude

$$\mathscr{M}|_{X\times\{y\}\times\{z\}} \simeq \mathcal{O}(E)$$

for *any* $y \in Y, z \in Z'$, not just y_0 or z_0 as in Equation (3). Since X is a curve, this means that D is of the form $\sum_i n_i(\{p_i\} \times Y \times Z')$ for some nonnegative integers n_i and points $p_i \in X$. But $\mathscr{M}$ was defined so that $\mathscr{M}|_{X\times\{y\}\times\{z\}} := \mathcal{O}(E) \otimes \mathscr{L}|_{X\times\{y\}\times\{z\}}$, so

$\mathscr{L}|_{X\times\{y\}\times\{z\}}$ must be trivial. Thus, triviality of $\mathscr{L}|_{\{x_0\}\times\{y\}\times\{z\}}$ and Corollary 10.8 shows that $\mathscr{L}$ is trivial.[8] ■

12 Projectivity of abelian varieties (02/12/2024)

12.1 The homomorphisms $\phi_{\mathscr{L}}$

Recall the theorem of the square (Theorem 10.1) and the subsequent Remark 10.2: given any line bundle $\mathscr{L}$ on an abelian variety A/k, we have a group homomorphism $A(\overline{k}) \to \mathrm{Pic}(A_{\overline{k}})$ defined by

$$\phi_{\mathscr{L}}(x) = t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}.$$

Right now this is just a group homomorphism, but we will soon upgrade this to a homomorphism of group schemes.

The maps $\phi_{\mathscr{L}}$ yield a group homomorphism $\phi : \mathrm{Pic}(A) \to \mathrm{Hom}(A(\overline{k}), \mathrm{Pic}(A_{\overline{k}}))$ via $\mathscr{L} \mapsto \phi_{\mathscr{L}}$.

Definition 12.1. $\mathrm{Pic}^0(A)$ is the subgroup $\ker\phi \subseteq \mathrm{Pic}(A)$, consisting of all translation-invariant line bundles on A.

Example 12.1. If A is an elliptic curve, then we have an exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(A) \longrightarrow \mathrm{Pic}(A) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

where the last map is the degree map, i.e. $\mathrm{Pic}^0(A)$ is just the group of degree zero line bundles on A. To see this, let $D = \sum_P n_P[P]$ be the divisor associated to a given line bundle $\mathscr{L}$. Another divisor $E = \sum_Q n_Q[Q]$ is linearly equivalent to D if and only if $\deg E = \deg D$ and $\sum_P n_P \cdot P = \sum_Q n_Q \cdot Q$, where the this sum is via the group law on A ([Sil09, Cor. 3.5]). Given a point $x \in A(\overline{k})$, we have

$$t_x(D) = \sum_P n_P[x+P],$$

which is linearly equivalent to D if and only if

$$\sum_P n_P \cdot P = \sum_P n_P \cdot (x+P) = \deg(D)\cdot x + \sum_P n_P \cdot P.$$

This shows that $\mathscr{L}$ is translation-invariant if $\deg(D) = \deg(\mathscr{L}) = 0$. Conversely, if $\deg(D)$ is nonzero, choosing $x \in A(\overline{k}) \setminus A[\deg(D)](\overline{k})$ (a point without order dividing $\deg(D)$) shows that $\mathscr{L}$ is not translation-invariant.

Beware: it is not true in general that $\mathrm{Pic}^0(A)$ is the subgroup of all degree 0 line bundles; this is just a happy coincidence in the case of elliptic curves.

[8] I find this proof very unintuitive. The ultimate idea is to show that $\mathscr{L}$ is trivial by showing $(\mathcal{O} \otimes \mathscr{L})_{X\times\{y\}\times\{z\}}$ is trivial for any y, z and then apply Seesaw. But juggling around the pushforwards and various divisors makes it very easy for the ideas to be lost. If anyone reading this has a good way to explain the intuition behind the proof in more detail, I would greatly appreciate hearing it.

Lemma 12.2. $\mathscr{L} \in \mathrm{Pic}^0(A)$ if and only if $m^*\mathscr{L} \simeq \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L}$, where the pr_i are the projection maps $A \times A \to A$ and $m : A \times A$ is the group law.

Proof. Suppose the second isomorphism holds. Choose a point $x \in X(k)$, yielding an embedding $i : A \simeq \{x\} \times A \hookrightarrow A \times A$. Then $t_x = m \circ i$, hence

$$t_x^*\mathscr{L} = i^*(m^*\mathscr{L}) \simeq i^*(\mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L}) \simeq \mathcal{O}_A \otimes \mathscr{L},$$

which means $\mathscr{L} \in \mathrm{Pic}^0(A)$.

Conversely, if $\mathscr{L} \in \mathrm{Pic}^0(A)$, let $\mathscr{M} := m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}$. Then for all $x \in A(\overline{k})$ we have $\mathscr{M}|_{A\times\{x\}} \simeq \mathcal{O}_A \simeq M|_{\{x\}\times A}$. By the Seesaw Principle, we conclude that $\mathscr{M} \simeq \mathcal{O}_{A\times A}$. ∎

Definition 12.2. For $L \in \mathrm{Pic}(A)$, we set $K(\mathscr{L}) := \ker \phi_L$, the subset of $x \in A(\overline{k})$ for which $t_x^*\mathscr{L} = \mathscr{L}$.

Hence $\mathscr{L} \in \mathrm{Pic}^0(A)$ if and only if $K(\mathscr{L}) = A(\overline{k})$.

Lemma 12.3. $K(\mathscr{L})$ is Zariski closed in $A(\overline{k})$.

Hence we may view $K(\mathscr{L})$ as a subvariety of A via the reduced induced structure.

Proof. $K(\mathscr{L})$ is the locus consisting of $x \in A(\overline{k})$ such that the following line bundle is trivial:

$$m^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}|_{A\times\{x\}}.$$

By the first part of the seesaw principle, this locus is closed. ∎

Note also that $K(\mathscr{L}) = K(\mathscr{L}^{-1})$.

12.2 Ampleness and projectivity

Theorem 12.4. Let D be an effective divisor on A, and let $\mathscr{L} = \mathcal{O}(D)$. Then the following are equivalent:

1. $\mathscr{L}$ is ample.
2. $K(\mathscr{L})$ is a finite set.
3. $H(D) := \{x \in A \text{ closed pt} : x + D = D\}$[a] is finite.
4. The linear system $|2D| := (\Gamma(X, \mathcal{O}(2D)) \setminus \{0\})/k^\times$, which is also in bijection with the set of all effective divisors rationally equivalent to $2D$, is base point free and defines a finite morphism $A \to \mathbb{P}^N$.

Additionally, for any ample line bundle $\mathscr{L}$ (not necessarily of the form $\mathcal{O}(D)$ for an effective D), the set $K(\mathscr{L})$ is finite.

[a] We require literal equality of divisors here, not just up to linear equivalence.

We'll prove this after the following corollary.

Corollary 12.5. Any abelian variety A/k is projective.

Proof. To show that a proper variety is projective, we need only exhibit a single ample line bundle, since then some power of that line bundle is very ample. Hence we need to find some effective D on A such that one of the conditions in Theorem 12.4 holds.

Pick an affine open neighborhood U of e in A. Then $D = A \setminus U$ is an effective divisor.[9] We observe:

1. $H(D) \subseteq U$, since if $x \in H(D)$, then $x + U = U$, hence $x = x + e \in U$.
2. $H(D)$ is closed in A, since it is $\mathrm{pr_A}(m|_{A\times D}^{-1}(D))$.

Conditions (1) and (2) together imply that $H(D)$ is simultaneously proper and affine, hence finite, yielding condition (3) of Theorem 12.4. ■

We now prove Theorem 12.4.

Proof.

- (1) $\implies$ (2): The subvariety $B := K(\mathscr{L})^0$ is an abelian variety. By definition, $t_x^*\mathscr{L}|_B \simeq \mathscr{L}|_B$ for all $x \in B$. By Lemma 12.2, $m^*\mathscr{L}|_B \simeq \mathrm{pr}_1^*\mathscr{L}|_B \otimes \mathrm{pr}_2^*\mathscr{L}|_B$ on $B \times B$. We are assuming $\mathscr{L}$, hence $\mathscr{L}|_B$, is ample, so this isomorphism implies

  $$\mathcal{O}_B \simeq \mathscr{L}|_B \otimes [-1]^*\mathscr{L}|_B$$

  by pulling back along $[1] \times [-1] : B \to B \times B$. Both factors in this tensor product are ample—the pullback of an ample line bundle by an isomorphism is again ample—so $\mathcal{O}_B$ is also ample. But the only way the trivial sheaf can be ample on a proper variety is if that variety has dimension 0, so B is the single point $\{e\}$ and $K(\mathscr{L})$ is finite.

  Note that this argument is valid for any ample $\mathscr{L}$, proving the final claim at the end of the theorem.

- (2) $\implies$ (3): Clear since $H(D)$ is a subset of $K(\mathscr{L})$.

- (3) $\implies$ (4):[10] By the theorem of the square, $t_x^*\mathscr{L} + t_{-x}^*\mathscr{L} \simeq \mathscr{L}^{\otimes 2}$, or in the notation of divisors, $t_{-x}(D) + t_x(D) \sim 2D$ (sum taken in $\mathrm{Div}(A)$). This supplies us with a lot of divisors that are linearly equivalent to $2D$, and maybe explains why $2D$ is the divisor appearing in condition (4).

  We need to show that for all $y \in A(\overline{k})$, there exists a section of $\Gamma(A, \mathcal{O}(2D))$ that does not vanish at y. Up to nonzero scalars, such global sections are in bijection with effective divisors linearly equivalent to $2D$, with a global section s associated to the effective divisor $\mathrm{div}(s)$. Therefore, we need to show that, for any $y \in A(\overline{k})$, there exists $D' \sim 2D$ with $y \notin \mathrm{supp}(D')$. To do this, we find $x \in X$ with $y \notin \mathrm{supp}(t_{-x}(D)) \cup \mathrm{supp}(t_x(D))$, setting $D' = t_{-x}(D) + t_x(D) \sim 2D$. Such x is supplied by any point in the (dense) complement of the codimension 1 set $\pm t_{-y}(D)$ (negation taken in the group law of A).

[9] The claim here is that D has pure codimension 1, which follows from an argument using the normality of A; we give the full argument in a handout on bCourses.

[10] We saved this part until the next lecture.

To show that $|2D|$ defines a finite morphism $\varphi : A \to \mathbb{P}^N$, it suffices to show that φ is quasi-finite, since quasi-finite + proper = finite for noetherian schemes. So let $y \in \mathbb{P}^N$ be a closed point; we want to show that $\varphi^{-1}(y)$ is finite. Suppose this is false; then $\varphi^{-1}(y)$ contains an irreducible projective curve $C \subseteq A$. This implies that if s is a global section of $2D$, then either the vanishing locus $V(s)$ contains C, or $V(s) \cap C = \emptyset$—that is, the linear system does not separate any points in C. Equivalently, for any effective $E \in |2D|$, we must either have $\mathrm{supp}(E) \supseteq C$, or $E \cap C = \emptyset$. Let $x \in A$ be any point such that $(x + D) \cup (-x + D) \cap C = \emptyset$. Then by Lemma 12.6 applied to the divisor $E' = x + D$, for any $y \in C$, we have $x - y + E' = E'$ as divisors; equivalently, $D = x - y + D$. Since $H(D)$ is finite, we conclude that there are only finitely many possibilities for $x - y \in H(D)$. But since C is a curve, there are infinitely many choices of y, contradiction.

Lemma 12.6. Let $C \subseteq A$ be an irreducible projective curve, and let $E' \subset A$ be an effective divisor with $E' \cap C = \emptyset$. Then for all $x, y \in C$, we have $x - y + E' = E'$.

Proof. Let $\mathscr{L}' = \mathcal{O}(E')$. The assumption $E' \cap C = \emptyset$ means $\mathscr{L}'|_C \simeq \mathcal{O}_C$. Consider $m^*\mathscr{L}'$ on $C \times \mathscr{L}'$ (via the restriction of the group law $m : C \times A \to A$). The morphism $C \times A \to A$ is flat and proper, so the Hilbert polynomials of the fibers of $m^*\mathscr{L}'|_{C\times A}$ over any $x \in A$ are constant; in particular, the degree is constant. This fiber is $t_x^*\mathscr{L}'|_C$, so we conclude that

$$\deg(t_x^*\mathscr{L}'|_C) = \deg(t_e^*\mathscr{L}|_C) = \deg(\mathscr{L}'|_C) = \deg(\mathcal{O}_C) = 0.$$

Since E' is an effective divisor, this implies that either $(x+E') \supseteq C$ or $(x+E')\cap C = \emptyset$, since any proper nonempty intersection would yield $\deg(t_x^*\mathscr{L}'|_C) \geq \#\{(x+E')\cap C\} > 0$.

Finally, let $x, y \in C$ and $z \in E'$. Then $z \in (z-y+C)\cap E'$, hence $z-y+C \subseteq E'$, hence, $z - y + x \in E'$. Since z is an arbitrary point in E', we conclude $E' - y + x = E'$. ■

- (4) $\implies$ (1): We need only show that $\mathscr{L}^{\otimes 2} = \mathcal{O}(2D)$ is ample, since radicals of ample sheaves are again ample. We claim that the pullback of an ample line bundle by a finite morphism is ample. Serre's criterion for ampleness states that a line bundle $\mathscr{L}/X$ is ample if and only if

$$H^i(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n}) = 0$$

for all coherent $\mathscr{F}$, all $i > 0$, and sufficiently large n (depending on $\mathscr{F}$).

Given (4), let $\varphi : A \to \mathbb{P}^N$ be the finite morphism associated to the linear system $|2D|$. Finite pushforward commutes with taking cohomology, so

$$H^i(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n}) = H^i(\mathbb{P}^N, \phi_*(\mathscr{F} \otimes \mathscr{L}^{\otimes n})) = H^i(\mathbb{P}^N, \phi_*\mathscr{F} \otimes \mathcal{O}(n)),$$

which is zero for sufficiently large n since $\mathcal{O}(1)$ is ample on $\mathbb{P}^N$. (The isomorphism $\phi_*(\mathscr{F} \otimes \mathscr{L}^{\otimes n}) \simeq \phi_*\mathscr{F} \otimes \mathcal{O}(n)$ follows from the projection formula.)

■

Definition 12.3. If $\mathscr{L}$ is a line bundle on A, we say that $\mathscr{L}$ is *nondegenerate* if $K(\mathscr{L})$ is finite.

13 Multiplication by n (02/14/2024 ♡)

We began class by finishing the (3) $\implies$ (4) part of Theorem 12.4; this argument has been recorded in the previous section.

13.1 Multiplication by n is an isogeny

Corollary 13.1. On an abelian variety A, the map $[n] : A \to A$ is an isogeny.

Proof. It turns out that being a self-isogeny is equivalent to being surjective, which is also equivalent to having finite kernel. We won't prove this; see [Mil86, Prop. 7.1].

So we only need to show that $[n]$ has finite kernel.[11] Since we now know that abelian varieties are projective, pick an ample line bundle $\mathscr{L}$. By Corollary 9.10, we have

$$[n]^*\mathscr{L} \simeq \mathscr{L}^{\otimes n(n+1)/2} \otimes [-1]^*\mathscr{L}^{\otimes n(n-1)/2}.$$

The right hand side is a product of ample line bundles, so $[n]^*\mathscr{L}$ is also ample. Since $[n]^*\mathscr{L}|_{\ker[n]}$ is a pullback of the trivial line bundle $\mathscr{L}|_e$, we have

$$[n]^*\mathscr{L}|_{(\ker[n])^0_{\mathrm{red}}} \simeq \mathcal{O}_{(\ker[n])^0_{\mathrm{red}}}.$$

But restriction of line bundles preserves ampleness, so the trivial bundle on the proper scheme $(\ker[n])^0_{\mathrm{red}}$ is ample, hence very ample since it remains unchanged by taking tensor powers of itself! Since $\mathcal{O}_{(\ker[n])^0_{\mathrm{red}}}$ is proper and geometrically irreducible (being a reduced proper connected group scheme), the global sections of $\mathcal{O}_{(\ker[n])^0_{\mathrm{red}}}$ are just k, so we conclude that $(\ker[n])^0_{\mathrm{red}}$ consists only of the single point $e \in A$, since the global sections of a very ample line bundle separate points. Since $\ker[n]$ has only finitely many components, and $(\ker[n])^0$ must have finite length if its reduction is a point, we conclude $\ker[n]$ is a finite subscheme of A. ■

Remark 13.2. This fact, as well as Corollary 13.5, does not depend on $\mathrm{char}(k)$. However, many other properties of $\ker[n]$ depend on whether $\mathrm{char}(k) \mid n$. For example, $[n]$ is inseparable iff $\ker[n]$ is nonreduced iff $\mathrm{char}(k) \mid n$.

[11] The kernel of a morphism of group schemes $f : X \to Y$ is the fiber X_{e_y}, which is a group subscheme of X. In positive characteristic, this might not be reduced even if f is a morphism of group varieties. The kernel subscheme represents the kernel on the functor of points; that is, if $f : X \to Y$ is a morphism of S-group schemes, then $(\ker f)(T) = \ker(f_T : X(T) \to Y(T))$ for S-schemes T.

13.2 Degree

Definition 13.1. Let $f : X \to Y/k$ be a dominant morphism with $\dim X = \dim Y$. We define $\deg f := [k(X) : k(Y)]$ via the induced embedding of function fields.

We say f is *separable* if this $k(X)/k(Y)$ is a separable field extension. In general, letting $k(Y)^s$ be the separable closure of $k(Y)$ in $k(X)$, we define the *inseparable degree* of f to be $[k(X) : k(Y)^s]$.

Definition 13.2. Let X/k be a proper variety with line bundle $\mathscr{L}$. For a coherent sheaf $\mathscr{F}$ on X, we define the *Hilbert polynomial* of $\mathscr{F}$ with respect to $\mathscr{L}$ as

$$p_{\mathscr{L}}(\mathscr{F}, n) := \chi(F \otimes \mathscr{L}^n).$$

where χ is the Euler characteristic. Fact: $p_{\mathscr{L}}(\mathscr{F}, n)$ is a numeric polynomial in n of degree at most $\dim X$, in fact of degree equal to the dimension of the support of $\mathscr{F}$. This is easier to show if $\mathscr{L}$ is ample, using Serre's criterion for ampleness, but it is true for general $\mathscr{L}$.

We define the *degree* $d_{\mathscr{L}}(\mathscr{F})$ of $\mathscr{F}$ with respect to $\mathscr{L}$ to be the number such that

$$p_{\mathscr{L}}(\mathscr{F}, n) = d_{\mathscr{L}}(\mathscr{F}) \frac{n^{\dim X}}{(\dim X)!} + O(n^{\dim X - 1}).$$

This is always an integer.

Finally, we define $\deg \mathscr{L} := d_{\mathscr{L}}(\mathcal{O}_X)$ to be the degree of $\mathscr{L}$. If $\mathscr{L}$ is very ample, then we also define this number to be the degree of X with respect to the corresponding embedding into projective space.

See [Vak, §18.6] for more discussion on Hilbert polynomials and degree.

Proposition 13.3. Let $f : X \to Y/k$ dominant with X, Y proper of equal dimension. Then

$$\deg(f) \cdot \deg(\mathscr{L}) = \deg(f^* \mathscr{L}).$$

Proof. See Proposition 14.1 from the next lecture. ■

Proposition 13.4. $\deg(\mathscr{L}^{\otimes m}) = m^{\dim X} \deg(\mathscr{L})$

Proof. Immediately from the definition, $p_{\mathscr{L}^{\otimes m}}(\mathcal{O}_X, n) = p_{\mathscr{L}}(\mathcal{O}_X, mn)$. Therefore, the degree $\dim X$ term of $p_{\mathscr{L}^m}(\mathcal{O}_X, n)$ is

$$\deg(\mathscr{L}) \cdot \frac{(mn)^{\dim X}}{(\dim X)!} = m^{\dim X} \deg(\mathscr{L}) \cdot \frac{n^{\dim X}}{(\dim X)!}.$$

■

Corollary 13.5. $[n] : A \to A$ has degree $n^{2 \dim A}$.

Proof. Take $\mathscr{L}/A$ ample. Then $\deg \mathscr{L} > 0$. We may assume $\mathscr{L}$ is symmetric by replacing it with $\mathscr{L} \otimes [-1]^* \mathscr{L}$ if needed. By 9.10, we have $[n]^* \mathscr{L} \simeq \mathscr{L}^{\otimes n^2}$. Then by Propositions

13.3 and 13.4, we have

$$\deg([n]) \cdot \deg(\mathscr{L}) = \deg([n]^*\mathscr{L}) = \deg(\mathscr{L}^{\otimes n^2}) = n^{2\dim A}\deg(\mathscr{L}),$$

so dividing both sides by $\deg(\mathscr{L})$ gives the formula. ∎

14 Separability (02/16/2024)

14.1 Degree of a sheaf under pullback

Proposition 14.1. Let X be a geometrically integral variety.

1. Let $\mathscr{F}$ be a coherent sheaf on X, say with rank r at the generic point $\eta \in X$. Then $d_{\mathscr{L}}(\mathscr{F}) = r\deg(\mathscr{L})$.
2. Let $f : X \to Y$ be dominant with $\dim X = \dim Y$, and let $\mathscr{L}/Y$ be a line bundle. Then $\deg f \cdot \deg(\mathscr{L}) = \deg(f^*\mathscr{L})$.

Proof. 1. See [Mum08, Appendix to §II.6]. This is a standard *dévissage* argument; we argue by induction on $\dim \operatorname{supp}(\mathscr{F})$. By the long exact sequence in cohomology, the Euler characteristic χ is additive in exact sequences. Suppose that we can show that there exists a coherent sheaf of ideals $\mathscr{I}$ such that

$$0 \longrightarrow \mathscr{I}^{\oplus r} \longrightarrow \mathscr{F} \longrightarrow \mathscr{T} \longrightarrow 0$$

where $\mathscr{T}$ is a torsion sheaf[12] with support contained in some closed subscheme of X of dimension $< \dim X$, and such that $\mathcal{O}_X/\mathscr{I}$ also has support in a closed subscheme of dimension $< \dim X$. Then by additivity of χ we get $d_{\mathscr{L}}(\mathscr{F}) = r \cdot d_{\mathscr{L}}(\mathscr{I}) = r \cdot \deg(\mathscr{L})$, as desired, since $p_{\mathscr{L}}(\mathscr{T})$ has degree strictly less than $\dim X$ and therefore does not contribute to the leading term in

$$d_{\mathscr{L}}(\mathscr{F}) = d_{\mathscr{L}}(\mathscr{I}^{\oplus r}) + d_{\mathscr{L}}(\mathscr{T}) = r \cdot d_{\mathscr{L}}(\mathscr{I}) + d_{\mathscr{L}}(\mathscr{T}).$$

We also have the exact sequence

$$0 \longrightarrow \mathscr{I} \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_X/\mathscr{I} \longrightarrow 0$$

so by the same reasoning and the assumption on $\mathcal{O}_X/\mathscr{I}$ we conclude $d_{\mathscr{L}}(\mathscr{I}) = d_{\mathscr{L}}(\mathcal{O}_X) =: \deg(\mathscr{L})$. Combining these two formulae gives the desired formula for $d_{\mathscr{L}}(\mathscr{F})$.

The fact that such a map $\mathscr{I}^{\oplus r} \to \mathscr{F}$ exists is a standard fact, but takes some legwork to prove (and Mumford omits the proof). For a full proof, we refer to [Sta24, Tag 01YE] and its prerequisites [Sta24, Tag 01YB] and [Sta24, Tag 01PQ], which give a proof using the Artin-Rees lemma.

[12] A sheaf with stalk 0 at all generic points; see [Vak, Def. 6.1.5].

2. In the case that f is finite, pushforward commutes with cohomology, hence

$$\begin{aligned} H^i(X, f^*\mathscr{L}^{\otimes n}) &\simeq H^i(Y, f_*f^*\mathscr{L}^{\otimes n}) \\ &\simeq H^i(Y, f_*\mathcal{O}_X \otimes \mathscr{L}^{\otimes n}), \end{aligned}$$

using the projection formula, so $\deg(f^*\mathscr{L}) = d_{\mathscr{L}}(f_*\mathcal{O}_X)$ equals $\deg(f)\deg(\mathscr{L})$ by part (1) with $\mathscr{F} = f_*\mathcal{O}_X$.

More generally, if $f : X \to Y$ is dominant with $\dim X = \dim Y$, then there is some open $V \subseteq Y$ such that $f : f^{-1}(V) \to V$ is finite, so that the higher pushforwards $R^i f_* f^* \mathscr{L}^{\otimes n}, i > 0$, have support outside V. One can show using the Leray spectral sequence that

$$\chi(f^*\mathscr{L}^{\otimes n}) = \sum_i (-1)^i \chi(R^i f_* f^* \mathscr{L}^{\otimes n}),$$

and the only term on the right hand side contributing to the leading coefficient of the Hilbert polynomial is the $i = 0$ term, i.e. the term $\chi(f_*f^*\mathscr{L}^{\otimes n}) = \chi(f_*\mathcal{O}_X \otimes \mathscr{L}^n)$, so we conclude as in the finite case.

■

14.2 (In)separability of $[n]$

Theorem 14.2. Let A be an abelian variety over a field k of characteristic $p > 0$. and let $[n] : A \to A$ be multiplication by n.

1. $[n]$ is a separable morphism if and only if $p \nmid n$.
2. $\deg_i([p]) \geq p^{\dim A}$ (inseparable degree).

Proof. 1. By definition, $[n]$ is separable if and only if $[n]$ is smooth at the generic point, if and only if $[n]$ is smooth on some nonempty open set U since smoothness is an open condition, if and only if $[n]$ is smooth at e by homogeneity considerations. The differential $d[n]|_e : \mathrm{Lie}(A) \to \mathrm{Lie}(A)$ is multiplication by n, since one can check that the differential of the group law

$$dm|_e : \mathrm{Lie}(A) \oplus \mathrm{Lie}(A) \to \mathrm{Lie}(A)$$

is just addition (see [Mum08, p.40]). Hence $d[n]|_e$ is the zero map if $p \mid m$ and an isomorphism otherwise. $[n]$ is smooth at e if and only its differential is an isomorphism, so we get separability if and only if $p \nmid m$.

2. As we just saw, the map $d[p]_e$ is the zero map, so $[p]^*\Omega^1_A \to \Omega^1_A$ is also the zero map, i.e. for all $f \in k(A)$, we have $[p]^*df = d([p]^*f) = 0$ as an element of $\Omega^1_{k(A)/k}$. Hence $[p]^*f \in (k(A))^p \cdot k$, since these are the only elements whose differential is 0 (exercise).

Therefore, $[p]^* : k(A) \to k(A)$ has image contained in $k(A)^p \cdot k$. We know $\mathrm{tr.deg}(k(A)) = \dim A$, so $k(A)/(k(A)^p \cdot k)$ is a purely inseparable extension of at least $p^{\dim A}$ (choose

a transcendence basis for $k(A)/k$ to see this). Therefore the inseparable degree of $[p]$ is at least $p^{\dim A}$.

■

Corollary 14.3. Let $\dim A = g$, and let $A(\overline{k})[n]$ be the kernel of $[n]$ on points $A(\overline{k})$. Then as an abstract group,

$$A(\overline{k})[n] = \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g} : & p \nmid n \\ (\mathbb{Z}/p^m\mathbb{Z})^{2g-\deg_i([p])} : & n = p^m \end{cases}$$

In the second case, $2g - \deg_i([p]) \leq g$. For a prime $\ell \neq p$, the Tate module is $T_\ell(A) = \mathbb{Z}_\ell^{2g}$.

Proof. The separable degree of a finite morphism of varieties is the number of points in a general fiber (working over $\overline{k}$). For a group scheme, by homogeneity considerations all fibers over $\overline{k}$-valued points are isomorphic, so in particular $\#[n]^{-1}(\{e\}) = \deg_s[n]$. This gives the correct order in the separable case. In the inseparable case, we deduce the separable degrees of $[p^e]$ from $[p]$: we have an exact sequence

$$0 \longrightarrow A(\overline{k})[p] \longrightarrow A(\overline{k})[p^e] \longrightarrow A(\overline{k})[p^{e-1}] \longrightarrow 0$$

so by induction we conclude that $\deg_s([p^e]) = (\deg_s([p])^e$.

Then the group structure can be determined by the fact that

$$A(\overline{k})[n] = \prod_\ell A(\overline{k})[\ell^{v_\ell(n)}]$$

via the Chinese remainder theorem, and the structure theorem for finitely generated abelian groups along with the fact that $A(\overline{k})[\ell^e]$ is ℓ^e-torsion determines the group structure in the prime power case. ■

Remark 14.4. This tells us that the p-adic Tate module of A is not necessarily very useful. Instead, the "correct" group would be the p-divisible group associated to A, or its corresponding Dieudonné module. This is the start of the story of crystalline cohomology—a p-adic Weil cohomology theory to remedy the failures of p-adic étale cohomology—but we won't discuss this further in this course.

14.3 Picard scheme

See also [Con15, Theorem 2.3.1] or [BLR90, §8]. Let X/k be a geometrically integral projective variety with a rational point $x \in X(k)$.[13]

Definition 14.1. The *Picard functor* $\mathrm{Pic}_{X/k} : \mathbf{Sch}_k^{\mathrm{op}} \to \mathbf{Set}$ is defined on objects (k-schemes T) by

$$\mathrm{Pic}_{X/k}(T) := \{\text{iso. classes of line bundles on } \mathrm{Pic}(X \times_k T)\}/\sim$$

[13]These assumptions are not strictly necessary but they make things a lot easier.

where we define the equivalence relation $\mathscr{L} \sim \mathscr{L}'$ if these two line bundles differ by the pullback of some line bundle on T (via $X \times T \to T$).

Alternatively, this is

$$\{(\mathscr{L}, \alpha) : \mathscr{L} \text{ line bundles on } X \times T, \alpha : \mathscr{L}|_{\{x\}\times T \simeq \mathcal{O}_T}\}/\sim$$

Here, the pair $(\mathscr{L}, \alpha)$ is a *rigidified line bundle*: $\mathscr{L}$ is a line bundle on $X \times T$ that becomes isomorphic to $\mathcal{O}_T$ under restriction to $\{x\} \times T$, and α is a *specific* choice of such an isomorphism $\alpha : \mathscr{L}|_{\{x\}\times T} \to \mathcal{O}_T$. The relation $\sim$ is isomorphism of rigidified line bundles, i.e. $(\mathscr{L}, \alpha) \sim (\mathscr{L}', \alpha')$ if there exists an isomorphism $\phi : \mathscr{L} \to \mathscr{L}'$ making the following diagram commute:

$$\begin{array}{ccc} \mathscr{L}|_{\{x\}\times T} & \xrightarrow{\phi|_{\{x\}\times T}} & \mathscr{L}'|_{\{x\}\times T} \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \alpha'} \\ & & \mathcal{O}_T \end{array}$$

Given a morphism of k-schemes $f : S \to T$, we define $\mathrm{Pic}_{X/k}(f) : \mathrm{Pic}_{X/k}(T) \to \mathrm{Pic}_{X/k}(S)$ via pullback of rigidified line bundles by f^*, i.e. sending $(\mathscr{L}, \alpha)$ to $((\mathbf{id}_X \times f^*)\mathscr{L}, f^*(\alpha))$.

Remark 14.5. One upshot of rigidified line bundles is that any isomorphism of rigidified line bundles is unique. It is necessary to define the Picard functor using isomorphism classes rigidified line bundles instead of just isomorphism classes of line bundles if we want it to be representable. In practice, this distinction is usually not a big deal: when K/k is a field extension, we have a natural group isomorphism $\mathrm{Pic}_{X/k}(K) = \mathrm{Pic}(X_K) : [(\mathscr{L}, \alpha)] \mapsto [\mathscr{L}]$. Surjectivity is just the fact that all line bundles on $\operatorname{Spec} k$ are trivial, and injectivity is also easy to check by appropriately adjusting trivialization.

We blackbox:

Theorem 14.6. *(Grothendieck.)* Let X/k be a smooth projective variety with $X(k) \neq \emptyset$.

1. $\mathrm{Pic}_{X/k}$ is representable by a separated k-scheme locally of finite type.
2. $\mathrm{Pic}^0_{X/k}$ (neutral component of the scheme $\mathrm{Pic}_{X/k}$) is quasi-projective, and is projective if X is smooth.

Corollary 14.7. $\mathrm{Pic}_{X/k}$ is a commutative group scheme.

Proof. For any k-scheme T, the set $\mathrm{Pic}_{X/k}(T)$ of classes of rigidified line bundles on $X \times T$ is a commutative group via tensor product, and pullback is compatible with this group structure, so we conclude that the functor $\mathrm{Pic}_{X/k}$ factors naturally through the category of abelian groups. By Yoneda, this is equivalent to being a commutative group scheme. ■

We will deduce other properties of the scheme $\mathrm{Pic}_{X/k}$ from these facts. We will be especially interested in the case that X is an abelian variety; this will be our construction of the dual abelian variety.

15 Comparison of $\mathrm{Pic}^0_{A/k}$ and $\mathrm{Pic}^0(A)$ (02/21/2024)

Let A/k be an abelian variety. We previously defined a group $\mathrm{Pic}^0(A) \subseteq \mathrm{Pic}(A)$ for an abelian variety A back in Definition 12.1, and last lecture we defined the Picard scheme $\mathrm{Pic}^0_{A/k}$. To justify the suggestive similarity in notation:

Theorem 15.1. $\mathrm{Pic}^0_{A/k}(k) \simeq \mathrm{Pic}^0(A)$ naturally. Here, $\mathrm{Pic}^0_{A/k}(k)$ is the group of k-valued points of neutral connected component of the Picard scheme, and $\mathrm{Pic}^0(A)$ is the group of translation-invariant line bundles $\mathscr{L}$ on A.

Definition 15.1. We notate $A^\vee = \mathrm{Pic}^0_{X/k}$, and call this the *dual abelian variety* to A. It turns out that this is a smooth projective group scheme over k, hence also an abelian variety. We will prove smoothness in Theorem 16.2 shortly.

Definition 15.2. Let $T = \mathrm{Pic}_{X/k}$, and consider $\mathbf{id}_T \in \mathrm{Hom}(T, T)$. By the Yoneda lemma, $\mathbf{id}_T$ corresponds to some "universal" rigidified line bundle $(\mathcal{P}_{\mathrm{univ}}, \alpha_{\mathrm{univ}})$, called the *Poincaré bundle*, on $X \times_k \mathrm{Pic}_{X/k}$, where $\mathcal{P}_{\mathrm{univ}}$ is a line bundle and $\alpha_{\mathrm{univ}} : \mathcal{P}_{\mathrm{univ}}|_{\{x\}\times \mathrm{Pic}_{X/k}} \simeq \mathcal{O}_{\mathrm{Pic}_{X/k}}$ is a trivialization.

Remark 15.2. This line bundle is universal in the sense that given any scheme T/k and rigidified line bundle $(\mathscr{L}, \alpha)$ over $X \times T$, there exists a unique morphism $\varphi : T \to \mathrm{Pic}_{X/k}$ such that $(\mathscr{L}, \alpha) = \varphi^*(\mathcal{P}_{\mathrm{univ}}, \alpha_{\mathrm{univ}})$. This more or less the content of the Yoneda lemma.
In particular, if $\lambda \in \mathrm{Pic}_{X/k}(k')$ for a field extension k'/k, the base change $\mathcal{P}_{\mathrm{univ}}|_{X\times\{\lambda\}}$ is the line bundle on $X_{k'}$ corresponding to λ. This is often the most concrete way to think about the Poincaré bundle and is very useful in practice.

Definition 15.3. Let $\mathscr{M}, \mathscr{N}$ be line bundles on $X_{\overline{k}}$. We say that these two line bundles are *algebraically equivalent* if there exists a connected $\overline{k}$-variety T, a line bundle $\mathscr{L}$ on $X_{\overline{k}} \times T$, and $t_1, t_2 \in T(\overline{k})$ such that $\mathscr{M} \simeq \mathscr{L}|_{\overline{k}\times\{t_1\}}$ and $\mathscr{N} \simeq \mathscr{L}|_{X_{\overline{k}}\times\{t_2\}}$.

Remark 15.3. A special case of algebraic equivalence is *rational equivalence*, which is when T can be taken to be $\mathbb{P}^1$ in the definition of algebraic equivalence.

Lemma 15.4. Let $\mathscr{L}'/X$ be a line bundle corresponding to $\lambda \in \mathrm{Pic}_{X/k}(k)$. Then $\lambda \in \mathrm{Pic}^0_{X/k}(k)$ if and only if $\mathscr{L}'_{\overline{k}}$ is algebraically equivalent to $\mathcal{O}_{X_{\overline{k}}}$.

Proof. $\implies$: If $\lambda \in \mathrm{Pic}^0_{X/k}(k)$, then let $T = ((\mathrm{Pic}^0_{X/k})_{\overline{k}})_{\mathrm{red}}$. Then, as we remarked above, $\mathcal{P}_{\mathrm{univ}}|_{X\times\{\lambda\}} \simeq \mathscr{L}'$, and $\mathcal{P}_{\mathrm{univ}}|_{X\times\{e_{A^\vee}\}} \simeq \mathcal{O}_X$, since by definition the identity element of $A^\vee(k)$ corresponds to the trivial line bundle on A.

$\Longleftarrow$: If we have algebraic equivalence by some T, write T as a union of connected open subschemes $\{U_i\}$ trivializing $\mathscr{L}|_{X\times U_i}$, with fixed choices of trivialization α_i. Each of these is the datum of a rigidified line bundle on $X \times U_i$ over U_i, so by the definition of $\mathrm{Pic}_{X/k}$, these data correspond to morphisms $\psi_i : U_i \to \mathrm{Pic}_{X/k}$ for each U_i. These glue to a map $\psi : T \to \mathrm{Pic}^0_{X/k}$, since the rigidified line bundles $(\mathscr{L}|_{X\times U_i}, \alpha_i)$ become isomorphic on overlaps $U_i \cap U_j$.

With t_1, t_2 as in the definition of algebraic equivalence, by hypothesis we have $\mathscr{L}|_{X_{\overline{k}}\times\{t_1\}} \simeq \mathscr{L}_{\overline{k}}$ and $\mathscr{L}|_{X_{\overline{k}}\times\{t_2\}} \simeq \mathcal{O}_{X_{\overline{k}}}$. Since the U_i cover T, at least one of the U_i, say U_2, contains t_2. The condition $\mathscr{L}|_{X_{\overline{k}}\times\{t_2\}} \simeq \mathcal{O}_{X_{\overline{k}}}$ means that $\psi_2(t_2)$ is the identity element in $\mathrm{Pic}^0_{X/k}$ (apply functoriality of $\mathrm{Pic}_{X/k}$ to the morphism $t_2 \hookrightarrow U_2$ and unravel the definitions; the same reasoning shows that $\lambda = \psi(t_1)$). Since we have taken U_2 to be connected, this means that $\psi_2(U_2) \subseteq \mathrm{Pic}^0_{X/k}$. Since T is also connected, we conclude $\psi(T) \subseteq \mathrm{Pic}^0_{X/k}$ too. In particular $\psi(t_1) = \lambda \in \mathrm{Pic}^0_{X/k}$. ■

We can now prove Theorem 15.1.

Proof. We first show $\mathrm{Pic}^0_{A/k}(k) \hookrightarrow \mathrm{Pic}^0(A)$ naturally. The desired map is given by sending a point in $\mathrm{Pic}^0_{A/k}(k)$ to the corresponding line bundle in $\mathrm{Pic}(A)$, which is injective by Remark 14.5. Thus we need to show that the image of this map lies in $\mathrm{Pic}^0(A)$; we will apply the criterion from Lemma 12.2. We remark that $\mathrm{Pic}^0_{A/k}(\overline{k}) \to \mathrm{Pic}^0(A_{\overline{k}})$ restricts to $\mathrm{Pic}^0_{A/k}(k) \to \mathrm{Pic}^0(A)$, and likewise the preimage of $\mathrm{Pic}^0(A)$ is contained in $\mathrm{Pic}^0_{A/k}(k) \subseteq \mathrm{Pic}^0_{A/k}(\overline{k})$, which is immediate from the definitions. Therefore we may and do assume that $k = \overline{k}$ for the remainder of this section.

Let $\mathcal{P} = \mathcal{P}_{\mathrm{univ}}|_{A\times(A^\vee)_{\mathrm{red}}}$. Consider the three morphisms $A \times A \times A^\vee_{\mathrm{red}} \to A \times A^\vee_{\mathrm{red}}$ given by $m \times \mathbf{id}, \mathrm{pr}_1 \times \mathbf{id}, \mathrm{pr}_2 \times \mathbf{id}$ (which we abbreviate to m, pr_1, and pr_2 in the sequel), and let

$$\mathscr{M} := m^*\mathcal{P} \otimes \mathrm{pr}_1^*\,\mathcal{P}^{-1} \otimes \mathrm{pr}_2^*\,\mathcal{P}^{-1}.$$

Note that $\mathcal{P}|_{\{e\}\times A^\vee_{\mathrm{red}}} \simeq \mathcal{O}_{A^\vee_{\mathrm{red}}}$—by definition the Poincaré bundle has a trivialization in this way—and also $\mathcal{P}|_{A\times\{e_{A^\vee}\}} \simeq \mathcal{O}_A$, again as a special case of Remark 15.2. Hence $\mathscr{M}|_{\{e\}\times A\times A^\vee_{\mathrm{red}}} \simeq \mathrm{pr}_1^*(\mathcal{P}|_{\{e\}\times A^\vee_{\mathrm{red}}}) \simeq \mathcal{O}$, likewise $\mathscr{M}|_{A\times\{e\}\times A^\vee_{\mathrm{red}}} \simeq \mathcal{O}$, and also $\mathscr{M}|_{A\times A\times\{e\}} \simeq (m^* \otimes \mathrm{pr}_1^* \otimes \mathrm{pr}_2^*)(\mathcal{P}|_{A\times\{e\}}) \simeq \mathcal{O}$. By the Theorem of the Cube[14] we conclude $\mathscr{M}$ is also trivial.

Let $\mathscr{L}/A$ correspond to $\lambda \in \mathrm{Pic}^0_{A/k}(k)$, so that $\mathcal{P}|_{A\times\{\lambda\}} \simeq \mathscr{L}$. Then

$$m^*\mathscr{L} \otimes \mathrm{pr}_1^*\,\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\,\mathscr{L}^{-1} = \mathscr{M}_{A\times\{\lambda\}} = \mathcal{O}.$$

Hence by Lemma 12.2 we conclude $\mathscr{L} \in \mathrm{Pic}^0(A)$, proving $\mathrm{Pic}^0_{A/k}(k) \hookrightarrow \mathrm{Pic}^0(A)$.

Now we show $\mathrm{Pic}^0_{A/k}(k) \hookrightarrow \mathrm{Pic}^0(A)$ is surjective. We will tackle this in the following way:

Lemma 15.5. Given $\mathscr{L} \in \mathrm{Pic}(A)$, the map $\phi_{\mathscr{L}} : A(k) \to \mathrm{Pic}^0(A_k)$ factors through the map $\mathrm{Pic}^0_{A/k}(k) \hookrightarrow \mathrm{Pic}^0(A_k)$ defined above; equivalently, $t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \in \mathrm{Pic}^0_{A/k}(k)$ for every $x \in A(k)$.

[14] To apply the Theorem of the Cube, we need everything to be reduced, which is why we are using $A^\vee_{\mathrm{red}}$. Of course, we will soon show that $A^\vee$ is already reduced.

Proof. We apply the criterion from Lemma 15.4; it suffices to show that $t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ is algebraically equivalent to $\mathcal{O}_A$. Consider the line bundle $m^*\mathscr{L}$ on $A \times A$; for any $y \in A(k)$, the translation map τ_y is the composition

$$A \simeq A \times \{y\} \hookrightarrow A \times A \xrightarrow{m} A$$

so $m^*\mathscr{L}|_{A\times\{x\}} = \tau_x^*\mathscr{L}$. Additionally, $\mathrm{pr}_1^*\mathscr{L}|_{X\times\{y\}} = \mathscr{L}$ for any y. Therefore, letting $\mathscr{M} = m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1}$, we have

$$\begin{aligned}\mathscr{M}|_{A\times\{x\}} &\simeq \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \\ \mathscr{M}|_{A\times\{e\}} &\simeq \tau_e^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathcal{O}_A,\end{aligned}$$

yielding the desired algebraic equivalence. ∎

In particular, if $\phi_{\mathscr{L}}$ is surjective for *any* line bundle $\mathscr{L}$, so is $\mathrm{Pic}^0_{A/k}(k) \hookrightarrow \mathrm{Pic}^0(A_k)$. Since we know abelian varieties have ample line bundles, it therefore suffices to prove:

Theorem 15.6. $\phi_{\mathscr{L}} : A(k) \to \mathrm{Pic}^0(k)$ is surjective when $\mathscr{L}/A$ is ample.

Lemma 15.7. Let $\mathscr{L}' \in \mathrm{Pic}^0(A)$ be nontrivial. Then $H^i(A, \mathscr{L}') = 0$ for all i.

Proof. We first show $H^0(A, \mathscr{L}') = 0$. Otherwise, we can write $\mathcal{O}(D) \simeq \mathscr{L}'$ for some effective divisor $D \subset A$. We have

$$\mathcal{O}_A = e^*\mathscr{L} = ((\mathbf{id} \times [-1])^* \circ m^*)\mathscr{L}' = \mathscr{L}' \otimes [-1]^*\mathscr{L}',$$

where we again apply Lemma 12.2 for the last isomorphism. Hence the trivial divisor is linearly equivalent to the effective divisor $D + [-1]^*D$, but this can only happen when $D = 0$ and $\mathscr{L}' \simeq \mathcal{O}_A$.

In general, if the lemma is false, let k be the smallest integer such that $H^k(A, \mathscr{L}') \neq 0$. We know $k > 0$. By functoriality of pullback on sheaf cohomology, the composition

$$H^k(A, \mathscr{L}') \xrightarrow{m^*} H^k(A \times A, m^*\mathscr{L}') \xrightarrow{(\{e\}\times\mathbf{id})^*} H^k(A, \mathscr{L}')$$

is the identity. Hence $H^k(A \times A, m^*\mathscr{L}') \neq 0$.

Again by Lemma 12.2, we have $m^*\mathscr{L} = \mathrm{pr}_1^*\mathscr{L}' \otimes \mathrm{pr}_2^*\mathscr{L}'$. Hence by the Künneth formula,

$$H^k(A \times A, m^*\mathscr{L}') = \bigoplus_{i+j=k} H^i(A, \mathscr{L}') \otimes H^j(A, \mathscr{L}')$$

But the terms with $i = 0$ or $j = 0$ are zero by the base case proven previously, so nonzero-ness of this direct sum contradicts minimality of k. ∎

We finally prove Theorem 15.6. Recall the standing assumption $k = \overline{k}$. We will need the Leray spectral sequence:

Lemma 15.8. *(Leray Spectral Sequence, [Sta24, Tag 01EY])* For a morphism $f : X \to Y$ of ringed spaces and an $\mathcal{O}_X$-module $\mathscr{F}$, there is a spectral sequence $E_2^{p,q} = H^p(Y, R^q f_* \mathscr{F})$ converging to $H^{p+q}(X, \mathscr{F})$.

We will not discuss spectral sequences in this course, so feel free to ignore the full statement.[15] Here are some consequences and reasons we care:

Corollary 15.9.

1. The cohomology group $H^n(X, \mathscr{F})$ has a filtration by subquotients of the cohomology groups $H^p(Y, R^q f_* \mathscr{F})$ for various p, q. In particular, if $H^p(Y, R^q f_* \mathscr{F}) = 0$ for all p, q, then $H^n(X, \mathscr{F}) = 0$ for all n, too.
2. If $H^p(Y, R^q f_* \mathscr{F}) = 0$ for all $p > 0$ and all q, then

$$H^p(X, \mathscr{F}) = H^0(Y, R^p f_* \mathscr{F}) = \Gamma(Y, R^p f_* \mathscr{F}).$$

Suppose, for the sake of contradiction, that there exists a line bundle $\mathscr{M} \in \mathrm{Pic}^0(A)$ not in the image of $\phi_{\mathscr{L}}$, i.e. such that

$$\mathscr{M} \not\simeq t_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$$

for all $x \in A(k)$. Consider $\mathscr{N} := m^* \mathscr{L} \otimes \mathrm{pr}_1^* \mathscr{L}^{-1} \otimes \mathrm{pr}_2^*(\mathscr{L}^{-1} \otimes \mathscr{M}^{-1})$ on $A \times A$. By the Leray Spectral Sequence, $H^i(A, R^j \mathrm{pr}_{1,*} \mathscr{N})$ converges to $H^{i+j}(A \times A, \mathscr{N})$. Note that

$$\mathscr{N}_{\{x\} \times A} = t_x^* \mathscr{L} \otimes \mathscr{L}^{-1} \otimes \mathscr{M}^{-1} \neq \mathcal{O}_A$$

by assumption, so Lemma 15.7 we have $H^j(A, \mathscr{N}|_{\{x\} \times A}) = 0$ for all j. By Grauert's theorem we conclude $R^j \mathrm{pr}_{1,*} \mathscr{N} = 0$, hence by Corollary 15.9 we have

$$H^n(A \times A, \mathscr{N}) = 0 \tag{7}$$

for all n.

Now consider $R^j \mathrm{pr}_{2,*} \mathscr{N}$. Then

$$\mathscr{N}|_{A \times \{x\}} = t_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$$

which is trivial if and only if $x \in K(\mathscr{L})$, so Lemma 15.7 states that $H^j(A, \mathscr{N}|_{A \times \{x\}}) = 0$ for all $x \in A \setminus K(\mathscr{L})$, so $R^j \mathrm{pr}_{2,*} \mathscr{N}|_{A \setminus K(\mathscr{L})} = 0$. Recall that $K(\mathscr{L})$ is finite since $\mathscr{L}$ is ample. Therefore, $R^j \mathrm{pr}_{2,*} \mathscr{N}$ is a coherent sheaf supported on the finite set $K(\mathscr{L})$. Since this is a zero dimensional set, we conclude $H^i(A, R^j \mathrm{pr}_{2,*} \mathscr{N}) = 0$ for all $i > 0$, so by Corollary 15.9 we have $H^n(A \times A, \mathscr{N}) = \Gamma(A, R^n \mathrm{pr}_{2,*} \mathscr{N})$, so both of these groups are 0 by Equation (7). Since $R^n \mathrm{pr}_{2,*} \mathscr{N}$ is a quasi-coherent sheaf supported on a zero dimensional (affine) set without any nonzero global sections, we conclude $R^n \mathrm{pr}_{2,*} \mathscr{N} = 0$ for all n.

[15] But if you haven't studied spectral sequences before, Corollary 15.9 should be good motivation.

In particular, $\mathrm{pr}_{2,*}\mathscr{N} = 0$, so Grauert's theorem tells us that

$$H^0(A \times \{e\}, \mathscr{N}|_{A\times\{e\}}) = 0.$$

However, $\mathscr{N}|_{A\times\{e\}} = \mathcal{O}_A$ since $e \in K(\mathscr{L})$ automatically. This implies

$$H^0(A \times \{e\}, \mathscr{N}|_{A\times\{e\}}) \neq 0;$$

contradiction. Hence $\mathscr{M}$ as described cannot exist, so $\mathrm{im}(\phi_{\mathscr{L}}) = \mathrm{Pic}^0(A)$, and so also $\mathrm{Pic}^0_{A/k}(k)$ surjects onto $\mathrm{Pic}^0(A)$.

■

16 Smoothness of the dual abelian variety (02/23/2024)

We started lecture by finishing the proof of Theorem 15.6, and hence Theorem 15.1. The proof has been moved to the previous section.

Let $\mathscr{L}/A$ be a line bundle. From now on we will write $\phi_{\mathscr{L}} : A \to \mathrm{Pic}^0_{A/k}$ using the isomorphism we just gave.

Corollary 16.1. Let $\mathscr{L}/A$ be ample. Then $\phi_{\mathscr{L}}$ is surjective and $\dim A = \dim A^\vee$. (Hence an isogeny once we know that $A^\vee$ is indeed an abelian variety.)

Proof. Theorem 15.6 shows that $\phi_{\mathscr{L}}$ is surjective, and the remark at the end of Theorem 12.4 shows that $\ker \phi_{\mathscr{L}} = K(\mathscr{L})$ is finite, so the dimensions of A and $A^\vee$ must be equal. ■

Theorem 16.2. $A^\vee = \mathrm{Pic}^0_{A/k}$ is smooth.

Proof. We know from 16.1 that $\dim A^\vee = g := \dim A$. Therefore, to show smoothness, it suffices to prove that $\dim T_e A^\vee \leq \dim A := g$, since the tangent space at e always has dimension at least that of the variety, with equality if and only if e is a smooth point, equivalently $A^\vee$ smooth by translation. This fact follows immediately from Lemma 16.3 and Proposition 16.4 below.

Lemma 16.3. $T_e A^\vee \simeq H^1(A, \mathcal{O}_A)$ canonically.

Proof. Let $\Lambda = \mathrm{Spec}\, k[\epsilon]/(\epsilon^2)$ be the ring of dual numbers. One definition of the tangent space is

$$T_e A^\vee = \ker(A^\vee(\Lambda) \to A^\vee(k)).$$

This turns out to have a natural k-vector space structure agreeing with the other standard definitions of the tangent space. By the definition of $A^\vee$, we conclude:

$$T_e A^\vee = \ker(\mathrm{Pic}_{A/k}(\Lambda) \to \mathrm{Pic}_{A/k}(k))$$

This kernel consists of triples $(\mathscr{L}, \alpha, \beta)$ where $\mathscr{L}$ is a line bundle on $A \times_k \Lambda$, $\alpha : \mathscr{L}|_{e\times\Lambda} \simeq \mathcal{O}_\Lambda$ is a trivialization (part of the data of a rigidified line bundle), and $\beta : \mathscr{L}_{A\hookrightarrow A\times\Lambda} \simeq \mathcal{O}_A$ is another trivialization (corresponding to the fact that this element lies in the kernel). Fact: for a scheme X, $\mathrm{Pic}(X) = H^1(X, \mathcal{O}_X^\times)$. We have a split exact sequence

$$0 \longrightarrow \mathcal{O}_A \xrightarrow{f\mapsto 1+\epsilon f} \mathcal{O}_{A\times\Lambda}^\times) \longrightarrow \mathcal{O}_A^\times \longrightarrow 1$$

with the section $\mathcal{O}_A^\times \to \mathcal{O}_{A\times\Lambda}^\times$ given by $a \mapsto a + \epsilon \cdot 0$. This exact sequence induces an exact sequence

$$0 \longrightarrow H^1(A, \mathcal{O}_A) \longrightarrow H^1(A \times \Lambda, \mathcal{O}_{A\times\Lambda}^\times) \longrightarrow H^1(A, \mathcal{O}_A^\times) \longrightarrow 0$$

(fully exact since the original sequence splits) which we identify as

$$0 \to H^1(A, \mathcal{O}_A) \to \mathrm{Pic}(A \times \Lambda) \to \mathrm{Pic}(A) \to 0.$$

But this description of $H^1(A, \mathcal{O}_A)$ is the same as our description of $T_e A^\vee$. ■

Proposition 16.4. Suppose $k = \overline{k}$ and $\dim A = g$. Then $\dim H^1(A, \mathcal{O}_A) = g$ and $\bigwedge^\bullet H^1(A, \mathcal{O}_A) \simeq H_A := \bigoplus_{i=0}^g H^i(A, \mathcal{O}_A)$ as Hopf algebras.

Proof to come next lecture after discussing Hopf algebras. ■

17 Hopf algebras (02/26/2024)

17.1 Hopf algebra structure of cohomology

In Proposition 16.4, we claimed that $H_A := \bigoplus_{i=0}^g H^i(A, \mathcal{O}_A)$ has a Hopf algebra structure. The k-algebra structure is the graded-commutative k-algebra structure arising from the cup product. This is defined by using the Künneth isomorphism $H_A \otimes_k H_A \simeq H_{A\times A}$ and composing with $\Delta_A^* : H_{A\times A} \to H_A$, where $\Delta_A : A \hookrightarrow A \times A$ is the diagonal map. Meanwhile, the coalgebra structure is defined via $m^* : H_A \to H_{A\times A} \simeq H_A \otimes H_A$, where $m : A \times A \to A$ is the group law and we again use Künneth for the last isomorphism. Since the group law is commutative, this is a cocommutative coalgebra. Finally, the antipode is induced by $[-1]^*$.

What do all these words mean?

Definition 17.1. Let H be a k-vector space equipped with (arbitrary) k-vector space homomorphisms:

- Multiplication $m : H \otimes H \to H$;
- Comultiplication $\Delta : H \to H \otimes H$;
- Antipode $s : H \to H$;
- Counit $\epsilon : H \to k$; and
- Unit $\delta : k \to H$.

We say that H is a *Hopf algebra* if:

1. (m, δ) makes H into a (not necessarily commutative) k-algebra.
2. (Δ, ϵ) makes H into a *k-coalgebra*, i.e. such that the following diagrams commute:

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes H \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \mathbf{id}\otimes\Delta} \\ H \otimes H & \xrightarrow{\Delta\otimes\mathbf{id}} & H \otimes H \otimes H \end{array}$$

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes H \\ \downarrow{\scriptstyle \Delta} & \searrow^{\mathbf{id}} & \downarrow{\scriptstyle \mathbf{id}\times\epsilon} \\ H \otimes H & \xrightarrow{\epsilon\otimes\mathbf{id}} & H \otimes H \otimes H \end{array}$$

   These diagrams encode dual versions of associativity and the axioms of the identity, respectively.

3. $\Delta : H \to H \otimes H$ is an algebra homomorphism and $m : H \otimes H \to M$ is a coalgebra homomorphism—note that $A \otimes A$ is itself an algebra via $m \otimes m$, and likewise a coalgebra via $\Delta \otimes \Delta$.
4. The antipode s satisfies a commuting hexagon:

$$\begin{array}{ccccc} & & H \otimes H & \xrightarrow{s\otimes\mathbf{id}} & H \otimes H \\ & \nearrow^{\Delta} & & & \searrow^{m} \\ H & & \xrightarrow{\epsilon} \quad k \quad \xrightarrow{\delta} & & H \\ & \searrow_{\Delta} & & & \nearrow_{m} \\ & & H \otimes H & \xrightarrow{\mathbf{id}\otimes s} & H \otimes H \end{array}$$

   This encodes the role of s as an inversion operator for both the algebra and the coalgebra structures.

If we omit the antipode s but axioms (1)-(3) still hold, then H is instead called a *bialgebra*.

Definition 17.2. We say that a graded (non-commutative) ring H is *graded-commutative* if for all homogeneous a, b we have $ab = (-1)^{(\deg a)(\deg b)} ba$. We similarly define cocommutativity for coalgebras.

The following lemma gives one reason why Hopf algebras are worthy objects of study. It won't apply directly to abelian varieties—which are never affine in the nontrivial case—but it will apply to the finite subgroups given by the kernel of an isogeny.

Lemma 17.1. The category of commutative Hopf algebras over k is equivalent to the category of affine group schemes via the essentially inverse functors Spec and $\Gamma(G, \mathcal{O}_G)$.

Proof. This follows by restricting the usual duality between affine schemes and rings—the coalgebra axioms are dual to the axioms required of a group object. ∎

We return to the Hopf algebra we were discussing at the beginning of the section, with the goal of proving Proposition 16.4 and thus our results on smoothness and the dimension of $A^\vee$.

Lemma 17.2. Let A/k be an abelian variety, and let $H = \bigoplus_{i=0}^{g} H^i(A, \mathcal{O}_A)$. Then $(\Delta_A^*, m^*, [-1]^*)$, along with the natural maps $k \to H, H \to k$, makes H into a finite dimensional and cocommutative k-Hopf algebra over k such that $H^0 = k$, and for all $h \in H$ we have $m^*(h) = 1 \otimes h + h \otimes 1$ plus higher degree terms.

Lemma 17.3. Let k be a perfect field and H a graded-commutative Hopf algebra over k such that $H^0 = k, m^*(h) = 1 \otimes h + h \otimes 1$ plus higher degree terms and $H^r = 0$ for all $r > g$. Then $\dim H^1 \leq g$. Moreover, if $\dim H^1 = g$, then $H \simeq \bigwedge^\bullet H^1$ as graded k-algebras.

Proof. See [Mil86, Lemma 15.2] and its reference to Borel's paper. Borel gives a classification of Hopf algebras satisfying these hypotheses: it turns out that H has a presentation as a k-algebra with finitely many generators x_i, all of positive degree, such that the only relations among the x_i are those imposed by graded-commutativity and nilpotence relations of the form $x_i^{n_i} = 0$. In particular, the product of the x_i is nonzero.

So consider $\prod x_i$. Since this is nonzero, it has degree $\sum \deg x_i \leq g$ by assumption, so in particular there are at most g generators, hence $\dim H^1 = \#\{x_i : \deg x_i = 1\} \leq g$ (where the first equality is $=$ and not $\leq$ because the x_i are linearly independent). This proves the first claim.

If additionally $\dim H^1 = g$, then all of the x_i must lie in H^1—else the vector space they span is not large enough—and there are g generators. We also conclude that all x_i are nilpotent of order 2: otherwise, if $x_i^2 \neq 0$, then $x_i^2 \prod_{j \neq i} x_j$ is nonzero of degree $g + 1$, contradiction. Thus the algebra structure of H is uniquely determined, and it must be

$$H = \bigwedge^\bullet H^1$$

since the right hand side is an example of a graded-commutative algebra satisfying all of the properties we require. ■

We now prove Proposition 16.4.

Proof. Since $H_A^r = 0$ for all $r > g = \dim A$ by dimensional vanishing, by Lemma 17.3 $\dim H^1(A, \mathcal{O}_A) \leq g$. Therefore $A^\vee$ is smooth and $\dim H^1(A, \mathcal{O}_A) = g$ exactly. By Lemma 17.3,

$$H_A = \bigwedge^\bullet H^1(A, \mathcal{O}_A)$$

as graded k-algebras, which gets upgraded to an isomorphism of Hopf algebras by calculating that the coalgebra structures match on both sides. ■

17.2 Polarizations

Definition 17.3. A *polarization* of A/k is an isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\overline{k}} : A_{\overline{k}} \to A_{\overline{k}}^\vee$ is equal to $\phi_{\mathscr{L}}$ for some ample line bundle $\mathscr{L}/A_{\overline{k}}$.

We say that a polarization is *principal* if λ is an isomorphism (i.e. $\deg \lambda = 1$).

Remark 17.4. For all $\mathscr{L}' \in \mathrm{Pic}^0(A)$, we have $\phi_{\mathscr{L}} = \phi_{\mathscr{L}\otimes\mathscr{L}'}$—that is, line bundles that differ by an element of $\mathrm{Pic}^0(A)$ give rise to the same polarization. Hence we may treat the set of polarizations as living in the quotient $\mathrm{Pic}(A_{\overline{k}})/\mathrm{Pic}^0(A_{\overline{k}})$.

Definition 17.4. The *Nerón-Severi group* of A is

$$\begin{aligned}\mathrm{NS}(A) = \mathrm{NS}(A_{\overline{k}}) &:= \frac{\mathrm{Pic}(A_{\overline{k}})}{\mathrm{Pic}^0(A_{\overline{k}})} \\ &= \frac{\mathrm{Pic}_{A/k}(\overline{k})}{\mathrm{Pic}^0_{A/k}(\overline{k})}.\end{aligned}$$

Remark 17.5. If $k = \mathbb{C}$, we have the exponential exact sequence (in the analytic category)

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_A \xrightarrow{\exp} \mathcal{O}_A^\times \longrightarrow 1.$$

The induced long exact sequence yields an exact sequence

$$0 \longrightarrow \tfrac{H^1(A,\mathcal{O}_A)}{H^1(A,\mathbb{Z})} = \mathrm{Pic}^0(A) \longrightarrow \mathrm{Pic}(A) \longrightarrow \mathrm{NS}(A),$$

viewing the Nerón-Severi group as the image of $\mathrm{Pic}(A)$ inside $H^2(A,\mathbb{Z})$.

Remark 17.6. The Nerón-Severi group is a finitely generated abelian group. We have an inclusion

$$\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, A^\vee_{\overline{k}}),$$

and by Tate's theorem we have, for $\ell \neq \mathrm{char}(p)$,

$$\mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, A^\vee_{\overline{k}}) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(T_\ell(A_{\overline{k}}), T_\ell(A^\vee_{\overline{k}})).$$

The latter is a finitely generated $\mathbb{Z}_\ell$-module, and it turns out that this is enough to conclude that $\mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, A^\vee_{\overline{k}})$ is a finitely generated abelian group. (We'll prove the required details when we get to proving Tate's theorem.)

Remark 17.7. If k is not algebraically closed, then there might not be any line bundle $\mathscr{L}$ on A/k such that $\lambda = \phi_{\mathscr{L}}$. But if k is perfect, let $G = \mathrm{Gal}(\overline{k}/k)$. (More generally, for any k, let $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.) The exact sequence of G-modules

$$0 \longrightarrow A^\vee(\overline{k}) \longrightarrow \mathrm{Pic}_{A/k}(\overline{k}) \longrightarrow \mathrm{NS}(A) \longrightarrow 0$$

induces a long exact sequence in Galois cohomology

$$0 \longrightarrow A^\vee(k) \longrightarrow \mathrm{Pic}(A) \longrightarrow \mathrm{NS}(A)^G \longrightarrow H^1(G, A^\vee(\overline{k})).$$

See also [Mil86, Remark 13.2].

Remark 17.8. Suppose that X is a projective curve over k with $x_0 \in X(k)$. We define the Jacobian $J(X) := \mathrm{Pic}^0_{X/k}$. It has dimension equal to the genus g of X. For all positive integers d, we get a map $X^d \to J(X)$ defined on points by $(x_1, \ldots, x_d) \mapsto \mathcal{O}(x_1) \otimes \cdots \otimes \mathcal{O}(x_d) \otimes \mathcal{O}(x_0)^{-d}$. In the case $X^{g-1} \to J(X)$, the Weil divisor defined by the image corresponds to an ample line bundle $\mathscr{L}$ that yields a principal polarization $\phi_{\mathscr{L}}$ of $J(X)$. See also [Mil86, III.1, III.6].

18 Duality and Descent (02/28/2024)

18.1 Cartier duality

Definition 18.1. Let A, B be abelian varieties over a field k, and let $f \in \mathrm{Hom}(A, B)$ (not necessarily an isogeny). Then we define the *dual morphism* $f^\vee : B^\vee \to A^\vee$ via the Yoneda lemma as the morphism inducing the group homomorphisms

$$f^* : \mathrm{Pic}^0_{B/k}(T) \to \mathrm{Pic}^0_{A/k}(T)$$

induced by pullback by $f \times \mathbf{id}_T : A \times T \to B \times T$, naturally for all k-schemes T,

Theorem 18.1. [Mum08, §15, Thm. 1] Let $f : A \to B$ be an isogeny between abelian varieties over k. Then $f^\vee : B^\vee \to A^\vee$ is also an isogeny and $\ker f^\vee = (\ker f)^\vee$.

Here, $(\ker f)^\vee$ denotes the *Cartier dual* of the finite commutative group scheme $\ker f$. To prove the theorem (which we will do next lecture), we need to define what this means and set up some descent theory.

Definition 18.2. (See also [Mum08, §14].) Let G be a finite commutative group scheme over k (hence affine). Then $H := \Gamma(G, \mathcal{O}_G)$ is a finite dimensional commutative and cocommutative Hopf algebra over k. We endow the k-vector space $H^* := \mathrm{Hom}_k(H, k)$ with the structure of a Hopf algebra by dualizing the Hopf algebra morphisms on H: comultiplication on H^* is the dual of multiplication on H, multiplication on H^* is the dual of comultiplication on H, and similarly for the counit, unit, and antipode.

Then the *Cartier dual* of G is the group scheme $G^\vee := \mathrm{Spec}\, H^*$, using the coalgebra structure on H^* to define the group law.

Remark 18.2. We need G to be commutative for this to work, otherwise H^* is not a commutative algebra and we can't use scheme theory. $G^\vee$ is always a commutative group scheme since commutativity of H implies cocommutativity of H^*. We have a canonical isomorphism $(G^\vee)^\vee = G$ coming from the canonical isomorphism with the double dual for finite dimensional vector spaces.

Definition 18.3. For commutative group schemes G_1, G_2 over S, we define the functor

$$\underline{\mathrm{Hom}}(G_1, G_2) : \mathbf{Sch}_S \to \mathbf{Ab}$$

on objects by sending $T \mapsto \mathrm{Hom}_{T-\text{gp. sch}}(G_{1,T}, G_{2,T})$.

Proposition 18.3. Let G be a finite commutative group scheme over k, and let $\mathbb{G}_m = \operatorname{Spec} k[t, t^{-1}]$ be the multiplicative group scheme. Then $G^\vee$ represents the functor $\underline{\mathrm{Hom}}(G, \mathbb{G}_m)$.

Proof. Let R be a k-algebra. We want to show that $G^\vee(R) = \mathrm{Hom}(G_R, \mathbb{G}_{m,R})$, where the Hom is as R-group schemes.[16] By our original definition of $G^\vee$, we have

$$\begin{aligned} G^\vee(R) &= \mathrm{Hom}_{k-\text{alg}}(H^*, R) \\ &= \mathrm{Hom}_{\mathrm{R}-alg}(H_R^*, R) \\ &\subseteq \mathrm{Hom}_{R-\text{lin}}(H_R^*, R) = H_R. \end{aligned}$$

where the last Hom is merely as R-modules rather than R-algebras.

We observe that, for $\varphi \in H_R$, we have $\varphi \in \mathrm{Hom}_{R-\text{alg}}(H_R^*, R)$ if and only if $\Delta_R(\varphi) = \varphi \otimes \varphi$ and $\epsilon_R(\varphi) = 1$, where $\Delta : H \to H \otimes H$ is the comultiplication and $\epsilon : H \to k$ is the counit. This description characterizes the elements in $\mathrm{Hom}_{R-\text{lin}}(H_R^*, R) = H_R$ that correspond to elements of $G^\vee(R)$—these are the *grouplike elements that pull back to* 1.

Meanwhile,

$$\begin{aligned} \mathrm{Hom}_{R-\text{gp. sch}}(G_R, \mathbb{G}_{m,R}) &= \mathrm{Hom}_{\text{Hopf alg}}(R[t, t^{-1}], H_R) \\ &= \{\varphi \in H_R : \Delta_R(\varphi) = \varphi \otimes \varphi, \varphi \text{ invertible in } H_R\}. \end{aligned}$$

But if $\Delta_R(\varphi) = \varphi \otimes \varphi$, then $\epsilon_R(\varphi) = 1$ if and only if φ is invertible in H_R. For we have $(\epsilon \otimes \epsilon) \circ \Delta = \epsilon$, so $\Delta_R(\varphi) = \varphi \otimes \varphi$ implies $\epsilon_R(\varphi)^2 = \epsilon_R(\varphi)$. If φ is a unit in H_R, then $\epsilon_R(\varphi)$ is also a unit, so we conclude that $\epsilon_R(\varphi) = 1$.

Thus we have—functorially in R—identified both groups with the same subgroup of H_R, so we conclude that these two functors are isomorphic. ∎

[16] It turns out that it is sufficient to check that functors are isomorphic on the subcategory of affine k-schemes, rather than arbitrary k-schemes, via a covering argument. See [Con15, Exercise 1.5.4].

Example 18.4. Let $G = \mathbb{Z}/n\mathbb{Z}$ (the étale constant group scheme with n elements). We claim that $G^\vee = \mu_n = \ker([n] : \mathbb{G}_m \to \mathbb{G}_m)$. Fact: the group algebra $k[G]$ is isomorphic to H^* as k-algebras, by sending a point g to evaluation at g. This allow us to identify the comultiplication structures of the two groups. For all $f, g \in H = \Gamma(G, \mathcal{O}_G)$, we have $fg(\overline{1}) = f(\overline{1})g(\overline{1}) = (f \otimes g)(\overline{1} \otimes \overline{1})$ on $H \otimes H$, where $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ is the generator, so on H^* comultiplication is $x \mapsto x \otimes x$, as desired.

18.2 fpqc descent

See various sources for more discussion: [BLR90, §6.1-6.2], [Con15, §6], [Poo17, Ch.4, §5.2].

Definition 18.4. A morphism of schemes $S_0 \to S$ is called *fpqc* if it is faithfully flat (flat and surjective) and quasicompact.

Most of what we will say will also work in the fppf site, although we definitely cannot work over the Zariski site.

Let $f : S_0 \to S$ be fpqc. We define $S_1 := S_0 \times_S S_0$, and $S_2 := S_0 \times_S S_0 \times S_0$. Then we have three maps $p_{12}, p_{13}, p_{23} : S_2 \to S_1$ given by projection to two of the three components, and also two maps $p_1, p_2 : S_1 \to S_0$ via projection onto either factor.

Definition 18.5. Let $\mathscr{F}$ be a quasicoherent sheaf on S_0. A *descent datum* on $\mathscr{F}$ is an isomorphism

$$\theta : p_1^*\mathscr{F} \to p_2^*\mathscr{F}$$

in $\mathbf{QCoh}(S_1)$ satisfying the cocycle conditions

$$p_{13}^*\theta = p_{23}^*\theta \circ p_{12}^*\theta$$

in $\mathbf{QCoh}(S_2)$. In more detail, we are requiring that the following diagram commutes:

$$\begin{array}{ccccc} p_{12}^*p_1^*\mathscr{F} & \xrightarrow{p_{12}^*\theta} & p_{12}^*p_2^*\mathscr{F} = p_{23}^*p_1^*\mathscr{F} & \xrightarrow{p_{23}^*\theta} & p_{23}^*p_2^*\mathscr{F} \\ \| & & & & \| \\ p_{13}^*p_1^*\mathscr{F} & & \xrightarrow{\qquad\qquad p_{13}^*\theta \qquad\qquad} & & p_{13}^*p_2^*\mathscr{F} \end{array}$$

A morphism of descent data $(\mathscr{F}, \theta) \to (\mathscr{G}, \psi)$ is a sheaf homomorphism $h : \mathscr{F} \to \mathscr{G}$ such that the following diagram commutes:

$$\begin{array}{ccc} p_1^*\mathscr{F} & \xrightarrow{p_1^*h} & p_1^*\mathscr{G} \\ \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\psi} \\ p_2^*\mathscr{F} & \xrightarrow{p_2^*h} & p_2^*\mathscr{G} \end{array}$$

Theorem 18.5. *(Grothendieck.)* For an fpqc morphism $f : S_0 \to S$, we have an equivalence of categories

$$\mathbf{QCoh}(S) \to \{\mathscr{F} \in \mathbf{QCoh}(S_0) \text{ with descent datum}\}$$

defined by the functor $\mathscr{F}' \mapsto (f^*\mathscr{F}', \theta_{\mathscr{F}'})$, where $\theta_{\mathscr{F}'}$ is the natural isomorphism

$$p_1^* f^* \mathscr{F}' = (f \circ p_1)^* \mathscr{F}' = (f \circ p_2)^* = p_2^* f^* \mathscr{F}'.$$

This means you can show that a quasicoherent sheaf $\mathscr{F}$ on S_0 is the pullback of a sheaf on S_0 by writing down a descent datum for $\mathscr{F}$. This is a very practical and useful condition; for example, one might wish to check whether a line bundle on $X_{\overline{k}}$ comes from a line bundle on X for a k-variety X.

We can also define descent data for schemes, rather than sheaves.

Definition 18.6. For an S_0-scheme X, a *descent datum* is an S_1-isomorphism

$$\theta : X \times_{S_0, p_1} S_1 \simeq X \times_{S_0, p_2} S_1$$

such that $p_{13}^*\theta = p_{23}^*\theta \circ p_{12}^*\theta$.

However, the scheme version of descent data turns out to be not quite as nice as the sheaf version. For example, we don't get an analogue of Theorem 18.5, in the sense that given a descent datum (X, θ) we do not always get an S-scheme Y such that $Y \times_S S_0 = X$; see [BLR90, §6.7] for a counterexample. We only get a weaker version descent

Theorem 18.6. [Poo17, Thm. 4.3.5], [BLR90, §6.1, Thm.6] Let $f : S_0 \to S$ be an fpqc morphism of schemes.

1. In general, the functor $Y \mapsto (Y \times_S S_0, \theta_Y)$ from the category of S-schemes to the category of S_0-schemes with descent data is fully faithful. Here, θ_Y is the the descent datum defined by the natural isomorphism

$$(Y \times_S S_0) \times_{S_0,p_1} S_1 \simeq Y \times_S S_1 \simeq (Y \times_S S_0) \times_{S_0,p_2} S_1.$$

   In particular, this means that if X, Y are S-schemes and $f_0 : X_{S_0} \to Y_{S_0}$ is an S_0-morphism compatible with the descent data θ_X, θ_Y, then f_{S_0} the base change of a unique S-morphism $f : X \to Y$. That is, we can uniquely descend morphisms with descent data, if not schemes.

2. If we restrict this functor to the subcategory of *quasi-affine*[a] S-schemes, then it becomes an equivalence between the category of quasi-affine S-schemes and the category of quasi-affine S_0-schemes with descent data.

3. Suppose furthermore that S and S_0 are affine. Then a descent datum θ on an S_0-scheme X is effective[b] if and only if X can be covered by quasi-affine open subschemes that are stable under θ.

[a] A morphism such that the preimage of every affine open is quasi-affine, i.e. isomorphic to an quasi-compact open subscheme of some affine scheme.

[b] We say a descent datum is *effective* if it lies in the essential image of the functor defined in part (1).

19 Duality and quotient schemes (03/01/2024)

19.1 Dual morphisms

We prove Theorem 18.1, citing some more results about quotient groups and descent theory.

Proof. Since f is an isogeny, we must have $\dim A = \dim B = \dim A^\vee = \dim B^\vee$. Therefore, once we show that $\ker f^\vee$ is finite—which follows once we know $(\ker f)^\vee = \ker f^\vee$—we can conclude that $f^\vee$ is an isogeny.

For k-schemes T, the scheme $\ker f^\vee$ has functor of points

$$\begin{aligned}(\ker f^\vee)(T) &= \{(\mathscr{L}, \alpha) : \mathscr{L}/B \times T, \alpha|_{\{e\}\times T} \simeq \mathcal{O}_Q, f^*(\mathscr{L}, \alpha) = (\mathcal{O}_{A\times T}, \mathbf{id})\} \\ &= \{\mathscr{L} : \mathscr{L}/B \times T, f^*\mathscr{L} \simeq \mathcal{O}_{A/T}\}/\{\text{iso. of line bundles}\}\end{aligned}$$

because $\mathscr{L}$ must be trivializable on $\{e_B\} \times T$ if it is trivial under pullback to $A \times T$ (write down an appropriate commutating diagram). Here, the trivialization we are notating $\mathbf{id} : e_A^*\mathcal{O}_{A\times T} \simeq \mathcal{O}_T$ is the unique isomorphism sending the section $1 \in_A^* \mathcal{O}_{A\times T}$ to $1 \in \mathcal{O}_T$; we have actually already been using this implicity to define the identity of the Picard scheme. We are also using the fact that $\ker f^\vee \subseteq \mathrm{Pic}^0$ already; we'll say more later.

We apply fpqc descent to $S_0 = A \times T \to S = B\times$. We claim that $(\ker f^\vee)(T)$ is the set of all descent data on θ on $\mathcal{O}_{A\times T}$ (up to isomorphism of descent data). Let $G = \ker f \subseteq A$.

We have

$$S_1 = S_0 \times_S S_0 = A \times T_{B\times T} \times A \times T \simeq A \times T \times G$$

where the last isomorphism is define by $(a, a+g) \leftarrow\!\shortmid (a, g)$. We also have

$$S_2 = S_0 \times_S S_0 \times_S S_0 = A \times T \times G \times G$$

Fix, once and for all, an isomorphism $\alpha_1 : \mathcal{O}_{A\times T\times G} \simeq p_2^*\mathcal{O}_{A\times T}$ and an isomorphism $\alpha_2 : \mathcal{O}_{A\times T\times G} \simeq p_2^*\mathcal{O}_{A\times T}$. A descent datum θ is an isomorphism $p_1^*\mathcal{O}_{A\times T} \simeq p_2^*\mathcal{O}_{A\times T}$; under our fixed identifications with $\mathcal{O}_{A\times T\times G}$, such an isomorphism is equivalent to multiplication by an element of

$$\Gamma(T \times G, \mathcal{O}^*_{T\times G}) = \Gamma(A \times T \times G, \mathcal{O}^*_{A\times T\times G}) = \mathrm{Aut}(\Gamma \times G, \mathcal{O}_{T\times G})$$

, since A is proper. The cocycle condition on θ translates to the condition that $\theta(a, g_1+g_2) = \theta(a, g_2)\theta(a+g_1, g_2)$, so $\Delta(\theta) = \mathcal{O}\otimes\mathcal{O}$. But this is exactly the functor of points for $G^\vee(T)$. ■

Corollary 19.1. If f is an isogeny, then $\deg f = \deg f^\vee$.

Proof. $\deg f = \dim_k \Gamma(G, \mathcal{O}_G) = \dim_k \Gamma(G^\vee, \mathcal{O}_{G^\vee}) = \deg f^\vee$. ■

Proposition 19.2. Let $f, g : A \to B$ be morphisms of abelian varieties (not necessarily isogenies or even homomorphisms). Then $(f+g)^\vee = f^\vee + g^\vee$.

Proof. For all $\mathscr{L} \in \mathrm{Pic}^0_{B/k}(\overline{k})$, we have $(f+g)^*\mathscr{L} \simeq f^*\mathscr{L} \otimes g^*\mathscr{L}$, using the fact that the morphism $f+g$ is the composition $m_B \circ (f \times g) : A \to B \times B \to B$ and $m^*\mathscr{L} = p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}$ from Lemma 12.2. ■

Corollary 19.3. $[n]_{A^\vee} = ([n]_A)^\vee$, hence $A^\vee[n] = (A[n])^\vee$.

Proof. Apply the previous proposition inductively, adding copies of the identity morphism to itself. ■

19.2 Quotient group schemes

Theorem 19.4. [Gro62, 3.I, VI.A, 3.2] If $A \hookrightarrow B$ is a closed normal[a] subgroup scheme, where A and B are both fppf group schemes over a field k, then there exists a unique fppf group scheme C fixing into an exact sequence

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1,$$

in the sense that the functor of points associated to C is the fppf sheafification of $T \mapsto B(T)/A(T)$.
In particular, we may always form $A/\ker f$ for an abelian variety A and a homomorphism $f : A \to B$.

[a] In the group scheme-theoretic sense, which has a precise scheme-theoretic statement.

Remark 19.5. It is fairly straightforward how to proceed in the affine case $B = \operatorname{Spec} R$—the quotient group scheme C ought to the the spectrum of the subring of elements of B that are invariant under translation by A. More technical is how to glue all of this together in the non-affine case; uniqueness is a descent argument.

Remark 19.6. Given a group homomorphism, then we get $G \twoheadrightarrow G/\ker f \hookrightarrow H$.

Remark 19.7. An exact sequence of group schemes does not generally have an exact functor of points—we need the fppf sheafification. For example, the following sequence should be considered exact:

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{G}_m \xrightarrow{x^2} \mathbb{G}_m \longrightarrow 1.$$

The map on the functor of points $\mathbb{G}_m(\mathbb{Q}) \to \mathbb{G}_m(\mathbb{Q})$ given by squaring is certainly not surjective—many rational numbers lack rational square roots. But when we pass to the fppf extension $\operatorname{Spec} \overline{\mathbb{Q}} \to \operatorname{Spec} \mathbb{Q}$, the functor of points does become exact.

Theorem 19.8. [BLR90, §8.2,Thm12] Let X be a group scheme. Assume X/k is quasi-projective, and let $R \subseteq X \times X$ be a subgroup scheme such that both projections $R \to X$ are proper and flat. Then the quotient X/R exists, is a quasi-projective scheme, and $X \to X/R$.

We also discussed more facts about descent. These have been incorporated into last lecture's notes.

20 More on the dual abelian variety (03/04/2024)

I was away at the Arizona Winter School for this lecture and the next. The notes for these have been reconstructed from Prof. Tang's written lecture notes.

20.1 Sketch of Mumford's construction of $A^\vee$

See also [Mil86, §10] or [Mum08, II.8, III.13]. Recall that for an ample line bundle on an abelian variety A, we have a morphism $\phi_{\mathscr{L}} : A \to \mathrm{Pic}^0_{A/k}$ defined on points by $x \mapsto \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. We set $K(\mathscr{L}) = (\ker \phi_{\mathscr{L}})(\overline{k})$, i.e. the set of $\overline{k}$-points under which $\mathscr{L}$ is translation-invariant.

The idea behind Mumford's construction of $\mathrm{Pic}^0_{A/k}$ is to give $K(\mathscr{L})$ the correct subscheme structure and then define $\mathrm{Pic}^0_{A/k} = A/K(\mathscr{L})$. We will use what we know about $A^\vee$ *a posteriori* to give us a hint on what to do. For a given ample $\mathscr{L}$ we set $\mathscr{M} := m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}$ on $A \times A$. This line bundle has the property

$$\begin{aligned}\mathscr{M}|_{\{e\}\times A} &= \mathscr{L} \otimes \mathscr{L}^{-1} = \mathcal{O}_A \\ \mathscr{M}|_{A\times\{x\}} &= t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} = \phi_{\mathscr{L}}(x)\end{aligned}$$

for any $x \in A(\overline{k})$. This ought to remind you of the Poincaré bundle on $A \times A^\vee$, the universal bundle with

$$\mathcal{P}|_{\{e\}\times A^\vee} = \mathcal{O}_{A^\vee}$$

and, if λ is the point on $A^\vee(\overline{k})$ associated to a given line bundle $\mathscr{L}'$ on A,

$$\mathcal{P}|_{A\times\{\lambda\}} = \mathscr{L}'.$$

In fact, we claim that $(\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P} \simeq \mathcal{M}$. This is another typical seesaw argument. We have

$$\begin{aligned}((\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P})|_{\{e\}\times A} &= (\phi_{\mathscr{L}}^*\mathcal{P}|_{\{e\}\times A^\vee}) = \mathcal{O}_A \\ ((\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P})|_{A\times\{x\}} &= (\mathbf{id}_A^*\mathcal{P}|_{A\times\{\phi_{\mathscr{L}}(x)\}}) = \phi_{\mathscr{L}}(x),\end{aligned}$$

abusing notation to consider $\phi_{\mathscr{L}}(x)$ both as a line bundle and as a point of $A^\vee(\overline{k})$. Setting $\mathscr{N} := (\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P} \otimes \mathscr{M}^{-1}$, the line bundles $\mathscr{N}|_{\{e\}\times A}$ and $\mathscr{N}|_{A\times\{x\}}$ are trivial for all $x \in A(\overline{k})$. By the Seesaw Principle, triviality of $\mathscr{N}|_{A\times\{x\}}$ everywhere implies $\mathscr{N} = \mathrm{pr}_2^*\mathcal{N}'$ for some $\mathcal{N}'$ on A. But then $\mathscr{N}|_{\{e\}\times A} = \mathcal{N}' = \mathcal{O}_A$, so $\mathscr{N}$ is trivial, whence the claim.

We can flip this relationship on its head: even if we don't know anything about $A^\vee$, we can still write down $\mathscr{M}$ (which lives on $A \times A$) and hope to recover $\mathcal{P}$ from $\mathscr{M}$. In characteristic 0, all group schemes are reduced, so we may endow the finite closed subset $K(\mathscr{L}) \subset A$ with its reduced induced subscheme structure. In general, we can let $K(\mathscr{L})$ be the maximal subscheme of A such that $\mathscr{M}|_{K(\mathscr{L})\times A}$ is trivial—for this, we need an upgraded version of the Seesaw Principle, see [Mum08, II.10]. Then set $A^\vee := A/K(\mathscr{L})$, which is a smooth quotient group scheme since A is smooth.

The map $\mathbf{id}_A \times \phi_{\mathscr{L}} : A \times A \to A \times A^\vee$ is fpqc: it is generically flat, which implies flatness for a homomorphism of group schemes, and it is surjective by our new definition of $A^\vee$ as a quotient. We use this map to define a fiber product

$$A \times A \times_{A\times A^\vee} A \times A = A \times A \times K(\mathscr{L}).$$

We define a descent datum on the sheaf $\mathscr{M}$ using the isomorphisms $\mathscr{M} \simeq (1 \times \tau_x)^*\mathscr{M}$) and

hence conclude that $\mathscr{M}$ descends to a line bundle $\mathcal{P}$ on $A \times A^\vee$. Then one checks that this $\mathcal{P}$ plays the role of the universal line bundle, and thus conclude that $A^\vee$ really is the dual abelian variety.

20.2 Symmetric definition of $A^\vee$

Definition 20.1. For abelian varieties A, B over k of equal dimension, a line bundle $\mathscr{Q}$ on $A \times B$ is a *divisorial correspondence* if $\mathscr{Q}|_{\{e\}\times B} \simeq \mathcal{O}_B$ and $\mathscr{Q}|_{A\times\{e\}} \simeq \mathcal{O}_A$.

Such $\mathscr{Q}$ induces a morphism $\kappa_{\mathscr{Q}} : B \to A^\vee$ sending $e \mapsto e$ via $b \mapsto \mathscr{Q}|_{A\times\{e\}}$—the image is contained in $A^\vee = \mathrm{Pic}^0_{A/k}$ because B is connected—so this morphism is in fact a group homomorphism. Swapping the roles of A and B, we also get a homomorphism $\kappa_{\sigma^*\mathscr{Q}} : A \to B^\vee$, where $\sigma : A \times B \to B \times A$ is the canonical switch morphism.

Example 20.1. For the Poincaré bundle $\mathcal{P}$ on $A \times A^\vee$, the map $\kappa_{\mathcal{P}} : A^\vee \to A^\vee$ is the identity, and $\kappa_{\sigma^*\mathcal{P}}$ is some homomorphism $A \to (A^\vee)^\vee$.

Proposition 20.2. For any line bundle $\mathscr{L}/A$, we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\kappa_{\sigma^*\mathcal{P}}} & (A^\vee)^\vee \\ & \searrow^{\phi_{\mathscr{L}}} & \downarrow{\scriptstyle (\phi_{\mathscr{L}})^\vee} \\ & & A^\vee \end{array}$$

Proof. From our discussion of Mumford's construction of the dual abelian variety in Section 20.1 that $(\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P} \simeq m^*\mathscr{L} \otimes \mathrm{pr}_1\,\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\,\mathscr{L}^{-1}$. (Our proof of this via seesaw remains true for general $\mathscr{L}$, not just ample $\mathscr{L}$.) For all $x \in A(\overline{k})$, we have

$$\begin{aligned} \phi_{\mathscr{L}}(x) &= t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \\ \kappa_{\sigma^*\mathcal{P}}(x) &= \mathcal{P}|_{\{x\}\times A^\vee} \end{aligned}$$

hence

$$\begin{aligned} \phi_{\mathscr{L}}^\vee(\kappa_{\sigma^*\mathcal{P}}(x)) &= \phi_{\mathscr{L}}^*(\mathcal{P}|_{\{x\}\times A^\vee}) \\ &= ((\mathbf{id}_A \times \phi_{\mathscr{L}})^*\mathcal{P})|_{\{x\}\times A} \\ &= t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \\ &= \phi_{\mathscr{L}}(x), \end{aligned}$$

and this equality shows commutativity of the diagram because a morphism is determined by its values on $\overline{k}$-points. ∎

Corollary 20.3.
1. $\kappa_{\sigma^*\mathcal{P}}$ is an isomorphism, hence $A \simeq (A^\vee)^\vee$ naturally.
2. The universal line bundle $\mathcal{P}_{A^\vee}$ on $A^\vee \times (A^\vee)^\vee \simeq A^\vee \times A$ is $\sigma^*\mathcal{P}_A$.

Proof. 1. Take $\mathscr{L}$ ample. Then $\phi_{\mathscr{L}}$ and $\phi_{\mathscr{L}}^\vee$ are isogenies of the same degree by Corollary

19.1, so by Proposition 20.2 the homomorphism $\kappa_{\sigma^*\mathcal{P}}$ must be an isogeny of degree 1, i.e. an isomorphism.

2. We have, for all $x \in A(\overline{k})$,

$$\begin{aligned}
\mathcal{P}_{A^\vee}|_{\{e\}\times A} &\simeq \mathcal{O}_A \\
\mathcal{P}_{A^\vee}|_{A^\vee\times\{x\}} &\simeq \text{ l.b. assoc. to } \kappa_{\sigma^*\mathcal{P}}(x) \\
&\simeq \mathcal{P}_A|_{\{x\}\times A^\vee} \\
\sigma^*\mathcal{P}_A|_{\{e\}\times A} &\simeq \mathcal{O}_A \\
\sigma^*\mathcal{P}_A|_{A^\vee\times\{x\}} &= \kappa_{\sigma^*\mathcal{P}}(x)
\end{aligned}$$

so another typical seesaw argument shows $\sigma^*\mathcal{P}_{A^\vee} \simeq \mathcal{P}_{A^\vee}$.

■

Definition 20.2. We say that a homomorphism $\lambda : A \to A^\vee$ is *symmetric* if $\lambda^\vee = \lambda$ under the identification $\kappa_{\sigma^*\mathcal{P}} : A \to (A^\vee)^\vee$ (a notation we will abuse from now on).

From Proposition 20.2, we see that $\phi_{\mathscr{L}} = (\phi_{\mathscr{L}})^\vee$; taking $\mathscr{L}$ ample, this shows that every polarization is symmetric. In general, if $\mathscr{L}$ is a line bundle on B and $f : A \to B$ is a homomorphism, then we have a commutative diagram

$$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{\scriptstyle \phi_{f^*\mathscr{L}}} & & \downarrow{\scriptstyle \phi_{\mathscr{L}}} \\
A^\vee & \xleftarrow[f^\vee]{} & B^\vee
\end{array}$$

In particular, when $\mathscr{L}$ is ample, f gives a morphism of $(A, \phi_{f^*\mathscr{L}})$ to $(B, \phi_{\mathscr{L}})$ is a homomorphism of polarized abelian varieties (this just means that the diagram above commutes.)

Corollary 20.4. Isogeny between abelian varieties is an equivalence relation. In fact, if $f : A \to B$ is an isogeny, there exists an isogeny $g : B \to A$ such that $g \circ f = [\deg f]$ on A (multiplication by $\deg f$).

Proof. Reflexivity and transitivity are clear; the hard part is symmetry, which follows from the existence of g.

Since $f : A \to B$ is faithfully flat and quasi-compact, by fpqc descent, for all k-schemes X we have an equalizer diagram

$$X(B) \xrightarrow{-\circ f} X(A) \rightrightarrows X(A \times_B A)$$

The slogan here is "representable functors are fpqc sheaves of sets," which is a special case of the full faithfulness of the fpqc descent datum functor for schemes in Theorem 18.6. See [Con15, Thm. 6.2.14] for more details.

By Yoneda, this means that we contravariantly have a coequalizer diagram

$$A \times_B A \rightrightarrows A \xrightarrow{f} B.$$

We know $A \times_B A \simeq A \times_k \ker f$. The group scheme $\ker f$ is a finite group scheme with order $\deg f$. By Theorem 20.5 below, we know that $\deg f$ kills $\ker f$. This implies that the morphism $[\deg f] : A \to A$ also coequalizes the diagram above—under our identifications,

the two morphisms $A \times_k \ker f \to A$ appearing in the coequalizer diagram are (1) the action map $(a, k) \mapsto ak$ and (2) the projection $(a, k) \mapsto a$, and post-composing with multiplication by $\deg f$ makes these two maps equal. Hence by the universal property of the coequalizer, we conclude there is some morphism $g : B \to A$ with $g \circ f = [\deg f]$, and such g is evidently surjective with finite kernel, i.e. an isogeny. ■

Theorem 20.5. *(Deligne.)* A commutative finite flat S-group scheme G of order m is killed by m.

Proof. See [TO70, §1]. ■

21 Finite commutative group schemes (03/06/2024)

21.1 Poincaré complete reducibility (algebraic category)

We can finally reprove complete reducibility in the algebraic setting over an arbitrary field.

Theorem 21.1. *(Poincaré complete reducibility.)* [Mum08, §19, Thm. 1] If $B \subseteq A$ are abelian varieties over k, then there exists a sub-abelian variety $B' \subseteq$ such that $B \times B' \to A$ is an isogeny.

Proof. Pick an ample line bundle $\mathscr{L}$ on A; then we have a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\iota} & A \\ \downarrow{\scriptstyle \phi_{\iota^*\mathscr{L}}} & & \downarrow{\scriptstyle \phi_{\mathscr{L}}} \\ B^\vee & \xleftarrow[\iota^\vee]{} & A^\vee \end{array}$$

Set

$$B' := (\ker(\iota^\vee \circ \phi_{\mathscr{L}}))^0_{\mathrm{red}},$$

which is another sub-abelian variety of A. The kernel of $B \times B' \to A$ is the scheme-theoretic intersection $B \cap B' = \ker \phi_{\iota^*\mathscr{L}}$, which is finite because $\iota^*\mathscr{L}$ is ample on B. Therefore, to show that $B \times B' \to A$ is an isogeny, we need only show that $\dim B + \dim B' \geq \dim A$ (implying surjectivity). But since the polarization $\phi_{\mathscr{L}}$ is finite, we have

$$\dim B' = \dim \ker \iota^\vee \geq \dim A^\vee - \dim B^\vee = \dim A - \dim B.$$

■

Qualitatively, this is the same proof as in the complex case from [Mil86]; we just had to do a lot to set up the algebraic theory of duality.

Corollary 21.2. Corollaries 3.5 and 3.9 remain valid in the algebraic setting over an arbitrary field: we may always decompose abelian varieties into simple isogeny factors, and $\mathrm{End}^0(A)$ correspondingly decomposes into a product of matrix algebras over division rings.

21.2 Étale and local finite group schemes

Definition 21.1. Let G be a finite group scheme over k, i.e. the spectrum of some finite-dimensional k-Hopf algebra.

- We say G is *local* if G is connected.
- We say that G is *étale* if $\Gamma(G, \mathcal{O}_G)$ is an étale k-algebra, i.e. a product of finite separable extensions of k, equivalently $\Omega^1_{G/k} = 0$.

Example 21.3. $\mu_n = \ker([n] : \mathbb{G}_m \to \mathbb{G}_m)$ is étale if and only if n is coprime to $p = \operatorname{char} k$, and it is local if and only if n is a p-th power.

Proposition 21.4. *(Étale-connected exact sequence.)* For any finite k-group scheme G, we have an exact sequence

$$1 \longrightarrow G_{\mathrm{loc}} \longrightarrow G \longrightarrow G_{\text{ét}} \longrightarrow 1,$$

where G_{loc} is local and $G_{\text{ét}}$ is étale.
Moreover, if k if perfect, then this sequence splits canonically: $G \simeq G_{\mathrm{loc}} \times G_{\text{ét}}$.

This roughly says that G may be group scheme-theoretically decomposed as a product of its "points" and the "fuzz near the identity."

Proof. The idea is to take $G_{\mathrm{loc}} = G^0$, which is certainly local, and show that G/G^0 is étale. We require some preparation.

Lemma 21.5. Letting k^s denote the separable closure of k, the following categories are equivalent:

- The category of finite étale k-algebras.
- The category of finite étale k-schemes.
- The category of finite sets equipped with a $\mathrm{Gal}(k^s/k)$-action.

The last equivalence is given by sending $X \mapsto X(k^s)$, with the Galois action induced by the Galois action on k^s.
This equivalence of categories restricts to an equivalence of:

- The category of finite étale k-Hopf algebras.
- The category of finite étale k-group schemes.
- The category of finite groups equipped with a $\mathrm{Gal}(k^s/k)$-action.

Proof. (Sketch.) Given a $\mathrm{Gal}(k^s/k)$-set T, its associated finite étale k-algebra is

$$\left(\prod_{t\in T} k^s\right)^{\mathrm{Gal}(k^s/k)},$$

(i.e. the subalgebra of this product fixed by $\mathrm{Gal}(k^s/k)$). Here we let $\gamma \in \mathrm{Gal}(k^s/k)$ act on the tuple $(s_t)_{t\in T}$ by sending it to the tuple with $\gamma(s_t)$ as its $\gamma(t)$-th component. ■

Example 21.6. Let $\mathrm{char}\, p \nmid n$. Then the group μ_n corresponds to the subgroup of n-th roots of unity in k^s with their natural $\mathrm{Gal}(k^s/k)$-action.

Proposition 21.7. Let X/k be a scheme of finite type. Then there exists a finite étale k-scheme $\pi_0(X)$ and a morphism $q : X \to \pi_0(X)$ which is universal in the sense that if $q' : X \to Y$ is another morphism with Y finite étale, then there exists a unique $f : \pi_0(X) \to Y$ with $q' = f \circ q$. Moreover, q is faithfully flat and the fibers of q are connected components of X (justifying the notation $\pi_0(X)$).

Proof. (Sketch.) Using Lemma 21.5, to define $\pi_0(X)$ we need only write down $\pi_0(X)(k^s)$ and endow this set with a $\mathrm{Gal}(k^s/k)$-action. So we simply take $\pi_0(X)(k^s)$ to be the set of connected components of $X_{k^s} = X \times_k \mathrm{Spec}\, k^s$, which is equipped with a natural Galois action via the action on k^s.

We construct the desired q via Galois descent: we have a map upstairs $q_{k^s} : X_{k^s} \to \pi_0(X)_{k^s}$ given by sending a connected component to its corresponding point in $\pi_0(X)_{k^s}(k^s)$. This morphism is $\mathrm{Gal}(k^s/k)$-invariant, hence descends to a unique $q : X \to \pi_0(X)$. The properties of q can even be checked after the k^s/k-faithfully flat base change. ■

Corollary 21.8. For a k-group scheme G of finite type, $\pi_0(G)$ is a finite étale k-group scheme and $q : G \to \pi_0(G)$ is a group homomorphism.

Returning to the proof of the connected-étale exact sequence, Proposition 21.7 and Corollary 21.8 give us the exact sequence with $G_{\text{ét}} = \pi_0(G)$. When k is perfect, $G_{\text{red}} \subseteq G$ is a k-subgroup scheme; the key point here is that $G_{\text{red}} \times_k G_{\text{red}}$ is again a reduced scheme if k is perfect.[17] Now note that the composition $G_{\text{red}} \hookrightarrow G \to \pi_0(G)$ is an isomorphism, which can be checked on k^s-points, yielding a section of the exact sequence. ■

Definition 21.2. We say that a finite commutative group scheme G is *étale-local* if G is étale and $G^\vee$ is local. We likewise define étale-étale, local-étale, and local-local group schemes based on all possible combinations.

Corollary 21.9. If k is perfect and G is a finite commutative group scheme, then we have a unique decomposition

$$G = G_{\text{ét-ét}} \times G_{\text{ét-loc}} \times G_{\text{loc-ét}} \times G_{\text{loc-loc}}$$

with the obvious notation.

Proof. Use the connected-étale exact sequence to first write $G \simeq G_{\text{ét}} \times G_{\text{loc}}$. By repeating this for for $G^\vee_{\text{ét}}$ and $G^\vee_{\text{loc}}$ and then (double) dualizing, we get our desired four-fold decomposition.

Uniqueness follows from the fact that there is no non-trivial morphism between these group types of groups:

- Étale $\to$ local is trivial because this is a map from a reduced scheme to a scheme whose reduced structure has one point;
- Local $\to$ étale is trivial because the neutral connected component of an étale group scheme is $\{e\} \simeq \operatorname{Spec} k$. (The neutral component cannot be $\operatorname{Spec} k'$ for a finite separable extension k'/k because the identity needs to be a k-valued point.)

The claim follows from these two cases and their duals. ■

Example 21.10. Let $\operatorname{char} k = p$. Recall that, in general, $\mathbb{Z}/n\mathbb{Z}$ and μ_n are Cartier duals. If $(n, p) = 1$, then both of these are étale-étale, whereas if $n = p^e$, then $\mathbb{Z}/n\mathbb{Z}$ is étale-local and μ_n is local-étale.
The kernel of Frobenius $\alpha_p := \ker F : \mathbb{G}_a \to \mathbb{G}_a$ is local and self-dual, hence local-local. (See Homework 3.)

[17] This is not true in general if k is not perfect. See [EvdGM24, Ex. 3.2] for a counterexample.

Remark 21.11. When $k = \overline{k}$, then there are not may possibilities for three out the four types of finite group schemes we have defined:

- All étale-étale commutative finite k-groups schemes are products of μ_n, where $(n, p) \neq 1$. (Note that this is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if we work over the algebraic closure via a choice of primitive root of unity.)
- All étale-locals are of products of various $\mathbb{Z}/p^n\mathbb{Z}$.
- All local-étales are products of various μ_{p^n}.

However, there is a huge variety of local-local group schemes, even with the simplification $k = \overline{k}$.

Remark 21.12. If $\operatorname{char} k = 0$, then G is always étale-étale, since all group schemes are reduced in characteristic 0.

We will investigate building blocks of local groups, which will also be useful when we study Frobenius actions. See also [Mum08, §III.11, §III.14] for more theory.

The following may remind you of the Chinese remainder theorem:

Proposition 21.13. Let A/k be an abelian variety with $\operatorname{char} k = p$. Let n be a positive integer, and write $n = n_1 p^m$ with p prime and $p \nmid n_1$. Then the natural morphism $A[n_1] \times A[p^m] \to A[n] : (a, b) \mapsto a + b$ us an isomorphism.

Proof. Since $(n_1, p) \neq 1$, $[n_1]$ is separable and so $A[n_1]$ is étale. Likewise, $A[n_1]^\vee \simeq A^\vee[n_1]$ is étale, so $A[n_1]$ is étale-étale. On the other hand, by Remark 21.11, since $A[p^m]$ has p-th power order p^{2mg}, it cannot have a nontrivial étale-étale component—all of those have order coprime to p (after base change to $\overline{k}$). So $A[n_1] \cap A[p^m] \subseteq A[n]$ (scheme theoretic intersection) is trivial; equivalently, $A[n_1] \times A[p^m] \to A[n]$ has trivial kernel, so by comparing orders we conclude this is an isomorphism. ∎

With notation as in the proposition, we must have $A[n_1]_{\overline{k}} \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. But $A[p^m]$ has many possible structures.

22 Lie algebras of local groups (03/08/2024)

22.1 p-rank

Let $\operatorname{char} k = p$. Last time, we discussed how $A[p^n]_{\overline{k}}$ decomposes as a group scheme. It has no étale-étale part, only étale-local, local-étale, and local-local components. The étale-local part is always of the form $(\mathbb{Z}/p^m\mathbb{Z})^r$, where $\mathbb{Z}/p^m\mathbb{Z}$ is a constant group scheme. The number r is called the *p-rank* of A. Meanwhile, the local-étale part is always of the form $(\mu_{p^m})^s$, and by duality $s = r$.

Proposition 22.1. The p-rank is an isogeny invariant.

Proof. Let $f : A \to B$ be an isogeny, say with kernel of order n, i.e. $\dim_k \Gamma(\ker f, \mathcal{O}_{\ker f}) = n$. To prove the claim, it suffices to look only at $\overline{k}$-points, eschewing finer non-reduced structure. Let r_A, r_B be the respective p-ranks of A and B. Then we get a map on points

$$f : A[p^m](\overline{k}) \to B[p^m](\overline{k})$$

which has kernel of order at most n, so we conclude $p^{mr_A} \leq np^{mr_B}$ for all m. Since n is fixed, taking $m \to \infty$ shows that $r_A \leq r_B$.

Recall that isogeny is an equivalence relation: if an isogeny $f : A \to B$ exists, there exists an isogeny $g : A \to B$. So we may apply the same argument to show that $r_B \leq r_A$, whence $r_A = r_B$. ∎

Corollary 22.2. The p-rank r of A is equal to the p-rank s of $A^\vee$.

Proof. Polarizations exist and are isogenies. ∎

22.2 Digression on Lie algebras

Recall that in the general setting, where we have an S-group scheme $G \to S$ of finite type, an *S-derivation* of $\mathcal{O}_G$ to a quasicoherent sheaf $\mathscr{M}$ on G is a map $D : \mathcal{O}_G \to \mathscr{M}$ satisfying:

1. Additivity;
2. For all $a \in \operatorname{im}(f^{-1}\mathcal{O}_S \to \mathcal{O}_G)$, we have $Da = 0$ on sections; and
3. The Leibniz rule holds: $D(ab) = aD(b) + bD(a)$ on sections.

One can show that there is a bijection $\operatorname{Hom}_{\mathcal{O}_G}(\Omega^1_{G/S}, \mathscr{M}) = \operatorname{Der}_S(\mathcal{O}_G, \mathscr{M})$, where the latter denotes the set of S-derivations and $\Omega^1_{G/S}$ is the sheaf of relative differentials.

We justify the identification $\operatorname{Lie} G = T_e G$ when $S = \operatorname{Spec} k$. We define $\operatorname{Lie} G$ as the set of left-invariant derivations in $\operatorname{Der}_S(\mathcal{O}_G, \mathcal{O}_G) = \operatorname{Hom}_{\mathcal{O}_G}(\Omega^1_{G/S}, \mathcal{O}_G)$, i.e. such that $D : \mathcal{O}_G \to \mathcal{O}_G$ satisfies $D \circ L_x^* = L_x^* \circ D$ for all $x \in G(\overline{k})$, with L_x denoting left-translation.

Proposition 22.3. $\operatorname{Lie} G \simeq T_e G$ via $D \mapsto D|_e$ (recall we define $T_e G = \operatorname{Hom}(\mathfrak{m}_e/\mathfrak{m}_e^2, k)$, and that $\Omega^1_{G/S}|_e \simeq \mathfrak{m}/\mathfrak{m}^2$).

Proof. See [Mum08, p. 92-94] for the case over $\mathbb{C}$, which generalizes. He constructs D using right-translations. ∎

Here are some more facts about $\operatorname{Lie} G$:

1. It is a Lie algebra in the algebraic sense: the Lie bracket is given by the commutator $[D_1, D_2] := D_1 \circ D_2 - D_2 \circ D_1$.
2. If $\operatorname{char} k = p$, then $D^{(p)} = D \circ D \circ \cdots \circ D$ (p iterations of D) is also in $\operatorname{Lie} G$ for any $D \in G$. In general, iterating a derivation is not a derivation, but in characteristic p one can show that the bad terms in the Leibniz rule all die.

That is, $\operatorname{Lie} G$ is a *p-Lie algebra*:

Definition 22.1. A *p-Lie algebra* $\mathfrak{g}$ over k is a Lie algebra (a k-vector space with a bracket operator $[\cdot,\cdot]$) equipped with a unary operator $(-)^{(p)} : \mathfrak{g} \to \mathfrak{g}$ such that

1. $(\lambda x)^{(p)} = \lambda^p x^{(p)}$ for all $\lambda \in k, x \in \mathfrak{g}$;
2. Letting ad_x be Lie algebra endomorphism sending $y \mapsto [x,y]$, we have $\mathrm{ad}_{x^{(p)}} = (\mathrm{ad}_x)^p$ (where the right hand side denotes iteration as an endomorphism).
3. $(x+y)^p = x^{(p)} + y^{(p)} + F_p(\mathrm{ad}_x, \mathrm{ad}_y)y$, where F_p is some universal noncommutative polynomial defined solely by the characteristic p. You can look up what this is explicitly, although we won't write it down here.

22.3 Height 1 local groups

Definition 22.2. A finite commutative local k-group scheme G is *height 1* if $x^p = 0$ whenever $x \in \mathfrak{m} = \mathfrak{m}_e$ (the maximal ideal at $e \in G$).

Lemma 22.4. For a finite local k-group scheme G of height 1, the coordinate ring $R = \Gamma(G, \mathcal{O}_G)$ is isomorphic to $k[x_1,\dots,x_n]/(x_1^p,\dots,x_n^p)$. In particular, $\dim_k R$ is a p-th power.

Proof. Let $x_1,\dots,x_n \in \mathfrak{m}_e$ such that $\overline{x}_1,\dots,\overline{x}_m$ form a k-basis in the cotangent space $\mathfrak{m}_e/\mathfrak{m}_e^2$. Since G is local, by Nakayama we must have $k[x_1,\dots,x_n] \twoheadrightarrow R$. By the height 1 assumption, this surjection descends to $k[x_1,\dots,x_n]/(x_1^p,\dots,x_n^p) \twoheadrightarrow R$.

Let $D_1,\dots,D_n \in \mathrm{Lie}\, G$ be a dual basis of $\overline{x}_1,\dots,\overline{x}_n \in \mathfrak{m}_e/\mathfrak{m}_e^2$, i.e. so that $D_i(x_j) \equiv \delta_{ij} \bmod \mathfrak{m}_e$ (Kronecker delta). Let α denote an n-tuple of integers in the range $0,\dots,p-1$, and let $\mathbf{x}^\alpha$ denote the corresponding monomial in the x_i and $D_\alpha := D_1^{\alpha_1} \circ \cdots \circ D_n^{\alpha_n}$, and let $|\alpha| := \sum_i \alpha_i$. Here are some important facts that ensure the derivations D_i behave roughly as expected:

1. The Leibniz rule implies that $D_i \mathfrak{m}_e^r \subseteq \mathfrak{m}_e^{r-1}$, so these derivations induce well-defined derivations $\tilde{D}_i$ of degree -1 the graded ring $\tilde{R} := \bigoplus_{r=0}^\infty \mathfrak{m}_e^r/\mathfrak{m}_e^{r+1}$.
2. We have $D_\alpha(\mathbf{x}_{\alpha'}) \equiv \prod_{i=1}^n \alpha_i(\alpha_i-1)\cdots(\alpha_i-\alpha_i'+1) \bmod \mathfrak{m}$ if $|\alpha| \geq |\alpha'|$, and otherwise this is 0 mod $\mathfrak{m}$. The second statement follows from (1), and the first statement follows from the Leibniz rule by induction via

$$D_i(\mathbf{x}^{\alpha'}) \equiv \sum_{j=1}^n D_i(x_j^{\alpha_j'}) \prod_{s\neq j} x_s^{\alpha_s'} \equiv \alpha_i' x_i^{\alpha_i'-1} \prod_{j\neq i} x_j^{\alpha_j'} \bmod \mathfrak{m}_e^{|\alpha|}.$$

   In particular, $D_\alpha(\mathbf{x}_{\alpha'}) \equiv 0 \bmod \mathfrak{m}_e$ if $\alpha \neq \alpha'$.

Now suppose we have a relation of k-linear dependence among the monomials in R, say of the form

$$\sum_\alpha c_\alpha \prod_{i=1}^n \mathbf{x}^\alpha = 0,$$

with each $c_\alpha \in k$. Then applying $D_{\alpha'}$ and reducing modulo $\mathfrak{m}_e$ leaves only the term $c_{\alpha'}\alpha'! \bmod \mathfrak{m}_e$, where $\alpha'! = \alpha_1'! \cdot \cdots \cdot \alpha_n'!$ denotes the multinomial. But D_α must respect

the linear dependence, so we conclude $c_{\alpha'}\alpha'! = 0$. Since all of the α_i are less than p, the only way this can happen is if $c_\alpha = 0$. Hence the original linear combination is trivial. This shows that the map $k[x_1, \ldots, x_n]/(x_1^p, \ldots, x_n^p) \twoheadrightarrow R$ is injective, hence a k-algebra isomorphism. ■

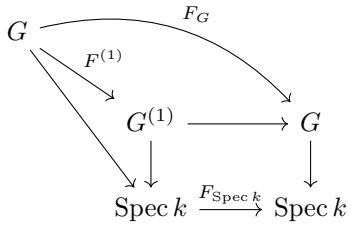
See also [Tat97, Lemma 3.7.1].

Remark 22.5. Note that this lemma does not say anything about the group/Hopf algebra structure; there are many possible group structures on height 1 group schemes, despite the fact that their k-algebras all look similar.

Theorem 22.6. The category of finite local k-group scheme of height 1 is equivalent to the category of p-Lie algebras over k via $G \mapsto \mathrm{Lie}(G)$.

Proof. See [Mum08, III.14, p.130-131]. ■

Definition 22.3. Let G be a k-group scheme of finite type. The absolute Frobenius map F_G, defined on sections by $f \mapsto f^p$, is not a morphism of k-schemes. Instead, we define the relative Frobenius $F^{(1)}$ (also denoted $F_{G/k}$) to be the map induced by the fiber product



where $F_G, F_{\mathrm{Spec}\, k}$ are absolute Frobenii, $G^{(1)}$ is the group scheme making the square Cartesian, and $F^{(1)}$ is the morphism induced by the universal property of the fiber product.

Intuitively, the relative Frobenius morphism acts by p-th powers on the coordinate functions, but also acts trivially on the base field.

Example 22.7. If $G = \mathbb{G}_a$, then we may identify the relative Frobenius map with the k-algebra homomorphism $k[x] \to k[x] : x \mapsto x^p$. Its kernel is denoted $\alpha_p = \mathrm{Spec}\, k[x]/(x^p)$, with comultiplication $x \mapsto 1 \otimes x + x \otimes 1$.

$F^{(1)}$ is a group homomorphism, and $\ker F^{(1)}$ is always a finite local k-group scheme of height 1. Indeed, $F^{(1)}$ is always purely inseparable and $\Gamma(\ker F^{(1)}, \mathcal{O}_{\ker F^{(1)}}) = \mathcal{O}_{G,e}/\{x^p, x \in \mathfrak{m}_{G,e}\}$, as we have a diagram

$$\begin{array}{ccc} \mathrm{Spec}\, \mathcal{O}_{G,e} & \longrightarrow & \mathrm{Spec}\, \mathcal{O}_{G^{(1)},e} \\ \downarrow & & \downarrow \\ G & \xrightarrow{F^{(1)}} & G^{(1)} \end{array}$$

Corollary 22.8. Let $p = \mathrm{char}\, k$. On a commutative finite local k-group scheme G of height 1, multiplication by p is the zero map.

Proof. Apply functoriality from Theorem 22.6 and the fact that $[p] = 0$ on $\operatorname{Lie} G$. Alternatively, without appealing to this equivalence of categories, one can argue along the lines of our proof of Theorem 14.2 that $[p]$ factors through Frobenius, which already kills the group scheme. One final way to do this is to define the Verschiebung map $V^{(1)}$ and then show directly that $[p] = V^{(1)} \circ F^{(1)} = F^{(1)} \circ V^{(1)}$ and similarly conclude. ■

We can now prove Theorem 20.5 for ourselves:

Corollary 22.9. If G has order m, then $[m] = 0$.

Proof. By base change to $\overline{k}$, this statement is clearly true for the étale part, so WLOG G is local. In this case, the order m is always a p-th power, say p^n. We have inclusions $\ker F^{(1)} \hookrightarrow F^{(2)} \hookrightarrow \cdots \hookrightarrow \ker F^{(n)} = G$. Each quotient is a group of height 1, so by applying Corollary 22.8 repeatedly we conclude that $[p^n] = 0$. ■

23 Riemann-Roch for abelian varieties (03/11/2024)

23.1 Homogeneity of the degree map

Definition 23.1. Let k, K be field sand V/k a (not necessarily finite-dimensional) vector space. A function $f : V \to K$ is a *homogeneous polynomial of degree n* if $f|_W$ is a homogeneous polynomial of degree n, where W is any finite dimensional subspace of V and the polynomial variables are given by the coordinates associated to some (equivalently, every) basis of W. Equivalently, for any fixed $v_1, v_2 \in V$, the function $f(\lambda_1 v_1 + \lambda_2 v_2)$ is a homogeneous polynomial in λ_1, λ_2.

Let A/k be a simple abelian variety of dimension g.

Definition 23.2. The degree map $\deg : \operatorname{End}(A) \to \mathbb{Z}$ is defined by

$$f \mapsto \begin{cases} \deg f : & f \text{ is an isogeny} \\ 0 : & f = 0 \end{cases}$$

These are the only two cases if A is simple, and deg is a ring homomorphism since $\deg(f \circ g) = \deg(f)\deg(g)$ for finite morphisms f, g. We extend the degree map linearly to a map $\operatorname{End}^0(A) \to \mathbb{Q}$: for any $f \in \operatorname{End}^0(A)$, there exists some nonzero $n \in \mathbb{Z}$ such that $nf \in \operatorname{End}(A)$, and we define

$$\deg f = \frac{\deg(nf)}{n^{2g}}.$$

which is well-defined and independent of the choice of n since $[n]$ has degree n^{2g}.

Theorem 23.1. For simple A/k, the degree map $\deg : \operatorname{End}^0(A) \to \mathbb{Q}$ is a homogeneous polynomial of degree $2g$.

Proof. See also [Mum08, IV.19, Thm. 2]. It suffices to show that, for any fixed $f_1, f_2 \in \mathrm{End}(A)$ and all integers n,

$$\deg(nf_1 + f_2)$$

is a polynomial in n. We know already that $\deg(nf) = n^{2g}\deg(f)$, i.e. deg satisfies the homogeneity criterion for integer scalars, so if deg is a polynomial function then it must be homogeneous of degree $2g$.

Pick a (very) ample line bundle $\mathscr{L}/A$, so that $\chi(\mathscr{L}) \neq 0$. Then by Lemma 23.2 below,

$$\deg(nf_1 + f_2) = \frac{\chi((nf_1 + f_2)^*\mathscr{L})}{\chi(\mathscr{L})}.$$

Set $\mathscr{L}_n = (nf_1 + f_2)^*\mathscr{L}$. Applying the Theorem of the Cube to the map $f \times g \times h : A \times A \times A \to A$ with $f = nf_1 + f_2, g = h = f_1$ yields

$$\begin{aligned}\mathscr{L}_{n+2} &\simeq \mathscr{L}_{n+1} \otimes \mathscr{L}_{n+1} \otimes (2f_1)^*\mathscr{L} \otimes \mathscr{L}_n^{-1} \otimes f_1^*\mathscr{L}^{-2} \\ &\simeq \mathscr{M}^{\otimes n(n-1)/2} \otimes \mathscr{N}^{\otimes n} \otimes \mathscr{Q},\end{aligned}$$

where $\mathscr{M}, \mathscr{N}, \mathscr{Q}$ are line bundles independent of n (Exercise: write down these line bundles explicitly).

The *Snapper theorem* states that for any projective variety X and any collection of line bundles $\mathscr{L}_1, \ldots, \mathscr{L}_r$ on X, the Euler characteristic $\chi(\mathscr{L}_1^{\otimes n_1} \otimes \cdots \otimes \mathscr{L}_r^{n_r})$ is a numerical polynomial in $n_1, \ldots, n_r$ of degree $\dim X$. (See [Kle66, §I.1] for a proof of the Snapper theorem in somewhat greater generality.) Hence $\chi(\mathscr{L}_n)$, and therefore also $\deg(nf_1 + f_2)$, is indeed a polynomial in n. ■

Lemma 23.2. If $f : A \to B$ is an isogeny, then for all line bundles $\mathscr{L}/B$ we have $\chi(f^*\mathscr{L}) = (\deg f) \cdot \chi(\mathscr{L})$.

Proof. See [Mum08, §12, Thm 2, p. 113] ■

Remark 23.3. Observe the similarity to Proposition 13.3, but N.B. that Lemma 23.2 is false for general varieties, even in nice cases. For example, if g is a morphism of smooth curves $A \to B$ and $\mathscr{L} = \mathcal{O}_B$, then the lemma is true only if g is unramified, since in this case the correct statement is given by the Riemann-Hurwitz formula

$$\chi(\mathcal{O}_A) = (\deg g) \cdot \chi(\mathcal{O}_B) - \deg R$$

where R is the ramification divisor.

23.2 Riemann-Roch for abelian varieties

Theorem 23.4. *(Riemann-Roch for abelian varieties.)* [Mum08, III.16] Let $\mathscr{L}$ be a line bundle on A (not necessarily ample).

1. $\chi(\mathscr{L}^{\otimes n})$ is a homogeneous polynomial of degree g. More precisely,
$$\chi(\mathscr{L}^{\otimes n}) = \frac{\deg(\mathscr{L})n^g}{g!}.$$
2. If $\mathscr{L} = \mathcal{O}(D)$ for a Weil divisor D, then $\chi(\mathscr{L}) = \frac{(D^g)}{g!}$, where (D^g) denotes the g-fold self-intersection number $D.D.\cdots.D$ (g copies of D).
3. $\phi_{\mathscr{L}} : A \to A^\vee$ has degree $\chi(\mathscr{L})^2$. In particular, $\chi(\mathscr{L}) \neq 0$ if and only if $K(\mathscr{L})$ is finite.

Proof. All of the formulas above remain unchanged if we base change to $\overline{k}$, so we might as well assume $k = \overline{k}$.

1.
- Claim 1: Let $\mathscr{L}_1, \mathscr{L}_2$ be line bundles on A with $\mathscr{L}_1 \otimes \mathscr{L}_2^{-1} \in \mathrm{Pic}^0(A)$. Then we claim $\chi(\mathscr{L}_1) = \chi(\mathscr{L}_2)$. The condition on $\mathscr{L}_1, \mathscr{L}_2$ shows that $\mathscr{L}_1$ and $\mathscr{L}_2$ are algebraically equivalent—recall Lemma 15.4—so we have a connected scheme T and a line bundle $\mathscr{L}/A \times T$ with $\mathscr{L}|_{t_1} \simeq \mathscr{L}_1$ and $\mathscr{L}|_{t_2} \simeq \mathscr{L}_2$. Connectedness of $A \times T$ and constancy of the Euler characteristic in flat families implies the desired equality.
- Claim 2: We claim that for any line bundle $\mathscr{L}/A$ there exist line bundles $\mathscr{L}_1, \mathscr{L}_2$ on A such that $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2$, $\mathscr{L}_1$ is symmetric (i.e. $[-1]^*\mathscr{L}_1 = \mathscr{L}_1$), and $\mathscr{L}_2 \in \mathrm{Pic}^0$. To show this, we show $\mathscr{L} \otimes [-1]^*\mathscr{L}^{-1}$ lies in Pic^0. We have
$$\tau_x^*(\mathscr{L} \otimes [-1]^*\mathscr{L}^{-1}) \otimes \mathscr{L}^{-1} \otimes [-1]^*\mathscr{L} = \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \otimes [-1]^*(\tau_{-x}^*\mathscr{L}^{-1} \otimes \mathscr{L}). \tag{8}$$
$\tau_{-x}^*\mathscr{L}^{-1} \otimes \mathscr{L}$ lies in Pic^0 by the theorem of the square. We change perspective: we can view $\tau_{-x}^*\mathscr{L}^{-1} \otimes \mathscr{L}$ as a point on $A^\vee$ and pullback by $[-1]$ as the map $[-1]_{A^\vee}$. This is the morphism defined on points by sending a line bundle to its inverse, so 8 may be rewritten as
$$\tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \otimes \tau_{-x}^*\mathscr{L} \otimes \mathscr{L}^{-1}$$
which is trivial—again by by the theorem of the square—proving translation-invariance of $\mathscr{L} \otimes [-1]^*\mathscr{L}^{-1}$, i.e. membership in $\mathrm{Pic}^0(A) = A^\vee(k)$.
Since $A^\vee(k)$ is a divisible group (here is where we use the assumption $\overline{k} = k$!), there exists a line bundle $\mathscr{L}_2/A$ in $\mathrm{Pic}^0(A)$ such that $\mathscr{L}_2^{\otimes 2} = \mathscr{L} \otimes [-1]^*\mathscr{L}^{-1}$. We set $\mathscr{L}_1 := \mathscr{L} \otimes \mathscr{L}_2^{-1}$; then
$$[-1]^*\mathscr{L}_1 = [-1]^*\mathscr{L} \otimes [-1]^*\mathscr{L}_2^{-1} = [-1]^*\mathscr{L} \otimes \mathscr{L}_2 = \mathscr{L} \otimes \mathscr{L}_2^{-1} = \mathscr{L}_1$$
so $\mathscr{L}_1$ is symmetric, proving our claim. Again we use the fact that $\mathscr{L}_2 \in \mathrm{Pic}^0(A)$

to conclude $[-1]^*\mathscr{L}_2 = \mathscr{L}_2^{-1}$.

- Claim 3: We claim that it suffices to prove (1) in the case $\mathscr{L}$ is symmetric. If $\mathscr{L}_1 \otimes \mathscr{L}_2^{-1} \in \mathrm{Pic}^0(A)$, then $\chi(\mathscr{L}_1^{\otimes n}) = \chi(\mathscr{L}_2^{\otimes n})$. For $\mathscr{L}_1$ and $\mathscr{L}_2$ lie in the same component of the full Picard scheme $\mathrm{Pic}_{A/k}$, so a slightly modified version of Lemma 15.4 shows that they are algebraically equivalent and we may apply the same argument as in Claim 1. The degree of a line bundle is determined by its Hilbert polynomial, so we conclude both sides of the desired formula (1) are the same for $\mathscr{L}_1$ and $\mathscr{L}_2$. By Claim 2, we can find a symmetric $\mathscr{L}_1$ with $\mathscr{L} \otimes \mathscr{L}_1^{-1} \in \mathrm{Pic}^0(A)$, so it suffices to prove the formula for $\mathscr{L}_1$ instead.

So we may assume $\mathscr{L}$ is symmetric. Then

$$\chi(\mathscr{L}^{\otimes n^2}) = \chi([n]^*\mathscr{L}) = \deg[n] \cdot \chi(\mathscr{L}) = n^{2g}\chi(\mathscr{L}).$$

where the middle equality is by Lemma 23.2. This is true for any square n^2, but $\chi(\mathscr{L}^{\otimes m})$ is a polynomial in m that agrees with $n^{2g}\chi(\mathscr{L})$ whenever $m = n^2$ is a square. If two integer polynomials agree infinitely often, they are equal, so we conclude $\chi(\mathscr{L}^{\otimes n}) = n^g\chi(\mathscr{L})$ even when n is not a square.

Homogeneity means that the only term in the Hilbert polynomial $\chi(\mathscr{L}^{\otimes n})$ is the leading term, which, by the definition of degree, is $\frac{\deg(\mathscr{L})}{g!}n^g$, giving the formula for (1).

2. (Sketch.) If $\mathscr{L}$ is very ample, then by intersection theory

$$\deg(\mathscr{L}) = (D^g).$$

In more detail, since $\mathscr{L}$ is very ample, we can pick $\sigma_0, \sigma_1, \ldots, \sigma_g \in \Gamma(A, \mathscr{L})$ with no common zeros such that divisors of zeros $\mathrm{div}(\sigma_1), \ldots, \mathrm{div}(\sigma_g)$ intersect transversely. Then $(D^g) = (\mathrm{div}\,\sigma_1).\cdots.(\mathrm{div}\,\sigma_g)$ is the number of points in the intersection. The sections σ_i define a finite morphism $\phi : A \to \mathbb{P}^g$, and (D^g) is the (multiplicity-free) preimage of $[1 : 0 : \cdots : 0]$, so we conclude $(D^g) = \deg\phi$ and

$$\deg(\mathscr{L}) = \deg\phi \cdot \deg(\mathcal{O}_{\mathbb{P}^g}(1)) = \deg\phi.$$

by Proposition 13.3.[18] This lets us conclude (2) from (1).

In general, we can reduce to the very ample case by writing an arbitrary line bundle as $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$ with $\mathscr{L}_1, \mathscr{L}_2$ very ample.

3. We first prove the claim when $K(\mathscr{L})$ is finite (this is implied by, but not equivalent to, ampleness). Recall the Mumford line bundle

$$\mathscr{M} = m^*\mathscr{L} \otimes \mathrm{pr}_1^*\,\mathscr{L}^{-1} \otimes \mathrm{pr}_2\,\mathscr{L}^{-1} = (\mathbf{id} \times \phi_{\mathscr{L}})^*\mathcal{P}.$$

The map $\mathbf{id} \times \phi_{\mathscr{L}}$ is an isogeny from $A \times A$ to $A \times A^\vee$, so Lemma 23.2 is applicable,

[18] But note that Lemma 23.2 is not applicable because $\mathbb{P}^g$ is not an abelian variety.

yielding

$$\chi(\mathscr{M}) = \deg(\phi_{\mathscr{L}})\chi(\mathcal{P}).$$

Recall from the proof of Theorem 15.6 that $R^i \operatorname{pr}_{1,*}\mathscr{M}$ is supported on the 0-dimensional subscheme $K(\mathscr{L})$ when $\mathscr{L}$ is ample. Using the Leray spectral sequence, we also had

$$H^i(A \times A, \mathscr{M}) = \Gamma(A, R^i \operatorname{pr}_{1,*}\mathscr{M}).$$

By the projection formula,

$$\begin{aligned} R^i \operatorname{pr}_{1,*}(m^*\mathscr{L} \otimes \operatorname{pr}_1^*\mathscr{L}^{-1} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1}) &= R^i \operatorname{pr}_{1,*}(m^*\mathscr{L} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1}) \otimes \mathscr{L}^{-1} \\ &= R^i \operatorname{pr}_{1,*}(m^*\mathscr{L} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1}) \end{aligned}$$

where we use the fact that this sheaf is supported on a finite set to conclude that tensoring with a line bundle does nothing. Hence

$$H^i(A \times A, \mathscr{M}) = \Gamma(A, R^i \operatorname{pr}_{1,*}(m^*\mathscr{L} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1})) = H^i(A \times A, m^*\mathscr{L} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1}).$$

Note that $(m, \operatorname{pr}_2) : A \times A \to A \times A$ is an isomorphism. By Künneth, we have

$$\chi(\mathscr{M}) = \chi(m^*\mathscr{L} \otimes \operatorname{pr}_2^*\mathscr{L}^{-1}) = \chi(\mathscr{L}) \cdot \chi(\mathscr{L}^{-1}),$$

and by (1) this last expression is $(-1)^g\chi(\mathscr{L})^2$. Mumford shows that $\chi(\mathcal{P}) = (-1)^g$ ([Mum08, III]), so plugging this into our formula for $\chi(\mathscr{M})$ shows that $\deg \phi_{\mathscr{L}} = \chi(\mathscr{L})^2$.

If instead $K(\mathscr{L})$ is infinite, then $\phi_{\mathscr{L}}$ has infinite kernel, hence degree 0. Moreover, $K(\mathscr{L})$ contains an abelian variety of positive dimension, hence also contains a finite subgroup F of arbitrarily large order. The map $\mathbf{id}_A \times \phi_{\mathscr{L}} : A \times A \to A \times A^\vee$ factors through the isogeny $\mathbf{id}_A \times q : A \times A \to A \times (A/F)$. We know that $m^*\mathscr{L} \otimes p_2^*\mathscr{L}^{-1} = (\mathbf{id}_A \times q)^*)(\mathcal{P} \otimes \operatorname{pr}_1^*\mathscr{L})$. The fact that $m^*\mathscr{L} \otimes p_2^*\mathscr{L}^{-1}$ is the pullback of some line bundle on $A \times A^\vee$ implies that it is also the pullback of a line bundle on $A \times (A/F)$, so we conclude by Proposition 23.2 that $\chi(m^*\mathscr{L} \otimes p_2^*\mathscr{L}^{-1})$ is a multiple of $|F|$. Since we can choose $|F|$ to be arbitrarily large, we conclude $\chi(m^*\mathscr{L} \otimes p_2^*\mathscr{L}^{-1}) = 0$. The same argument as before, using the isomorphism $(m, \operatorname{pr}_2) : A \times A \to A \times A$ and Künneth, shows that $\chi(m^*\mathscr{L} \otimes p_2^*\mathscr{L}^{-1}) = (-1)^g\chi(\mathscr{L})^2$, hence $\chi(\mathscr{L}) = 0$ too.

■

Corollary 23.5. The degree of any polarization is a perfect square.

Proposition 23.6. If $K(\mathscr{L})$ is ample, then $H^i(A, \mathscr{L}) = 0$ for all $i > 0$ and $H^i(A, \mathscr{L}) \neq 0$.

Proof. (Sketch, assuming two major results from Mumford.) The Vanishing Theorem [Mum08, §16, p. 140] states that if $K(\mathscr{L})$ is finite, then that $H^p(A, \mathscr{L}) = 0$ for all but

one p, but that the remaining cohomology group, whose degree we define to be the *index* $i(\mathscr{L})$ of $\mathscr{L}$, is nonzero. [Mum08, Cor. on p.148] tells us that $i(\mathscr{L}) = i(\mathscr{L}^{\otimes n})$ for any positive integer n. If $\mathscr{L}$ is ample, take n large enough so that $\mathscr{L}^{\otimes n}$ is very ample. Very ample line bundles always have global sections, so we conclude $i(\mathscr{L}^{\otimes n}) = i(\mathscr{L}) = 0$. ■

24 Tate's theorem: injectivity (03/13/2024)

Next week's RTG seminar will be on purity for abelian 3-folds; it might be worth going to.

We started lecture by finishing part (3) of the Riemann-Roch theorem; this has been moved to the previous section.

Theorem 24.1. *(Injectivity part of Tate's theorem)* [Mum08, IV.19, Thm. 3, p. 164] Let A, B be abelian varieties over k. Then $\mathrm{Hom}(A, B)$ is a finitely generated free abelian group, and

$$T_\ell : \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathrm{Gal}(k^s/k)}(T_\ell(A), T_\ell(B)) \subseteq \mathrm{Hom}(T_\ell(A), T_\ell(B))$$

is injective for all prime $\ell \neq \mathrm{char}\, k$.

Proof. We can reduce to the case $A = B$ and with A simple. Via Poincaré complete reducibility, A is isogenous to $\prod_i A_i$ and B is isogenous to $\prod_j B_j$ with A_i, B_j simple, and

$$\mathrm{Hom}(A, B) \hookrightarrow \prod_{i,j} \mathrm{Hom}(A_i, B_j)$$
$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \hookrightarrow \prod_{i,j} \mathrm{Hom}(A_i, B_j) \otimes \mathbb{Z}_\ell$$

so it suffices to prove the claim for each of the $\mathrm{Hom}(A_i, B_j)$, i.e. we can reduce to the case A and B are simple.

If A and B are simple and isogenous, then we (noncanonically) get $\mathrm{Hom}(A, B) \hookrightarrow \mathrm{End}(A)$ by choosing an isogeny $g : B \to A$ and sending $\psi \mapsto g \circ \psi$ for $\psi \in \mathrm{Hom}(A, B)$, so it suffices to prove the claim for $A = B$ in this case. If A and B are simple and nonisogenous, then $\mathrm{Hom}(A, B) = 0$, so we can ignore this case.

Therefore let A be simple. The fact that the degree map is a homogeneous polynomial of degree $2 \dim A$ shows that $\mathrm{End}(A)$ is torsion-free. We claim that for all finitely generated $\mathbb{Z}$-submodules $M \subseteq \mathrm{End}(A)$, we have

$$\mathbb{Q}M \cap \mathrm{End}(A) := \{f \in \mathrm{End}(A) : \exists n \in \mathbb{Z}, nf \in M\},$$

i.e. with the intersection occurring in $\mathrm{End}^0(A)$, is a finitely generated $\mathbb{Z}$-module; this shows that $\mathrm{End}(A)$ is not "infinitely divisible." $\mathbb{Q}M$ is a finite-dimensional $\mathbb{Q}$-vector space, so the homogeneous polynomial function $\deg|_{\mathbb{Q}M}$ extends to $\mathbb{R}M$. The open neighborhood of $0 \in \mathbb{R}M$ given by

$$U := \{x \in \mathbb{R}M : |\deg(x)| < 1\}$$

satisfies $U \cap \mathrm{End}(A) = \{0\}$ because all nonzero endomorphisms of A have positive integer degree. Therefore, $\mathbb{Q}M \cap \mathrm{End}(A) \hookrightarrow \mathbb{R}M$ is discrete, i.e. a (not-necessarily full rank) lattice

in a Euclidean space, hence of finite $\mathbb{Z}$-rank, proving the claim.

To prove injectivity of T_ℓ, it suffices to show that, for all finitely generated $\mathbb{Z}$-modules $M \subseteq \mathrm{End}(A)$, the map $M \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell A)$ is injective, since $\mathrm{End}(A)$ is a direct limit of its finitely generated submodules. By the previous claim, we may even enlarge M so that $M = \mathbb{Q}M \cap \mathrm{End}(A)$. For such M, which is always free, pick a $\mathbb{Z}$-basis $f_1, \ldots, f_r$. Suppose we have a linear dependence

$$T_\ell \left(\sum a_i f_i \right) = 0$$

where $a_i \in \mathbb{Z}_\ell$. If this relation is nontrivial, by multiplying by an appropriate power of ℓ we may assume that at least one of the a_i lies in $\mathbb{Z}_\ell^\times$. For each i, pick a rational integer $a_i' \equiv a_i \bmod \ell$. Then the endomorphism $T_\ell(\sum a_i' f_i)$ maps $T_\ell(A)$ into $\ell T_\ell(A)$. By the definition of $T_\ell(A)$, this means that $\ker \sum a_i' f_i \supseteq A[\ell]$, so there exists $f' \in \mathbb{Q}M \cap \mathrm{End}(A) = M$ such that $\sum a_i' f_i = f' \circ \ell$. Hence $\ell \mid a_i'$ for all a_i', hence $\ell \mid a_i$ for all i, contradicting our assumption. Hence T_ℓ is injective.

Injectivity of any particular T_ℓ shows that $\mathrm{End}^0(A)$ is a finite-dimensional $\mathbb{Q}$-vector space. Therefore, there exists a finitely generated $M \subseteq \mathrm{End}(A)$ with $\mathbb{Q}M = \mathrm{End}^0(A)$. Then we have $\mathbb{Q}M \cap \mathrm{End}(A) = \mathrm{End}(A)$, and this is finitely generated by our first claim. ∎

Remark 24.2. Theorem 24.1 immediately gives a bound $\mathrm{rk}_{\mathbb{Z}}(A, B) \leq 4 \dim A \dim B$, since the Tate module has $\mathbb{Z}_\ell$-rank $2g$. This is usually not an equality, but sometimes is, for example in the case of supersingular elliptic curves.

Remark 24.3. If k is finitely generated over its prime field, then in fact the injection in Theorem 24.1 is an isomorphism. The positive characteristic case was proven by Zarhin, and the characteristic 0 case was proven by Faltings.

Corollary 24.4. The Néron-Severi group $\mathrm{NS}(A) \subseteq \mathrm{Hom}(A_{\overline{k}}, A^\vee_{\overline{k}})$ is a finitely generated free $\mathbb{Z}$-module.

Proof. By Remark 17.6. ∎

Corollary 24.5. $\mathrm{End}^0(A)$ is a finite dimensional semisimple algebra.

Definition 24.1. Let $B/\mathbb{Q}$ be a finite dimensional simple algebra. A map $T : B \to \mathbb{Q}$ is said to be a *trace form* if T is $\mathbb{Q}$-linear and symmetric, i.e. $T(ab) = T(ba)$ for all $a, b \in B$. A map $N : B \to \mathbb{Q}$ is said to be a *norm form* if N is a polynomial function and $N(ab) = N(a)N(b)$ for all $a, b \in \mathbb{Q}$.

Proposition 24.6. [Mum08, IV.19, Lem. on p. 165] Let B/k be a finite dimensional simple algebra with center K. Then there exists a canonical norm form $\mathrm{Nm}^0_{B/K} : B \to K$ such that any norm form on B/k may be written as

$$(\mathrm{Nm}_{K/k} \circ \mathrm{Nm}^0_{B/K})^k$$

for some integer $k \geq 0$, where $\mathrm{Nm}_{K/k}$ is the field-theoretic norm map. We likewise have a canonical trace $\mathrm{Tr}^0_{B/K} : B \to K$ such that any trace form on B/k may be written as

$$\phi \circ \mathrm{Tr}^0_{B/K}$$

for some k-linear map $\phi : K \to k$.

Definition 24.2. $\mathrm{Nm}_{K/k} \circ \mathrm{Nm}^0_{B/K}$ is called the *reduced norm form* of B/k and $\mathrm{Tr}_{K/k} \circ \mathrm{Tr}^0_{B/K}$ is called the *reduced trace form* of B/k (where $\mathrm{Tr}_{K/k}$ is the field-theoretic trace map).

Remark 24.7. When D is central simple, so that $K = k$, the reduced norm form and the reduced trace form are descended from the determinant and trace map, respectively, on $D \otimes_k \overline{k} \simeq M_n(k)$.

25 Weil pairing (03/15/2024)

25.1 Computations on the Tate module

Theorem 25.1. [Mum08, IV.19, Thm. 4]

1. $\deg(f) = \det(T_\ell(f))$ for $f \in \mathrm{End}^0(A)$. (Determinant via treating $T_\ell(f)$ as a $2g \times 2g$ matrix.)
2. The characteristic polynomial $P(x)$ of $T_\ell(f)$, i.e. $P(x) = \det(x - T_\ell(f)) \in \mathbb{Q}_\ell[x]$, actually has $\mathbb{Z}$-coefficients. By (1), $P(n) = \deg([n]_A - f)$ for integers n.

We will first need:

Lemma 25.2. For an isogeny $f : A \to B$, we have an exact sequence of $\mathbb{Z}_\ell[\mathrm{Gal}(k^s/k)]$-modules

$$0 \longrightarrow T_\ell(A) \xrightarrow{T_\ell(f)} T_\ell(B) \longrightarrow (\ker f(k^s))_\ell \longrightarrow 0.$$

Here, $(\ker f(k^s))_\ell$ denotes the ℓ-primary part of $\ker f(k^s)$.

Proof. (Sketch; see also [EvdGM24, §10.5-6].) By definition,

$$\begin{aligned} T_\ell(A) &= \varprojlim_n A[\ell^n](k^s) \\ &= \varprojlim_n \mathrm{Hom}(\mathbb{Z}/\ell^n\mathbb{Z}, A(k^s)) \\ &= \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s)). \end{aligned}$$

Given an exact sequence $0 \to N \to A \to B \to 0$ of fppf group schemes, we get an exact sequence $0 \to N(k^s) \to A(k^s) \to B(k^s) \to 0$. Applying the functor $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, -)$, we get a long exact sequence

$$0 \longrightarrow T_\ell(A) \longrightarrow T_\ell(B) \longrightarrow \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^s)) \longrightarrow \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s))$$

The last Ext group is 0 if $k^s = \overline{k}$, i.e. k is perfect, since in this case $A(k^s)$ is divisible, hence an injective object in the category of abelian groups. (Additional arguments need to be made in the imperfect case.) We may also write $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^s)) = \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^s)_\ell)$, since any homomorphism from $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ must land in the ℓ-primary part.

We also consider the exact sequence $0 \to \mathbb{Z}_\ell \to \mathbb{Q}_\ell \to \mathbb{Q}_\ell/\mathbb{Z}_\ell \to 0$. Applying $\mathrm{Hom}(-, N(k^s)_\ell)$ to this exact sequence, all of the $\mathrm{Ext}^i(\mathbb{Q}_\ell, N(k^s)_\ell)$ terms vanish because $\mathbb{Q}_\ell$ is ℓ-divisible, so we get $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(k^s)) = \mathrm{Hom}(\mathbb{Z}_\ell, N(k^s)_\ell) = N(k^s)_\ell$, yielding the lemma. ∎

We prove Theorem 25.1:

Proof. 1. Let $f \in \mathrm{End}(A)$, and let $|\deg(f)|_\ell$ be the ℓ-adic valuation of $\deg(f)$ on $\mathbb{Q}_\ell$ (normalized so that $|\ell|_\ell = 1/\ell$). If f is not any isogeny, then $\deg(f) = 0$, and $T_\ell(T)$ cannot be invertible[19], so $\det(T_\ell(f)) = 0$ too. Otherwise, if f is an isogeny, then

$$|\deg(f)|_\ell = |\#(\ker(f))_\ell(k^s)|_\ell$$

since the ℓ-torsion part of $\ker(f)$ is étale. By Lemma 25.2, the right hand side is $|\det T_\ell(f))|_\ell$—the determinant of a lattice endomorphism measures how large the cokernel is. Therefore, for all $f \in \mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$, we have $|\deg_{\mathbb{Q}_\ell}(f)|_\ell = |\det(T_\ell(f))|_\ell$.

But we want more than this: we want actual equality, not just equality of ℓ-adic norms. To get this, we may write $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{End}(A) = \prod_i D_i$ a a product of finite dimensional simple algebras over $\mathbb{Q}_\ell$; let K_i be the center of D_i. The maps $\deg_{\mathbb{Q}_\ell}, \det : \mathrm{End}(A) \otimes \mathbb{Q}_\ell \to \mathbb{Q}_\ell$ both define norm forms, so by Proposition 24.6 they are each of the form

$$\begin{aligned} \deg_{\mathbb{Q}_\ell}(\alpha_1, \dots, \alpha_n) &= \prod_i (\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i})^{v_i}(\alpha_i) \\ \det(\alpha_1, \dots, \alpha_n) &= \prod_i (\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i})^{w_i}(\alpha_i) \end{aligned}$$

for some $v_i, w_i \in \mathbb{Z}_{>0}$. We already proved that

$$|\deg_{\mathbb{Q}_\ell}(1, \dots, \ell, \dots, 1)|_\ell = |\det(1, \dots, \ell, \dots, 1)|_\ell$$

[19] Taking a decomposition of A into simple factors, f must kill one of the factors, hence $T_\ell(f)$ kills the corresponding factor in the corresponding decomposition of $T_\ell(A)$.

(taking the endomorphism to be the identity on all components except one, where it is multiplication by ℓ), so

$$|(\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i})^{v_i}(\ell)|_\ell = |(\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i})^{w_i}(\ell)|_\ell$$

for all i. so that $v_i = w_i$ for all i, hence det $=$ deg $\mathbb{Q}_\ell$. Since $\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i}$ is homogeneous of positive degree, $(\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^0_{D_i/K_i})(\ell)$ has positive ℓ-adic valuation, so we conclude that $v_i = w_i$ for all i, yielding equality of $\deg_{\mathbb{Q}_\ell}$ and det.

2. Since $P(n) = \deg([n]_A - f) \in \mathbb{Z}$ for all n, we conclude that $P(x)$ is a numerical polynomial, so in particular $P(x) \in \mathbb{Q}[x]$. $\mathrm{End}(A)$ is finitely generated over $\mathbb{Z}$, f is satisfies some monic integer polynomial, so $T_\ell(f)$ also satisfies an integer monic polynomial. We conclude that all eigenvalues of $T_\ell(f)$ are algebraic integers. This means that $P(x)$ is a monic polynomial with $\mathbb{Q}$-coefficients and algebraic integer roots. Therefore the coefficients of $P(x)$ must actually lie in $\mathbb{Z}$, since $P(x)$ is a product of powers of the integral minimal polynomials of its roots.

■

25.2 Weil pairing

Definition 25.1. We let $\mathbb{Z}_\ell(1)$ denote the Tate module of the multiplicative group:

$$\mathbb{Z}_\ell(1) := T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}.$$

This is a rank 1 free $\mathbb{Z}_\ell$-module with Galois action by the cyclotomic character.

Definition 25.2. Let M be a finitely generated free $\mathbb{Z}_\ell$-module with a $\mathrm{Gal}(k^s/k)$-action. The *Tate twists* of M are

$$M(n) := M \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1)^{\otimes n}$$

for $n \in \mathbb{Z}_{\geq 0}$, and $M(n) := M \otimes_{\mathbb{Z}_\ell} (\mathbb{Z}_\ell(1)^\vee)^{\otimes -n}$ for $n < 0$. (Here $\mathbb{Z}_\ell(1)^\vee$ is the rank 1 free $\mathbb{Z}_\ell$-module with Galois action by the inverse of the cyclotomic character.)

We want to construct the Weil pairing, which we want to be a pairing $T_\ell(A) \times T_\ell(A^\vee) \to \mathbb{Z}_\ell(1)$ that is nondegenerate, $\mathbb{Z}_\ell$-bilinear, and such that if $\phi_{\mathscr{L}}$ is a polarization, then composing $(\mathbf{id}, \phi_\ell) : T_\ell(A) \times T_\ell(A) \to T_\ell(A) \times T_\ell(A^\vee)$ with the Weil pairing gives a symplectic form $T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1)$. In particular, the pairing defines an isomorphism $T_\ell(A^\vee) \simeq (T_\ell(A))^\vee(1)$.

Recall that $A^\vee[\ell^n] \simeq (A[\ell^n])^\vee$, so we already get a nondegenerate pairing $A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$ for each power of ℓ. We need to verify that this pairing is compatible with the inverse limit defining the Tate module. That is, we want the following diagram to commute:

$$\begin{array}{ccc} A[\ell^n] \times A^\vee[\ell^n] & \longrightarrow & \mu_{\ell^n} \\ {\scriptstyle \ell\times\ell}\uparrow & & \uparrow{\scriptstyle \ell} \\ A[\ell^{n+1}] \times A^\vee[\ell^{n+1}] & \longrightarrow & \mu_{\ell^{n+1}} \end{array}$$

To do this, we will give a more explicit description of Cartier duality.

Let $f : A \to A$ be any isogeny, let $x \in (\ker f)(\overline{k})$, and let $\mathscr{L} \in (\ker f^\vee)(\overline{k})$, which means that there exists a trivialization $\beta : f^*\mathscr{L} \simeq \mathcal{O}_A$ (choose one arbitrarily). There is a natural isomorphism $t_x^*\mathcal{O}_A \to \mathcal{O}_A$ sending $1 \mapsto 1$;[20] we denote this with equality. Recall from the proof of $(\ker f)^\vee \simeq \ker(f^\vee)$ that we have

$$\begin{array}{ccc} t_x^*f^*\mathscr{L} & \xrightarrow{t_x^*\beta} & t_x^*\mathcal{O}_A \\ \| & & \| \\ f^*t_{f(x)}^*\mathscr{L} & & \mathcal{O}_A \\ \| & \overset{\beta}{\nearrow} & \\ f^*\mathscr{L} & & \end{array}$$

Note that $f(x) = e \in A$, so we obtain a certain automorphism $\tau^*\beta \circ \beta^{-1} : \mathcal{O}_A \to \mathcal{O}_A$, which must be an element of $\overline{k}^\times$. Note that this morphism is independent of the choice of β, since any different choice $\beta' : f^*\mathscr{L} \to \mathcal{O}_A$ differs from β by another constant. We claim that the pairing from Cartier duality is given by

$$e_f(x, \mathscr{L}) = t_x^*\beta \circ \beta^{-1} \in \overline{k}^\times$$

Verifying that this indeed the pairing we got from the proof of Theorem 18.1 amount to unwinding the descent datum we defined there; we omit these checks, but it is a good exercise in descent theory to work this out.

The Weil pairing concerns the case $f = [n]$. With the explicit description in hand, we can show compatibility with the inverse limit in the Tate module:

Lemma 25.3. Let $\mathscr{L} \in A^\vee[m](\overline{k}) \subseteq A^\vee[mn](\overline{k})$ and $x \in A[mn](\overline{k})$. Then we have $e_{mn}(x, \mathscr{L}) = e_m(nx, \mathscr{L})$. In particular,

$$e_{\ell^n}(\ell x, \ell\mathscr{L}) = e_{\ell^{n+1}}(x, \ell\mathscr{L}) = e_{\ell^{n+1}}(x, \mathscr{L})^\ell$$

when $x \in A[\ell^{n+1}](\overline{k}), \mathscr{L} \in A^\vee[\ell^{n+1}](\overline{k})$.

Proof. Pick an isomorphism $\beta : [m]^*\mathscr{L} \to \mathcal{O}_A$. Then we also get an isomorphism $[n]^*\beta : [mn]^*\mathscr{L} = [n]^*[m]^*\mathscr{L} \to \mathcal{O}_A$, so using the explicit description we may write

$$\begin{aligned} e_{mn}(x, \mathscr{L}) &= t_x^*([n]^*\beta) \circ ([n]^*\beta)^{-1} \\ &= [n]^*(t_{nx}^*\beta \circ \beta^{-1}) \\ &= [n]^* e_m(nx, \mathscr{L}) \\ &= e_m(nx, \mathscr{L}). \end{aligned}$$

(Here we are treating $e_m(nx, \mathscr{L}) \in \overline{k}^\times$ as an automorphism of $\mathcal{O}_{A_{\overline{k}}}$ for this notation to make sense.) ∎

[20] In general, if $f : X \to Y$ is a morphism and $\mathscr{F}$ is a sheaf on Y, then we get a natural map $\Gamma(Y, \mathscr{F}) \to \Gamma(X, f^*\mathscr{F})$ defined affine-locally by $s \mapsto s \otimes 1$, using the identification $f^*\widetilde{M} = \widetilde{M \otimes_A B}$ when $X = \operatorname{Spec} B, Y = \operatorname{Spec} A$. The canonical isomorphism $\tau_x^*\mathcal{O}_A = \mathcal{O}_A$ we are using is the one induced by this map on global sections.

On the homework, you will show that if $f : A \to B$ is any homomorphism, then $e_{\ell^\infty}(T_\ell(f)x, y) = e_{\ell^\infty}(x, T_\ell(f^\vee)y)$. That is, the dual (in the abelian variety sense) is the adjoint for the Weil pairing.

26 Weil pairing continued (03/18/2024)

26.1 Alternative description of the Weil pairing

Let $\mathscr{L} \in A^\vee[n](\overline{k})$. Because abelian varieties are smooth, we may write $\mathscr{L} = \mathcal{O}(D)$ for some Weil divisor D on A, and we get a corresponding embedding $i : \mathscr{L} \hookrightarrow \mathscr{K}_A$ into the constant sheaf of rational functions on A. (We think of sections of $\mathscr{L}$ as meromorphic functions having poles "at worst of order D.")

For $x \in A[n](\overline{k})$, we get

$$\mathscr{K}_A \simeq [n]^*\mathscr{K}_A \xleftarrow[[n]^*i]{} [n]^*\mathscr{L} \xrightarrow{\beta} \mathcal{O}_A$$

where $\beta : [n]_x^*\mathscr{L} \to \mathcal{O}_X$ is a choice of trivialization. Then $g := [n]^*i \circ \beta^{-1}(1)$ is a rational function on A. By definition, $\operatorname{div}(g^{-1}) = [n]^{-1}D$ (preimage of the divisor D with multiplicity).

Recall from the previous lecture that $e_n(x, \mathscr{L})$ may be computed as $\tau_x^*\beta \circ \beta^{-1} \in k^\times$. We claim that this constant is $\frac{g(z+x)}{g(z)}$ for all $z \in A$, independently of the choice of $z \in A$; this is the generalization of how [Sil09, §3.8] defines the Weil pairing in the case of elliptic curves. Indeed, we can pin down the constant $e_n(x, \mathscr{L})$ by evaluating the action of $\tau_x^*\beta \circ \beta^{-1}$ on any nonzero test function in $\mathscr{K}$ (this endomorphism of $\mathcal{O}_A$ yields an action $K(A)$ at the generic point). We test on the constant function 1:

$$\tau_x^*\beta \circ \beta^{-1}(1) =$$

26.2 (Anti)symmetry of the Weil pairing

We notate $e_{\ell^\infty} = \varprojlim_n e_{\ell^n}$. This is a $\mathbb{Z}$-linear nondegenerate pairing. We will notate the group law on $\mathbb{Z}_\ell(1) = \mu_{p^\infty}$ additively for the rest of this section.

Theorem 26.1. [Mum08, IV.20, Thm. 1] For all line bundles $\mathscr{L}/A$, the pairing

$$E^{\mathscr{L}} : T_\ell(A) \times T_\ell(A) \xrightarrow{\mathbf{id} \times T_\ell(\phi_{\mathscr{L}})} T_\ell(A) \times T_\ell(A^\vee) \xrightarrow{e_{\ell^\infty}} \mathbb{Z}_\ell(1)$$

is alternating. In particular, if $\phi_{\mathscr{L}}$ is an isogeny, e.g. if $\mathscr{L}$ is ample, then $E^{\mathscr{L}}$ is a symplectic form (alternating and nondegenerate).

Proof. We want to show that $E^{\mathscr{L}}(x, x) = e_{\ell^\infty}(x, T_\ell(\phi_{\mathscr{L}})x) = 0 \in \mathbb{Z}_\ell(1)$ for all $x \in A[\ell^n]$—it suffices to prove this for all finite n. Write $\mathscr{L} = \mathcal{O}(D)$. Then

$$\phi_{\mathscr{L}}(x) = t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} = \mathcal{O}(t_x^*D - D) = \mathcal{O}(t_{-x}(D) - D)$$

Let g be as in the explicit description of the Weil pairing above. Then $\operatorname{div}(g^{-1}) = [\ell^n]^{-1}(t_{-x}D - D)$. We need to show $t_x^*g = g$, i.e. $g(z + x) = g(z)$.

Pick $y \in A(\overline{k})$ such that $\ell^n y = x$. Then $\operatorname{div}(g^{-1}) = t_{-y}([\ell^n]^{-1}D - [\ell^n]^{-1}D)$, and

$$\begin{aligned}\operatorname{div}\left(\prod_{i=1}^{\ell^n-1} t_{iy}^*(g^{-1})\right) &= t_{-x}([\ell^n]^{-1}D) - [\ell^n]^{-1}D \\ &= 0\end{aligned}$$

because $x \in A[\ell^n](\overline{k})$. We conclude that $h(z) := \operatorname{div}(\prod_{i=1}^{\ell^n-1} t_{iy}^*(g^{-1}))$ is some constant function, so in particular $h(z+y) = h(z)$, so $g(x+z) = g(z)$. ■

For all $\phi : A \to A^\vee$, we get a $\mathbb{Z}_\ell$-bilinear form $E^\phi = e_{\ell^\infty}(-, T_\ell(\phi)(-))$. Then E^ϕ is skew-symmetric if ϕ is a polarization.

Theorem 26.2. [Mum08, IV.20, Thm. 2 + IV.23] Let $\phi : A \to A^\vee$ be a homomorphism. The following are equivalent:

1. ϕ is symmetric (recall Definition 20.2).
2. E^ϕ is skew-symmetric.
3. $2\phi = \phi_{\mathscr{L}}$ for some line bundle $\mathscr{L}/A$.
4. Over $\overline{k}$, $\phi = \phi_{\mathscr{L}'}$ for some $\mathscr{L}'/A_{\overline{k}}$.

Proof. We will only do some of these. For (3) $\implies$ (4), see [Mum08, IV.23, Thm. 3, p.214]. We already did (4) $\implies$ (1) in Proposition 20.2 and (4) $\implies$ (2) in Theorem 26.1. We will prove (1) $\implies$ (3) and (2) $\implies$ (3).

On your homework, you will show that if $f : A \to B$ is a homomorphism, then $e_{\ell^\infty}(T_\ell(f)x, y) = e_{\ell^\infty}(x, T_\ell(f^\vee)y)$. If $\mathscr{L}/B$ is a line bundle, then there is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \phi_{f^*\mathscr{L}}} & & \downarrow{\scriptstyle \phi_{\mathscr{L}}} \\ A^\vee & \xleftarrow[f^\vee]{} & B \end{array}$$

so $E^{f^*\mathscr{L}}(x,y) = E^{\mathscr{L}}(T_\ell(f)(x), T_\ell(f)(y))$. We also know that $(A \times B)^\vee = A^\vee \times B^\vee$, so in particular $(A \times A^\vee)^\vee = A^\vee \times A$, and $T_\ell(A \times B) = T_\ell(A) \times T_\ell(B)$. Let $\mathcal{P}$ be the Poincaré line bundle on $A \times A^\vee$.

Lemma 26.3. $E^{\mathcal{P}}((x, x^\vee), (y, y^\vee)) = e_{\ell^\infty}(x, y^\vee) - e_{\ell^\infty}(y, x^\vee)$ for all $x, y \in T_\ell(A)$ and $x^\vee, y^\vee \in T_\ell(A^\vee)$.

Proof. It suffices to show $E^{\mathcal{P}}((x,0),(y,0)) = 0 = E^{\mathcal{P}}((0,x^\vee),(0,y^\vee))$ and $E^{\mathcal{P}}((x,0),(0,y^\vee)) = e_{\ell^\infty}(x, y^\vee)$.

For the first claim, we have

$$A \xrightarrow{\mathbf{id} \times e_{A^\vee}} A \times A^\vee$$

so $E^{\mathcal{P}}((x,0),(y,0)) = E^{\mathcal{O}_A}(x,y) = e_{\ell^\infty}(x,0) = 0$; for the other part, use $(e \times \mathbf{id}) : A^\vee \to A \times A^\vee$.

For the second claim, we have

$$\phi_{\mathcal{P}} : A \times A^\vee \to (A \times A^\vee)^\vee = A^\vee \times A$$

given by $(x, x^\vee) \mapsto t_{(x,x^\vee)}\mathcal{P} \otimes \mathcal{P}^{-1} \mapsto (t_x^* \mathscr{L}_{x^\vee}, x)$ via the restrictions $A \times e_{A^\vee}, e_A \times A^\vee$. Then

$$\begin{aligned} E^{\mathcal{P}}(x,0),(0,y^\vee)) &= e_{\ell^\infty}((x,0),(y^\vee,0)) \\ &= e_{\ell^\infty}(x,y^\vee) \end{aligned}$$

on A. ■

(1) $\implies$ (3): Given $\phi : A \to A^\vee$, set $\mathscr{L} := (\mathbf{id} \times \phi)^* \mathcal{P}$. For $x \in A$, we have

$$\begin{aligned} \phi_{\mathscr{L}}(x) &= (1 \times \phi)^\vee \circ \phi_{\mathcal{P}} \circ (1 \times \phi)(x) \\ &= (1 \times \phi)^\vee(\phi(x), x) \\ &= \phi(x) + \phi(x) = 2\phi(x). \end{aligned}$$

so $\mathscr{L}$ is the line bundle desired by (3).

(2) $\implies$ (3):

$$\begin{aligned} E^{\mathscr{L}}(x,y) &= E^{\mathcal{P}}(T_\ell(1 \times \phi)(x), T_\ell(1 \times \phi)(y)) \\ &= e_{\ell^\infty}(x, T_\ell(\phi)y) - e_{\ell^\infty}(y, T_\ell(\phi)(x)) \\ &= E^\phi(x,y) - E^\phi(y,x) = 2E^\phi(x,y) \end{aligned}$$

where the last step uses the fact that E^ϕ is skew-symmetric. Since e_{ℓ^∞} is nondegenerate, we conclude that $\phi_{\mathscr{L}} = 2\phi$. ■

Remark 26.4. The image of $\mathrm{NS}(A) = \mathrm{NS}(A_{\overline{k}}) \hookrightarrow \mathrm{Hom}(A_{\overline{k}}, A^\vee_{\overline{k}})$ is exactly the sub-$\mathbb{Z}$-module of symmetric homomorphisms. Recall that this embedding is given by sending a class $[\mathscr{L}]$ in $\mathrm{NS}(A) = \frac{\mathrm{Pic}(A)}{\mathrm{Pic}^0(A)}$ to the homomorphism $\phi_{\mathscr{L}} : A \to A^\vee$. Theorem 26.2 shows that the $\phi_{\mathscr{L}}$ are precisely the symmetric homomorphisms $A \to A^\vee$.

26.3 Rosati involution revisited

Definition 26.1. Given a polarization $\lambda : A \to A^\vee$, we define the *Rosati involution* $(-)^\dagger$ on $\mathrm{End}^0(A)$ by

$$\phi^\vee = \lambda^{-1} \circ \phi \circ \lambda$$

for $\phi \in \mathrm{End}^0(A)$.

Remark 26.5. In this definition, λ^{-1} and ϕ are quasi-isogenies; multiplying by a sufficiently large integer makes these into genuine isogenies. However, if λ is a principal polarization, then the Rosati involution restricts to a well-defined endomorphism on $\mathrm{End}(A)$.

Remark 26.6. The Rosati involution depends on the choice of λ. However, if $\lambda_1 = \lambda_2 \circ f$ for some nonzero $f \in \mathrm{End}^0(A)$ with corresponding Rosatis $\dagger_1, \dagger_2$ (so $f \in \mathrm{End}^0(A)^\times$), then

$$\phi^{\dagger_1} = f^{-1} \circ \phi^{\dagger_2} \circ f$$

so the two Rosatis differ by conjugacy.

27 Albert's classification (03/20/2024)

27.1 Facts about the Rosati involution

For any choice of polarization with associated Rosati involution, and any $\varphi, \psi \in \mathrm{End}^0(A)$:

- $(\varphi + \psi)^\dagger = \varphi^\dagger + \psi^\dagger$
- $(\varphi \circ \psi)^\dagger = \psi^\dagger \circ \varphi^\dagger$ (for this reason the Rosati involution is sometimes called an *anti-involution*)
- $(\varphi^\dagger)^\dagger = \varphi$
- $E^\lambda(T_\ell(\varphi)x, y) = E^\lambda(x, T_\ell(\varphi^\dagger))$

Theorem 27.1. *(Positivity of the Rosati involution.)* For all nonzero $\varphi \in \mathrm{End}^0(A)$, we have

$$\mathrm{Tr}(\varphi \circ \varphi^\dagger) = \mathrm{Tr}(\varphi^\dagger \circ \varphi) > 0.$$

Here the trace is the usual trace on endomorphisms of the $\mathbb{Q}_\ell$-vector space $T_\ell(A) \otimes \mathbb{Q}_\ell$. When A is simple, so that $D = \mathrm{End}^0(A)$ is a division algebra, then this trace is the reduced trace map $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathrm{Tr}^0_{D/K}$, where K is the center.

Proof. WLOG $k = \overline{k}$, and let λ be the choice of polarization. Then $\lambda = \phi_{\mathscr{L}}$ for some ample $\mathscr{L}$. Replacing $\mathscr{L}$ with a power of itself gives $\phi_{\mathscr{L}^{\otimes n}} = [n] \circ \phi_{\mathscr{L}}$, and this factor of $[n]$ cancels itself out in the Rosati involution. Therefore we may assume $\mathscr{L}$ is very ample and write $\mathscr{L} = \mathcal{O}(D)$ for an effective divisor D.[21]

We claim that

$$\mathrm{Tr}(\varphi \circ \varphi^\dagger) = \frac{2g}{(D^g)}(D^{g-1}.\varphi^{-1}(D)),$$

[21] It turns out that all ample line bundles are already of this form, i.e. Theorem 12.4 actually accounts for all ample line bundles, but we never proved this.

expressing the trace as an intersection product. This claim gives the theorem because $\varphi^{-1}(D)$ is also effective and D comes from a very ample line bundle, so the intersections $D^{g-1}.\varphi^{-1}(D)$ and (D^g) are positive integers. (This is more or less point counting when we cut down an effective divisor by hyperplanes.)

To prove the claim, we extract the trace from the characteristic polynomial of $\varphi^\dagger \circ \varphi$. We have

$$\begin{aligned}\deg([n] \circ \phi_{\mathscr{L}} - \phi_{\varphi^*\mathscr{L}}) &= \deg([n] \circ \varphi_{\mathscr{L}} - \varphi^\vee \circ \varphi_{\mathscr{L}} \circ \varphi) \\ &= \deg(\phi_{\mathscr{L}} \circ ([n] - \phi_{\mathscr{L}}^{-1} \circ \varphi^\vee \circ \phi_{\mathscr{L}} \circ \varphi)) \\ &= \deg \phi_{\mathscr{L}} \cdot \deg([n] - \phi_{\mathscr{L}}^{-1} \circ \varphi^\vee \circ \phi_{\mathscr{L}} \circ \varphi) \\ &= \deg \phi_{\mathscr{L}} \cdot \deg([n] - \varphi^\dagger \circ \varphi)\end{aligned}$$

The term $\deg([n] - \varphi^\dagger \circ \varphi)$ is the characteristic polynomial $P(n)$ of $\varphi^\dagger \circ \varphi$ on $T_\ell(A)$ by Theorem 25.1. By the Riemann-Roch Theorem, we may rewrite the above as

$$\begin{aligned}P(n) &= \frac{\deg([n] \circ \phi_{\mathscr{L}} - \phi_{\varphi^*\mathscr{L}})}{\deg \phi_{\mathscr{L}}} \\ &= \frac{\chi(\phi^*\mathscr{L}^{-1} \otimes \mathscr{L}^{\otimes n})^2}{\chi(\mathscr{L})^2} \\ &= \left(\frac{(nD - \varphi^{-1}(D))^g}{(D^g)}\right)^2 \\ &= \frac{1}{(D^g)^2}(n^g D^g - g n^{g-1} D^{g-1}\varphi^{-1}(D) + \dots)^2 \\ &= \frac{n^{2g}}{(D^g)} - n^{2g-1}\frac{2g \cdot D^{g-1}\varphi^{-1}(D)}{(D^g)} + \dots\end{aligned}$$

We use part (3) of Theorem 23.4 to get from the first line to the second line, and we use part (2) to get from the second line to the third; note that in the third line, the additive notation refers to addition in the group of Weil divisors, over which the intersection product distributes. We extract the trace from the n^{2g-1}-term in the last line: it is $\frac{2g \cdot D^{g-1}\varphi^{-1}(D)}{(D^g)}$, as desired. ∎

27.2 Endomorphism algebras of simple abelian varieties

Let A/k be a simple polarized abelian variety, let K be the center of D, and let $K_0 := \{x \in K : x^\dagger = x^\dagger\}$ be the fixed subfield of the Rosati involution.

Lemma 27.2. K_0 is totally real and either $K = K_0$ or K is a quadratic totally imaginary extension of K_0. (In the latter case, this means K is CM.)

Proof. (Sketch.) Split $K_0 \otimes \mathbb{R} = \mathbb{R} \times \cdots \times \mathbb{R} \times \mathbb{C} \times \cdots \times \mathbb{C}$ into the product of the archimedean places of K_0. Total reality of K_0 is equivalent to having all terms in this product be $\mathbb{R}$. Since $x^\dagger = x$ on K_0, we get $\mathrm{Tr}(xx^\dagger) = \mathrm{Tr}(x^2) =: q(x)$ is a quadratic form, where we view K_0 as a $\mathbb{Q}$-vector space. By continuity on $K_0 \otimes \mathbb{R}$ and positivity of the Rosati involution restricted to K_0, $q_{\mathbb{R}}$ is positive semidefinite. The kernel of $q(x)$ is trivial and defined over $\mathbb{Q}$, so the kernel of $q_{\mathbb{R}}$ is also trivial, so $q_{\mathbb{R}}$ is nondegenerate. Hence $q_{\mathbb{R}}$ is positive definite.

If there are any factors of $\mathbb{C}$ in the decomposition of $K_0 \otimes \mathbb{R}$, then taking $x = (0, 0, \ldots, 0, i)$ yields $q_{\mathbb{R}}(x) = -1$, so we conclude that there are no copies of $\mathbb{C}$ in $K_0 \otimes \mathbb{R}$.

Since K_0 is a subfield of K fixed by an involution, we either have $[K : K_0] = 1$ or 2. If this extension is of degree 2, then write $K = K_0(\sqrt{\alpha})$ for some $\alpha \in K_0$, $\sqrt{\alpha} \notin K_0$. Then $(\sqrt{\alpha})^\dagger = -\sqrt{\alpha}$. Suppose embeddings $i_1, i_2 : K \hookrightarrow \mathbb{R}$ exist with $i_1(\sqrt{\alpha}) = -i_2(\sqrt{\alpha})$ (iff K is totally real). Then, restricting to the factors $\mathbb{R} \times \mathbb{R}$ of $K \otimes \mathbb{R}$ corresponding to i_1, i_2, we get

$$\mathrm{Tr}((x, y) \cdot (x, y)^\dagger)) = \mathrm{Tr}((x, y) \cdot (y, x)) = 2xy.$$

But this is certainly not always positive, so we conclude K has no real embeddings if $[K : K_0] = 2$. ■

Definition 27.1. Let D be a non split quaternion algebra over a totally real field $K = K_0$. The *standard involution* on D is $x^* = \mathrm{Tr}^0_{D/K} x - x$.

Example 27.3. If we write D as $H(a, b)$, so that D has K-basis $1, i, j, k$ with $i^2 = a, j^2 = b, ij = -ji = k$, then the standard involution is $x + yi + zj + wk \mapsto x - yi - zj - wk$.

Theorem 27.4. *(Albert's classification.)* [Mum08, IV.21, Thm 2], [EvdGM24, §12.4] Let D be a division algebra of $\mathbb{Q}$ with center K equipped with a positive involution $(-)^\dagger$, and let K_0 be the totally real subfield of K fixed by K_0.

- Type I: $D = K = K_0$ is a totally real field and $(-)^\dagger$ is the identity map.
- Type II: $K = K_0$, and D is a quaternion algebra over K with $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{K \hookrightarrow \mathbb{R}} M_2(\mathbb{R})$ (we say D is *totally indefinite* over $\mathbb{R}$). Under an appropriate choice of such an isomorphism, $(-)^\dagger$ is given by transposition of matrices: $(X_1, \ldots, X_e) \mapsto (X_1^t, \ldots, X_e^t)$. Letting $x \mapsto x^*$ be the standard involution on D, there is an element $a \in D$ with $a^2 \in K$ totally negative such that $x^\dagger = ax^*a^{-1}$ for all $x \in D$.
- Type III : $K = K_0$ and D is quaternion algebra over K with $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H}$ (Hamilton quaternions; we say D is *totally definite* over $\mathbb{R}$). The Rosati involution $x^\dagger = x^*$ is exactly the standard involution.
- Type IV: K is CM with totally real subfield K_0. For all finite places v of K, we have $\mathrm{inv}_v(D) + \mathrm{inv}_{c(v)}(D) = 0$, and moreover $\mathrm{inv}_v(D) = \mathrm{inv}_{cv}(D) = 0$ if $v = c(v)$, where inv_v is the Hasse invariant of the class of D in $\mathrm{Br}(K_v) = \mathbb{Q}/\mathbb{Z}$ and c denotes complex conjugation. There exists an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq_{K \hookrightarrow \mathbb{C}/\text{ conjugation}} M_d(\mathbb{C})$ such that the Rosati is $(X_1, \ldots, X_{e_0}) \mapsto (\overline{X}_1^t, \ldots, \overline{X}_{e_0}^t)$, where $e_0 = [K_0 : \mathbb{Q}]$.

Unfortunately, we will not have time to prove Albert's classification in this course; see Mumford for a full proof. We will see next time that the subspace of $\mathrm{End}^0(A)$ fixed by Rosati (denoted $\mathrm{End}^0(A)^\dagger$) is related to the Néron-Severi group.

28 Applications of Albert's classification (03/22/2024)

28.1 Restrictions on $\mathrm{End}^0(A)$

Let A/k be simple of dimension g. With notation as in Albert's classification, write $e = [K : \mathbb{Q}], e_0 = [K_0 : \mathbb{Q}]$ (so that either $e = 2e_0$ or $e = e_0$), and $d = \sqrt{[D : K]}$ (always an integer). We will show that the types in Albert's classification impose various restrictions, listed in Figure 1. (We only consider the last column when $k = \overline{k}$.)

Type	e	d	char 0	char > 0	$\frac{\dim_{\mathbb{Q}} \mathrm{NS} \otimes_{\mathbb{Z}} \mathbb{Q}}{\dim_{\mathbb{Q}} \mathrm{End}(A)}$
I	e_0	1	$e \mid g$	$e \mid g$	1
II	e_0	2	$2e \mid g$	$2e \mid g$	3/4
III	e_0	2	$2e \mid g$	$e \mid g$	1/4
IV	$2e_0$	d	$e_0 d^2 \mid g$	$e_0 d \mid g$	1/2

Figure 1: Numerical restrictions on $\mathrm{End}^0(A)$

Remark 28.1. If $k = \overline{k}$, pick a polarization $\lambda : A \to A^\vee$. Then $\mathrm{NS}(A) \otimes \mathbb{Q}$ embeds into $\mathrm{Hom}(A, A^\vee) \otimes \mathbb{Q} \simeq \mathrm{End}^0(A)$—using λ to get this isomorphism—as the submodule of symmetric homomorphisms; see Remark 26.4.
Let $\lambda' \in \mathrm{NS}(A) \otimes \mathbb{Q} \hookrightarrow \mathrm{End}^0(A)$. Write $\lambda' = \lambda \circ f$ for some $f \in \mathrm{End}^0(A)$. Since $\lambda' : A \to A^\vee$ is symmetric, i.e. $(\lambda')^\vee = \lambda'$, we obtain $\lambda \circ f = f^\vee \circ \lambda$, i.e. $f = f^\dagger$ (taking the Rosati with respect to λ). This logic is reversible, so we identify $\mathrm{NS}(A) \otimes \mathbb{Q} = \mathrm{End}^0(A)^\dagger$ (submodule fixed by $\dagger$).

Remark 28.2. In general, we do not know whether all $(D, \dagger)$ with the dimension restrictions required by Figure 1 show up as the endomorphism algebra of some simple abelian variety. However, in characteristic 0, we do have a full answer: we always get every possibility of type I and II, and we get all possibilities for type III when $g/2e \geq 3$, and for type IV with $g/e_0 d^2 \geq 3$. For type III with $g/2e \leq 2$ or type IV with $g/e_0 d^2 \leq 2$, Shimura gives a more precise answer.

Recall that in characteristic 0, WLOG $k \subseteq \mathbb{C}$, we know $\mathrm{End}^0(A) \subseteq \mathrm{End}^0(A_{\mathbb{C}})$. Under this embedding, $\mathrm{End}^0(A)$ is a $\mathbb{Q}$-simple division algebra with $d^2 e \mid 2g$ that acts faithfully on the singular cohomology group $H^1_{\mathrm{sing}}(A(\mathbb{C}), \mathbb{Q}) \simeq \mathbb{Q}^{2g}$.

We deduce some of the restrictions in Figure 1 from the following three results.

Lemma 28.3. Let k be any field and let A/k be a simple abelian variety. Then, with notation as before, we have $de \mid 2g$.

Proof. Write $D = \mathrm{End}^0(A)$ with center K. Recall that the degree function $\deg : D \to \mathbb{Q}$ is a homogeneous polynomial function of degree $2g$, and it is a norm form. Any norm form on D is of the form $(\mathrm{Nm}_{K/\mathbb{Q}} \circ \mathrm{Nm}^0_{D/K})^m$ for some $m \in \mathbb{Z}_{\geq 0}$. The homogeneous form $\mathrm{Nm}^0_{D/K}$, which is descended from a determinant map on a d-dimensional vector space, has degree d,

and the form $\mathrm{Nm}_{K/\mathbb{Q}}$ has degree e, since the norm form on a degree e field extension always has homogeneous degree e. Hence $med = 2g$. ■

Proposition 28.4. Let L be a subfield of D fixed by Rosati. Then $[L : \mathbb{Q}] \mid g$. Hence, with notation as before, $e_0 \mid g$.

Proof. Let $L \subseteq \mathrm{NS}(A_{\overline{k}}) = \mathrm{End}^0(A_{\overline{k}})^\dagger$. Write the chosen polarization $\lambda : A \to A^\vee$ as $\lambda_{\overline{k}} = \phi_{\mathscr{L}}$ for a line bundle $\mathscr{L}/A_{\overline{k}}$. By Theorem 26.2, under this identification every element of $\mathrm{NS}(A_{\overline{k}})$ is of the form $\phi_{\mathscr{M}}$ for some line bundle $\mathscr{M}$, so it makes sense to define $f : \mathrm{NS}(A) \otimes \mathbb{Q} \to \mathbb{Q}$ by $\phi_{\mathscr{M}} \mapsto \frac{\chi(\mathscr{M})}{\chi(\mathscr{L})}$ (extend by $\mathbb{Q}$-linearity). Recall by Riemann-Roch that $\chi(\mathscr{M})^2/\chi(\mathscr{L})^2 = \frac{\deg(\phi_{\mathscr{M}})}{\deg(\phi_{\mathscr{L}})}$. Since χ is a homogeneous polynomial function of degree g, we deduce $f = \chi(\mathscr{M})/\chi(\mathscr{L})$ is a norm form. (The sign ambiguity is resolved by testing the case $\mathscr{M} = \mathscr{L}$.) Using the reduced norm form on $\mathscr{L}$ in $\mathrm{Nm}_{L/\mathbb{Q}}$, we have $[L : \mathbb{Q}] = g$. ■

Lemma 28.5. If $\mathrm{char}(k) = 0$ and A/k is simple, then $ed^2 \mid 2g$.

Proof. (Sketch.) By finite generation shenanigans and the fact that $\dim_{\mathbb{Q}} \mathrm{End}^0(X)$ divides $\dim_{\mathbb{Q}} \mathrm{End}^0(X/\overline{k})$, without loss of generality we may assume $k = \mathbb{C}$. Then $\mathrm{End}^0(A/\mathbb{C})$ acts on $H_1(X(\mathbb{C}), \mathbb{Q})$, and this action must be free since $\mathrm{End}^0(A/\mathbb{C})$ is a division algebra, so $\dim_{\mathbb{Q}} \mathrm{End}^0(A) = ed^2$ divides $\dim_{\mathbb{Q}} H_1(X(\mathbb{C}), \mathbb{Q}) = 2g$. ■

We assemble these results to get the divisibility requirements in Figure 1. First, we note that the last column of Figure 1 can be deduced by identifying $\mathrm{NS}(A) \otimes \mathbb{Q}$ with $\mathrm{End}^0(A)^\dagger$ and using the explicit descriptions of $\dagger$ on $D \otimes_{\mathbb{Q}} \mathbb{R}$ in Albert's classification.

- For type I, we have $e = e_0$, so Proposition 28.4 gives $e \mid g$.
- For type II and III, we again have $e = e_0$. In any case, Lemma 28.3 gives $2e \mid 2g$, hence $e \mid g$. In characteristic 0, we moreover get $ed^2 = 4e \mid 2g$ by Lemma 28.5, hence $2e \mid g$. Finally, to deduce $2e \mid g$ also in the type II case of positive characteristic, we have

$$\frac{\mathrm{NS}(A) \otimes \mathbb{Q}}{\dim_{\mathbb{Q}} \mathrm{End}^0(A)} = \frac{\dim_{\mathbb{Q}} \mathrm{End}^0(A)^\dagger}{\dim_{\mathbb{Q}} \mathrm{End}^0(A)} = \frac{3}{4}.$$

  Since $[D : K] = 4$, we conclude there exists $\alpha \in \mathrm{End}^0(A)^\dagger \setminus K$. For such α, the field $L := K(\alpha)$ satisfies the hypotheses in Proposition 28.4. Since by the tower law we must have $[L : K] = 2$, Proposition 28.4 gives $2e \mid g$.
- For type IV we have $e = 2e_0$, so in characteristic 0 Lemma 28.5 gives $2ed^2 \mid 2g$, hence $ed^2 \mid 2g$. In positive characteristic, we only get $2ed \mid 2g \implies ed \mid g$ by Lemma 28.3.

28.2 Examples in dimensions 1 and 2

Example 28.6. Let E be an elliptic curve. In characteristic 0, the endomorphism algebra of an elliptic curve is commutative, so the only possibilities are:

- Type I with $e = 1$ and $\mathrm{End}^0(E) = \mathbb{Q}$
- Type IV when E has complex multiplication, with $d = e_0 = 1$ and $\mathrm{End}^0(E)$ a quadratic imaginary field.

In positive characteristic:

- Type I cannot happen if E is defined over $\overline{\mathbb{F}}_p$ (equivalently, over a finite field), since we get a Frobenius morphism. But it can occur when E is defined over, say, $\mathbb{F}_p(t)$.
- If E is ordinary and defined over $\overline{\mathbb{F}}_p$, then it is type IV with $e_0 = d = 1$, since an appropriate power of the Frobenius morphism π does not lie in $\mathbb{Z} \subseteq \mathrm{End}^0(E)$.
- Type II never occurs, since we cannot have $2e \mid g$ if $g = 1$.
- Type III occurs with $e = e_0 = 1$ and $\mathrm{End}^0(E)$ a quaternion algebra ramified only at ∞ and p. This is the case of a supersingular curve (necessarily defined over $\mathbb{F}_{p^2}$). To see the ramification conditions, we have for $\ell \neq p$

  $$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell(A) \otimes \mathbb{Q}_\ell)$$

  is actually an isomorphism, since the left side has $\mathbb{Q}_\ell$-dimension 4 and the right side has $\mathbb{Q}_\ell$ dimension at most 4, hence exactly 4. This also implies that the Galois action is by scalars, since these are the only endomorphism that commute with everything. This gives $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}(T_\ell(A) \otimes \mathbb{Q}) = M_2(\mathbb{Q}_\ell)$. Since we are assuming that D is ramified at ∞, it must also be ramified at p, since the sum of the Hasse invariants must be 0 by the exact sequence of Brauer groups from class field theory.

Example 28.7. Let A/k be a simple abelian surface. In characteristic 0:

- Type I: Then either
  - $e = 1$ and $\mathrm{End}^0(A) = \mathbb{Q}$. In the moduli space of polarized abelian surfaces $\mathcal{A}_2$, this is the "open piece" away from a countable union of loci of dimension ≤ 2.
  - $e = 2$ and $\mathrm{End}^0(A)$ is a real quadratic field, and the moduli locus for a fixed order in a field has dimension 2.
- Type II: $e = 1$ and $\mathrm{End}^0(A)$ is a quaternion algebra split at ∞, with moduli locus of dimension 1.
- Type III would require $e = 1$, but this case never occurs by a result of Shimura.
- Type IV:
  - $e_0 = 2$: This is the case of CM abelian surfaces, where $\mathrm{End}^0(A)$ is a degree 4 CM field.
  - $e_0 = 1$: This case cannot occur if $k = \overline{k}$. If it did, then WLOG $k = \mathbb{C}$ and $\mathrm{End}^0(A)$ would contain a product of quadratic imaginary fields, which implies that $A = E^2$ for an elliptic curve E, contradicting simplicity. But it can occur for non-algebraically closed fields. For example, over $\mathbb{Q}$, we can take the Jacobian of $y^8 = x(x-1)$ modulo a copy of the Jacobian of $y^4 = x(x-1)$; this has an action by $\mathbb{Q}(\zeta_8)$.

Part III

The Main Theorem of Complex Multiplication

29 Néron models (04/01/2024)

Let R be a discrete valuation ring, e.g. $\mathbb{Z}_p$, let $K := \mathrm{Frac}(R)$, and let k be the residue field of R. Let A/K be an abelian variety.

Definition 29.1. A *Néron model* $\mathscr{A}$ of A over R is a smooth separated R-scheme of finite type such that:

1. $\mathscr{A}_K \simeq A$;
2. (*Néron mapping property*) For every smooth R-scheme $\mathscr{X}$ and a K-morphism $u_K : X := \mathscr{X}_K \to A$, there exists a unique map $u : \mathscr{X} \to \mathscr{A}$ extending u_K.

Remark 29.1. The Néron mapping property is a universal property, which implies that Néron models are unique up to unique isomorphism if they exist.

Remark 29.2. The formation of Néron models commutes with étale base change, i.e. if $\mathscr{A}$ is a Néron model of A and $\operatorname{Spec} R' \to \operatorname{Spec} R$ is an étale morphism of DVRs (e.g. an unramified extension of p-adic rings of integers), then $\mathscr{A}_{R'}$ is the Néron model of $A_{\operatorname{Frac}(R)}$. Unramifiedness is important for preserving smoothness.

Proposition 29.3. Let $\mathscr{A}/R$ be an abelian scheme. Then $\mathscr{A}$ is the Néron model of $A = \mathscr{A}_K$.

Proof. We need only verify the Néron mapping property. Let $\mathscr{X}$ be a smooth R-scheme with $X := \mathscr{X}_K$, and let $X \to A$ be a K-morphism. It suffices to demonstrate the Néron mapping property for a finite-type connected open subscheme of X, since then the uniqueness of the Néron mapping property and separatedness of $\mathscr{A}$ implies that the morphisms agree and glue, so we may assume $\mathscr{X}$ is finite type. Because everything is finite type, we may spread out to obtain an R-scheme $\mathscr{Y} \subseteq \mathscr{X}$ such that $\mathscr{Y}_K = X$ and $\mathscr{Y} \subseteq \mathscr{X}$ is open dense and such that there exists a unique morphism $\mathscr{Y} \to \mathscr{A}$ that base changes to $X \to A$.

We would like to extend the map $\mathscr{Y} \to \mathscr{A}$ to a rational map $\mathscr{X} \dashrightarrow \mathscr{A}$ defined in codimension 2. Let η be a generic point of $\mathscr{X}_k$ (which is possibly reducible). Then $\mathcal{O}_{\mathscr{X},\eta}$ is a DVR. Since $\mathscr{A} \to \operatorname{Spec} R$ is proper, by the valuative criterion applied to $\operatorname{Frac}(\mathcal{O}_{X,\eta}) \to A$, there exists a unique morphism $\operatorname{Spec} \mathcal{O}_{\mathscr{X},\eta} \to \mathscr{A}$. This glues with our previously defined morphism $\mathscr{Y} \to \mathscr{A}$ to yield a rational map $\mathscr{X} \dashrightarrow \mathscr{A}$ defined in codimension 2.

Theorem 29.4. (Weil, [BLR90, §4.4., Thm. 1], [Mil10, Lem. 6.5]) Let R be a DVR, let G be a smooth separated R-group scheme, and let Z be a smooth R-scheme with a rational map $f : Z \dashrightarrow G$ defined in codimension 1 (i.e. the locus where f is not defined has codimension at least 2). Then $f : Z \to G$ is actually defined everywhere.

Proof. (Sketch.) Consider $F : Z \times_R Z \dashrightarrow G : (x, y) \mapsto f(x)f(y)^{-1}$. The f being defined at a point x is equivalent to F being defined at (x, x)—the reverse implication holds because if F is defined on (x, U), then there exists $U_0 \subseteq U$ such that f is defined on U_0, so that we may set $f(x) = F(x, y)f(y)$ for any $u \in U_0$.

Theorem 29.5. *(Algebraic Hartog Theorem.)* If $\operatorname{Spec} A$ is a normal scheme, then $A = \bigcap_{\mathfrak{p} \text{ ht. } 1} A_{\mathfrak{p}}$, where the intersection is taken inside $\operatorname{Frac}(A)$ over all height 1 prime ideals of A.

We have F is defined at (x, x) if $\mathcal{O}_{G,e} \to K(Z \times Z)$ factors through $\mathcal{O}_{Z\times Z,(x,x)}$. This gives the theorem because F is defined on codimension 1. ∎

From Weil's theorem, we conclude that $\mathscr{X} \dashrightarrow \mathscr{A}$ extends uniquely to a map $\mathscr{X} \to \mathscr{A}$. ∎

Corollary 29.6. Let $\mathscr{A}, \mathscr{B}$ be abelian schemes over R, with $A := \mathscr{A}_K, B := \mathscr{B}_K$. Then $\mathrm{Hom}_{\text{R-gp}}(\mathscr{A}, \mathscr{B}) \simeq \mathrm{Hom}(A, B)$ via $f \mapsto f_K$.

Proof. Since $\mathscr{B}$ is the Néron model of B and $\mathscr{A}$ is smooth, the Néron mapping property supplies a unique extension $F : \mathscr{A} \to \mathscr{B}$ to any homomorphism $f : A \to B$. To see that this is again a homomorphism, we again apply the Néron mapping property to the morphism $A \times A \to B : (a_1, a_2) \mapsto f(a_1 + a_2) - f(a_1) - f(a_2)$, which simultaneously lifts uniquely to the trivial map $\mathscr{A} \times \mathscr{A} \to \mathscr{B}$ but also to $F(x_1 + x_2) - F(x_1) - F(x_2)$. ■

Theorem 29.7. [BLR90, §1.3, Thm. 1+§1.2 Prop. 6] Any abelian variety A/K admits a Néron model $\mathscr{A}$. Moreover, $\mathscr{A}$ is a smooth R-group scheme, and ([BLR90, §7.4, Thm. 1]) there exists a finite extension L/K such that the Néron model of A_L has semiabelian neutral component (an extension of an abelian variety by copies of $\mathbb{G}_m$).

30 Proof of the Shimura-Taniyama formula (04/03/2024)

We began this at the end of lecture on 4/01, but most of the proof was done today.

Theorem 30.1. Let K be a number field, and let A/K be a CMAV with CM by (E, Φ). Let $\mathfrak{p}$ be a prime of K and let $k = \mathcal{O}_K/\mathfrak{P}$. Assume that:

- K contains the Galois closure of E
- $\mathfrak{P}$ is a prime of good reduction for A, i.e. the Néron model $\mathscr{A}/\mathcal{O}_{K_\mathfrak{P}}$ is an abelian scheme.[a]
- $K_\mathfrak{P}/\mathbb{Q}_p$ is unramified, so that $\mathrm{End}(A) \cap E = \mathcal{O}_E$.

Recall the Frobenius map[b] $\mathrm{Frob} : \mathscr{A}_k \to \mathscr{A}_k$ sending a function $f \mapsto f^q$, where $q = \#k$. Then:

1. There exists $\pi \in \mathcal{O}_E$ such that $\mathrm{Frob} = \pi$, i.e. under the embedding $\mathcal{O}_E \subseteq \mathrm{End}(A) \simeq \mathrm{End}(\mathscr{A}) \hookrightarrow \mathrm{End}(\mathscr{A}_k)$.
2. For a place $v \mid p$ of E and a fixed algebraic closure $\mathbb{Q}_p$, write $H_v = \mathrm{Hom}(E_v, \overline{\mathbb{Q}}_p)$, so that $\mathrm{Hom}(E, \overline{\mathbb{Q}}_p) = \coprod_{v|p} H_v$. A fixed embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ induces a bijection $\mathrm{Hom}(E, \overline{\mathbb{Q}}_p) = \mathrm{Hom}(E, \mathbb{C})$, yielding an identification $\mathrm{Hom}(E, \mathbb{C}) = \coprod H_v$. Therefore it makes sense to define $\Phi_v := \Phi \cap H_v \subseteq \mathrm{Hom}(E, \mathbb{C})$.

   Then with π as in part (1), we have

$$(\pi) = \prod_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)} \mathfrak{P})$$

   where ord_v is the normalized discrete valuation on E_v.

[a] We know a Néron model always exists. We showed previously that if $\mathscr{A}/R$ is an abelian scheme, then it is the Néron model of A/K, but the converse does not hold: it is possible for the Néron model of A/K to fail to be an abelian scheme, and this is what bad reduction captures.

[b] This is simultaneously the absolute and relative Frobenius.

We will soon see that CMAVs have everywhere potentially good reduction. We may always pass to a finite extension K'/K that yields good reduction, so the restrictions imposed in our version of the formula are easily sidestepped.

Proof. For (1), we show that the reduction map $\mathrm{End}(\mathscr{A}) \to \mathrm{End}(\mathscr{A}_k)$ is injective.

Lemma 30.2. For $(m, p) = 1$, we have $A(\overline{K})[m] = A(K_\mathfrak{P}^{\mathrm{ur}})[m] = \mathscr{A}_k(\overline{k})[m]$. In particular, the reduction map induces a natural isomorphism $T_\ell(A) \simeq T_\ell(\mathscr{A}_k)$ when $\ell \neq p$, and this identification is compatible with the Galois action of the decomposition group $D_\mathfrak{P}$ of $\mathfrak{P}$. Here, we identify $D_\mathfrak{P}/I_\mathfrak{P} \subseteq \mathrm{Gal}(\overline{k}/k)$, where $I_\mathfrak{P}$ is the inertia subgroup, noting that the action of $D_\mathfrak{P}/I_\mathfrak{P}$ on $T_\ell(A)$ is well-defined because the ℓ^∞-torsion subgroups are defined over K^{ur}.

Proof. By the Néron mapping property, $A(K_\mathfrak{P}^{\mathrm{ur}}) = \mathscr{A}(\mathcal{O}_{K_\mathfrak{P}^{\mathrm{ur}}})$, and we have a reduction map

$\mathscr{A}(\mathcal{O}_{K^{\mathrm{ur}}_{\mathfrak{P}}}) \to \mathscr{A}_k(\overline{k})$. The map $A(K^{\mathrm{ur}}_{\mathfrak{P}}) \to \mathscr{A}_k(\overline{k})[m]$ is bijective by Hensel's lemma and the fact that $[m]$ is étale on $\mathscr{A}$ (since $[m]$ is given by multiplication by m on the Lie algebra).

Therefore, we have $\#A(K^{\mathrm{ur}}_{\mathfrak{P}})[m] = \mathscr{A}_k(\overline{k})[m] = m^{2\dim A} = \#A(\overline{K})[m]$, so all of the m-torsion points are unramified. ∎

Corollary 30.3. If A/K has good reduction at $\mathfrak{P}$, then $\mathrm{End}(A) = \mathrm{End}(\mathscr{A}) \to \mathrm{End}(\mathscr{A}_k)$ is injective.

Proof. If an endomorphism φ on $\mathrm{End}(\mathscr{A})$ has image contained in the kernel of the reduction map $\mathscr{A} \to \mathscr{A}_k$, then by Lemma 30.2 the image of φ has trivial intersection with $\mathscr{A}(\overline{K})[m]$ when $(m, p) = 1$. This means that φ kills the Tate module $T_\ell(\mathscr{A})$ for $\ell \neq p$, hence the corresponding endomorphism of A also kills $T_\ell(A)$. But we already know that the map $T_\ell : \mathrm{End}(A) \to \mathrm{End}(T_\ell(A))$ is injective from Theorem 24.1. ∎

We prove (1) in Theorem 30.1. We have $\mathrm{End}(A) = \mathrm{End}(\mathscr{A}) \hookrightarrow \mathrm{End}(\mathscr{A}_k)$, so we obtain an embedding $E \subseteq \mathrm{End}^0(\mathscr{A}_k)$ and

$$E \otimes \mathbb{Q}_\ell \subseteq \mathrm{End}^0(\mathscr{A}_k) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell(\mathscr{A}_k) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell).$$

$T_\ell(\mathscr{A}_k) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has $\mathbb{Q}_\ell$-dimension $2\dim A$, but $E \otimes \mathbb{Q}_\ell$ is also a $\mathbb{Q}_\ell$-algebra of $\mathbb{Q}_\ell$-dimension $2\dim A$. We conclude $T_\ell(\mathscr{A}_k) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell =: V_\ell(\mathscr{A}_k)$ is a free rank 1 $E \otimes \mathbb{Q}_\ell$-module. Hence Frobenius is an $E \otimes \mathbb{Q}_\ell$-linear endomorphism on a free rank 1 $E \otimes \mathbb{Q}_\ell$-module, so it must be scalar multiplication by some element of $E \otimes \mathbb{Q}_\ell$. Frobenius also lies in $\mathrm{End}(\mathscr{A}_k)$, so it must lie in $(E \otimes \mathbb{Q}_\ell) \cap \mathrm{End}(\mathscr{A}_k) \subseteq \mathcal{O}_E$. Therefore we may identify it with some $\pi \in \mathcal{O}_E$.

For part (2), since $[q]$ factors through Frobenius on $\mathscr{A}_k$ (see Proposition 30.6), we may write $(\pi) = \prod_{v|p} \mathfrak{p}_v^{m_v}$ as a product of prime ideals dividing p. Let $h = \#\mathrm{Cl}(E)$ be the class number, so that $\mathfrak{p}_v^{m_v h}$ is always principal, say equal to the ideal (γ_v) with $\gamma_v \in \mathcal{O}_E$. Consider $\gamma_v : \mathscr{A}_k \to \mathscr{A}_k$, using $\mathcal{O}_E \hookrightarrow E \hookrightarrow \mathrm{End}(\mathscr{A}_k)$. We want to compute $\deg \gamma_v$.

Lemma 30.4. For all $\alpha \in \mathcal{O}_E$, the morphism $\alpha : \mathscr{A}_k \to \mathscr{A}_k$ has degree $\mathrm{Nm}_{E/\mathbb{Q}}(\alpha)$.

Proof. Consider α acting on $V_\ell(\mathscr{A}_k) \simeq E \otimes \mathbb{Q}_\ell$. Then $\deg \alpha = \det(\alpha|_{V_\ell(\mathscr{A}_k)}) = \mathrm{Nm}_{E/\mathbb{Q}}(\alpha)$. Here, we use that the determinant of multiplication by α on the field extension E, treated as a $\mathbb{Q}$-linear endomorphism, is by definition the norm of α. ∎

By the lemma, we conclude that $\deg \gamma_v = \mathrm{Nm}_{E/Q}\, \mathfrak{p}_v^{m_v h}$, since the ideal norm is compatible with the field norm.

Lemma 30.5. Let $k = \overline{k}$ have characteristic p, let $q = p^m$, and let $f : A \to B$ be an isogeny of AVs over k such that $\alpha^*(k(B)) \supset k(A)^q$ (fields of fractions). Then $\deg f \leq q^d$, where $d = \dim \ker(f : \mathrm{Lie}\, A \to \mathrm{Lie}\, B)$.

Proof. Sketch; see also [Mil15, Thm. 11.29] and [Mil10, §7]. The proof idea is that $\ker f$ is a local finite group scheme over k. Such a scheme always has coordinate ring of the form $k[x_1, \ldots, x_n]/(x_1^{p^{r_1}}, \ldots, x_n^{p^{r_n}})$ with $r_i \leq m$ (we saw something similar in the height 1 case in

Lemma 22.4; the general case follows by induction). Then $\deg(f) = \prod_{i=1}^{n} p^{r_i} \leq p^{mn} = q^n$ for $n = \dim\ker(T_\ell f) = \dim\ker(\alpha : \operatorname{Lie} A \to \operatorname{Lie} B) = d$. ■

By what we know from the analytic setting, $\operatorname{Lie} A$ admits a K-basis $(e_\varphi)_{\varphi\in\Phi}$ such that any $a \in E$ act by $a\cdot(e_\varphi)_{\varphi\in\Phi} = (\varphi(a)e_\varphi)_{\varphi\in\Phi}$. Since $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified, $\operatorname{Lie}\mathscr{A}$ also admits such an $\mathcal{O}_{K_{\mathfrak{P}}}$-basis $(e_\varphi)_{\varphi\in\Phi}$, since unramifiedness gives

$$\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{K_{\mathfrak{P}}} = \bigoplus_{\sigma: E\hookrightarrow K_{\mathfrak{P}}} \mathcal{O}_{K_{\mathfrak{P}}},$$

hence $\operatorname{Lie}\mathscr{A}_k = \operatorname{Lie}\mathscr{A}_{\mathcal{O}_{K_{\mathfrak{P}}}} \otimes k$ has k-basis $(\overline{e}_\varphi)_{\varphi\in\Phi}$ and

$$\ker(\gamma_v : \operatorname{Lie}\mathscr{A}_k \to \operatorname{Lie}\mathscr{A}_k) = \operatorname{Span}\{\overline{e}_\varphi : \varphi(\gamma_v) \in \mathfrak{P}\}.$$

We have assumed that K contains all Galois conjugates of E, so choices of embeddings $K_{\mathfrak{P}} \hookrightarrow \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ identify $\operatorname{Hom}(E,K) = \operatorname{Hom}(E,\overline{\mathbb{Q}}_p) = \operatorname{Hom}(E,\mathbb{C})$. Under this identification, we get

$$\begin{aligned} H_v &= \operatorname{Hom}(E_v,\overline{\mathbb{Q}}_p) = \operatorname{Hom}(E_v,K_{\mathfrak{P}}) = \{\tau \in \operatorname{Hom}(E,K) \mid \tau^{-1}(\mathfrak{P}) = \mathfrak{p}_v\} \\ \Phi_v &= \Phi \cap H_v = \{\varphi \in \Phi \mid \varphi^{-1}(\mathfrak{P}) = \mathfrak{p}_v\}, \end{aligned}$$

where $\mathfrak{p}_v$ denotes the prime of $\mathcal{O}_E$ associated to the finite place v. We claim that $\overline{e}_\varphi \in \ker(\gamma_v)$ if and only if $\varphi \in \Phi_v$. The element $\gamma_v \in \mathcal{O}_E$ lies in $\mathfrak{p}_v$, but it cannot lie in any other $\mathfrak{p}_{v'}$, since that would imply $\mathfrak{p}_v^{hm_v} \subseteq \mathfrak{p}_{v'}$, contradicting unique factorization. Hence, $\gamma_v \in \varphi^{-1}(\mathfrak{P})$ means that $\varphi^{-1}(\mathfrak{P}) = \mathfrak{p}_v$—this preimage must be one of the $\mathfrak{p}_{v'}$, and the presence of γ_v rules out all the other possibilities. By our identification of Φ_v, this gives $\overline{e}_\varphi \in \ker(\gamma_v)$ if and only if $\varphi \in \Phi_v$. Hence $\dim\ker(\gamma_v|_{\operatorname{Lie}\mathscr{A}_k}) = |\Phi_v|$, and this is the critical observation that lets us access the numerator in the Shimura-Taniyama formula.

We apply Lemma 30.5 to γ_v. By construction, the q^h-th power Frobenius π_A^h factors through γ_v, i.e. $\pi_A^h = a \circ \gamma_v$ as endomorphisms of $\mathscr{A}_k$ for some other $a \in \mathcal{O}_E$. Since $(\pi_A^h)^*(k(\mathscr{A}_k)) = k(\mathscr{A}_k)^{q^h}$, essentially by the definition of Frobenius, we conclude that $\gamma_v^*(k(\mathscr{A}_k)) \supseteq k(\mathscr{A}_k)^{q^h}$. Therefore Lemma 30.5 yields $\deg(\gamma_v) \leq q^{h\cdot|\Phi_v|}$. Taking h-th roots,

$$\operatorname{Nm}_{E/\mathbb{Q}} \mathfrak{p}_v^{m_v} \leq q^{|\Phi_v|}$$

for all $v \mid p$. We wish to show that this is an equality. The degree of Frobenius is

$$\deg(\mathrm{Frob}) = \operatorname{Nm}_{E/\mathbb{Q}}(\pi) = \operatorname{Nm}_{E/\mathbb{Q}}\left(\prod_{v|p} \mathfrak{p}_v^{m_v}\right) \leq \prod_{v|p} q^{|\Phi_v|} = q^{|\Phi|} = q^{\dim A},$$

noting that $\coprod \Phi_v = \Phi$. But we also know *a priori* that Frobenius has degree at least $q^{\dim A}$ by considering its effect on a transcendence basis of $k(\mathscr{A}_k)$, so the above inequality must actually be an equality. We conclude

$$\operatorname{Nm}_{E/\mathbb{Q}} \mathfrak{p}_v^{m_v} = q^{|\Phi_v|} = (\operatorname{Nm}_{K/\mathbb{Q}} \mathfrak{P})^{|\Phi_v|},$$

which equals

$$\mathrm{Nm}_{E/\mathbb{Q}}\left(\prod_{\varphi\in\Phi_v}\varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)}\,\mathfrak{P})\right)=\prod_{\varphi\in\Phi}(\mathrm{Nm}_{K/\mathbb{Q}}\,\mathfrak{P})$$

so in fact $\mathfrak{p}_v^{m_v}=\prod_{\varphi\in\Phi_v}\varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)}\,\mathfrak{P})$. Then finally (2) follows by taking $\prod_{v|p}$. ■

Proposition 30.6. $\mathrm{Frob}\circ\mathrm{Frob}^\dagger=\mathrm{Frob}^\dagger\circ\mathrm{Frob}=[q]$.

Proof. Let $\lambda:A\to A^\vee$ be a polarization defined over $\mathbb{F}_q$ inducing a Rosati involution $\dagger$. Then

$$\mathrm{Frob}_A^\dagger\circ\mathrm{Frob}_A=\lambda^{-1}\circ\mathrm{Frob}_A^\vee\circ\lambda\circ\mathrm{Frob}_A=\lambda^{-1}\circ\mathrm{Frob}_A^\vee\circ\mathrm{Frob}_{A^\vee}\circ\lambda,$$

noting that λ is Frobenius-equivariant. So it is equivalent to show that $\mathrm{Frob}_A^\vee\circ\mathrm{Frob}_{A^\vee}=[q]_{A^\vee}$.

We will show this equality on the functor of points. Let T be a scheme and $\mathscr{L}$ a line bundle on $A\times T$ such that $[L]\in A^\vee$. Write $q=p^m$. Then

$$\mathrm{Frob}_{A^\vee}([\mathscr{L}])=[(\mathbf{id}\times F_T^{(m)})^*\mathscr{L}]$$

so

$$\begin{aligned}\mathrm{Frob}_A^\vee\circ\mathrm{Frob}_{A^\vee}([\mathscr{L}])&=[(\mathrm{Frob}_A\times\mathbf{id})^*\circ(\mathbf{id}\times F_T^{(m)})^*\mathscr{L}]\\&=[(\mathrm{Frob}_A\times F_T^{(m)})^*\mathscr{L}].\end{aligned}$$

We claim that this is $[\mathscr{L}^{\otimes q}]$.

The endomorphism $\mathrm{Frob}_A\times F_T^{(m)}$ on $A\times T$ is its q-th power (absolute and relative) Frobenius endomorphism over k. In general, a line bundle $\mathscr{L}$ on a scheme X is defined by a collection of trivializing charts U_i and cocycles φ_{ij} describing the transition functions between charts. If $f:Y\to X$ is a morphism, the line bundle $f^*\mathscr{L}$ is the line bundle on Y with trivializing charts $f^{-1}(U_i)$ and cocycles $f^*(\varphi_{ij})$. In the case where f is the Frobenius morphism $F_X^{(m)}$, we have $F_X^{(m),*}(\sigma_{ij})=\sigma_{ij}^q$. After all, cocycles are just sections of the structure sheaf, and Frobenius sends a section to its q-th power. The cocycles σ_{ij}^q are precisely the cocycles of the line bundle $\mathscr{L}^{\otimes q}$, essentially by the definition of the tensor product. Hence, we conclude $[(\mathrm{Frob}_A\times F_T^{(m)})^*\mathscr{L}]=[\mathscr{L}^{\otimes q}]$. This means that $\mathrm{Frob}_A^\vee\circ\mathrm{Frob}_{A^\vee}$ acts by multiplication by q in the group law on the functor of points, hence it also acts so as a morphism on $A^\vee$ by the Yoneda lemma. ■

31 Main Theorem of Complex Multiplication (04/05/2024)

31.1 Reflex norm

Let (E,Φ) be a CM type (E not necessarily a field). We let E^* denote the reflex field, which is always a CM field. We will think of $\Phi\subseteq\mathrm{Hom}(E,\overline{\mathbb{Q}})$—recall that we have shown that all CMAVs are already defined over $\overline{\mathbb{Q}}$. Let K be a field containing all images of $E\hookrightarrow\overline{\mathbb{Q}}$, so

that $E^* \subseteq K$ by Lemma 7.4; if E is a field, then we may take K to be the Galois closure of E in $\overline{\mathbb{Q}}$. Then we may write $E \otimes_{\mathbb{Q}} K \simeq \prod_{\sigma \in \mathrm{Hom}(E,K)} K_\sigma$. By Galois descent for vector spaces, there exists a unique $E \otimes_{\mathbb{Q}} E^*$-module V_Φ such that $V_\Phi \otimes_{E^*} K \simeq \prod_{\varphi \in \Phi} K_\varphi$.

Definition 31.1. The *reflex norm* $N_\Phi : (E^*)^\times \to E^\times$ is defined by $a \mapsto \det(a|_{V_\Phi})$, viewing V_Φ as a free E-module and $a|_{V_\Phi}$ as a linear transformation on this space.

More generally, for any $K \supseteq E^*$, we have $N_{K,\Phi} : K^\times \to E^\times$ via $a \mapsto \det(a|_{V_\Phi \otimes_{E^*} K})$, and we have the compatibility $N_{K,\Phi} = N_\Phi \circ \mathrm{Nm}_{K/E^*}$.

Proposition 31.1. If K contains all images of homomorphisms $E \to \overline{\mathbb{Q}}$, then for all $a \in K^\times$, we have $N_{K,\Phi}(a) = \prod_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)}\, a)$.

Proof. See [Mil10, Prop. 1.26]. ∎

Remark 31.2. Proposition 31.1 gives a more concrete way to think about the reflex norm. It is similar to the usual norm map, except that instead of taking into account *all* embeddings, it only uses the embeddings from the CM type Φ, giving us only one half of the usual norm.

Corollary 31.3. For any $a \in E^*$, $N_\Phi(a)\overline{N_\Phi(a)} = \mathrm{Nm}_{E^*/\mathbb{Q}}(a)$. In particular, this element lies in $\mathbb{Q}$. (Here the notation of complex conjugation is unambiguous since $E \ni N_\Phi(a)$ is CM.)

Proof. Norms are transitive, so $\mathrm{Nm}_{E^*/\mathbb{Q}}(a) = \mathrm{Nm}_{E/\mathbb{Q}}(\mathrm{Nm}_{E^*/E}(a))$. We may expand this as

$$\begin{aligned}
\mathrm{Nm}_{E^*/\mathbb{Q}}(a) &= \prod_{\varphi \in \mathrm{Hom}(E,\mathbb{C})} \varphi^{-1}(\mathrm{Nm}_{E^*/\varphi(E)}(a)) \\
&= \prod_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{E^*/\varphi(E)}(a)) \prod_{\varphi \in \overline{\Phi}} \varphi^{-1}(\mathrm{Nm}_{E^*/\varphi(E)}(a)) \\
&= N_\Phi(a)\overline{N_\Phi(a)}
\end{aligned}$$

since $\mathrm{Hom}(E, \mathbb{C}) = \Phi \coprod \overline{\Phi}$. ∎

By tensoring N_Φ and $N_{K,\Phi}$ with $\mathbb{Q}_\ell$ and $\mathbb{R}$, we get an induced map on idèles

$$N_{K,\Phi} : \mathbb{A}_K^\times \to \mathbb{A}_E^\times,$$

which also induces a similar map on fractional ideals.

31.2 Statement of the Main Theorem

Now let $A/\overline{\mathbb{Q}}$ be a CMAV with CM by (E, Φ) and reflex field E^*. Consider $\sigma \in \mathrm{Gal}(\overline{E^*}/E^*)$. Let ${}^\sigma A := A \times_{\mathrm{Spec}\,\overline{\mathbb{Q}}, \sigma} \mathrm{Spec}\,\overline{\mathbb{Q}}$, which is again a CMAV with CM by $\sigma\Phi = \Phi$ since σ fixes E^*. (Recall that the reflex field is precisely the fixed field of all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma\Phi = \Phi$.) We have a map $x \mapsto \sigma(x)$ giving an isomorphism $\sigma : A \to {}^\sigma A$ compatible with

the E-action. Since we have two CMAVs with the same CM type, by our classification of CMAVs (Proposition 4.2) there exists an isogeny $\alpha : A \to {}^{\sigma}A$ compatible with the E-action that is unique up to multiplication by $E^{\times}$.

The content of the main theorem of complex multiplication is to compare the the two maps $\sigma : A \to {}^{\sigma}A$ and $\alpha : A \to {}^{\sigma}A$. The first of these maps arises arithmetically, from the Galois action, and the latter arises geometrically, from an isogeny of abelian varieties.

To make our comparison, we "adèlicize" the Tate module: write $\hat{T}(A) := \prod_{\ell} T_{\ell}(A)$ and $\hat{V}(A) = \hat{T}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then the two maps $\sigma, \alpha : A \to {}^{\sigma}A$ induce maps $\sigma, \alpha : \hat{V}(A) \to \hat{V}({}^{\sigma}A)$, which are both $E \otimes \mathbb{A}_f = \mathbb{A}_{E,f}$-linear, where $\mathbb{A}_f = \prod_p \mathbb{Z}_p$ denotes the finite adèles over $\mathbb{Q}$ and $\mathbb{A}_{E,f}$ denotes the finite adèles over E. We have seen previously that each $V_{\ell}(A)$ is a rank 1 free $E \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$-module, and from this it follows that $\hat{V}(A)$ and $\hat{V}({}^{\sigma}A)$ are rank 1 free $\mathbb{A}_{E,f}$-modules. Therefore there exists some $\eta(\sigma) \in \mathbb{A}_{E,f}^{\times}$ such that $\alpha(\eta(\sigma)x) = \sigma(x)$ for all $x \in \hat{V}(A)$, yielding a well-defined group homomorphism $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) \to \mathbb{A}_{E,f}^{\times}/E^{\times}$, necessarily factoring through $\mathrm{Gal}(E^{*,\mathrm{ab}}/E^*)$ since the image is abelian. (This homomorphism is only well-defined as a homomorphism to the quotient $\mathbb{A}_{E,f}^{\times}/E^{\times}$, rather than $\mathbb{A}_{E,f}^{\times}$, because α itself is only well-defined up to a multiple in $E^{\times}$.)

From global class field theory, we have the global Artin map

$$\mathbb{A}_{E^*,f}/(E^*)^{\times} \to \mathrm{Gal}(E^{\mathrm{ab}}/E^*),$$

and we claim that the map $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) \to \mathbb{A}_{E,f}^{\times}/E^{\times}$ we have just defined corresponds to the reflex norm

$$N_{\Phi} : \mathbb{A}_{E^*,f}^{\times}/(E^*)^{\times} \to \mathbb{A}_{E,f}^{\times}/E^{\times},$$

in the sense that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) & \xrightarrow{\eta} & \mathbb{A}_{E,f}^{\times}/E^{\times} \\ \downarrow & \nearrow & \uparrow{\scriptstyle N_{\Phi}} \\ \mathrm{Gal}(E^{*,\mathrm{ab}}/E^*) & \xleftarrow[\mathrm{Art}]{} & \mathbb{A}_{E^*,f}^{\times}/(E^*)^{\times} \end{array}$$

Commutativity of this diagram is the **Main Theorem of Complex Multiplication**.

Theorem 31.4. *(Shimura-Taniyama Main Theorem of Complex Multiplication.)* The well-defined map η is given by $\eta(\sigma) = N_{\Phi}(s)$, where $s \in \mathbb{A}_{E^*,f}^{\times}/(E^*)^{\times}$ is such that $\mathrm{Art}_{E^*}(s) = \sigma|_{E^{*,\mathrm{ab}}}$.
Equivalently, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$, and any $s \in \mathbb{A}_{f,E^*}^{\times}$ with $\mathrm{Art}(s) = \sigma|_{E^{*,\mathrm{ab}}}$, there exist a unique E-isogeny $\alpha : A \to \sigma A$ such that $\alpha(N_{\Phi}(s) \cdot x) = \sigma(x)$ for all $x \in \hat{V}(A)$.

Remark 31.5. Such an s always exists. In contrast to the global function field case, the Artin map for number fields $\mathrm{Art}_K : \mathbb{A}_K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is always surjective. Its kernel contains $K^\times \cdot \prod_{v|\infty} K_v^+$, where v ranges over the infinite places and K_v^+ denotes the connected component of $K_v^\times$ containing 1. The field E^* is CM, so it has no real places and the the Artin map kills all of the infinite places in $\mathbb{A}_{E^*}$. Therefore it descends to a surjective homomorphism $\mathbb{A}_{E^*,f}^\times/(E^*)^\times \to \mathrm{Gal}(E^{*,\mathrm{ab}}, E^*)$.
In the second statement of 31.4, the isogeny α depends on the exact choice of $s \in \mathbb{A}_{E^*,f}^\times$.

Remark 31.6. Let $\lambda : A \to A^\vee$ be a polarization that is compatible with the E-action in the sense that the associated Rosati involution $\dagger$ induces complex conjugation on E. Using the Weil pairing/Riemann form and this polarization, we have a symplectic map $\psi : \hat{V}(A) \times \hat{V}(A) \to \mathbb{A}_f(1)$ obtained by amalgamating all of the Weil pairings $T_\ell(A) \times T_\ell(A^\vee) \to \mathbb{Z}_\ell(1)$. This pairing is $\mathbb{A}_f$-bilinear, and the Rosati involution again acts as an adjoint for the pairing.

We state one consequence of the main theorem. We choose α so that $\alpha(\eta(\sigma)x) = \sigma(x)$ exactly, i.e. adjusting α by a constant in $E^\times$ so that these two things agree exactly, not just up to $E^\times$. Define another pairing

$$\begin{aligned} {}^\sigma\psi : \hat{V}({}^\sigma A) \times \hat{V}({}^\sigma A) &\to \mathbb{A}_f(1) \\ (x, y) &\mapsto \sigma\psi(\sigma^{-1}, \sigma^{-1}y). \end{aligned}$$

Equivalently, since σ acts on the target of the Weil pairing by the cyclotomic character χ, we write

$${}^\sigma\psi(\sigma x, \sigma y) = \chi(\sigma) \cdot \psi(\sigma x, \sigma y).$$

The main theorem lets us substitute: if $\mathrm{Art}_K(s) = \sigma$, then

$$\begin{aligned} {}^\sigma\psi(\sigma x, \sigma y) &= {}^\sigma\psi(\alpha(N_\Phi(s)x), \alpha(N_\Phi(s)y)) \\ &= {}^\sigma\psi(N_\Phi(s)\overline{N_\Phi(s)}\alpha(x), \alpha(y)) \\ &= {}^\sigma\psi(\mathrm{Nm}_{E^*/\mathbb{Q}}(s)\alpha(x), \alpha(y)) \\ &= \mathrm{Nm}_{E^*/\mathbb{Q}}(s) \cdot {}^\sigma\psi(\alpha(x), \alpha(y)). \end{aligned}$$

Here we use Corollary 31.3 to get $N_\Phi(s)\overline{N_\Phi(s)} = \mathrm{Nm}_{E/\mathbb{Q}}(s)$—since this lies in $\mathbb{A}_f^\times$, we may use the $\mathbb{A}_f$-bilinearity of the Weil pairing. We conclude that $\psi(x, y)$ and ${}^\sigma\psi(\alpha(x), \alpha(y))$ differ by the factor $c := \frac{\chi(\sigma)}{N_{E^*/\mathbb{Q}}(s)}$:

$$\frac{\chi(\sigma)}{N_{E^*/\mathbb{Q}}(s)}\psi(x, y) = {}^\sigma\psi(\alpha(x), \alpha(y))$$

It turns out that the ratio c lies in $\mathbb{Q}_{>0}^\times$. The kernel of the Artin map $\mathrm{Art} : \mathbb{A}_f^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is $\mathbb{Q}_{>0}$, since the kernel of "full" Artin map $\mathbb{A}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ (including the real place) is the closure of $\mathbb{Q}^\times \cdot \mathbb{R}_{>0}$. By class field theory, $\mathrm{Art}(\mathrm{Nm}_{E/\mathbb{Q}}(s)) = \sigma|_{\mathbb{Q}^{\mathrm{ab}}}$—this follows from functoriality of the Artin map, which is commutativity of the diagram

$$\begin{array}{ccc} \mathbb{A}_{E^*}^\times/(E^*)^\times & \xrightarrow{\mathrm{Art}_{E^*}} & \mathrm{Gal}((E^*)^{\mathrm{ab}}/E^*) \\ \downarrow{\scriptstyle \mathrm{Nm}_{E^*/\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbb{A}^\times/\mathbb{Q}^\times & \xrightarrow{\mathrm{Art}_{\mathbb{Q}}} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}). \end{array}$$

Another property of $\mathrm{Art} : \mathbb{A}_f^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is that it sends $\chi(\sigma)$, treated as an element of $\widehat{\mathbb{Z}} \subseteq \mathbb{A}_f^\times$, to $\sigma|_{\mathbb{Q}^{\mathrm{ab}}}$. Therefore, since $\chi(\sigma)$ and $\mathrm{Nm}_{E^*/\mathbb{Q}}(s)$ map to the same element under the Artin map, they must differ by a factor in $\mathbb{Q}_{>0}^\times$. See also [Mil10, Rmk. 9.11].

We will postpone the proof of the main theorem until the end of the semester. Before doing this, we will discuss another important application of the main theorem. Whereas much is unknown about L-functions of general abelian varieties, the main theorem lets us say quite a lot about L-functions of CMAVs. In particular, we get the existence of an analytic continuation and functional equation by expressing this L-function as a product of Hecke L-functions; see Theorem 33.5.

31.3 Review of the Artin map

See [Ked21, §6.4] or [Mil20, §I.1, §V.5] for more on the statements of class field theory.

Let K be a number field with maximal abelian extension K^{ab}. There exists a map $\mathrm{Art} : \mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ known as the *Artin map* which is a continuous homomorphism such that, for all finite abelian extensions L/K and all places v of K, the following diagram commutes:

$$\begin{array}{ccccc} K_v & & \xrightarrow{\quad\mathrm{Art}_{L_w/K_v}\quad} & & \mathrm{Gal}(L_w/K_v) \\ \big\downarrow & & & & \big\downarrow \\ \mathbb{A}^\times/K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \twoheadrightarrow & \mathrm{Gal}(L/K), \end{array}$$

where Art_{L_w/K_v} is the *local Artin map*, which is the unique continuous homomorphism satisfying the following properties.

- If v is finite, then
  - If π_v is a uniformizer of $\mathcal{O}_{K_v}$ and L_w/K_v is unramified, we have $\mathrm{Art}_{L_w/K_v}(\pi_v) = \mathrm{Frob}_{L_w/K_v}^{-1} \in \mathrm{Gal}(L_w/K_v)$.
  - The kernel of Art_{L_w/K_v} is $\mathrm{Nm}_{L_w/K_v}(L_w^\times)$, inducing an isomorphism $K_v^\times / \mathrm{Nm}_{L_w/K_v}(L_w^\times) \to \mathrm{Gal}(L_w/K_v)$.
- If v is real, then the composition $\mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\pm 1\}$ is the sign map.
- If v is complex, $\mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\}$ is the trivial map.

Moreover, for any finite extension L/K, the Artin map descends to an isomorphism $\mathrm{Art}_{L/K} : \mathbb{A}_K^\times / (K^\times \cdot \mathrm{Nm}(\mathbb{A}_L)) \to \mathrm{Gal}(L/K)$.

Remark 31.7. Beware that there are two common conventions for the local, hence also global, Artin map: one can require it to either send π_v to Frob_{L_w/K_v} ("arithmetic Frobenius") or to $\mathrm{Frob}_{L_w/K_v}^{-1}$ ("geometric Frobenius"). We use the latter convention, which agrees with [Mil10] but disagrees with [Con05], so make note of which convention holds if you are looking at the references, since it changes some of the formulas slightly.

32 The homomorphism λ_s (10/08/2024)

We will discuss L-functions of CM abelian varieties and their relationship with Hecke L-functions. We will make some simplifying assumptions. Let K be a number field, A/K

an abelian variety with CM by $E \subseteq \mathrm{End}^0(A)$, and let $E^* \subseteq K \subseteq \overline{\mathbb{Q}}$. We have a Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Aut}_{\mathbb{A}_{E,f}}(\hat{V}(A))$$

and the image of this commutes with E since $E \subseteq \mathrm{End}^0(A/K)$. We also know that $\hat{V}(A)$ is a rank 1 free $\mathbb{A}_{E,f}$-module, hence $\mathrm{Aut}_{\mathbb{A}_{E,f}}(\hat{V}(A)) \simeq \mathbb{A}_{E,f}^\times$. This is an abelian group, so ρ factors through $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. From the main theorem of CM, for all $s \in \mathbb{A}_{K,f}^\times$ there exists a unique $\lambda_s \in E^\times$ such that

$$\rho(\mathrm{Art}_K(s)) = N_\Phi(N_{K/E^*}(s)) \cdot \lambda_s^{-1}.$$

That is, the homomorphism $\lambda : \mathbb{A}_{K,f}^\times \to E^\times, s \mapsto \lambda_s$ measures how far the Galois representation ρ differs from the reflex norm, where we identify the two domains using the Artin map, and the main theorem tells us that this difference lies in $E^\times$.

By the functoriality of the Artin map, the following diagram commutes:

$$\begin{array}{ccc} \mathbb{A}_K^\times/K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow{\scriptstyle \mathrm{Nm}_{K/E^*}} & & \downarrow \\ \mathbb{A}_{E^*}^\times/E^{*,\times} & \xrightarrow{\mathrm{Art}_{E^*}} & \mathrm{Gal}(E^{*,\mathrm{ab}}/E) \end{array}$$

where the map on the right is induced by abelianization of the inclusion $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$.

Our goal for this section is to prove that λ is a continuous homomorphism, which will be Proposition 32.7.

Proposition 32.1. [Mum08, §21, Prop. on p. 188] Let A be a polarized abelian variety, and let $\alpha \in \mathrm{End}(A)$ satisfy $\alpha^\dagger \circ \alpha = a \in \mathbb{Z}$. Then $\mathbb{Q}[\alpha] \subseteq \mathrm{End}^0(A)$ is semisimple and α acts semisimply on $T_\ell(A)$. Letting $\{\omega_i\}$ denote the roots of the characteristic polynomial of α acting on $T_\ell(A)$, we have $|\omega_i|^2 = a$ for all i, and moreover these roots satisfy the symmetry $\{\omega_i\} = \{a/\omega_i\}$ as multisets.

Proof. Setting $\alpha^\dagger = a \cdot \alpha^{-1} \in \mathbb{Q}[\alpha]$, the Rosati involution restricts to $\mathbb{Q}[\alpha] \subseteq \mathrm{End}^0(A)$. The space $\mathbb{Q}[\alpha]$ carries a positive definite quadratic form $\mathrm{Tr}(x \circ x^\dagger)$. If $\mathfrak{a} \subseteq \mathbb{Q}[\alpha]$ is an ideal, let $\mathfrak{a}^\perp$ be its orthogonal complement with respect to this quadratic form. Then $\mathfrak{a} \oplus \mathfrak{a}^\perp = \mathbb{Q}[\alpha]$ and $\mathfrak{a} \cap \mathfrak{a}^\perp = \{0\}$, so $\mathbb{Q}[\alpha]$ satisfies complete reducibility into ideals, so we may write $\mathbb{Q}[\alpha] = K_1 \times \cdots \times K_n$ as a product of fields. Again using positivity of $\dagger$, we have $\dagger$ acting on each K_i, so each K_i is either totally real or CM by Albert's classification, with $\dagger$ acting by the identity or complex conjugation accordingly.

The statement about semisimplicity of the action of α follows from the fact that if A is a semisimple algebra (i.e. a direct sum of simple algebras), then any A-module is semisimple, and semisimplicity of a $\mathbb{Q}[\alpha]$-representation implies that the element α acts semisimply; see [Mil20, §IV.1] for more details.

The ω_i are the images of α via all homomorphisms $\varphi_j : \mathbb{Q}[\alpha] \to K_i \to \mathbb{C}$. But for all

such homomorphisms, since $a \in \mathbb{Q}$ we have

$$a = \varphi_j(a) = \varphi_j(\alpha^\dagger \circ \alpha) = \varphi_j(\alpha) \cdot \overline{\varphi_j(\alpha)} = |\omega_j|^2.$$

■

Corollary 32.2. *(Riemann hypothesis for abelian varieties.)* Let A/k be an abelian variety over a finite field k of order q. Then Frobenius acts semisimply on the Tate modules $T_\ell(A), \ell \nmid q$, and all the roots of the characteristic polynomial of Frobenius have absolute value $\sqrt{q}$.

Proof. Apply Proposition 32.1 to the Frobenius morphism, which satisfies $\mathrm{Frob}^\dagger \circ \mathrm{Frob} = [q]$ by Proposition 30.6, where $q = \#k$. ■

Remark 32.3. Corollary 32.2 is the starting point for Honda-Tate theory, which we will discuss later.

Remark 32.4. Abelian varieties are essentially the only case where we know how to show that Frobenius acts semisimply on étale cohomology. The Grothendieck-Serre conjecture states that Frobenius action is semisimple on the étale cohomology of any smooth projective variety.

Definition 32.1. Let A be an abelian variety with polarization $\phi = \phi_{\mathscr{L}}$ for ample $\mathscr{L}$. Then the group of *automorphisms preserving the polarization* $\mathrm{Aut}(A, \phi)$, also written as $\mathrm{Aut}(A, \mathscr{L})$, is the set of automorphisms α of A such that $\alpha^\vee \circ \phi \circ \alpha = \phi$. Equivalently, $\alpha^\dagger \circ \alpha = 1$.

Proposition 32.5. If A/k is any abelian variety with polarization $\phi : A \to A^\vee$ and $M \geq 3$ is an integer, then $\mathrm{Aut}(A, \phi) \hookrightarrow \mathrm{Aut}(A[M])$.

Remark 32.6. This a theorem attributed to Serre; see [Mum08, IV.21, Thm 5]. This means that, although $\mathrm{Aut}(A)$ may be infinite, $\mathrm{Aut}(A, \phi)$ is finite and more easily controlled, which makes it much better suited for moduli problems. In particular, the moduli space of polarized abelian varieties of a given degree is representable as a scheme, whereas the moduli space of all abelian varieties is not.

Proof. All of the eigenvalues ω_i of α are algebraic integers, and by Proposition 32.1, $\alpha^\dagger \circ \alpha = 1$ means that all $|\omega_i| = 1$. If all conjugates of an algebraic integer have absolute value 1, then that algebraic integer is a root of unity, so the ω_i are roots of unity.

Suppose that α lies in the kernel of $\mathrm{Aut}(A, \phi) \to \mathrm{Aut}(A[M])$. This means that $\alpha - 1$ kills $A[M]$, so we may write $\alpha - 1 = [M] \circ \beta$ for some $\beta \in \mathrm{End}(X)$, so that each $\omega_i - 1 = M\eta_i$ for some algebraic integer η_i arising as a root of the characteristic polynomial of β.

To finish the proof, it therefore suffices to show that if η is an algebraic integer and $\omega = 1 + M\eta$ is a root of unity, then in fact $\omega = 1$. This would imply that all of the ω_i are

1, hence α is the identity map (recall that α acts semisimply on the Tate module). For any $n > 0$, the expression $(1 + M\eta)^n$ is again of the form $1 + M\eta'$ for an algebraic integer η', so if $\omega \neq 1$ then by raising to an appropriate power we may assume that ω is a primitive p-th root of unity. Then $1 - \omega = M\eta$ has norm

$$\prod_{i=1}^{p-1}(1 - \omega^i) = \pm M^{p-1}\,\mathrm{Nm}(\eta).$$

The expression on the left is $\Phi_p(1)$, where Φ_p is the p-th cyclotomic polynomial $\sum_{i=0}^{p-1} X^i$, which evaluates to p. We conclude that p is divisible over the integers by M^{p-1}, which can only happen if $p = 2$, but that would imply $M \mid 2$, contradicting the assumption $M \geq 3$. ■

Proposition 32.7. [Con05, Thm. 3.2] The group homomorphism $\lambda : \mathbb{A}_{K,f}^\times \to E^\times$ is continuous for the discrete topology on $E^\times$.

Proof. We want to show that that for $s \in \mathbb{A}_{K,f}^\times$ sufficiently close to 1, we have $\lambda_s = 1$—equivalently, the kernel of λ is open. Since ρ, Art_K, the norm maps, and inversion are all continuous, we do at least know that λ is continuous as a homomorphism $\mathbb{A}_{K,f}^\times \to \mathbb{A}_{E,f}^\times$, or equivalently as a homomorphism $\mathbb{A}_{K,f}^\times \to E^\times$ where $E^\times$ is endowed with its subspace topology in $\mathbb{A}_{E,f}^\times$.[22] Therefore we take s sufficiently close to 1 such that $\lambda_s \in \mathcal{O}_E^\times, \lambda_s \equiv 1 \bmod M$ for a fixed integer $M \geq 3$, and $\lambda_s^\pm \in \mathcal{O}_E \cap \mathrm{End}(A_{\overline{\mathbb{Q}}})$, since all of these conditions are open in the subspace topology for $E^\times \hookrightarrow \mathbb{A}_{E,f}^\times$.

Our assumptions mean that $\lambda_s \in \mathcal{O}_E \cap \mathrm{Aut}(A_{\overline{\mathbb{Q}}})$, so we may and do treat λ_s as an automorphism of $A_{\overline{\mathbb{Q}}}$. The assumption $\lambda_s \equiv 1 \bmod M$ means that λ_s acts trivially on $A(\overline{\mathbb{Q}})[M]$. By Proposition 32.5, we are done if we can find a polarization $\phi : A \to A^\vee$ such that $\lambda_s \in \mathrm{Aut}(A, \phi)$ is an open condition on $s \in \mathbb{A}_{K,f}^\times$.

We take ϕ to be an E-linear polarization $\phi : A_{\overline{\mathbb{Q}}} \to A_{\overline{\mathbb{Q}}}^\vee$, i.e. compatible with the action of $E \hookrightarrow \mathrm{End}^0$ on both sides.[23]We may take $s \in \mathbb{A}_{K,f}^\times$ sufficiently close to 1 such that $\mathrm{Art}_K(s)$ fixes the number field of definition L/K of ϕ. More precisely, we can take s such that $\mathrm{Art}_K(s) \in \mathrm{Gal}(K^{\mathrm{ab}}/(K^{\mathrm{ab}} \cap L))$, so that there exists a lift of $\mathrm{Art}_K(s)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$.

Let $\mathrm{Art}_K(s) = \sigma$. By the definition of λ_s, σ acts on $\hat{V}(A)$ by the scalar $N_\Phi(N_{K/E^*}(s)) \cdot \lambda_s^{-1}$. Using the results from Remark 31.6, there exists $c = \frac{\chi(\sigma)}{\mathrm{Nm}_{E^*/\mathbb{Q}}(s)} \in \mathbb{Q}^\times$ such that

$$c\psi(x, y) = {}^\sigma\psi(\lambda_s^{-1}x, \lambda_s^{-1}y).$$

Since σ acts trivially on the field of definition for ϕ, unwinding definitions shows that ${}^\sigma\psi(x, y) = \psi(x, y)$, hence rearranging the above gives

$$c^{-1}\psi(x, y) = \psi(\lambda_s x, \lambda_s y) = \psi(\lambda_s\overline{\lambda}_s x, y).$$

Since the Weil pairing is nondegenerate, this means that in fact $\lambda_s\overline{\lambda}_s = c \in \mathbb{Q}^\times$. We've chosen λ_s to lie in $\mathcal{O}_E$, so by positivity of the Rosati involution $\lambda_s\overline{\lambda}_s$ must be a positive integer. However, we have also ensured that λ_s is invertible (as an element of $\mathcal{O}_E \cap \mathrm{Aut}\, A_{\overline{\mathbb{Q}}}$),

[22]This subspace topology is not discrete since we've removed the archimedean places, so we have more to prove.

[23]Such a polarization exists by the complex analytic theory—the Riemann form $\mathrm{tr}_{E/\mathbb{Q}}(\xi c(x)y)$ works.

which forces $\lambda_s\overline{\lambda}_s = c = 1$. That is, $\lambda_s \in \mathrm{Aut}(A,\phi)$. Yet we have chosen s such that λ_s acts trivially on $A[M]$, so by Proposition 32.5 we conclude $\lambda_s = \mathbf{id}_A$. ■

33 L-functions (04/10/2024)

33.1 Hecke L-functions

Definition 33.1. A *Hecke character* is a continuous homomorphism $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$, where K is a number field.

Remark 33.1. Some authors require Hecke characters to be unitary, i.e. with the image of χ contained in the unit circle. These two definitions are essentially the same, since there is a unique factorization of $\chi = \chi_0 \otimes \|\cdot\|^\sigma$, where $\chi_0 : \mathbb{A}_K^\times/K^\times \to S^1$ is unitary, $\sigma \in \mathbb{R}$, and $\|\cdot\| : \mathbb{A}^\times/K^\times \to K^\times$ is the norm map $x \mapsto \prod_v |x|_v$, where $\{|\cdot|_v\}$ is a compatible collection of v-adic norms such that the product formula holds. This factorization comes from the decomposition $\mathbb{A}^\times/K^\times = \mathbb{A}_K^{\times,1}/K^\times \times \mathbb{R}_+^\times$, where $\mathbb{A}_K^{\times,1}$ denotes the norm 1 idèles.

Definition 33.2. Let A/K be an abelian variety with CM by $E \subseteq \mathrm{End}^0(A)$, and let $\tau : E \hookrightarrow \mathbb{C}$ denote the various embeddings of E into $\mathbb{C}$. Let $N_{\Phi,K,\infty} : \mathbb{A}_L^\times \to E_\infty^\times$ denote the composition of the maps $N_{\Phi,K} : \mathbb{A}_K^\times \to \mathbb{A}_E^\times$ and the projection $\mathbb{A}_E^\times \twoheadrightarrow \prod_{v|\infty} E_v^\times := E_\infty^\times$ (projection onto the product of all archimedean places, all of which are complex since E is CM). Recall the continuous homomorphism $\lambda : \mathbb{A}_{K,f}^\times \to E^\times$; by projecting onto the finite places, we abuse notation and extend λ to $\mathbb{A}_K^\times$. The *Hecke characters associated to* A are

$$\alpha^\tau : \mathbb{A}_K^\times \xrightarrow{N_{\Phi,K,\infty}^{-1}\cdot\lambda} E_\infty^\times \twoheadrightarrow E_\tau^\times \xrightarrow{\tau} \mathbb{C}^\times.$$

That is, we get one Hecke character per τ. The recipe $N_{\Phi,K,\infty}^{-1}\cdot\lambda$ should be thought of as incorporating information from both the archimedean and nonarchimedean places. We prove that α^τ is indeed a Hecke character, i.e. it satisfies:

Lemma 33.2. α^τ is continuous and $\alpha^\tau|_{K^\times} = 1$.

Proof. For $s \in \mathbb{A}_K^\times$ write $s_f \in \mathbb{A}_{K,f}^\times$ for the finite part of s. From the definition of λ_s we have have $\lambda_s \cdot N_\Phi^{-1}(\mathrm{Nm}_{K/E^*}(s_f)) = \rho(\mathrm{Art}_K^{-1}(s))$. (Recall that $N_{K,\phi} = N_\Phi \circ \mathrm{Nm}_{K/E^*}$.) For $s \in K^\times$, we have $\mathrm{Art}_K^{-1}(s) = 1$—the Artin map kills $K^\times$. We also have

$$(N_\Phi \circ (\mathrm{Nm}_{K/E^*}(s_f))^{-1} = N_{K,\Phi}(s_f)^{-1} = N_{K,\Phi,\infty}^{-1}(s),$$

hence $N_{K,\Phi,\infty}(s)^{-1}\cdot\lambda_s = 1$.

Continuity of α^τ is clear from continuity of λ, the reflex norm, and the various projection maps. ■

If χ is a Hecke character, write $\chi_\infty := \chi|_{K_\infty^\times}$ for its restriction to the archimedean places.

Definition 33.3. A Hecke character χ is *algebraic* if $\chi_\infty(x_\infty) = \prod_{v \text{ real}} x_v^{n_v} \prod_{v \text{ complex}} x_v^{n_{\tau_v}} \overline{x}_v^{n_{\overline{\tau}_v}}$ for some $n_v, n_\tau, n_{\overline{\tau}_v} \in \mathbb{Z}$. Another way to state this is that this is a group scheme homomorphism $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m \to \mathbb{G}_m$ over $\overline{\mathbb{Q}}$.

We can check that the α^τ are algebraic. We will not need this fact, or even the definition of an algebraic Hecke character, but we mention it because this is a common feature of all Hecke characters associated to motives (whatever that means). More interestingly, it turns out that the converse is true: all algebraic Hecke characters arise from motives! See [Sch88], especially Theorem 4.1, for more discussion.

Definition 33.4. The (incomplete) L-function associated to a Hecke character χ is

$$L(\chi, s) := \prod_{\mathfrak{p} \nmid \mathfrak{m}} (1 - \chi_{\mathfrak{p}}(\varpi_{\mathfrak{p}}) \operatorname{Nm}_{K/\mathbb{Q}}(\mathfrak{p})^{-1})^{-1}$$

the product ranges over (finite) primes $\mathfrak{p} \subset \mathcal{O}_K$ (uniformizer $\varpi_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}$) not dividing the *conductor* $\mathfrak{m}$ of χ. This is the smallest integral ideal $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$ such that

$$\chi|_{\prod_{\mathfrak{p}} (1+\mathfrak{p}^{m_{\mathfrak{p}}})} = 1,$$

where all the $m_{\mathfrak{p}}$ are finite and almost always zero by the continuity of χ and the topology on $\mathbb{A}_K^\times$. In particular, if $\mathfrak{p} \nmid \mathfrak{m}$, then $\chi_{\mathfrak{p}}(\varpi_{\mathfrak{p}})$ is independent of the choice of uniformizer $\varpi_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$.

Theorem 33.3. *(Hecke, Tate's Thesis.)* After completing $L(\chi, s)$ to a function $\Lambda(\chi, s)$ by adding a suitable factor $L_\infty(\chi, s)$, $L(\chi, s)$ admits a meromorphic continuation to $\mathbb{C}$, satisfying a functional equation, and it is an entire analytic function if χ_0 (the norm 1 part of χ) is nontrivial, analogous to how a Dirichlet L-function $L(\chi, s)$ is holomorphic if χ is not the trivial Dirichlet character.

Proof. See [Neu99, §VII.8], or [Bum97, §3.1] ■

Definition 33.5. Assume for simplicity that an abelian variety A/K has good reduction everywhere. The (Hasse-Weil) L-function of A is

$$L(A, s) := \prod_{\mathfrak{p} \subset \mathcal{O}_K} \det(1 - \operatorname{Frob}_{\mathfrak{p}} (\operatorname{Nm}_{K/\mathbb{Q}} \mathfrak{p})^{-s} |_{V_\ell(A)})^{-1}.$$

We can make a similar definition using $H^1_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ instead of V_ℓ when A has good reduction at $\mathfrak{p}$, but for this we need to use the geometric Frobenius rather than the arithmetic Frobenius, since $H^1_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ is dual to V_ℓ. More generally, geometric Frobenius acts on $H_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)^{I_{\mathfrak{p}}}$, where $I_{\mathfrak{p}}$ is the inertia subgroup, which already acts trivially if we have good reduction.

Proposition 33.4. Let A/K have CM, and let $\mathfrak{p}$ be a prime of K.

1. If A has good reduction at $\mathfrak{p}$, then $\lambda_{\mathfrak{p}} := \lambda|_{K_{\mathfrak{p}}^\times}$ is trivial on $\mathcal{O}_{K_{\mathfrak{p}}}^\times$.
2. $\lambda_{\mathfrak{p}}(\varpi_{\mathfrak{p}}) \in \mathcal{O}_E$ acts on $\mathscr{A}_{k(\mathfrak{p})}$ as $\operatorname{Frob}_{\mathfrak{p}}$, where $\mathscr{A}_{k(p)}$ is the special fiber of the Néron model of A over $\mathcal{O}_{K_{\mathfrak{p}}}$.

Proof. 1. Recall from local class field theory that $I_{\mathfrak{p}} \subseteq \operatorname{Gal}(K^{\text{ab}}/K)$ is the image of $\mathcal{O}_{K_{\mathfrak{p}}}^\times$ under the local Artin map. Choose any prime ℓ not equal to the residue char-

acteristic of $\mathfrak{p}$. By the criterion of Néron-Ogg-Shafarevich (Theorem 34.3), good reduction means that $I_\mathfrak{p}$ acts trivially on $T_\ell(A)$, so for $s \in \mathcal{O}_{K_\mathfrak{p}}^\times \subseteq \mathbb{A}_K^\times$ we get $\rho(\mathrm{Art}_K(s)) = N_{K,\Phi}(s)\lambda_s^{-1} = 1$ acting on $\hat{V}(A)$. But $N_{K,\Phi}(s)$ also acts trivially because $s_\ell = 1$, so λ_s acts trivially.

2. We have $\varpi_\mathfrak{p} \in K_\mathfrak{p}^\times \subseteq \mathbb{A}_K^\times$. Again choose ℓ as in part (1), so that $N_{K,\Phi}(s)$ again acts trivially on $T_\ell(A)$. Then $\lambda_\mathfrak{p}(\varpi_\mathfrak{p}) = \rho(\mathrm{Art}_K(\varpi_\mathfrak{p}^{-1})) = \rho(\mathrm{Frob}_\mathfrak{p})$, acting on $T_\ell(A) \simeq T_\ell(\mathscr{A}_{k(\mathfrak{p})})$—recall that $\mathrm{Art}_K(\varpi_\mathfrak{p}^{-1}) = \mathrm{Frob}_\mathfrak{p}$ is part of the unique characterization of Artin map.

■

Theorem 33.5. If A/K has CM, then for $\mathrm{Re}(s) > \frac{3}{2}$ we have $L(A,s) = \prod_{\tau:E\to\mathbb{C}} L(\alpha^\tau, s)$. In particular, $L(A,s)$ has an analytic continuation and functional equation via Tate's thesis.

Intuitively, we expect the L-function of A to decompose into a product of Hecke L-functions because the Galois representation on the Tate modules is abelian. Indeed, one could argue that the fact that the Galois representation attached to a CMAV is one of the main reasons why they are the easiest case to work with, since number theorists know a lot about abelian extensions by now...

We won't prove the fact about the half-plane of convergence, but the reason that it is $\mathrm{Re}(s) > \frac{3}{2}$ is that the eigenvalues of Frobenius all have absolute value $q^{1/2} = \mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p})^{1/2}$.

Proof. To simplify notation, write $X = (\mathrm{Nm}_{K/\mathbb{Q}}\,\mathfrak{p})^{-s}$. Since $V_\ell(A)$ is a rank 1 free $E \times \mathbb{Q}_\ell$-module, we have

$$\det(1 - \mathrm{Frob}_\mathfrak{p}\, X \mid V_\ell(A)) = \mathrm{Nm}_{E/\mathbb{Q}}(1 - \mathrm{Frob}_\mathfrak{p}\, X),$$

where on the RHS we treat $\mathrm{Frob}_\mathfrak{p}$ as an element of $E \hookrightarrow V_\ell(A)$. By Proposition 33.4, this equals

$$\begin{aligned} &= \mathrm{Nm}_{E/\mathbb{Q}}(1 - \lambda_\mathfrak{p}(\varpi_\mathfrak{p})X) \\ &= \prod_{\tau:E\to\mathbb{C}} (1 - \alpha_\mathfrak{p}^\tau(\varpi_\mathfrak{p})X). \end{aligned}$$

Hence the Euler product for $L(A,s)$ matches that of $\prod_{\tau:E\to\mathbb{C}} L(\alpha^\tau, s)$. ■

34 Criterion of Néron-Ogg-Shafarevich (04/12/2024)

34.1 Potentially good reduction of CMAVs

We have frequently been using the assumption that a CMAV has everywhere good reduction. It turns out that this is not overly restrictive.

Definition 34.1. Let A/K be an abelian variety over a number field K, and let $\mathfrak{p}$ be a prime of K. We say that A has *potentially good reduction* at $\mathfrak{p}$ if there exists a finite extension $L/K_\mathfrak{p}$ such that A_L has good reduction at $\mathfrak{p}$. That is, we have a good integral model after passing to a finite extension.

Remark 34.1. If K is a number field, then A always has good reduction at all but finitely many primes $\mathfrak{p}$. Therefore, if A has potentially good reduction at all primes, then there is a finite extension L/K such that A has good reduction everywhere—take the compositum of all of the individual extensions giving good reduction for each prime, since good reduction is stable under field extension.

Proposition 34.2. If A/K is a CMAV over a number field K, then A has potentially good reduction everywhere.

Proof. See also [Mil10, Prop. 7.12]. We use the criterion of Néron-Ogg-Shafarevich:

Theorem 34.3. *(Criterion of Néron-Ogg-Shafarevich.)* [Mil10, Thm. 6.12] Let R be a DVR with fraction field K and residue field k. Let $\ell \neq \mathrm{char}(k)$ be a prime, and let A/K be an abelian variety. Then A has good reduction if and only if the inertia group $I \subseteq \mathrm{Gal}(\overline{K}/K)$ acts trivially on $T_\ell(A)$.

Proof. (Sketch.) We have already seen that good reduction means inertia acts trivially from Lemma 30.2. This is the fact that all ℓ-torsion points are defined over an unramified extension of K.

For the reverse direction, we use Néron models. Let $\mathscr{A}/R$ be the Néron model of A/K. We have isomorphisms

$$\mathscr{A}(K^{\mathrm{ur}})[\ell^n] \simeq \mathscr{A}(\mathcal{O}_{K^{\mathrm{ur}}})[\ell^n] \simeq \mathscr{A}(\overline{k})[\ell^n]$$

using the Néron mapping property for the first isomorphism and Hensel's lemma for the second condition. We may also write

$$\mathscr{A}(K^{\mathrm{ur}})[\ell^n] = \left(\mathscr{A}(\overline{K})[\ell^n]\right)^I,$$

so inertia acting trivially means that this is just $A(\overline{K})[\ell^n]$. So all of these groups have order $\ell^{2n \dim A}$.

$\mathscr{A}_k$ is a smooth finite type commutative group scheme, although not *a priori* an abelian variety. There is a classification of such groups (see also [Mil15]): $\mathscr{A}_k/\mathscr{A}_k^0$ is a finite group, and we have exact sequences

$$1 \to U \to \mathscr{A}_k^0 \to G \to 1,$$

where U is unipotent and G is semiabelian, i.e. an extension of an algebraic torus by an abelian variety:

$$1 \to T \to G \to B \to 1$$

for some torus T and abelian variety B. Then

$$\dim A = \dim \mathscr{A}_k = \dim U + \dim T + \dim B.$$

We have

$$\begin{aligned}\#B[\ell^n](\overline{k}) &= \ell^{2n\dim B}\\ \#T[\ell^n](\overline{k}) &= \ell^{n\dim T}\\ \#U[\ell^n](\overline{k}) &= 0,\end{aligned}$$

using the fact that $T_{\overline{k}} = \mathbb{G}_{m,\overline{k}}^{\dim T}$ and a general result about lack of torsion in unipotent groups. Since we must have

$$\#\mathscr{A}_k[\ell^n](\overline{k}) = \#B[\ell^n](\overline{k}) \cdot \#T[\ell^n](\overline{k}) \cdot \#T[\ell^n](\overline{k})$$

letting $n \to \infty$ and comparing asymptotics shows that

$$2\dim A = 2\dim B + \dim T.$$

Comparing this with our previous dimension formula, we get $2\dim U = -\dim T$, so since dimension is nonnegative we conclude that $U = T = \{1\}$ are both trivial. This means that $\mathscr{A}_k^0 = G = B$ is an abelian variety, so $\mathscr{A}$ is an abelian scheme. ■

Applying this in the case of CM, we have $\#k(\mathfrak{p}) < \infty$ and the image of $\rho_\ell : \mathrm{Gal}(\overline{K}/L) \to \mathrm{Aut}(T_\ell(A))$ is an abelian, where L/K is a finite extension such that all CM endomorphisms are defined; WLOG $L = K$ for ease of notation. This Galois representation restricts to $\rho_\ell : \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}}) \to \mathrm{Aut}(T_\ell(A))$. We have a diagram

$$\begin{array}{ccccc} I_{\mathfrak{p}} & \xrightarrow{\rho_\ell} & \mathrm{Aut}(T_\ell(A)) & \hookleftarrow & 1 + \ell\,\mathrm{End}(T_\ell(A)) \\ {\scriptstyle \mathrm{Art}}\uparrow & & & \nearrow & \\ \mathcal{O}_K^\times & \hookleftarrow & 1 + p\mathcal{O}_{K_{\mathfrak{p}}} & & \end{array}$$

where the left upwards arrow is the local Artin map, both inclusions are finite index, and all arrows are continuous homomorphisms. The group $1 + \ell\,\mathrm{End}(T_\ell(A))$ is a *pro-ℓ group*, but the group $1 + p\mathcal{O}_{K_{\mathfrak{p}}}$ is a *pro-p group*.

Definition 34.2. For a prime p, a *pro-p* group is a topological group that is the inverse limit of finite p-groups, equipped with the Krull topology.

Lemma 34.4. For distinct primes ℓ, p, there are no nontrivial continuous homomorphisms from a pro-p group to a pro-ℓ group.

Proof. Suppose we have a continuous homomorphism $\rho : G \to H$ for a pro-p group G and a pro-ℓ group G. Let K an open normal subgroup in H such that H/K is a finite ℓ-group, which always exists by the construction of H as an inverse limit. By continuity, $\rho^{-1}(K)$ is open, hence a normal open subgroup of G. Open subgroups are finite index, and one can show that the quotient of a finite index normal subgroup of a pro-p group is a p-group (this is an alternative definition of a pro-p group). Therefore the homomorphism ρ descends to a well-defined homomorphism $G/\rho^{-1}(K) \to H/K$ between a p-group and an ℓ-group—but the only such homomorphism is the trivial one by finite group theory. We conclude that the image of ρ is contained inside K. But this is true for an arbitrary normal open subgroup of

H, and such subgroups form a basis of open neighborhoods of the identity, so we conclude that $\rho(G) = \{1\} \subseteq H$ since profinite groups are Hausdorff. ■

Therefore the image of $1 + p\mathcal{O}_{K_\mathfrak{p}}$ in $\mathrm{Aut}(T_\ell(A))$ must have trivial intersection with $1 + \ell \,\mathrm{End}(T_\ell(A))$, so that this image is finite in $\mathrm{Aut}(T_\ell(A))$, since it descends injectively to the finite quotient $\mathrm{Aut}(T_\ell(A))/(1 + \ell \,\mathrm{End}(T_\ell(A))$. Since $1 + p\mathcal{O}_{K_\mathfrak{p}}$ has finite index in $\mathcal{O}_K^\times$, we conclude that the image $\rho(I_\mathfrak{p}) \subseteq \mathrm{Aut}(T_\ell(A))$ is also finite. Therefore, there exists a finite extension $K_\mathfrak{p}$ such that the inertia group of that field acts trivially on $T_\ell(A)$, so the criterion of Néron-Ogg-Shafarevich tells us that A has potentially good reduction. ■

34.2 Honda-Tate theory

Let q be a p-th power. We wish to classify isogeny classes of simple AVs over $\mathbb{F}_q$.

Definition 34.3. A *Weil q-number* is an algebraic integer π such that for every embedding $\mathbb{Q}(\pi) \to \mathbb{C}$, we have $|\tau(\pi)| = q^{1/2}$. We will also refer to these as Weil numbers when q is fixed.

Given two Weil numbers π, π', define an equivalence relation $\pi \sim \pi'$ (π is *conjugate* to π') if π and π' are Galois conjugates over $\mathbb{Q}$, i.e. they have the same minimal polynomial over $\mathbb{Q}$.

Recall that for an abelian variety over $A/\mathbb{F}_q$, we have the q-th power Frobenius automorphism $\pi_A := \mathrm{Frob}_A$ and $\mathbb{Q}[\pi_A]$ is semisimple (from Proposition 32.1), hence a field when A is simple. We also previously showed that π_A is a Weil q-number (this is the Riemann Hypothesis for Abelian Varieties, Corollary 32.2).

Theorem 34.5. *(Honda-Tate theorem.)* Taking eigenvalues of Frobenius induces a bijection

$$\{\text{isogeny classes of simple AVs}/\mathbb{F}_q\} \leftrightarrow \{\text{conj. classes of Weil } q\text{-numbers}\}$$
$$A \mapsto \pi_A$$

This is a great tool for classifying abelian varieties over a finite field, since in general working with integer polynomials is easier than trying to wrangle unknown geometric objects, and the characteristic polynomial of Frobenius is already an important invariant.

Injectivity of the map in the Honda-Tate theorem follows from Tate's isogeny theorem:

Theorem 34.6. *(Tate's isogeny theorem.)* Let $\ell \neq p$, and let $A, B/\mathbb{F}_q$ be abelian varieties. Then

$$\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}(T_\ell(A), T_\ell(B)).$$

This is often just called Tate's theorem.[24] We already showed that this map is injective (Theorem 24.1). Unfortunately, we omit the proof of surjectivity.

[24] Not to be confused with Tate's theorem on Tate cohomology.

Remark 34.7. When we deal with L-functions or other similar objects, the Galois representation is easier to work with than the geometric objects. Tate's theorem allows us to work abstractly with Tate modules rather than abelian varieties, where constructing homomorphisms is easier.

Corollary 34.8. For $A, B/\mathbb{F}_q$, the following are equivalent:

1. $A \sim B$ over $\mathbb{F}_q$.
2. For *at least one* $\ell \neq p$, we have $V_\ell(A) \simeq V_\ell(B)$ as Galois representations.
3. For *all* $\ell \neq p$, we have $V_\ell(A) \simeq A_\ell(B)$ as Galois representations.
4. $P_A(t) = P_B(t)$, where P_A, P_B are the respective characteristic polynomials of Frobenius.

Proof. (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) are on your homework. For (4) $\implies$ (3), we know Frobenius acts semisimply, so $P_A = P_B$ implies we have a Frobenius-equivariant isomorphism $V_\ell(A) \simeq V_\ell(B)$ by standard linear algebra. In more detail, we know that the Frobenius actions are at least conjugate over $\overline{\mathbb{Q}}_\ell$, so by a descent argument and Hilbert Theorem 90 we find that this is actually already defined over $\mathbb{Q}_\ell$. This is in fact a Galois-equivariant map because Frobenius topologically generates the Galois group. (3) $\implies$ (2) is trivial, and (2) $\implies$ (1) is immediate from Tate's isogeny theorem 34.6—an isogeny $A \to B$ exists if and only if there is an isomorphism $V_\ell(A) \simeq V_\ell(B)$. ∎

Injectivity of the map in the Honda-Tate theorem is then immediate from (4) $\implies$ (1) in Corollary 34.8.

35 Honda-Tate theorem: surjectivity part I (04/15/2024)

Somewhat more is true than Corollary 34.8:

Corollary 35.1. : For $A, B/\mathbb{F}_q$, the following are equivalent:

1. There exists a morphism $A \to B$ that is an isogeny onto its image.
2. For all/at least one $\ell \neq p$, $V_\ell(A)$ is a Galois subrepresentation of $V_\ell(B)$.
3. $P_A(t)$ divides $P_B(t)$, where P_A, P_B are the respective characteristic polynomials of Frobenius.

Remark 35.2. We can conclude that isogenous abelian varieties have the same characteristic polynomial by looking at the local invariants of End^0.

Given $A_0/\mathbb{F}_q$, there exists a CMAV A over some number field (constructed using π_{A_0}) such that $A \bmod \mathfrak{p}$ lies in the isogeny class of $A_{0,k}$ for a finite extension $k/\mathbb{F}_q$. See [CCO14, §1.7.6] for some more information without passing to the isogeny class. We can also have

CM liftings with extra endomorphisms and algebraic cycles, originally done by Kisin '17 and Kisin-Mudapusi-Shin. To get the CM field associated to the lifting, we will use local invariants of the endomorphism algebra, and to get the CM type we will apply the Shimura-Taniyama formula "in reverse."

Lemma 35.3. Let π be a Weil q-number. There are three possibilities for $\mathbb{Q}[\pi]$:

1. (Even case) $q = p^{2m}, \pi = \pm p^m$, $\mathbb{Q}(\pi) = \mathbb{Q}$.
2. (Odd case) $q = p^{2m+1}, \pi = \pm\sqrt{p^{2m+1}}$, $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$.
3. $\mathbb{Q}(\pi)$ is a CM field.

Note that in the first two cases $\mathbb{Q}(\pi)$ is totally real and the last case is totally imaginary.

Proof. Suppose neither (1) nor (2) holds. Then every embedding $\tau : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ is complex, since $\pm\sqrt{q}$ are the only real numbers with absolute value $q^{1/2}$, i.e. $\mathbb{Q}(\pi)$ is a totally imaginary field. Since $|\tau(\pi)| = \sqrt{q}$ for any embedding τ, we conclude $\overline{\tau(\pi)} = q/\tau(\pi)$, so that $\pi + q/\pi$ is totally real. Then $\mathbb{Q}(\pi)/\mathbb{Q}(\pi + q/\pi)$ is a quadratic extension of a totally imaginary field over a totally real field, so $\mathbb{Q}(\pi)$ is CM. ∎

Theorem 35.4. Let $A/\mathbb{F}_q$ be simple, and let $D := \mathrm{End}^0(A), K$ the center of D, $d = [D : K]^{1/2}, e = [K : \mathbb{Q}]$. Then:

1. $K = \mathbb{Q}(\pi_A)$
2. $de = 2 \dim A$.
3. For a place v of K, we may compute $\mathrm{inv}_v(D) = \frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)}[K_v : \mathbb{Q}_p]$ if $v \mid p$, $\mathrm{inv}_v(D) = 1/2$ if v is real, and 0 otherwise.

Remark 35.5. We will have $P_A = (\text{min. poly of } \pi)^d$, where the *order* d is the lcm of all denominators of all invariants. This comes from class field theory.

Proof. 1. By Tate's isogeny theorem, for $\ell \neq p$, we have $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}_{\mathbb{Q}(\pi_A)}(V_\ell(A))$. We apply the Double Centralizer Theorem (see [Mil20, §IV, Thm. 1.14] for this, and also for other results on central simple algebras):

Theorem 35.6. *(Double Centralizer.)* Let k be a field. If B is a k-algebra and V is a faithful semisimple B-module, then $C(C(B)) = B$, where $C(-)$ denotes the centralizer of $(-)$ in $\mathrm{End}_k(V)$.

We take $k = \mathbb{Q}_\ell$, $B = \mathbb{Q}(\pi_A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, $V = V_\ell(A)$. The statement $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}_{\mathbb{Q}(\pi_A)}(V_\ell(A))$ is the same as saying $C(B) = D \otimes \mathbb{Q}_\ell$ so $C(D \otimes \mathbb{Q}_\ell) = \mathbb{Q}(\pi) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ by the Double Centralizer Theorem. Meanwhile, the center of D is $C(D \otimes \mathbb{Q}_\ell) \cap D = K$, so since $\mathbb{Q}(\pi) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is already contained in $D \otimes \mathbb{Q}_\ell$ we conclude that $K = \mathbb{Q}(\pi_A)$.

2. Write $K \otimes \mathbb{Q}_\ell = K_{v_1} \times \cdots \times K_{v_r}$, where the v_i are the places of K above ℓ. The ring $K_{v_1} \times \cdots \times K_{v_r}$ acts faithfully on $V_\ell(A)$, which we may decompose as $V_\ell(A) = V_1 \oplus \cdots \oplus V_r$ with K_{v_i} acting on V_i.

   Writing $D \otimes \mathbb{Q}_\ell = \mathrm{End}_K(V_\ell(A)) = \prod_i \mathrm{End}_{K_{v_i}}(V_i)$, we can compute its $\mathbb{Q}_\ell$-dimension as

$$d^2 e = \sum_i e_i d_i^2$$

   where $e_i = [K_{v_i} : \mathbb{Q}_\ell]$ and $d_i = \dim_{K_{v_i}} V_i$. However, we have $e = \sum_{i=1}^r e_i$ from $K \otimes \mathbb{Q}_\ell = \prod_i K_{v_i}$, and we also have $2g := 2 \dim A = \dim_{\mathbb{Q}_\ell} V_\ell(A) = \sum e_i d_i$ as a general fact about Tate modules. Hence,

$$(2g)^2 \geq (de)^2 = \left(\sum_i e_i d_i^2 \right) \left(\sum_i e_i \right) \geq \left(\sum_{i=1}^r e_i d_i \right)^2 = (2g)^2$$

   where the first inequality comes from $ed \mid 2g$ in Albert's classification, the second inequality is an application of Cauchy-Schwarz. Therefore all of the inequalities are in fact equalities, so taking square roots gives $2g = de$. (Also note that the equality condition on the Cauchy-Schwarz inequality implies that all of the d_i are equal to d.)

3. For $v \mid \ell \neq p$, the proof of (2) shows that $D \otimes_{v_i} K_{v_i} = \mathrm{End}_{K_{v_i}}(V_i) = M_d(K_{v_i})$. Hence $\mathrm{inv}_v(D) = 0$. For $v \mid \infty$, Albert's classification gives, by type:

$$\begin{aligned} \text{I} &: e \mid g, d = 1 \\ \text{II} &: 2e \mid g, d = 2 \\ \text{III} &: e \mid g, d = 2 \\ \text{IV} &: e \mid g, d = 2 \end{aligned}$$

   The first three cases are totally real. The first two cases contradict (2), so they do not occur, and Type III gives the correct invariant $1/2$ for real places, since $D \otimes \mathbb{R}$ is nonsplit in this case. Type IV means that K is CM, so there are no real places to worry about.

   We will only be able to prove the formula for the invariant at $v \mid p$ later, using Dieudonné theory, so we omit this for now.

■

Lemma 35.7. Given a Weil number π, let $F = \mathbb{Q}(\pi)$. Then there exists a division algebra D/F satisfying all of the local invariant conditions in the conclusions (1), (2), (3) of Theorem 35.4.

Proof. See also [Mil20]. Such D exists and is unique up to isomorphism iff $\sum_v \mathrm{inv}_v = 0$, using the exact sequence from global class field theory. To check this condition, there are two cases:

1. The case F where is totally real is on your homework.

2. If F is CM, we have $\pi \cdot \overline{\pi} = q$ (under any complex embedding), and the only possibly nonzero contributions to $\sum_v \mathrm{inv}_v$ come from places $v \mid p$. For $v \mid p$, if $v \neq \overline{v}$, then

$$\mathrm{inv}_v + \mathrm{inv}_{\overline{v}} = \frac{\mathrm{ord}_v(\pi) + \mathrm{ord}_v(\overline{\pi})}{\mathrm{ord}_v(q)}[K_v : \mathbb{Q}_\ell] = 0 \bmod \mathbb{Z}$$

and if $v = \overline{v}$, we have

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = 1/2$$

but $\sum_{v:\ v=\overline{v}}[K_v : \mathbb{Q}_p]$ is even ($[L : \mathbb{Q}]$ is even and the v with $v \neq \overline{v}$ come in pairs), so the overall contribution to the global invariant is 0.

■

36 Honda-Tate theorem: surjectivity part II (04/17/2024)

Let π be a Weil q-number. Recall that we showed that $F := \mathbb{Q}(\pi)$ is either totally real or a CM field. Using local invariants, we got a division algebra D with center F and local invariants as prescribed in Theorem 35.4, in particular with D_v split if $v \nmid p\infty$ and D_v nonsplit if v is a real place.

Proposition 36.1. There exists a CM field $L \supseteq F$ such that $D \otimes_F L$ splits at all places of L. For such L, we have $[L : F] = \sqrt{[D : F]}$.

Remark 36.2. See [Mil20, §IV , Cor. 3.7]. If $[L : F] = \sqrt{[D : F]}$, splitting of $D \otimes_F L$ (everywhere) is equivalent to the existence of an F-algebra embedding $L \hookrightarrow D$.

Proof. The totally real case is on your homework; the answer will be $L = F(\sqrt{p})$. So assume F is CM, and let $F_0 := \mathbb{Q}(\pi + q/\pi)$ be its maximally totally real subfield. There exists a totally real extension L_0/F_0 of degree d such that all places v of F dividing p are *totally inert* in L_0/F_0, i.e. such L_0 is unramified at p, has one place above any given $v \mid p$, and the splitting polynomial defining L_0 has all real roots.[25] In particular, this means that $[L_{0,w} : K_{0,v}] = d$ for the unique place of L lying above v. Then $L := FL_0$ is a CM field, and $[L : F] = [L_0 : F_0] = d$.

Local invariants satisfy the compatibility $\mathrm{inv}_w(D \otimes_F L) = \mathrm{inv}_v(D)[L_w : F_v]$ for any $w \mid v$ ([Mil20, §IV.4, Rmk 4.4.(c), §III.2, Thm. 2]). Since we already have $\mathrm{inv}_v(D) = 0$ for all $v \mid p$, we conclude automatically that

$$\mathrm{inv}_w(D \otimes_F L) = 0 \cdot [L_w : F_v] = 0$$

for all $w \nmid p$ for all $w \mid v$. In the case $v \mid p$, $\mathrm{inv}_v(D)$ is a multiple of $1/d$ and we have specifically chosen L so that $[L_w : F_v] = d$. Hence we also get $\mathrm{inv}_w(D \otimes_F L) = 0$ when $w \mid p$.

[25] One way to do this is to find a degree d integer polynomial f that is irreducible in the residue fields of $F_{0,v}$ for all $v \mid p$ and then adjust the coefficients by multiples of p suitably to ensure f has all real roots. Then let L_0 be obtained by adjoining a root of f to F_0.

Since we are assuming F, hence also L, is CM, there are no real places to consider. ■

Proposition 36.3. There exists an abelian scheme $\mathscr{A}$ over $\mathcal{O}_{K'}$, where $K'/\mathbb{Q}_p$, such that $\mathscr{A}_{K'}$ admits CM by L as in Proposition 36.1 and $\mathscr{A}_k$ has Frobenius conjugate to π^N for some $N \in \mathbb{Z}$.

Proof. We will use the Shimura-Taniyama formula to reverse-engineer exactly the CM type Φ we want. Let $A_0 := \mathscr{A}_k$. Recall the formula: let $L \otimes \mathbb{Q}_p = \prod_{w|p} L_w$, and $\Phi \subseteq \prod_{w|p} H_w := \mathrm{Hom}(L, \overline{\mathbb{Q}}_p)$ a CM type, $\Phi_w = \Phi \cap H_w$. Then Frobenius π_{A_0} of A is descended from some element of $\mathcal{O}_L$ and $\frac{\mathrm{ord}_w(\pi_{A_0})}{\mathrm{ord}_w \#k} = \frac{\#\Phi_w}{\#H_w}$.

Lemma 36.4. If π, π_0 are a Weil q- and q_0-numbers, respectively, with $\mathbb{Q}(\pi), \mathbb{Q}(\pi_0) \subseteq L$ such that $\frac{\mathrm{ord}_w(\pi_0)}{\mathrm{ord}_w(q_0)} = \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)}$ for all places $w \mid p$ of L, then there exists $N, N_0 \in \mathbb{Z}_{\geq 1}$ such that $\pi^N = \pi_0^{N_0}$.

Proof. We have $\pi\overline{\pi} = q$ and $\pi_0\overline{\pi}_0 = q_0$. Pick N', N_0' such that $q^{N'} = q_0^{N_0'}$. We may assume by raising π and π_0 to a suitable power that $q = q'$. Then it suffices to show that π/π_0 is a root of unity. This will follow if we can show that π/π_0 is an algebraic integer, since $|\pi/\pi_0|_\tau = 1$ for all embeddings $\tau : L \hookrightarrow \mathbb{C}$, and the only algebraic integers with all embeddings of absolute value ≤ 1 are the roots of unity. For integrality, it suffices to show that $|\pi/\pi_0|_w = 1$ for all finite places w—but this immediately follows from our hypotheses on the w-adic absolute values of π_0 and π. ■

We choose subsets $\Phi_v \subseteq \mathrm{Hom}(L_w, \overline{\mathbb{Q}}_p) \subseteq \mathrm{Hom}(L, \overline{\mathbb{Q}}_p)$ such that $\frac{\#\Phi_w}{\#H_w} = \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_q(q)}$ for all $w \mid p$ of L. This is possible because

$$\#H_w \cdot \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)} = [L_w : \mathbb{Q}_p]\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = [L_w : F_v][F_v : \mathbb{Q}_p]\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_{v(q)}} = [L_w : F_v]\,\mathrm{inv}_v(D) \in \mathbb{Z}.$$

We have $\pi \cdot \overline{\pi}$, and $\mathrm{ord}_w(\pi) = \mathrm{ord}_w(\overline{\pi}) = \mathrm{ord}_w(q)$, so that $\#\Phi_v + \#\Phi_{\overline{w}} = \#H_w = \#H_{\overline{w}}$. This means that we may actually choose each pair $\Phi_w, \Phi_{\overline{w}}$ so that $\overline{\Phi_w}$ is the complement of $\Phi_{\overline{w}}$ in $H_{\overline{w}}$. (There are no cases where $w = \overline{w}$ since L is totally imaginary.) Therefore, we get a CM type $\Phi = \bigcup \Phi_v$, where the union is appropriately understood under some fixed embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$. (Note that the $\Phi_w \hookrightarrow \mathrm{Hom}(L, \mathbb{C})$ are disjoint.)

Now let $\mathscr{A}$ have CM by (L, Φ)—certainly we can construct such an abelian variety over a number field, and CMAVs have potentially good reduction everywhere. By the Shimura-Taniyama formula, we have

$$\frac{\mathrm{ord}_w(\pi_{A_0})}{\mathrm{ord}_w(\#k)} = \frac{\#\Phi_w}{\#H_w} = \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)}.$$

Then by Lemma 36.4 we conclude $\pi_{A_0}^{N_0} = \pi^N$ for some integers N, N_0, and we may replace L with a $\deg N_0$ totally ramified extension to in fact get $\pi_{A_0} = \pi^N$. ■

We finally prove the surjectivity part of Honda-Tate. We have done the hard part of showing that there exists an abelian variety that is close to what we want, only off by a power: we have an abelian variety A_0/k with $\pi^N = \pi_{A_0}$ for a finite field k. Then then formula

$\frac{\mathrm{ord}_w(\pi_{A_0})}{\mathrm{ord}_w(\#k)} = \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)}$ shows that $[k:\mathbb{F}_q] = N$. Consider the Weil restriction $\mathrm{Res}_{k/\mathbb{F}_q} A_0$—this is an abelian variety over $\mathbb{F}_q$ of dimension $N \cdot \dim A_0$.

Definition 36.1. Let k be a ring, let k' be a k-algebra, and let X be a k'-scheme. Then $\mathrm{Res}_{k'/k} X$ is the k-scheme representing the functor of points $R \rightsquigarrow X(R \otimes_k k')$ for k-algebras R. (This doesn't always exist, but it does when X is an abelian variety and k'/k is a finite field extension.)

On the homework, you will show that $V_\ell(\mathrm{Res}_{k/\mathbb{F}_q} A_0) = \mathrm{Ind}_{\mathrm{Gal}(\overline{k}/k)}^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)} V_\ell(A)$ (induced Galois representation). When we induce a representation and then restrict it back to the original representation, we get a direct sum of copies of the original representation. Therefore, as a $\mathrm{Gal}(\overline{k}/k)$-representation we may identify $V_\ell(B_0) = \bigoplus_{i=1}^N V_\ell(A_0)$, with $\mathrm{Frob}_{B_0}^N = \mathrm{Frob}_{B_{0,k}}$ acting by Frob_{A_0} on each component. Hence $\pi_{B_0}^N \sim \pi_{A_0}$ and $P_{B_0}(t) = P_{A_0}(t^N)$, so that $\pi = \pi_{A_0}^N$ is a root of P_{B_0}. We conclude that there exists a simple factor of B_0 over $\mathbb{F}_q$ with Frobenius conjugate to π by Corollary 35.1.

37 Local invariants at p (04/19/2024)

37.1 Dieudonné theory

We will only be able to give a brief outline of the local invariants at p that we ignored in our proof of the Honda-Tate theorem, specifically in Theorem 35.4. See [CCO14, A.1,§1] and [CO19] if you are interested in more about Dieudonné theory and p-divisible groups. Let $D = \mathrm{End}^0(A)$ for an abelian variety A/k with k a perfect field of characteristic $p > 0$. The p-divisible group $A[p^\infty]$ is the inductive system $\{A[p^n]\}_{n \geq 1}$, where each $A[p^n]$ is a finite group scheme over k with a natural embedding $A[p^n] \hookrightarrow A[p^{n+1}]$ identifying $A[p^n]$ with the kernel of $[p^n] : A[p^{n+1}] \to A[p^{n+1}]$.

Theorem 37.1. *(Tate, see also Milne-Waterhouse.)* Let A, B be abelian varieties over a finite field. Then $\mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}(A[p^\infty], B[p^\infty])$ is an isomorphism.

Theorem 37.2. *(Dieudonné theory.)* Let k be a perfect field of positive characteristic p, and let $W := W(k)$ be its ring of Witt vectors.[a] There is a (dual)[b] equivalence of categories between:

- p-divisible groups
- Dieudonné modules, i.e. finite rank free W-modules with semilinear actions by Frobenius F and Vershiebung V, subject to the relation $FV = VF = p$.[c] The Frobenius action on k lifts uniquely to an action σ on $W(k)$. The semilinearity requirement is that F is σ-linear and V is σ^{-1}-linear, i.e. $F(ax) = a^{\sigma}F(x)$ and $V(ax) = a^{\sigma^{-1}}V(x)$ for $a \in W(k)$, x an element of the Dieudonné module.

We write $X \rightsquigarrow \mathbb{D}(X)$ for the (contravariant) Dieudonné functor. This functor is Frobenius- and Verschiebung-equivariant, and satisfies other various nice compatibilites.

[a] We won't define these here, but the Witt vectors are a natural lifting of k to a characteristic 0 complete DVR with residue field k. An important example is that for $q = p^n$, $W(\mathbb{F}_q)$ is the ring of integers of the unique degree n unramified extension of $\mathbb{Q}_p$.

[b] There are covariant and contravariant versions of the Dieudonné functors; both define equivalences of categories. We will use the contravariant version.

[c] We showed that $[p]$ factors through $F = F^{(1)} : A \to A^{(1)}$ on abelian varieties; this is also true for p-divisible groups. The Vershiebung is the morphism $V : A^{(1)} \to A$ such that $V \circ F = [p]$.

Remark 37.3. Some more details on p-divisible groups: we will always have a inductive (a.k.a directed) system of finite groups schemes $\{X_n, \iota_n\}_{n \geq 0}$ of rank p^{nh} for some fixed h (called the *height*) with $\iota_n : X_n \hookrightarrow X_{n+1}$ a closed embedding. We additionally require $[p] : X_n \to X_n$ to factor as $\pi_n \circ \iota_{n-1}$ for a faithfully flat map $\pi_n : X_n \to X_{n-1}$.

Let A/k be an abelian variety with $D = \mathrm{End}^0(A)$ with Frobenius π, and recall that $\mathbb{Q}(\pi) =: K$ is a number field. Using Dieudonné theory, we have $D \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathrm{End}(\mathbb{A}[p^\infty])^{\mathrm{opp}} \otimes W[1/p]$, and $\mathbb{Q}_p \otimes_{\mathbb{Q}} K = \prod_{v|p} K_v$ gives a decomposition $A[p^\infty] \sim \prod_{v|p} G_v$ in the isogeny category. We correspondingly get

$$\mathbb{D}(A[p^\infty]) \otimes_W W[1/p] = \bigoplus_{v|p} \mathbb{D}(G_v) \otimes_W W[1/p]$$

Now set $D_v := D \otimes_K K_v = \mathrm{End}(\mathbb{D}(G_v) \otimes_W W[1/p])^{\mathrm{opp}}$. These are $W[1/p]$ linear maps of the $W[1/p]$-vector space $\mathbb{D}(G_v) \otimes_W W[1/p]$ compatible with the Frobenius action.

Let $g \in \mathbb{Z}[t]$ be the minimal polynomial of π_A, so that $g = \prod_{v|p} g_v$ in $\mathbb{Q}_p[t]$ for the minimal polynomial g_v of π_A in K_v. Then π_A acts on $\mathbb{D}(A[p^\infty])$ as F^r, where $q = p^r$, and we claim:

Theorem 37.4. $\mathrm{inv}_v(D_v)$ is the same as the local invariant of $W[1/p][F]/(g_v(F^r))$, which is $\frac{v(\pi)}{v(q)}[K_v : \mathbb{Q}_p]$.

This is the local invariant we were hunting in our proof of the Honda-Tate theorem; we'll leave this at that.

37.2 Proof of Main Theorem: tori

We will spend the remainder of the course proving the Main Theorem of Complex Multiplication. Our presentation generally follows that of [Mil10]

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, E^*)$, or really $\sigma \in \mathrm{Gal}(E^{*,\mathrm{ab}}/E^*)$, pick $s \in \mathbb{A}_{E^*,f}^\times / E^{*,\times}$ mapping to σ under the Artin map, i.e. with $\mathrm{Art}_{E^\times}(s) = \sigma|_{E^{*,\mathrm{ab}}}$. We defined elements $\eta(\sigma) \in \mathbb{A}_{E,f}^\times$ and $N_\Phi(s) \in \mathbb{A}_{E,f}^\times / E^\times$. Recall that the claim of the Main Theorem of Complex Multiplication is that these two elements are the same modulo $E^\times$.

For a number field K, we notate $T^K = \mathrm{Res}_{\mathbb{Q}}^K \mathbb{G}_m$, which is an algebraic torus over $\mathbb{Q}$. Recall that T^K is the $\mathbb{Q}$-scheme representing the functor of points $R \rightsquigarrow (R \otimes_{\mathbb{Q}} K)^\times$ for $\mathbb{Q}$-algebras R.

Definition 37.1. Let F be the maximal totally real subfield of E. Then set $T := \mathbb{G}_m \times_{T^F} T^E$:

$$\begin{array}{ccc} T & \longrightarrow & T^E \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Nm}_{E/F}} \\ \mathbb{G}_m & \longrightarrow & T^F. \end{array}$$

Here $\mathrm{Nm}_{E/F} : T^E \to T^F$ is the group scheme homomorphism induced on points via

$$(R \otimes_{\mathbb{Q}} E)^\times \to (R \otimes_{\mathbb{Q}} F)^\times : r \otimes x \mapsto r \otimes \mathrm{Nm}_{E/F}(x),$$

and the homomorphism $\mathbb{G}_m \to T^F$ is given by the inclusion $R^\times \hookrightarrow (R \otimes_{\mathbb{Q}} F)^\times$.

More concretely, we can identify the functor of points of T as

$$T(R) = \{r \in (R \otimes_{\mathbb{Q}} E)^\times : \mathrm{Nm}_{E/F}(r) \in R^\times\}$$

for $\mathbb{Q}$-algebras R, so in particular

$$T(\mathbb{Q}) = \{a \in E^\times : \mathrm{Nm}_{E/F}(a) \in \mathbb{Q}^\times\}$$
$$T(\mathbb{A}_f) = \{a \in \mathbb{A}_{E,f}^\times : \mathrm{Nm}_{E/F}(a) \in \mathbb{A}_f^\times\}.$$

We topologize $T(\mathbb{A}_f)$ by its subspace topology in $\mathbb{A}_{E,f}^\times$ using this description of $T(\mathbb{A}_f)$ as a subset of $\mathbb{A}_{E,f}^\times$. The reason why we bother with all of this is that we can look at idèlic points on T rather than attempting to directly analyze idèles. This is useful because $T(\mathbb{A}_f)/T(\mathbb{Q})$ is much nicer than $\mathbb{A}_{E,f}^\times / E^\times$ due to the following:

Lemma 37.5.

1. The map $T \to T^E$ induces an injective map $T(\mathbb{A}_f)/T(\mathbb{Q}) \to T^E(\mathbb{A}_f)/T^E(\mathbb{Q}) = \mathbb{A}_{E,f}^\times/E^\times$, and a closed embedding as a topological subspace.
2. $T(\mathbb{A}_f)/T(\mathbb{Q})$ is Hausdorff.

Therefore, to see that two elements in $T(\mathbb{A}_f)/T(\mathbb{Q})$ are the same, we can compare them using arbitrarily small open neighborhoods $U \subseteq \mathbb{A}_{E,f}^\times$.

Note that $\mathbb{A}_{E,f}^\times/E^\times$ is not itself Hausdorff—omitting the archimedean places means that $E^\times$ is no longer a discrete subgroup. If we include the archimedean places, then $\mathrm{Art} : \mathbb{A}_E^\times/E^\times \to \mathrm{Gal}(E^{\mathrm{ab}}/E)$ is not injective.

Proof. 1. The map $T \to T^E$ is defined using polynomials over $\mathbb{Q}$, so if we have $x \in T(\mathbb{A}_f)$ with x mapping to $T^E(\mathbb{Q})$, then $x \in T(\mathbb{Q})$. The topological assertion is an easy check.

2. We prove $T(\mathbb{Q}) \subseteq T(\mathbb{A}_f)$ is discrete; since $T(\mathbb{Q})$ is also closed, this implies that $T(\mathbb{A}_f)/T(\mathbb{Q})$ is Hausdorff. Since $T(\mathbb{A}_f)$ is Hausdorff, it suffices to show that there is an open subset U of $T(\mathbb{A}_f)$ such that $T(\mathbb{Q}) \cap U$ is finite. We take $U = \mathcal{O}_E^\times$, which is open in $T(\mathbb{A}_f)$. By the Dirichlet unit theorem, $\mathcal{O}_F^\times$ has finite index in $\mathcal{O}_E^\times$—the signatures of F and E are $([F:\mathbb{Q}], 0)$ and $(0, [F:\mathbb{Q}])$, respectively, so the free parts of $\mathcal{O}_F^\times$ and $\mathcal{O}_E^\times$ both have rank $[F:\mathbb{Q}] - 1$ by Dirichlet. Therefore $T(\mathbb{Q}) \cap \mathcal{O}_E^\times$ is finite iff $T(\mathbb{Q}) \cap \mathcal{O}_F^\times$ is finite, so it suffices to show that the latter is finite. We have

$$T(\mathbb{Q}) \cap \mathcal{O}_F^\times = \{a \in \mathcal{O}_F^\times : \mathrm{Nm}_{E/F}(a) \in \mathbb{Q}^\times\}$$

However, the restriction of the norm map $\mathrm{Nm}_{E/F}$ to $F^\times$ is just squaring, so the requirement is that $a^2 \in \mathbb{Q}^\times$. Since a is a totally real unit, this implies $a^2 = 1$, hence $a = \pm 1$ and so $|T(\mathbb{Q}) \cap \mathcal{O}_F^\times| = 2$.

■

38 Proof of the Main Theorem: preliminaries (04/22/2024)

Recall our conventions: E is a CM field with reflex field E^* and maximal totally real subfield F, $T^E = \mathrm{Res}_{\mathbb{Q}}^E \mathbb{G}_m$, and $T := \mathbb{G}_m \times_{T_F} T^E$. Let A be an abelian variety with CM by E. Also recall a key fact we have used repeatedly: $\hat{V}(A)$ is a rank 1 free $\mathbb{A}_{E,f}$-module.

38.1 Proof the main theorem: norms

Lemma 38.1. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$ and $s \in \mathbb{A}_{E^*,f}^\times/(E^*)^\times$ such that $\mathrm{Art}(s) = \sigma|_{E^{*,\mathrm{ab}}}$. Pick an isogeny $\alpha : A \to {}^\sigma A$, and let $\eta = \eta(\sigma) \in \mathbb{A}_{E,f}^\times$ be such that $\alpha(\eta(x)) = \sigma x$ for all $x \in \hat{V}(A)$.
Then $\frac{\eta(\sigma)}{N_\Phi(s)} \in T(\mathbb{A}_f)/T(\mathbb{Q}) \subseteq T^E(\mathbb{A}_f)/T^E(\mathbb{Q})$.

Recall that we ultimately wish to show that $\eta(\sigma) = N_\Phi(s) \bmod E^\times$, so Lemma 38.1 is a partial result in this direction.

Proof. We take advantage of the polarization ψ. Using the same computations and notation as in Remark 31.6, we have

$$\begin{aligned}\chi_{\text{cyc}}(\sigma)\psi(x,y) &= {}^{\sigma}\psi(\sigma x, \sigma y)\\ &= {}^{\sigma}\psi(\alpha(\eta(x)), \alpha(\eta(y)))\\ &= {}^{\sigma}\psi(\eta(\sigma)\overline{\eta(\sigma)}\alpha x, \alpha y).\end{aligned}$$

Both ψ and ${}^{\sigma}\psi(\alpha(-),\alpha(-))$ are polarizations on $A/\overline{\mathbb{Q}}$ compatible with the E-action. In the complex analytic setting, these correspond to two different Riemann forms on $A/\mathbb{C}$. From our discussion of Riemann forms over $\mathbb{C}$ with compatible E-action (all the way back in Lemma 6.4), we know that these are both of the form $\text{tr}_{E/\mathbb{Q}}(\xi\overline{x}y)$ for a totally imaginary $\xi \in E$, treating the Riemann form as a form on $H_1(A(\mathbb{C}),\mathbb{Q}) \simeq E$. Changing the polarization is equivalent to changing ξ by a totally positive element $b \in E$, necessarily lying in F. This implies that $\eta(\sigma)\overline{\eta(\sigma)} = \chi_{\text{cyc}}(\sigma)\cdot b$ for some totally positive $b \in F$. On the other hand, Corollary 31.3 implies

$$N_\Phi(s)\overline{N_\Phi(s)} = \text{Nm}_{\mathbb{A}_{E^*,f}/\mathbb{A}_f}(s) \equiv \sigma|_{\mathbb{Q}^{\text{ab}}} \bmod \mathbb{Q}^\times \equiv \chi(\sigma) \bmod \mathbb{Q}^\times$$

where we use the Kronecker-Weber theorem $\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_\infty)$ to observe that $\sigma|_{\mathbb{Q}^{\text{ab}}}$ acts through the cyclotomic character, which we may identify as having image in $\widehat{\mathbb{Z}}^\times \subset \mathbb{A}_f^\times$ acting on $\mu_\infty \simeq \widehat{\mathbb{Z}}$. By positivity, we know that the ambiguity $\frac{\sigma|_{\mathbb{Q}^{\text{ab}}}}{N_\Phi(s)\overline{N_\Phi(s)}}$ actually lies in $\mathbb{Q}^\times_{>0}$.

Write $t := \frac{\eta(\sigma)}{N_\Phi(s)}$. Then our work shows that $t\cdot\bar{t}$ is a totally positive element of $F^\times \hookrightarrow \mathbb{A}_{E,f}^\times$. We cite:

Theorem 38.2. *(Hasse Norm Theorem.)* Let L/K be a cyclic extension of number fields. If $x \in K$ is a local norm at all places, i.e. for all places v of K and all places $w \mid v$ of L, there exists $y_w \in L_w$ such that $\text{Nm}_{L_w/K_v}(y_w) = x$, then x is in fact a global norm, i.e. there exists $y \in L$ such that $\text{Nm}_{L/K}(y) = x$.

Proof. See [Mil86, §VIII, Thm. 3.1]. ∎

The element t is, a priori, an element lying in $\mathbb{A}_{E,f}^\times$, so $t\cdot\bar{t}$ is visibly a local norm at all finite places. Since we've also shown that $t\cdot\bar{t}$ is totally positive, $t\cdot\bar{t}$ is also a local norm at all archimedean places—an element of $\mathbb{R}^\times$ is a norm from $\mathbb{C}^\times$ if and only it is positive. Since E/F is cyclic of degree 2, by Theorem 38.2 there exists $e \in E$ such that $e\bar{e} = t\bar{t}$. We conclude $t \bmod E^\times \in T(\mathbb{A}_f)/T(\mathbb{Q})$, since t/e has norm $1 \in \mathbb{A}_f^\times$. ∎

Indeed, by definition, we already know that $N_\Phi(s)$ lies in $T(\mathbb{A}_f)/T(\mathbb{Q})$. Lemma 38.1 then shows that $\eta : \text{Gal}(\overline{\mathbb{Q}}/E^*) \to \mathbb{A}_{E,f}^\times/E^\times$ factors through $\text{Gal}(E^{*,\text{ab}}/E^*) \to T(\mathbb{A}_f)/T(\mathbb{Q}) \to \mathbb{A}_{E,f}^\times/E^\times$.

38.2 Review of ray class groups

See also [Mil20, §V.1, §V.4]; note that when we refer to a "prime," we mean a finite prime, whereas Milne allows this to refer to an arbitrary place.

Let K be a totally imaginary number field. A *modulus* $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ is a product of finitely many prime[26] ideals in $\mathcal{O}_K$. We let $S(\mathfrak{m})$ denote the support of $\mathfrak{m}$, i.e. those $\mathfrak{p}$ such that $\mathfrak{m}(\mathfrak{p}) > 0$, and we let $I^{S(\mathfrak{m})}$ be the subgroup of the group of fractional ideals coprime to $S(\mathfrak{m})$.

Definition 38.1. The *ray class group* is

$$C_{\mathfrak{m}}(K) := I^{S(\mathfrak{m})}/K_{\mathfrak{m},1},$$

where

$$K_{\mathfrak{m},1} := \{a \in K^\times : a_{\mathfrak{p}} \in 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_{K_{\mathfrak{p}}}\},$$

which we map inside $I^{S(\mathfrak{m})}$ by taking principal ideals. The subgroup $K_{\mathfrak{m},1} \subseteq K^\times$ should be thought of as elements that are sufficiently $\mathfrak{p}$-adically close to 1 for all $\mathfrak{p}$; exactly how close is dictated by the multiplicity of $\mathfrak{p}$ in S. If $\mathfrak{p} \notin S(\mathfrak{m})$, i.e. $\mathfrak{m}(\mathfrak{p}) = 0$, then there are no conditions at $\mathfrak{p}$. We also define an idèlic analogue of $K_{\mathfrak{m},1}$:

$$\mathbb{A}^\times_{K,\mathfrak{m}} := \prod_{v \nmid \mathfrak{m}}{}' K_v^\times \times \prod_{v|\mathfrak{m}} 1 + \mathfrak{p}_v^{\mathfrak{m}(\mathfrak{p}_v)}\mathcal{O}_{K_{\mathfrak{p}_v}}$$

where as usual the primed summation notation means that all but finitely many components lie in $\mathcal{O}_v^\times$. We also write

$$W_{\mathfrak{m}}(K) = \prod_{v \nmid \mathfrak{m}, v|\infty} K_v^\times \times \prod_{v|\mathfrak{m}} (1 + \mathfrak{p}_v^{\mathfrak{m}(\mathfrak{p}_v)}\mathcal{O}_K) \times \prod_{v \nmid \mathfrak{m}, v \nmid \infty} \mathcal{O}_{K_v}^\times,$$

which is an open subgroup of $\mathbb{A}^\times_{K,\mathfrak{m}} \subseteq \mathbb{A}^\times_K$. We can re-express the ray class groups as

$$C_{\mathfrak{m}}(K) = \mathbb{A}^\times_{E,\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} = \mathbb{A}^\times_{E,\mathfrak{m},f}/U_{\mathfrak{m}} \cdot K_{\mathfrak{m},1},$$

where $U_{\mathfrak{m}}(K) = \prod_{v|\mathfrak{m}}(1 + \mathfrak{p}_v^{\mathfrak{m}(\mathfrak{p}_v)}\mathcal{O}_K) \times \prod_{v \nmid \mathfrak{m}, v \nmid \infty} \mathcal{O}_{K_v}^\times$.

Finally, if $\mathfrak{m} = (m)$ for an integer m, then we will also use the notation $K_{m,1}, \mathbb{A}^\times_{K,m}$, etc.

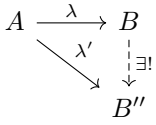
The ray class groups are all finite, and the images of the sets $\{U_m(E) \cap T(\mathbb{A}_f)\}_{m \in \mathbb{Z}_{>0}}$ form a basis of open neighborhood of the identity in $T(\mathbb{A}_f)/T(\mathbb{Q})$. The maps $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) \to \mathbb{A}^\times_{E,f}/E^\times$ and $N_\Phi : \mathbb{A}^\times_{E^*,f}/(E^*)^\times \to \mathbb{A}^\times_{E,f}/E^\times$ are continuous, so for any m their compositions with $\mathbb{A}^\times_{E,f} \to C_m(E)$ have open finite index kernel.

38.3 $\mathfrak{a}$-multiplication

Definition 38.2. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_E \subseteq \mathrm{End}(A)$. A surjective homomorphism $\lambda : A \to B$ is said to be an $\mathfrak{a}$-*multiplication* if:

1. For all $a \in \mathfrak{a}$, the homomorphism $a : A \to A$ factors uniquely through $\lambda : A \to B$.
2. The homomorphism λ is universal for this property, meaning that if $\lambda' : A \to B'$ also satisfies (1), then there exists a unique map $B' \to B$ making the diagram commute:

[26] Since K is totally imaginary we need not worry about archimedean places.



Fact: for every ideal $\mathfrak{a} \subseteq \mathcal{O}_E$, there exists an abelian variety B and an $\mathfrak{a}$-multiplication $\lambda : A \to B$. More specifically, $B = A/\ker(\mathfrak{a})$ where

$$\ker(\mathfrak{a}) := \bigcap_{a \in \mathfrak{a}} \ker(a).$$

(This intersection may be taken to be finite since $\mathfrak{a}$ is finitely generated.) We can also write $B = A \otimes_{\mathcal{O}_E} \mathfrak{a}^{-1}$.

38.4 Statement of the ideal-theoretic version of the Main Theorem

We will first prove a version of the Main Theorem stated in terms of ray class groups rather than idèles, and from this we will eventually deduce the idèlic version. For a modulus $\mathfrak{m}$ of a field K, we let $L_{\mathfrak{m}}$ denote the ray class field for the modulus $\mathfrak{m}$ and we let

$$\mathrm{rec}_{K,\mathfrak{m}} : C_{\mathfrak{m}}(K) \to \mathrm{Gal}(L_{\mathfrak{m}}/K)$$

denote the ideal-theoretic version of the Artin map for the modulus $\mathfrak{m}$, again normalized to send a geometric Frobenius to its corresponding prime.

Theorem 38.3. *(Shimura-Taniyama Main Theorem of Complex Multiplication, ideal-theoretic version.)* Let $A/\overline{\mathbb{Q}}$ have CM by (E, Φ). Assume[a] that $\mathrm{End}(A) \cap E = \mathcal{O}_E$. Fix $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$ and $m \in \mathbb{Z}_{>0}$, where E^* is the reflex field.
Then

1. There exists an ideal $\mathfrak{a}(\sigma)$ of $\mathcal{O}_E$, coprime to m, and an isogeny $\alpha : A \to {}^{\sigma}A$ such that $\alpha(x) = \sigma(x)$ for all $x \in A[m]$ and α is a $\mathfrak{a}(\sigma)$-multiplication. Moreover, the class $[\mathfrak{a}(\sigma)]$ in $C_m(E)$ is uniquely determined by σ.

2. For a sufficiently divisible modulus $\mathfrak{m}$ of E^*, $[\mathfrak{a}(\sigma)]$ only depends on $\sigma|_{L_{\mathfrak{m}}}$. More specifically, for such $\mathfrak{m}$ we have $[\mathfrak{a}(\sigma)] = [N_\Phi(\mathfrak{a}^*)^{-1}]$, where $[\mathfrak{a}^*] \in C_{\mathfrak{m}}(E^*)$ is the ideal class such that $\mathrm{rec}_{E^*,\mathfrak{m}}([\mathfrak{a}^*]) = \sigma|_{L_{\mathfrak{m}}}$.

[a] This assumption is harmless because there is always a representative of the isogeny class of A with this property, and the theorem will be invariant under isogeny.

39 Finishing the proof of Main Theorem (04/24/2024)

39.1 Properties of $\mathfrak{a}$-multiplication

We will omit some details about the Serre tensor construction, which is apparently mostly formal and not hard in characteristic 0. Here is the definition:

Definition 39.1. *(Serre tensor construction, CM case.)* Let A/k be an abelian variety with CM by a field E, and assume that $\mathcal{O}_E \subset \mathrm{End}(E)$. Then for a fractional ideal $\mathfrak{a}$ of E we

denote by $A \otimes_{\mathcal{O}_E} \mathfrak{a}$ the scheme representing the functor $S \rightsquigarrow A(S) \otimes_{\mathcal{O}_E} \mathfrak{a}$ for k-schemes S.

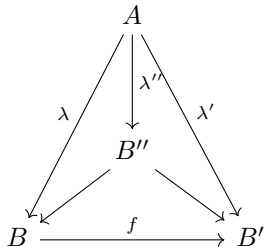
That is, we treat A as an $\mathcal{O}_E$-module, so that the idea of tensoring with another $\mathcal{O}_E$-module makes sense. Fact: $A \otimes_{\mathcal{O}_E} \mathfrak{a}$ always exists, i.e. the given functor is representable. See also [Mil10, §II.7] and [CCO14, §1.7.4] for more details.

Let A have CM type (E, Φ) and let $\mathcal{O}_E \subseteq \mathrm{End}(A)$. If $\lambda : A \to B$ is an $\mathfrak{a}$-multiplication, then $B \simeq A/\ker(\mathfrak{a})$, which is also isomorphic to $A \otimes_{\mathcal{O}_E} \mathfrak{a}^{-1}$. If $A = \mathbb{C}^g/\Phi(\Lambda)$, then we can write $B = \mathbb{C}^g/\Phi(\mathfrak{a}^{-1}\Lambda)$.

Proposition 39.1. Let $\lambda : A \to B$ and $\lambda' : A \to B'$ be $\mathfrak{a}$- and $\mathfrak{a}'$-multiplications, respectively. Then there is an E-isogeny $f : B \to B'$ such that $f \circ \lambda = \lambda'$ if and only if $\mathfrak{a} \supseteq \mathfrak{a}'$. In particular, there exists an E-isomorphism $f : B \to B'$ with $f \circ \lambda = \lambda'$ if and only if $\mathfrak{a} = \mathfrak{a}'$.

Proof. If $\mathfrak{a} \supseteq \mathfrak{a}'$, then the existence of f is immediate from the universal property of λ'.

Conversely, suppose such f exists. Then choose an $\mathfrak{a} + \mathfrak{a}'$-multiplication $\lambda'' : A \to B''$. We have $\lambda'' \circ a = \lambda''$ for either $a \in \mathfrak{a}$ or $a \in \mathfrak{a}'$, so by the universal property of λ and λ' we get unique morphisms $B'' \to B$ and $B'' \to B'$ making the upper-left and upper-right triangles in the diagram commute:



Note that the outer triangle commutes by assumption. We deduce that the bottom triangle, hence the entire diagram, commutes by chasing universal property.

The diagram shows the inclusion

$$\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a} + \mathfrak{a}')} = \ker(B'' \to B) \subseteq \ker(B'' \to B') = \frac{\ker \mathfrak{a}'}{\ker(\mathfrak{a} + \mathfrak{a}')}.$$

But this implies that $\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a}+\mathfrak{a}')}$ is trivial: we have $\ker(\mathfrak{a}) \cap \ker(\mathfrak{a}') = \ker(\mathfrak{a} + \mathfrak{a}')$, hence $\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a}+\mathfrak{a}')} \cap \frac{\ker \mathfrak{a}'}{\ker(\mathfrak{a}+\mathfrak{a}')} = 0$, hence $\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a}+\mathfrak{a}')} \subseteq \frac{\ker \mathfrak{a}'}{\ker(\mathfrak{a}+\mathfrak{a}')}$ implies $\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a}+\mathfrak{a}')} = 0$. Equivalently, $B'' \to B$ is injective, which implies $\mathfrak{a} \subseteq \mathfrak{a}'$. ∎

Proposition 39.2. If $\lambda : A \to A', \lambda' : A' \to A''$ are $\mathfrak{a}$- and $\mathfrak{a}'$-multiplications respectively, then $\lambda' \circ \lambda : A \to A''$ is an $\mathfrak{a}\mathfrak{a}'$-multiplication.

Proof. Omitted; the idea is that we write $A' = A \otimes_{\mathcal{O}_E} \mathfrak{a}^{-1}$. ∎

Proposition 39.3. If λ is an $\mathfrak{a}$-multiplication, then $\deg \lambda = [\mathcal{O}_E : \mathfrak{a}]$.

Proof. (Sketch.) The idea is that over $\mathbb{C}$, we use $\deg \lambda = [\mathfrak{a}^{-1}\Lambda : \Lambda] = [\mathcal{O}_E : \mathfrak{a}]$. In general, for $a \in \mathcal{O}_E$, we first note that $[a] : A \to A$ is an (a)-multiplication of degree

$$[\mathcal{O}_E : (a)].$$

Then we use the principal case to get the general one by finding λ' with degree coprime to λ such that $\lambda' \circ \lambda = [a]$. ■

Proposition 39.4. Let $A, B/\overline{\mathbb{Q}}$ have CM by E with $\mathcal{O}_E \subseteq \mathrm{End}(A), \mathrm{End}(B)$. If there exists an E-isogeny $A \to B$, then there exists an ideal $\mathfrak{a} \subseteq \mathcal{O}_E$ and an E-isogeny $A \to B$ that is also an $\mathfrak{a}$-multiplication.

Proof. Proof idea: We may assume $A, B/\mathbb{C}$, so that $A(\mathbb{C}) = \mathbb{C}^g/\Phi(\mathfrak{b}_1)$ and $B(\mathbb{C}) = \mathbb{C}^g/\Phi(\mathfrak{b}_2)$ for fractional ideals $\mathfrak{b}_1, \mathfrak{b}_2$ of E. We can adjust $\mathfrak{b}_1$ by multiplying in elements in E in order to arrange $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$, so we get an E-quasi-isogeny $A \to B$ that is a $\mathfrak{b}_1\mathfrak{b}_2^{-1}$-multiplication with $\mathfrak{b}_1\mathfrak{b}_2^{-1} \subseteq \mathcal{O}_E$ an integral ideal. ■

Proposition 39.5. Let A, B be E-isogenous CMAVs over a number field K with with $\mathcal{O}_E \subseteq \mathrm{End}(A), \mathrm{End}(B)$ with good reduction at a prime $\mathfrak{p}$ of K. Let A_0, B_0 denote their reductions modulo $\mathfrak{p}$.

1. The reduction $\lambda_0 : A_0 \to B_0$ of any $\mathfrak{a}$-multiplication $\lambda : A \to B$ is another $\mathfrak{a}$-multiplication.
2. Let $\lambda_0 : A_0 \to B_0$ be an E-isogeny. Then λ_0 lifts to an $\mathfrak{a}$-multiplication $\lambda : A \to B$ for some ideal $\mathfrak{a} \subseteq \mathcal{O}_E$ after taking a finite extension of K. Hence by part (1), λ_0 is also an $\mathfrak{a}$-multiplication after taking a finite extension.

Proof. 1. Let $a \in \mathfrak{a}$. Then there exists a unique α such that $a = \alpha \circ \lambda$ by the definition of $\mathfrak{a}$-multiplication:

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & B \\ & \searrow^{a} & \downarrow{\scriptstyle \exists!\alpha} \\ & & A \end{array}$$

The maps λ, α, a all extend uniquely to the Néron models $\mathscr{A}, \mathscr{B}$ of A_0, B_0 over $\mathcal{O}_{K_\mathfrak{p}}$, giving a diagram

$$\begin{array}{ccc} \mathscr{A} & \xrightarrow{\lambda} & \mathscr{B} \\ & \searrow^{a} & \downarrow{\scriptstyle \exists!\alpha} \\ & & \mathscr{A} \end{array}$$

and by the Néron mapping property this diagram descends uniquely to diagram

$$\begin{array}{ccc} A_0 & \xrightarrow{\lambda_0} & B_0 \\ & \searrow^{a} & \downarrow{\scriptstyle \exists!\alpha_0} \\ & & A_0 \end{array}$$

Since this holds for any $a \in \mathfrak{a}$, we conclude $\lambda_0 : A_0 \to B_0$ satisfies the universal property of $\mathfrak{a}$-multiplication.

2. (Sketch.) Proposition 39.4 tells us that there exists some $\mathfrak{b}$-multiplication $\lambda' : A \to B$ for some ideal $\mathfrak{b} \subseteq \mathcal{O}_E$ after possibly taking a finite extension of K. By part (1), its reduction λ_0' is also a $\mathfrak{b}$-multiplication. By properties of the Serre tensor construction, we have $\mathrm{Hom}_{\mathcal{O}_E}(A, B) \simeq \mathfrak{b}^{-1}$ with the isomorphism given by sending $\lambda' \mapsto 1$, and likewise $\mathrm{Hom}_{\mathcal{O}_E}(A_0, B_0) \simeq \mathfrak{b}^{-1}$ by sending $\lambda_0' \mapsto 1$. Hence the reduction map

$$\mathrm{Hom}_{\mathcal{O}_E}(A, B) \to \mathrm{Hom}_{\mathcal{O}_E}(A_0, B_0)$$

is an isomorphism. Thus any given $\mathcal{O}_E$-isogeny $\lambda_0 : A_0 \to B_0$ lifts to an isogeny $\lambda : A \to B$, which is an $\mathfrak{a}$-multiplication for some ideal $\mathfrak{a}$.

Proposition 39.6. Let $\alpha : A \to B$ be an $\mathfrak{a}$-multiplication, and choose identifications $\hat{T}(A) \simeq \hat{T}(B) \simeq \prod_{v \nmid \infty} \mathcal{O}_{E_v}$, which is unique up to multiplication by $\prod_{v \nmid \infty} \mathcal{O}_{E_v}^\times$. Then under this identification, $\alpha : \hat{T}(A) \to \hat{T}(B)$ is given by multiplication by an element $x \in \mathbb{A}_{E,f}^\times$ with $v(x) = v(\mathfrak{a})$ for all finite places v of E.

Proof. The universal property of $\mathfrak{a}$-multiplication tells us that $a : A \to A$ factors through α. Take some identification $\hat{T}(A) \simeq \hat{T}({}^\sigma A) \simeq \prod_{v \nmid \infty} \mathcal{O}_{E_v}$, the choice of which is unique up to a multiple of $\prod_{v \nmid \infty} \mathcal{O}_{E_v}^\times$. Then, up to a multiple of $\prod_{v \nmid \infty} \mathcal{O}_{E_v}^\times$, we may identify $a : \hat{T}(A) \to \hat{T}({}^\sigma A)$ with multiplication by its image in $\prod_{v \nmid \infty} \mathcal{O}_{E_v}$. Therefore, α acts by some element dividing a in $\prod_{v \nmid \infty} \mathcal{O}_{E_v}$. Since this is true for all $a \in \mathfrak{a}$, we conclude that α acts by an element $x \in \mathbb{A}_{E,f}^\times$ with $v(x) \leq \min_{a \in \mathfrak{a}}\{v(a)\} = v(\mathfrak{a})$ for all finite places v. Conversely, we know from Proposition 39.3 that α has degree $[\mathcal{O}_E : \mathfrak{a}]$. If an isogeny has degree d, then its determinant on T_ℓ (as a $\mathbb{Q}_\ell$-linear map) has valuation $v_\ell(d)$. Therefore $[\mathcal{O}_E : \mathfrak{a}]_\ell = \det_{\mathbb{Q}_\ell}(T_\ell(\alpha))_\ell = \prod_{v|\ell} \#k_v^{v(x)}$, where $\#k_v$ denotes the order of the residue field of the place v. But we also have the formula

$$[\mathcal{O}_E : \mathfrak{a}]_\ell = \prod_{v|(\ell)} \#k_v^{v(\mathfrak{a})},$$

so by comparing the two expressions we conclude the inequality $v(x) \leq v(\mathfrak{a})$ must actually be an equality for all places v. ∎

∎

See [Mil10, §II.7] for more details on the properties of $\mathfrak{a}$-multiplication.

39.2 Proof of ideal-theoretic Main Theorem part (1)

After all this setup, we can prove Theorem 38.3. By Proposition 39.4, there exists an ideal $\mathfrak{a} = \mathfrak{a}(\sigma)$, with $\mathfrak{a}$ depending on σ, such that there exists an $\mathfrak{a}$-multiplication

$$\alpha : A \to {}^\sigma A$$

compatible with the E-action. By Proposition 39.3, $\deg(\alpha) = [\mathcal{O}_E : \mathfrak{a}]$. We may choose $a \in \mathfrak{a}^{-1}$ such that $[\mathcal{O}_E : a\mathfrak{a}]$ is prime to m. Then $a\alpha : A \to {}^{\sigma}A$ is an $(a\mathfrak{a})$-multiplication, an E-isogeny, and of degree coprime to m, so without loss of generality we may choose $\mathfrak{a}$ and α with $\deg \alpha = [\mathcal{O}_E : \mathfrak{a}]$ coprime to m.

Therefore $\mathfrak{a}$ defines a class in $C_m(E)$ and $\alpha : A[m] \to {}^{\sigma}A[m]$ is an isomorphism; we also know that $\sigma : A[m] \to {}^{\sigma}A[m]$ is an isomorphism. The fact that $\hat{V}(A)$ is a rank 1 free $\mathbb{A}_{E,f}$-module implies that $A[m]$ is a rank 1 free $\mathcal{O}_E/(m)$-module, which implies that any two $\mathcal{O}_E$-endomorphisms differ by some element of $\mathcal{O}_E$. We conclude that there exists some $b \in \mathcal{O}_E$, coprime to m, such that $(\alpha \circ b)|_{A[m]} = \sigma|_{A[m]}$. Therefore, replacing α with $\alpha \circ b$ and $\mathfrak{a}$ with $b\mathfrak{a}$, we may further assume that $\alpha|_{A[m]} = \sigma|_{A[m]}$.

We know that any two E-isogenies α, α' differ by an element of $E^{\times}$. However, only multiplication by elements of $E_{m,1}$ will preserve the property $\alpha|_{A[m]} = \sigma|_{A[m]}$, since these are precisely the elements of $E^{\times}$ that act by 1 on $A[m]$. We require $\mathfrak{a}$ to induce this property, so we conclude that all choices for $\mathfrak{a}$ with this property differ by an element in $E_{m,1}$. Therefore, we have produced a canonical ideal class $[\mathfrak{a}(\sigma)]$ in $I^{S(m)}/E_{m,1} = C_m(E)$ that depends only on σ. This is part (1) of Theorem 38.3.

39.3 Ideal-theoretic Shimura-Taniyama formula

We will need to determine the ideal class $[\mathfrak{a}(\sigma)] \in C_m(E)$ in terms of σ. The key to doing this is the Shimura-Taniyama formula! We prove a formula for $[\mathfrak{a}(\sigma)]$ when σ is a Frobenius element associated to some prime $\mathfrak{P}/\mathfrak{p}$ in K/E^*. Since the Frobenii exhaust any given finite Galois group by the Chebotarev density theorem, this will let us identify $[\mathfrak{a}(\sigma)]$ in general.

Theorem 39.7. *(Shimura-Taniyama Formula, ideal-theoretic version.)* Let A/K have CM by (E, Φ), let K be Galois and contain all Galois conjugates of E, and assume $\mathcal{O}_E \subseteq \mathrm{End}(A)$. Let $\mathfrak{P}/\mathfrak{p}/p$ be primes of $K/E^*/\mathbb{Q}$ such that $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified, and assume A has good reduction at $\mathfrak{P}$. Let $\sigma \in \mathrm{Gal}(K/E^*)$ be a lift of the arithmetic Frobenius $\mathrm{Frob} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Then:

1. The lift $\alpha : A \to {}^{\sigma}A$ of the $\#k(\mathfrak{p})$-th power Frobenius morphism $A_0 \to {}^{\sigma}A_0$ is an $\mathfrak{a}$-multiplication for
$$\mathfrak{a} = \mathrm{Nm}_{\Phi}(\mathfrak{p}).$$
2. The ideal $\mathfrak{a}(\sigma)$ in part (1) of Theorem 38.3 has ideal class $[\mathfrak{a}(\sigma)] = [N_{\Phi}(\mathfrak{a}^*)]^{-1} \in C_m(E)$, where $[\mathfrak{a}^*]$ is the ideal class such that $\mathrm{rec}_{E^*,\mathfrak{m}}([\mathfrak{a}^*]) = \sigma|_{L_{\mathfrak{m}}}$.

Proof. 1. Let $\sigma \in \mathrm{Gal}(K/E^*)$ be the lift of Frobenius from $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Let $\pi \in \mathcal{O}_E$ be an element that lifts the $\#k(\mathfrak{P})$-th power Frobenius morphism $A_0 \to A_0$, which satisfies
$$(\pi) = \prod_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)}\, \mathfrak{P}) = N_{K,\Phi}(\mathfrak{P}) = N_{\Phi}(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}$$
where the first equality is the Shimura-Taniyama formula (Theorem 30.1) and the second is Proposition 31.1, and $f(\mathfrak{P}/\mathfrak{p})$ is the residue index. By Proposition 39.5, there exists an $\mathfrak{a}$-multiplication $\alpha : A \to {}^{\sigma}A$ that lifts the $\#k(\mathfrak{p})$-th power Frobenius

map $A_0 \to {}^{\sigma}A_0$. This is arranged so that the two maps π and

$$ {}^{\sigma^{f(\mathfrak{P}/\mathfrak{p})-1}}\alpha \circ \cdots \circ {}^{\sigma}\alpha \circ \alpha \tag{9}$$

are both endomorphisms on A that descend to the $\#k(\mathfrak{P})$-th power Frobenius endomorphism on A_0. Therefore, by the Néron mapping property, these two endomorphisms are equal.

Immediately from the definition of $\mathfrak{a}$-multiplication, π is a (π)-multiplication, and the endomorphism (9) is a $\mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})}$-multiplication by Proposition 39.2. Therefore, since these two endomorphisms are equal, by Proposition 39.1 we conclude that the corresponding ideals are also equal:

$$N_\Phi(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})} = (\pi) = \mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})}.$$

Therefore, by unique factorization of ideals, we conclude that $\mathfrak{a} = N_\Phi(\mathfrak{p})$, as desired.

2. Part (1) tells us that $[\mathfrak{a}(\sigma)] = [\mathrm{Nm}_\Phi(\mathfrak{p})]$. But $\mathfrak{p}$ is the image of $\sigma|_{L_\mathfrak{m}}^{-1}$ under the Artin map, which sends a *geometric* Frobenius element to its corresponding prime ideal under our conventions (i.e. the conversion from arithmetic to geometric Frobenius introduces the inverse in this formula).

■

39.4 Proof of ideal-theoretic Main Theorem part (2)

Let $\sigma, \sigma' \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. By part (1) of Theorem 38.3, we have isogenies $\alpha : A \to {}^{\sigma}A, \alpha' : A \to {}^{\sigma'}A$ that are $\mathfrak{a}(\sigma)$-, $\mathfrak{a}(\sigma')$-multiplications, respectively. Then ${}^{\sigma}\alpha' \circ \alpha : A \to {}^{\sigma}A \to {}^{\sigma\sigma'}A$ is an $\mathfrak{a}(\sigma)\mathfrak{a}(\sigma')$-multiplication by Proposition 39.2. Thus the map $\mathrm{Gal}(\overline{\mathbb{Q}}/E^*) \to C_m(E)$ given by $\sigma \mapsto [\mathfrak{a}(\sigma)]$ is continuous group homomorphism. By continuity, there exists a modulus $\mathfrak{m}$ of E^* such that we have the following factorization:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) & \xrightarrow{\sigma \mapsto [\mathfrak{a}(\sigma)]} & C_m(E) \\ \big\downarrow{\scriptstyle \mathrm{res}} & & \big\uparrow \\ \mathrm{Gal}(L_\mathfrak{m}/E^*) & \xrightarrow{\mathrm{rec}_{E^*,\mathfrak{m}}} & C_\mathfrak{m}(E^*) \end{array}$$

where $\mathrm{rec}_{E^*,\mathfrak{m}}$ is the Artin reciprocity map for the modulus $\mathfrak{m}$. Hence $[\mathfrak{a}(\sigma)]$ only depends on $\sigma|_{L_\mathfrak{m}}$, and we have defined a homomorphism $C_\mathfrak{m}(E^*) \to C_m(E)$ determined by

$$\mathrm{rec}_{E^*,\mathfrak{m}}(\sigma|_{L_\mathfrak{m}}) \mapsto [\mathfrak{a}(\sigma)].$$

Recall that we wish to show $[\mathfrak{a}(\sigma)] = [N_\Phi(\mathrm{rec}_{E^*,\mathfrak{m}}(\sigma|_{L_\mathfrak{m}}))^{-1}]$. Theorem 39.7 tells us this is true whenever σ is the Frobenius element associated to an extension K/E^* unramified over a given prime $\mathfrak{p}$. By the Chebotarev density theorem (or Dirichlet's theorem), such $\mathfrak{p}$ exhaust $C_\mathfrak{m}(E^*)$, so we have proven part (2) of Theorem 38.3 for all $\sigma|_{L_\mathfrak{m}} \in \mathrm{Gal}(L_\mathfrak{m}/E^*)$. Since $[\mathfrak{a}(\sigma)]$ depends only on $\sigma|_{L_\mathfrak{m}}$, this prove part (2) of Theorem 38.3 for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$.

39.5 Idèlic version from ideal-theoretic version

Proposition 39.8. Theorem 38.3 implies Theorem 31.4.

Proof. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$ and let $s \in \mathbb{A}_{E^*,f}^\times/(E^*)^\times$ such that $\mathrm{Art}(s) = \sigma|_{E^{*,\mathrm{ab}}}$, and let α and $\mathfrak{a}(\sigma)$ be as in Theorem 31.4. Recall that $\eta(\sigma) \in \mathbb{A}_{E,f}^\times$ is defined to be the unique idéle such that

$$\alpha(\eta(\sigma) \cdot x) = \sigma(x)$$

for all $x \in \hat{V}(A)$, which is well-defined up to multiplication by $E^\times$ since α is also unique up to multiplication by $E^\times$.

From Lemma 38.1 we know that

$$\frac{\eta(\sigma)}{N_\Phi(s)} \in T(\mathbb{A}_f)/T(\mathbb{Q}) = \frac{\{a \in \mathbb{A}_{E,f}^\times : \mathrm{Nm}_{E/F}(a) \in \mathbb{A}^\times\}}{\{a \in E^\times : \mathrm{Nm}_{E/F}(a) \in \mathbb{Q}^\times\}} \hookrightarrow \mathbb{A}_{E,f}^\times/E^\times.$$

Therefore, by Lemma 37.5, to check that $\eta(\sigma)$ and $N_\Phi(s)$ are the same, it suffices to check that an arbitrarily small open neighborhood of $\eta(\sigma)$ contains $N_\Phi(s)$.[27] Recall that the subgroups $U_m \subseteq \mathbb{A}_{E,f}^\times$ restrict and descend to a basis of open subgroups at the identity for $T(\mathbb{A}_f)/T(\mathbb{Q})$ ranging over $m \in \mathbb{Z}_{>0}$.

Fix $m > 0$, and adjust α by a multiple of $E^\times$ so that $\alpha|_{A[m]} = \sigma|_{A[m]}$ as we did in Section 39.2, so that α is an $\mathfrak{a}(\sigma)$-multiplication (unique up to multiplication by $E_{m,1}$).

We need to relate $\eta(\sigma)$ to $\mathfrak{a}$:

Lemma 39.9. The image of $\eta(\sigma)$ in $C_m(E)$ is $[\mathfrak{a}(\sigma)^{-1}]$.

Proof. We may choose an isomorphism $\hat{V}(A) \simeq \hat{V}({}^\sigma A) \simeq \mathbb{A}_{E,f}$ such that the action of $\sigma : A \to {}^\sigma A$ is identified with multiplication by $1 \in \mathbb{A}_{E,f}^\times$, since σ induces an isomorphism on the Tate modules. By Proposition 39.6, α acts on the Tate module by an idèle $x \in \mathbb{A}_{E,f}^\times$ with $v(x) = v(\mathfrak{a}(\sigma))$ for all finite places of E. Therefore, the idèle $\eta(\sigma)$ such that

$$\alpha(\eta(\sigma) \cdot y) = \sigma(y)$$

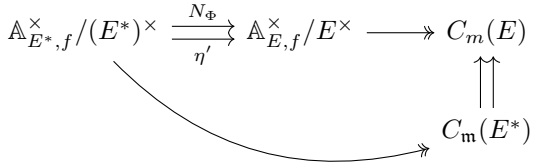
for all $y \in \hat{V}(A)$ must satisfy $v(\eta(\sigma)) + v(\mathfrak{a}(\sigma)) = 0$. Hence $\eta(\sigma)$ maps to the inverse of $[\mathfrak{a}(\sigma)]$ in $C_m(E)$. (Note also that the assumption $\alpha|_{A[m]} = \sigma|_{A[m]}$ implies that $\eta(\sigma) \in \mathbb{A}_{E,m}$.) ∎

Let $\eta' = \eta \circ \mathrm{Art} : \mathbb{A}_{E^*,f}^\times/(E^*)^\times \to \mathbb{A}_{E,f}^\times/E^\times$. For any fixed m, we have continuous compositions

$$\mathbb{A}_{E^*,f}^\times/(E^*)^\times \underset{\eta'}{\overset{N_\Phi}{\rightrightarrows}} \mathbb{A}_{E,f}^\times/E^\times \twoheadrightarrow C_m(E)$$

both of which have open kernel. Therefore, we can find some open subgroup of the form $U_{\mathfrak{m}} \subseteq \mathbb{A}_{E^*,f}^\times$ contained in this kernel. This gives two factorizations

[27] This is the reason why we went through the trouble of introducing the torus T: while $T(\mathbb{A}_f)/T(\mathbb{Q})$ is Hausdorff, $\mathbb{A}_{E,f}^\times/E^\times$ is not, making this sort of approximation argument via the ray class groups impossible if we were to only work in $\mathbb{A}_{E,f}^\times/E^\times$.



(one for each of η' and N_Φ).

Theorem 38.3 and Lemma 39.9 tell us that the two maps $C_{\mathfrak{m}}(E^*) \to C_m(E)$ agree whenever σ restricts to a Frobenius element in $\mathrm{Gal}(L_{\mathfrak{m}}/E^*)$ (note that the negative signs from these two results cancel each other). By the Chebotarev density theorem, we conclude that these maps are in fact equal for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$.

Hence $N_\Phi(s)$ and $\eta'(s)$ map to the same element $[N_\Phi(s)] = [\mathfrak{a}(\sigma)]$ in $C_m(E)$ for any $s \in \mathbb{A}^\times_{E^*,f}/(E^*)^\times$. This shows that $\frac{\eta'(s)}{N_\Phi(s)} = \frac{\eta(\sigma)}{N_\Phi(s)}$ lies in U_m. Since the U_m define a basis of open neighborhoods at the identity, this means $\eta(\sigma)$ and $N_\Phi(s)$ are arbitrarily close inside $T(\mathbb{A})/T(\mathbb{Q})$, so by the Hausdorff property we conclude that $\eta(\sigma) = N_\Phi(s)$ as elements in $\mathbb{A}^\times_{E,f}/E^\times$. This statement is Theorem 31.4. ■

References

[Ben11] Olivier Benoist. Le théorème de Bertini en famille. *Bull. Soc. Math. France*, 139(4):555–569, 2011.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bum97] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[CCO14] Ching-Li Chai, Brian Conrad, and Frans Oort. *Complex multiplication and lifting problems*, volume 195 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2014.

[CO19] Ching-Li Chai and Frans Oort. Moduli of abelian varieties. In *Open problems in arithmetic algebraic geometry*, volume 46 of *Adv. Lect. Math. (ALM)*, pages 95–177. Int. Press, Somerville, MA, [2019] ©2019.

[Con05] Brian Conrad. Main theorem of complex multiplication. `https://math.stanford.edu/~conrad/vigregroup/vigre04/mainthm.pdf`, 2005. Notes from the 2004-05 VIGRE Number Theory Working Group.

[Con15] Brian Conrad. Abelian varieties. `https://virtualmath1.stanford.edu/~conrad/249CS15Page/`, 2015. Lecture notes by Tony Feng.

[CP16] François Charles and Bjorn Poonen. Bertini irreducibility theorems over finite fields. *J. Amer. Math. Soc.*, 29(1):81–94, 2016.

[EvdGM24] Bas Edixhoven, Gerard van der Gee, and Ben Moonen. *Abelian varieties*. 2024. Preliminary version of the first chapters.

[Gro62] Alexander Grothendieck. *Fondements de la géométrie algébrique. [Extraits du Séminaire Bourbaki, 1957–1962.]*. Secrétariat mathématique, Paris, 1962.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[Jou83] Jean-Pierre Jouanolou. *Théorèmes de Bertini et applications*, volume 42 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1983.

[Ked21] Kiran S. Kedlaya. Notes on class field theory. https://kskedlaya.org/cft, 2021.

[Kle66] Steven L. Kleiman. Toward a numerical theory of ampleness. *Ann. of Math. (2)*, 84:293–344, 1966.

[Lan83] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[Mil10] J. S Milne. Complex multiplication (v0.10), 2010. Available at www.jmilne.org/math/.

[Mil15] James S. Milne. Algebraic groups (v2.00), 2015. Available at www.jmilne.org/math/.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. 2008.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[Sch88] Norbert Schappacher. *Periods of Hecke characters*, volume 1301 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1988.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sta24] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2024.

[Tat97] John Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 121–154. Springer, New York, 1997.

[TO70] John Tate and Frans Oort. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)*, 3:1–21, 1970.

[Vak] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. February 6, 2024 version.