254B: Complex Multiplication of Abelian Varieties

Nir Elber

Spring 2024

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Working over $\mathbb{C}$

Every person believes that he knows what a curve is until he has learned so much mathematics that the countless possible abnormalities confuse him.

—Felix Klein, [Kle16]

1.1 January 17

Let's get going.

Warning 1.1. The proofs in this first chapter of the course will be somewhat sketchy. We will later go back and prove things in more generality using the machinery of algebraic geometry (instead of the theory of complex manifolds).

1.1.1 Course Notes

Here are some course notes.

- The professor for this course is Yunqing Tang. Her research is in arithmetic geometry. Office hours will begin next week.
- This course is on complex multiplication of abelian varieties.
- There will be homework, and it completely determines the grade. There will be (on average) biweekly homeworks, which can be found and turned in on bCourses.
- There is a syllabus on the bCourses: https://bcourses.berkeley.edu/courses/1532318/. The syllabus has many references, on abelian varieties, complex multiplication, and class field theory.
- There is a schedule page on the bCourses, though it does not refer to every possible reference.
- It is encouraged to seek out examples, such as by emailing Professor Yunqing Tang. For example, elliptic curves are important, but their theory is often significantly simpler than the general theory.

- Our main goal is to discuss the main theorem of complex multiplication. We will give some version of it in the first part of the class, and then we will give a second version later after a more thorough discussion of abelian varieties.
- Much of the language will be scheme-theoretic, so it is highly recommended having some algebraic geometry background on the level of Math 256A.

1.1.2 Complex Tori

Let's just jump on in. The most basic example of an abelian variety is an elliptic curve, so that is where we will begin.

Definition 1.2 (elliptic curve)**.** Fix a field k. Then an *elliptic curve* is a pair (E, e) of a smooth proper k-curve E of genus 1 and a marked point $e \in E(k)$.

Remark 1.3. One can replace "proper" with "projective" here without tears.

Example 1.4. Take $k := \mathbb{C}$. It turns out that an elliptic curve (E, e) then makes $E(\mathbb{C})$ into a Riemann surface of genus 1: smooth makes this a manifold, proper makes it compact, and the genus is preserved. But then $E(\mathbb{C})$ will have universal cover given by $\mathbb{C}$ (in reality, we're looking at some kind of torus), and the projection map identifies $E(\mathbb{C})$ with $\mathbb{C}/\Lambda$ for a lattice $\Lambda \subseteq \mathbb{C}$. By translating, we may as well move the marked point $e \in E(\mathbb{C})$ to $0 \in \mathbb{C}/\Lambda$.

The above examples motivates us to look at higher-dimensional quotients, as follows.

Definition 1.5 (complex torus)**.** A *complex torus* is a quotient of the form V/Λ where V is a finite-dimensional $\mathbb{C}$-vector space, and $\Lambda \subseteq V$ is a lattice of full rank.

Remark 1.6. In the sequel, it may be helpful to note that a complex vector space V is just a real vector space V together with an $\mathbb{R}$-linear map $J : V \to V$ such that $J^2 = \mathrm{id}_V$. Namely, given a complex vector space V, we can build J by the action of i. Conversely, given a real vector space V with $J : V \to V$ such that $J^2 = -\mathrm{id}_V$, we note that we have a map $\mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V)$ by $i \mapsto J$ because $\mathbb{C} \cong \mathbb{R}[x]/\left(x^2+1\right)$; as such, V becomes a complex vector space restricting to the underlying real vector space. These constructions are inverse to each other by tracking back through that the action of i is given by J.

It turns out that a complex torus need not be an abelian variety, but one does have the following result to get projectivity from [Mum08, I.3, p. 33].

Theorem 1.7. Fix a complex torus $X := V/\Lambda$. Then the following are equivalent.

(i) X can be embedded into a complex projective space.

(ii) X is the analytification of an algebraic $\mathbb{C}$-variety.

(iii) There exists a positive-definite Hermitian form H on V such that H sends Λ to $\mathbb{Z}$.

Proof. We will discuss this more later in the course. ∎

Remark 1.8. Later on, we will understand the positive-definite Hermitian form as a polarization.

Satisfying any of these equivalent conditions turns out to produce an abelian variety.

Definition 1.9 (abelian variety)**.** An *abelian variety* is a $\mathbb{C}$-variety A which is a complex torus satisfying one of the equivalent conditions of Theorem 1.7. In practice, we will choose to define an abelian variety as a complex torus satisfying (iii).

This definition is rather unsatisfying because it only works over the base field $\mathbb{C}$, but it is good enough for now.

Remark 1.10. It turns out that there is a unique algebraic structure on the variety, so there is no worry about this being vague.

Theorem 1.7 involves Hermitian forms, so we will want to get a better handle on these.

Lemma 1.11. Fix a finite-dimensional complex vector space V. Then there is a bijection between Hermitian forms H on V and skew-symmetric forms ψ on the underlying real vector space of V such that

$$\psi(iv, iw) = \psi(v, w).$$

Proof. We begin by describing our maps.

- In the forward direction, send $H : V \times V \to \mathbb{C}$ to its imaginary part $\psi := \operatorname{im} H$. Then we have a map $\psi : V \times V \to \mathbb{R}$, and here are our checks on it.
  - Skew-symmetric: note that $\psi(v, v) = \operatorname{Im} H(v, v) = 0$ because $H(v, v) \in \mathbb{R}$ because H is Hermitian.
  - Bilinear: note that $\psi(cv, w) = \operatorname{Im} H(cv, w) = c \operatorname{Im} H(v, w) = \operatorname{Im} H(v, cw) = \psi(v, cw)$ and
    $$\psi(v_1 + v_2, w) = \operatorname{Im} H(v_1 + v_2, w) = \operatorname{Im} H(v_1, w) + \operatorname{Im} H(v_2, w) = \psi(v_1, w) + \psi(v_2, w)$$
    and similarly $\psi(v, w_1 + w_2) = \psi(v, w_1) + \psi(v, w_2)$.
  - Note that $\psi(iv, iw) = \operatorname{Im} H(iv, iw) = \operatorname{Im} i(-i)H(v, w) = \operatorname{Im} H(v, w) = \psi(v, w)$.
- For the backward direction, send ψ to the form $H(v, w) := \psi(iv, w) + i\psi(v, w)$. Here are our checks.
  - Conjugate symmetry: note $\psi(v, w) = -\psi(v, w)$ implies that $\operatorname{Im} H(v, w) = -\operatorname{Im} H(w, v)$. Then we must show that $\operatorname{Re} H(v, w) = \operatorname{Re} H(w, v)$, or $\psi(iv, w) = \psi(iw, v)$. Well,
    $$\psi(iw, v) = -\psi(v, iw) = \psi\left(i^2 v, iw\right) = \psi(iv, w)$$
  - Bilinear: note
    $$\begin{aligned} H(v_1 + v_2, w) &= \psi(i(v_1 + v_2), w) + i\psi(v_1 + v_2, w) \\ &= \psi(iv_1, w) + i\psi(v_1, w) + \psi(iv_2, w) + i\psi(v_2, w) \\ &= H(v_1, w) + H(v_2, w). \end{aligned}$$
    Also, for $c \in \mathbb{R}$, we see that $H(cv, w) = \psi(icv, w) + i\psi(cv, w) = c(\psi(iv, w) + i\psi(v, w)) = cH(v, w)$. So it remains to check that $H(iv, w) = iH(v, w)$. Well,
    $$H(iv, w) = \psi\left(i^2 v, w\right) + i\psi(iv, w) = -\psi(v, w) + i\psi(iv, w) = iH(v, w).$$

We now show that the constructions are inverse.

- Given ψ, we constructed H_ψ, and we see that $\operatorname{Im} H_\psi = \psi$ by construction.
- Given H, we set $\psi := \operatorname{Im} H$. Then we must show that the constructed H_ψ is equal to H. Note that $\operatorname{Im} H_\psi = \psi = \operatorname{Im} H$ by construction, and
  $$\operatorname{Re} H_\psi(v, w) = \psi(iv, w) = \operatorname{Im} H(iv, w) = \operatorname{Im} iH(v, w) = \operatorname{Re} H(v, w),$$
  so the result follows. ∎

Remark 1.12. We remark that H is a positive-definite Hermitian form if and only if the form $(v,w) \mapsto \operatorname{Re} H(v,w)$ is a positive-definite symmetric form. In terms of the above construction, this corresponds to the map $(v,w) \mapsto \psi(iv,w)$ being positive-definite; i.e., $\psi(iv,v) \geq 0$ for all v and equal to 0 if and only if $v = 0$.

The moral of Lemma 1.11 is that we are allowed to only pay attention to the imaginary part. It is worth having a name for this.

Definition 1.13 (Riemann form)**.** Fix a lattice Λ of full rank in a finite-dimensional complex vector space V. Then a skew-symmetric form $\psi\colon \Lambda \times \Lambda \to \mathbb{Z}$ is a *Riemann form* if and only if $\psi_{\mathbb{R}}\colon V \times V \to \mathbb{R}$ defined by $\psi_{\mathbb{R}}(x,y) \coloneqq \psi(ix,y)$ produces a symmetric positive-definite.

Remark 1.14. Quickly, we claim that $\psi_{\mathbb{R}}$ is symmetric and positive-definite if and only if $\psi(iv,iw) = \psi(v,w)$ always and $(v,v) \mapsto \psi(iv,v)$ is positive-definite. Indeed, $\psi_{\mathbb{R}}$ is the real part of the Hermitian form constructed in Lemma 1.11, and we can track through symmetry in the proof and positive-definiteness from Remark 1.12.

1.1.3 CM Fields

We want to give some examples of what "complex multiplication" means. This begins with a discussion of CM fields.

Lemma 1.15. Fix a number field $E/\mathbb{Q}$. Then the following are equivalent.

(i) There is a quadratic subextension $E^+ \subseteq E$ such that $E^+/\mathbb{Q}$ is totally real, and E/E^+ is totally imaginary.

(ii) There exists a nontrivial field involution $c\colon E \to E$ such that $\sigma(c(\alpha)) = \overline{\sigma(\alpha)}$ for any $\sigma\colon E \to \mathbb{C}$ and $\alpha \in E$.

(iii) There exists a unique nontrivial field involution $c\colon E \to E$ such that $\sigma(c(\alpha)) = \overline{\sigma(\alpha)}$ for any $\sigma\colon E \to \mathbb{C}$ and $\alpha \in E$.

(iv) There exists a totally real subfield $E^+ \subseteq E$ such that $E = E^+(\alpha)$ where $\alpha^2 \in E^+$ is "totally negative" (i.e., it maps to a negative real element for every complex embedding $E^+ \to \mathbb{C}$).

Proof. We show our implications in sequence.

- We show (i) implies (iv). By completing the square in the quadratic extension E^+/E, we may select $\alpha \in E^+ \setminus E$ such that $\alpha^2 \in E^+$. Being quadratic implies that $E = E^+(\alpha)$.

  It remains to check that α is totally negative. Fix an embedding $\sigma\colon E \to \mathbb{C}$, and let $\overline{\sigma}\colon E \to \mathbb{C}$ be the complex conjugate embedding. Because E is totally imaginary, we note $\sigma \neq \overline{\sigma}$, but $\sigma|_{E^+} = \overline{\sigma}|_{E^+}$ because E^+ is totally real, so we must then have $\sigma(\alpha) \neq \overline{\sigma(\alpha)}$. On the other hand, $\alpha^2 \in E^+$ implies that
  $$\sigma(\alpha)^2 = \overline{\sigma(\alpha)}^2 \in \mathbb{R},$$
  so $\sigma(\alpha) = -\overline{\sigma(\alpha)}$. Thus, $\sigma(\alpha)$ must be imaginary, so $\sigma(\alpha)^2 < 0$.

- We show (ii) implies (i). Set $E^+ \coloneqq E^c$; because $c^2 = \mathrm{id}_E$, we see that E/E^+ is quadratic. To see that E^+ is totally real, we note that any embedding $\sigma\colon E^+ \to \mathbb{C}$ can be extended to $\widetilde{\sigma}\colon E \to \mathbb{C}$. Now, for any $\alpha \in E^+$, we see that
  $$\overline{\sigma(\alpha)} = \overline{\widetilde{\sigma}(\alpha)} = \widetilde{\sigma}(c(\alpha)) = \widetilde{\sigma}(\alpha) = \sigma(\alpha),$$
  so $\sigma(\alpha) \in \mathbb{R}$. Thus, σ actually outputs to $\mathbb{R}$.

Lastly, we must see that E is totally imaginary. Suppose that $\sigma\colon E \to \mathbb{C}$ is a complex embedding, and we show that the image is not contained in $\mathbb{R}$. Indeed, if $\sigma(\alpha) \in \mathbb{R}$, then

$$\sigma(\alpha) = \overline{\sigma(\alpha)} = \sigma(c(\alpha)),$$

so $\alpha \in E^+$. Thus, $\sigma(\alpha) \notin \mathbb{R}$ for any $\alpha \in E \setminus E^+$.

- We show (ii) and (iii) are equivalent; of course (iii) implies (ii). To see that (ii) implies (iii), suppose that c_1 and c_2 are such field automorphisms $E \to E$. Then for any embedding $\sigma\colon E \to \mathbb{C}$, we see that $\sigma(c_1(\alpha)) = \sigma(c_2(\alpha))$ for any $\alpha \in E$, so $c_1 = c_2$ follows.
- We show (iv) implies (ii). Define $c \in \mathrm{Gal}(E^+/E)$ by $c(\alpha) \coloneqq -\alpha$. Then c is an automorphism with $c^2 = \mathrm{id}_E$. Also, for any embedding $\sigma\colon E \to \mathbb{C}$, we know that $\sigma(a) \in \mathbb{R}$ for any $a \in E^+$, and $\sigma(\alpha)^2 < 0$ by total negativity, so $\sigma(\alpha)$ is purely imaginary. Thus, for any $a + b\alpha \in E$, we see

$$\sigma(c(a+b\alpha)) = \sigma(a - b\alpha) = \sigma(a) - \sigma(b)\sigma(\alpha) = \overline{\sigma(a) + \sigma(b)\sigma(\alpha)} = \overline{\sigma(a+b\alpha)},$$

as needed. ∎

Remark 1.16. The proof of (iv) implies (ii) has shown that if E has been embedded into $\mathbb{C}$ already, then c is literally complex conjugation.

This produces the following definition.

Definition 1.17 (CM field)**.** A number field $E/\mathbb{Q}$ is a *CM field* if and only if E satisfies one of the equivalent conditions of Lemma 1.15. We call the involution $c\colon E \to E$ the *complex conjugation* of E.

Remark 1.18. The field E need not be Galois.

Remark 1.19. It turns out that $E^+ = E^c$ and is the maximal totally real subfield. Certainly $E^+ \subseteq E$ is totally real. Conversely, suppose $F \subseteq E$ is a totally real subfield. We will show that c fixes F, which then implies $F \subseteq E^c$. Well, for any $\alpha \in F$, we pick up any embedding $\sigma\colon E \to \mathbb{C}$, and we see that

$$\sigma(c(\alpha)) = \overline{\sigma(\alpha)} = \sigma(\alpha),$$

so $\alpha = c(\alpha)$ follows.

Being CM is a fairly nice adjective.

Lemma 1.20. Fix CM fields $E_1, \dots, E_n \subseteq \overline{\mathbb{Q}}$. Then the composite field $E_1 \cdots E_n$ is CM.

Proof. By induction, we may take $n = 2$; define $E \coloneqq E_1E_2$ for brevity. Let $c_1\colon E_1 \to E_1$ and $c_2\colon E_2 \to E_2$ be the complex conjugations, which we would like to extend to a complex conjugation map $c\colon E \to E$. Well, a generic element of E can be written as $\alpha = \sum_{i=1}^d a_{1i}a_{2i}$ where $a_{1i} \in E_1$ and $a_{2i} \in E_2$, so we define

$$c(\alpha) \coloneqq \sum_{i=1}^d c_1(a_{1i})c_2(a_{2i}).$$

We ought to check that c is well-defined. Suppose that $\sum_{i=1}^d a_{1i}a_{2i} = \sum_{i=1}^d a'_{1i}a'_{2i}$, and choose an embedding $\sigma\colon E_1E_2 \to \mathbb{C}$. Then σ will restrict to embeddings $\sigma_1\colon E_1 \to \mathbb{C}$ and $\sigma_2\colon E_2 \to \mathbb{C}$, and we see that

$$\sigma\left(\sum_{i=1}^d c_1(a_{1i})c_2(a_{2i})\right) = \sum_{i=1}^d \sigma_1(c_1(a_{1i}))\sigma_2(c_2(a_{2i})) = \overline{\sigma\left(\sum_{i=1}^d a_{1i}a_{2i}\right)}$$

and similar holds when we add primes. So the injectivity of σ provides that c is well-defined.

Now, the above has actually automatically shown that $\sigma(c(\alpha)) = \overline{\sigma(\alpha)}$ for any complex embedding $\sigma\colon E_1E_2 \to \mathbb{C}$ and $\alpha \in E_1E_2$. It remains to show that $c^2 = \mathrm{id}_E$ and that c is a nontrivial field homomorphism. To see that c is a field homomorphism, we note $c = \sigma^{-1} \circ \iota \circ \sigma \circ c$, where $\iota\colon \mathbb{C} \to \mathbb{C}$ is complex conjugation. To see that c is nontrivial, we note that it extends $c_1\colon E_1 \to E_1$, which is nontrivial. Lastly, to see that $c^2 = \mathrm{id}_E$, choose $\sigma\colon E_1E_2 \to \mathbb{C}$, and we note that $\sigma \circ c^2 = \iota^2 \circ \sigma = \sigma$, so $c^2 = \mathrm{id}_E$ is forced. ∎

Corollary 1.21. Fix a CM field E. Then its Galois closure M in $\overline{\mathbb{Q}}$ is CM.

Proof. Without loss of generality, choose an embedding $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Let $\sigma_1, \dots, \sigma_n\colon E \to \mathbb{C}$ denote the complex embeddings of E, and we note that the Galois closure of E is the composite

$$\sigma_1(E) \cdots \sigma_n(E).$$

By Lemma 1.20, it thus suffices to show that $\sigma(E)$ is a CM field for any embedding $\sigma\colon E \to \mathbb{C}$.

Well, let $c\colon E \to E$ denote the complex conjugation of E; we note that this agrees with the complex conjugation in $\mathbb{C}$ by Remark 1.16. Then to show that $\sigma(E)$ is a CM field, we note that we have a complex conjugation $c_\sigma\colon \sigma(E) \to \sigma(E)$ by

$$c_\sigma(\sigma(\alpha)) \coloneqq \sigma(c(\alpha)).$$

This is also $\overline{\sigma(\alpha)}$, which establishes that c_σ is a nontrivial field involution. (Being nontrivial follows because E is totally imaginary.) Lastly, for any complex embedding $\tau\colon \sigma(E) \to \mathbb{C}$, we must show that $\tau(c_\sigma(\sigma(\alpha))) = \overline{\tau(\sigma(\alpha))}$. However, we simply note that $(\tau \circ \sigma)\colon E \to \mathbb{C}$ is another embedding, and

$$\tau(c_\sigma(\sigma(\alpha))) = (\tau \circ \sigma)(c(\alpha)) = \overline{\tau(\sigma(\alpha))},$$

as desired. ∎

Having CM fields allow us to define CM types.

Definition 1.22 (CM type)**.** Fix a CM field E with complex conjugation c. Then a *CM type* on E is a subset $\Phi \subseteq \mathrm{Hom}(E, \mathbb{C})$ such that

$$\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup c\Phi.$$

We call the pair (E, Φ) a *CM pair*.

Remark 1.23. When $E/\mathbb{Q}$ is imaginary quadratic (which is what happens for elliptic curves), one does not really have a choice in CM type. But for higher degrees, which exist for higher-dimensional abelian varieties, there is indeed structure we want to keep track of.

This allows us to write down an abelian variety.

Exercise 1.24. Fix a CM pair (E, Φ), and set $n \coloneqq \frac{1}{2}[E : \mathbb{Q}]$. For a lattice $\mathfrak{a} \subseteq E$, set $\Lambda \coloneqq \mathfrak{a}$, and use Φ to produce an embedding $\mathfrak{a} \to \mathbb{C}^\Phi$ by $\alpha \mapsto (\sigma(\alpha))_{\sigma \in \Phi}$. Then $\mathbb{C}^\Phi/\mathfrak{a}$ is an abelian variety.

Proof. Quickly, we show that $\mathfrak{a}$ is a lattice of full rank in $\mathbb{C}^\Phi$. Fix an integral basis $\{\alpha_1, \dots, \alpha_{2n}\}$ of $\mathfrak{a}$. Now, by viewing $\mathbb{C}^\Phi$ as $\mathbb{R}^{2n}$ by taking real and imaginary parts, we see that the determinant of the map $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}^{2n}$ is, up to sign and a factor of 2, equal to

$$\det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_{2n}) \\ \vdots & \ddots & \vdots \\ \sigma_{2n}(\alpha_1) & \cdots & \sigma_{2n}(\alpha_{2n}) \end{bmatrix},$$

which is the discriminant of the $\alpha_\bullet$, which is nonzero. (Here, we enumerate $\Phi = \{\sigma_1, \dots, \sigma_n\}$ and then $\sigma_{n+i} := \overline{\sigma_i}$ for $i \in \{1, \dots, n\}$.) This is sufficient because then $\mathcal{O}_E$ is a lattice of rank $2n$ in $\mathbb{R}^{2n}$. So we do indeed have a complex torus.

To provide the abelian variety structure, it suffices to provide the ψ of Lemma 1.11. We will choose $\xi \in \mathfrak{a}$ judiciously and then set

$$\psi(x, y) := \operatorname{Tr}_{E/\mathbb{Q}}(\xi x c(y)).$$

Check the signs: c(x)y?

For concreteness, we go ahead and embed E into $\mathbb{C}$ so that c is literally complex conjugation by Remark 1.16. As such, we will write $c(y)$ as $\overline{y}$. Now, to choose ξ, we note that a weak approximation argument grants $\xi_0 \in \mathfrak{a}$ such that $\operatorname{Im} \sigma(\xi_0) > 0$ for each $\sigma \in \Phi$; such a thing exists by a strong approximation argument. Then set $\xi := \xi_0 - \overline{\xi_0}$ so that $\overline{\xi} = -\xi$ while still having

$$\operatorname{Im} \sigma(\xi) = \operatorname{Im} \sigma(\xi_0) - \operatorname{Im} \sigma(\overline{\xi_0}) = \operatorname{Im} \sigma(\xi_0) + \operatorname{Im} \sigma(\xi_0) > 0.$$

We are now ready to conduct our checks.

- Bilinear: the map $(x, y) \mapsto (\xi x, \overline{y})$ is $\mathbb{Z}$-linear in both coordinates, and the map $(x, y) \mapsto \operatorname{Tr}_{E/\mathbb{Q}}(xy)$ is bilinear in both coordinates, so the composite $(x, y) \mapsto \psi(x, y)$ is also bilinear in both coordinates.
- Skew-symmetric: we must show that $\psi(x, x) = 0$ for any $x \in \mathcal{O}_E$. Now, it will be helpful to expand

  $$\psi(x, x) = \operatorname{Tr}_{E/\mathbb{Q}}(\xi x \overline{x}) = \sum_{i=1}^{n} (\sigma_i(\xi x \overline{x}) + \overline{\sigma_i}(\xi x \overline{x})).$$

  Now, we note that $\overline{\sigma_i}(\xi x \overline{x}) = \overline{\sigma_i(\xi x \overline{x})} = \sigma_i(\overline{\xi} \cdot x \overline{x}) = -\sigma_i(\xi x \overline{x})$, so each term of this sum vanishes.
- Upon tensoring with $\mathbb{R}$ to produce $\psi_{\mathbb{R}}$, we must show that $\psi_{\mathbb{R}}(ix, iy) = \psi_{\mathbb{R}}(x, y)$. By scaling x and y, we may assume that $x, y \in \mathcal{O}_E$. We also note that ξ is purely imaginary, so by scaling ix and iy, it suffices to show that

  $$\psi(x, y) = \frac{1}{|\xi|^2} \psi(\xi x, \xi y).$$

  However, this is immediate from the linearity of the trace.
- Positive-definite: we must show that $\psi_{\mathbb{R}}(ix, x) \geq 0$ for each x and is zero if and only if $x = 0$. We may as well check this for $x \in \mathcal{O}_E$, and a direct expansion produces

  $$\psi(ix, x) = \sum_{i=1}^{n} (\sigma_i(\xi i x \overline{x}) + \overline{\sigma_i}(\xi i x \overline{x})),$$

  where one makes sense of i by some kind of $\mathbb{R}$-linearity. Expanding somewhat naively, we see

  $$\psi(ix, x) = \sum_{i=1}^{n} (\sigma_i(i\xi) + \sigma_i(-i\overline{x}))\sigma_i(x\overline{x}) = \sum_{i=1}^{n} 2\sigma_i(i\xi)\sigma_i(x\overline{x}).$$

  Now, each term of the sum is nonnegative because $\operatorname{Im} \sigma_i(\xi) > 0$ already, so the total sum can only vanish provided that all the individual terms vanish. For example, this requires that $\sigma_i(x\overline{x}) = 0$ for all i, so $x\overline{x} = 0$, so $x = 0$ or $\overline{x} = 0$, so $x = 0$ is forced. ∎

Remark 1.25. In general, one can replace E by a CM algebra and replace $\mathcal{O}_E$ by certain fractional ideals. This will turn out to provide all isomorphism classes of abelian varieties with CM.

Next class we will define an abelian variety when not over $\mathbb{C}$.

1.2 January 19

Here we go. Today we will define an abelian variety in general, but we will stay focused on the analytic theory.

1.2.1 Defining Abelian Varieties

Abelian varieties are special kinds of group objects.

Definition 1.26 (group scheme)**.** Fix a base scheme S. Then a *group S-scheme* is a group object G in the category Sch_S of S-schemes. In other words, there exist S-morphisms $m\colon G \times_S G \to G$ (for multiplication) and $i\colon G \to G$ (for inversion) and $e\colon S \to G$ (for identity) making the following diagrams commute.

- Associativity:

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

- Identity:

$$\begin{array}{ccccc} & & G \times_S G & & \\ & \nearrow & & \searrow^{m} & \\ G & & = & & G \\ & \searrow & & \nearrow_{m} & \\ & & S \times_S G & & \end{array} \qquad \begin{array}{l} \xrightarrow{\mathrm{id}_G \times e} \\ \\ \\ \\ \xrightarrow{e \times \mathrm{id}_G} \end{array} \begin{array}{c} \\ \\ \\ \\ G \times_S G \end{array}$$

- Inversion:

$$\begin{array}{ccccc} & & G \times_S G & & \\ & \nearrow^{\mathrm{id}_G \times i} & & \searrow^{m} & \\ G & \longrightarrow & S & \xrightarrow{e} & G \\ & \searrow_{i \times \mathrm{id}_G} & & \nearrow_{m} & \\ & & G \times_S G & & \end{array}$$

Remark 1.27. Equality of morphisms of k-varieties can be checked on geometric points, so we could just check the above commutativity on $G(\overline{k})$.

In particular, we want to be a variety.

Definition 1.28 (group variety)**.** Fix a base field k. Then a *group k-variety* is a group scheme which is also a k-variety (i.e., reduced and separated).

Remark 1.29. By way of analogy, we also note that a Lie group is a group object in the category Man of smooth manifolds.

Abelian varieties are special kinds of group varieties.

Definition 1.30 (abelian variety)**.** Fix a field k. Then an *abelian k-variety* is a group k-variety which is smooth, connected, and proper.

Here, smoothness is something like requiring that we are a manifold, and proper is something like requiring that we are projective. (It turns out that the conditions imply that A is projective, though this is not obvious.)

Remark 1.31. One can even replace "k-variety" with "k-scheme" because being smooth over a scheme implies being regular, which implies reduced.

Remark 1.32. It turns out that being geometrically integral is equivalent to being connected, by some argument involving the connected component.

Remark 1.33. It turns out that being proper implies that the group law on A is abelian, which we have notably not included in the hypotheses.

While we're here, we go ahead and define abelian schemes; these will be desirable because we may (perhaps) want to define varieties via equations in a ring which is not a field (like $\mathbb{Z}$) and then reduce to a field (like $\mathbb{F}_p$) later.

Definition 1.34 (abelian scheme)**.** Fix a base scheme S. An *abelian S-scheme* is a group S-scheme A which is proper and smooth over S such that the structure map $\pi\colon A \to S$ has connected geometric fibers. (This last condition means that any geometric point $\overline{s} \to S$ makes $A_{\overline{s}}$ connected.)

Remark 1.35. Here, smoothness can be verified by something like a Jacobian criterion, analogous to smoothness for embedded manifolds.

Remark 1.36. Notably, by the hypotheses, the geometric fibers $A_{\overline{s}}$ are abelian varieties.

1.2.2 Working over $\mathbb{C}$

We now return to working over $k = \mathbb{C}$. We quickly compare with Definition 1.9: being an abelian variety over $\mathbb{C}$ as defined in the previous subsection implies that $A(\mathbb{C})$ is a smooth complex analytic manifold which is connected and compact, simply by reading off the adjectives. Now, this means that $A(\mathbb{C})$ is connected and compact, so we have a connected compact complex Lie group $A(\mathbb{C})$, which one can show is always of the form V/Λ where V is a finite-dimensional $\mathbb{C}$-vector space and $\Lambda \subseteq \mathbb{C}$ is a lattice of full rank, as sketched in Remark 1.38. From there, being algebraic does imply one of the equivalent conditions of Theorem 1.7, and the converse is similar.

Anyway, for a taste of the analytic theory, we show the following for $k = \mathbb{C}$.

Proposition 1.37. Fix an abelian k-variety A. Then the group law for A is commutative.

Sketch for $k = \mathbb{C}$. For brevity, set $g \coloneqq \dim A$. Consider the tangent space at the identity $e \in A$, which we will label T_eA; it is a g-dimensional $\mathbb{C}$-vector space. Now, for $e \in A(\mathbb{C})$, we have a holomorphic map $c_x\colon A(\mathbb{C}) \to A(\mathbb{C})$ given by conjugation $y \mapsto xyx^{-1}$, and then this induces a linear map $dc_x\colon T_eA \to T_eA$. This construction $x \mapsto dc_x$ produces a holomorphic map

$$A(\mathbb{C}) \to \mathrm{GL}(T_eA).$$

Indeed, this is holomorphic because dc_x, on an open subset of $A(\mathbb{C})$ holomorphic to $\mathbb{C}^g$, is simply a matrix made of the derivatives of c, each of which continue to be holomorphic functions.

Now, the key point is that properness of A implies that $A(\mathbb{C})$ is compact, but $\mathrm{GL}(T_eA)$ is an open submanifold, so the map $A(\mathbb{C}) \to \mathrm{GL}(T_eA)$ must be bounded (by the compactness) and hence constant: $A(\mathbb{C})$ is connected, so it is enough to show that we are locally constant, and in particular, it is enough to show that we are locally constant on trivializing open covers for $A(\mathbb{C})$ and $\mathrm{GL}(T_eA)$. But then we are looking at some

bounded holomorphic map $\mathbb{C}^g \to \mathbb{C}^{g^2}$, which must be constant by using Liouville's theorem on suitable projections.

Finishing up, we note that $de_x = \mathrm{id}_{T_eA}$, we see that actually $dc_e = \mathrm{id}_{T_eA}$ (conjugating by e does nothing), which implies that c_x must be the identity for any $x \in A(\mathbb{C})$, so the group law is commutative. To move this up to the level of the scheme group law being commutative, we note that we want the diagram

$$\begin{array}{ccc} A \times A & \xrightarrow{\text{swap}} & A \times A \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & A \end{array}$$

to commute, but we already know that it commutes on $\mathbb{C}$-points, which is enough for $\mathbb{C}$-varieties [Vak17, Exercise 11.4.B]. ■

Remark 1.38. Continuing with $k = \mathbb{C}$, we note that the theory of complex Lie groups produces a group homomorphism $\exp\colon T_eA \to A(\mathbb{C})$, which one can show is a covering space map. So $A(\mathbb{C})$ must then be a compact quotient of T_eA, and actually it is a quotient by something discrete, meaning that $A(\mathbb{C}) \cong V/\Lambda$ as above.

Here are some nice corollaries of realizing abelian varieties as complex tori.

Corollary 1.39. Fix an abelian $\mathbb{C}$-variety A of dimension g. For any positive integer n, the multiplication-by-n map $[n]\colon A(\mathbb{C}) \to A(\mathbb{C})$ is a surjective group homomorphism, and its kernel is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. Note $[n]$ is a group homomorphism because $A(\mathbb{C})$ is abelian. For the other claims, write $A = V/\Lambda$ for V a g-dimensional $\mathbb{C}$-vector space. In particular, V/Λ is a divisible group, so $[n]$ is surjective, and the kernel is isomorphic to

$$\frac{1}{n}\Lambda/\Lambda \cong \frac{1}{n}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \cong (\mathbb{Z}/n\mathbb{Z})^{2g},$$

essentially by choosing a basis for Λ. ■

Corollary 1.40. Fix an abelian $\mathbb{C}$-variety A of dimension g. Then

$$\pi_1(A(\mathbb{C})) \cong H_1(A(\mathbb{C}), \mathbb{Z}) \cong \Lambda \cong \mathbb{Z}^{2g}.$$

Proof. Again, write $A = V/\Lambda$ for V a g-dimensional $\mathbb{C}$-vector space. Then V is the universal covering space for V/Λ (indeed, it's a simply connected covering space), so $\pi_1(A(\mathbb{C})) \cong \Lambda$, from which the rest of the isomorphisms follow quickly. For example, the abelianization of $\pi_1(A(\mathbb{C}))$ is still Λ, so $H_1(A(\mathbb{C}), \mathbb{Z}) \cong \Lambda$ too. Lastly, $\Lambda \cong \mathbb{Z}^{2g}$ by choosing a basis. ■

1.2.3 Isogenies

While we're here, we define isogenies, which are "squishy" isomorphisms.

Definition 1.41 (isogenies)**.** Fix abelian k-varieties A and B. A k-morphism $f\colon A \to B$ is a surjective homomorphism with finite kernel.

Example 1.42. For any positive integer n, the map $[n]\colon A \to A$ is an isogeny. We will prove this in general later, but over $\mathbb{C}$, it follows from Corollary 1.39. In particular, we know $[n]$ is a homomorphism. Also, the kernel has finitely many $\mathbb{C}$-points, so it must be zero-dimensional and thus finite because it is a closed subscheme of A.

Lastly, surjectivity is seen on $\mathbb{C}$-points, but it also follows purely formally because the domain and codomain of $[n]\colon A \to A$ have the same dimension; see [Mil08, Proposition I.7.1]. We will discuss this later in the course, so I won't bother being formal here.

We would like to describe isogenies (over $\mathbb{C}$) from the perspective of the complex tori. So we pick up the following proposition.

Proposition 1.43. Fix complex tori V/Λ and V'/Λ'. Then holomorphic maps $V/\Lambda \to V'/\Lambda'$ fixing 0 are in bijection with $\mathbb{C}$-linear maps $V \to V'$ sending $\Lambda \to \Lambda'$.

Proof. The backward map simply sends the $\mathbb{C}$-linear map to the quotient map $V/\Lambda \to V'/\Lambda'$.

For the forward map, we are given a holomorphic map $\overline{\varphi}\colon V/\Lambda \to V'/\Lambda'$ sending $\varphi\colon [0] \mapsto [0]$. As in the proof of Corollary 1.40, we note that V and V' are the universal covers of V/Λ and V'/Λ', respectively, because V and V' are simply connected. Thus, the quotient map $\overline{\varphi}$ will induce a unique map $\varphi\colon V \to V$ on the universal covering spaces upon fixing a single point, and we must send $\varphi(0) \coloneqq 0$ to be linear. In particular, the diagram

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V' \\ \downarrow & & \downarrow \\ V/\Lambda & \xrightarrow{\overline{\varphi}} & V'/\Lambda' \end{array} \qquad \begin{array}{ccc} 0 & \longmapsto & 0 \\ \downarrow & & \downarrow \\ 0+\Lambda & \longmapsto & 0+\Lambda' \end{array}$$

commutes, and the relevant map φ is unique. So thus far we have shown that maps holomorphic $V/\Lambda \to V'/\Lambda'$ fixing 0 are in bijection with holomorphic maps $V \to V$ fixing 0 and sending $\Lambda \to \Lambda'$.

It remains to show that any such φ is linear. Note that it is holomorphic because it is locally given by the holomorphic map $V/\Lambda \to V'/\Lambda'$. Because $\varphi(0) = 0$, it is enough to show that the derivative $d\varphi_v\colon T_vV \to T_{\varphi(v)}V'$ does not depend on $v \in V$. In other words, we would like the map

$$V \to \operatorname{Hom}_{\mathbb{C}}(T_vV, T_{\varphi(v)}V'),$$

given by $v \mapsto d\varphi_v$, to be constant. Well, we use the same trick as in Proposition 1.37: note that this map actually only depends on the class of $v \in V$ modulo Λ, so we really have a holomorphic map

$$V/\Lambda \to \operatorname{Hom}_{\mathbb{C}}(T_vV, T_{\varphi(v)}V') \cong \mathbb{C}^{(\dim V)(\dim V')},$$

which is bounded because V/Λ is compact and hence compact by using Liouville's theorem on suitable projections. ∎

Remark 1.44. Basically, we can see that being an isogeny means that the underlying linear map will be a surjective linear map with finite kernel; in particular, $\dim_{\mathbb{C}} V = \dim_{\mathbb{C}} V'$. This motivates us thinking about isogenies as "squishy" isomorphisms.

1.3 January 22

Today we will talk more about the analytic theory.

1.3.1 More on Isogenies

We begin by picking up a piece of language.

Definition 1.45 (isogenous)**.** Fix abelian k-varieties A and B. We say that A and B are *isogenous*, written $A \sim B$, if and only if there is an isogeny $A \to B$.

It turns out that having an isogeny is an equivalence relation, so we will not care about the direction of being "isogenous." Here are the checks over $\mathbb{C}$.

Lemma 1.46. Fix abelian k-varieties A and B.

(a) Reflexive: $\mathrm{id}_A \colon A \to A$ is an isogeny.

(b) Symmetric: if $\varphi \colon A \to B$ is an isogeny, there is a nonzero integer n and another isogeny $\psi \colon B \to A$ such that
$$\varphi \circ \psi = [n]_B \qquad \text{and} \qquad \psi \circ \varphi = [n]_A.$$

(c) Transitive: if $\varphi \colon A \to B$ and $\psi \colon B \to C$ are isogenies, then $(\psi \circ \varphi) \colon A \to C$ is an isogeny.

Proof over $\mathbb{C}$. We dispose of the easier claims first. Note (a) has little content: id_A is a surjective homomorphism with trivial kernel and hence an isogeny. Similarly, (c) follows because being surjective, being a homomorphism, and having finite kernel are all properties preserved by composition. Perhaps it is notably that finite kernel is preserved by composition, but this is equivalent to all fibers being finite, and the fiber of $(\psi \circ \varphi)$ over some $c \in C$ will simply be the (finite!) union of the fibers of φ over points $b \in \psi^{-1}(\{c\})$.

It remains to show (b), which is perhaps the most interesting. We will show this by working with complex tori and appealing to Proposition 1.43. Fix isomorphisms of compact complex Lie groups $A \cong V/\Lambda$ and $B \cong V'/\Lambda'$. Then the isogeny $\varphi \colon V/\Lambda \to V'/\Lambda'$ arises from a linear map $\widetilde{\varphi} \colon V \to V'$ sending $\Lambda \to \Lambda'$. We are thus looking at the following commutative diagram.

$$\begin{array}{ccc} V & \xrightarrow{\widetilde{\varphi}} & V' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ V/\Lambda & \xrightarrow{\varphi} & V'/\Lambda' \end{array}$$

We claim that $\widetilde{\varphi}$ is an isomorphism of $\mathbb{C}$-vector spaces.

- Injective: because $\ker \widetilde{\varphi} \subseteq V$ is a $\mathbb{C}$-subspace, it suffices to show that $\ker \widetilde{\varphi}$ is discrete. Well, tracking around the diagram, $\ker \widetilde{\varphi}$ is contained in $\ker(\pi \circ \widetilde{\varphi}) = \ker(\varphi \circ \pi)$, which is
$$\bigcup_{[x] \in \ker \varphi} (x + \Lambda).$$
Because $\ker \varphi$ is finite, the above set is discrete in V, so we are done.
- Surjective: let $\alpha \in (0,1)$ be transcendental. Fix a $\mathbb{Z}$-basis $\lambda_1', \dots, \lambda_{2n}'$ of Λ'. Then for any $\lambda_1'', \dots, \lambda_{2n}'' \in \Lambda'$, we see that the set
$$\{\alpha\lambda_1' + \lambda_1'', \dots, \alpha\lambda_{2n}' + \lambda_{2n}''\}$$
is still a $\mathbb{R}$-basis of V': the transition matrix from the basis $\{\lambda_1', \dots, \lambda_{2n}'\}$ to the above basis is αI_{2n} plus some matrix in $\mathbb{Z}^{2n}$, which will surely have nonzero determinant because α is transcendental. Anyway, φ hits all $\alpha\lambda_\bullet'$ in its image (modulo Λ'), so $\widetilde{\varphi}$ will hit some vector in $\alpha\lambda_i' + \Lambda'$ for each i. However, these vectors will form a basis, as needed.

Now, to continue, fix isomorphisms $\alpha \colon \Lambda \cong \mathbb{Z}^{2n}$ and $\alpha' \colon \Lambda' \cong \mathbb{Z}^{2n}$. Up to these isomorphisms, $\widetilde{\varphi} \colon \Lambda \to \Lambda'$ (which is an isomorphism upon $- \otimes_{\mathbb{Z}} \mathbb{R}$) becomes a map $\widetilde{\varphi}_0' \colon \mathbb{Z}^{2n} \to \mathbb{Z}^{2n}$ (which is still an isomorphism upon

$-\otimes_{\mathbb{Z}}\mathbb{R}$). In particular, $\det\widetilde{\varphi}_0'$ is some nonzero integer n, and the adjugate matrix $\widetilde{\psi}_0' \coloneqq \operatorname{adj}\widetilde{\varphi}_0'$ provides a map such that $\widetilde{\psi}_0' \circ \widetilde{\varphi}_0' = \widetilde{\varphi}_0' \circ \widetilde{\psi}_0'$ are multiplication by n.

Passing back through α and α', we have produced some map $\widetilde{\psi}\colon \Lambda' \to \Lambda$ such that $\widetilde{\varphi}\circ\widetilde{\psi}$ and $\widetilde{\psi}\circ\widetilde{\varphi}$ are both multiplication by n. Tensoring by $\mathbb{R}$ extends $\widetilde{\psi}$ to an $\mathbb{R}$-linear map $V' \to V$ satisfying the same conditions; note that because multiplication by n is an isomorphism of $\mathbb{C}$-vector spaces, it follows that $\widetilde{\psi}$ is in fact $\mathbb{C}$-linear.

Now, modding out Λ and Λ', Proposition 1.43 provides us with a map $\psi\colon V'/\Lambda' \to V/\Lambda$ of complex tori such that $\varphi\circ\psi$ and $\psi\circ\varphi$ are both multiplication by n. Note ψ is surjective with finite kernel because $\widetilde{\psi}$ is an isomorphism of vector spaces. (In particular, surjectivity is automatic, and finite kernel follows because the kernel of ψ is contained in the kernel of $\varphi\circ\psi = [n]_B$, which is finite.) ∎

Remark 1.47. Being an equivalence relation, and in particular part (b) in Lemma 1.46, provides more evidence that we should think about isogenies as "squishy" isomorphisms. Indeed, up to multiplication by an integer, we are a bona fide isomorphism.

Remark 1.48. The end of the above proof has shown that an isomorphism of vector spaces $\widetilde{\varphi}\colon V \to V'$ carrying $\Lambda \to \Lambda'$ will have the needed map $\widetilde{\psi}\colon V' \to V$ carrying $\Lambda' \to \Lambda$ such that the composites are multiplication by some nonzero integer n. In particular, merely being an isomorphism of vector spaces implies that the quotient map $\varphi\colon (V/\Lambda) \to (V'/\Lambda')$ is an isogeny: surjectivity is clear, and finite kernel follows because the composite with the quotient map $\psi\colon (V'/\Lambda') \to (V/\Lambda)$ is multiplication by a nonzero integer, which has finite kernel.

We can decompose abelian varieties based on their isogeny class.

Theorem 1.49 (Poincaré reducibility)**.** Fix an abelian k-variety A, and let $B \subseteq A$ be an abelian subvariety. Then there exists another abelian subvariety $B' \subseteq A$ such that $B \cap B'$ is a finite scheme, and

$$B + B' = \{b + b' : b \in B, b' \in B'\}$$

is equal to A. In other words, the canonical map $B \times_k B' \to A$ given by summing is an isogeny.

Proof. This is [Mum08, p. 160] or [Mil20b, Theorem 2.12]. In the complex analytic situation, the proof idea is not so complicated: the point is to take an "orthogonal complement" to B.

Explicitly, set $V \coloneqq \operatorname{Lie} A$ and $W \coloneqq \operatorname{Lie} B$. Functoriality of the tangent space tells us that $W \subseteq V$, and functoriality of the exponential map implies that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & V & \xrightarrow{\exp} & A & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \Lambda\cap W & \longrightarrow & W & \xrightarrow{\exp} & B & \longrightarrow & 0 \end{array}$$

commutes. Here, Λ is the kernel of $\exp\colon V \twoheadrightarrow A$, so the diagram tells us that $\Lambda \cap W$ must be the kernel of $\exp\colon W \twoheadrightarrow B$. (Namely, the kernel of $\exp\colon W \twoheadrightarrow A$ is W intersected with the kernel of $V \twoheadrightarrow A$.) So $A = V/\Lambda$ and $B = W/(W \cap \Lambda)$.

Now, let H be the required Hermitian form on V, taking integral values on Λ, and set $\psi_{\mathbb{R}} \coloneqq \operatorname{Re} H$ so that $\psi_{\mathbb{R}}$ is a positive-definite symmetric form on the underlying $\mathbb{R}$-vector space of V. Quickly, note that H continues to be positive-definite and Hermitian on W, so H is also a Hermitian form on W by restriction (and still taking integer values on $\Lambda \cap W$).

As promised, we now define $W' \coloneqq W^{\perp}$, where we take the orthogonal complement with respect to $\psi_{\mathbb{R}}$. We have the following checks.

- Subspace: we claim W' is a $\mathbb{C}$-subspace of V. By construction, it is an $\mathbb{R}$-subspace. Now, if $w \in W'$, we would like for $iw \in W'$; namely, if $\psi_{\mathbb{R}}(w, v) = 0$ for all $v \in W$, then we want $\psi_{\mathbb{R}}(iw, v) = 0$ for all $v \in W$. Well, we compute
$$\psi_{\mathbb{R}}(iw, v) = \operatorname{Re} H(iw, v) = \operatorname{Re} H(w, -iv) = \psi_{\mathbb{R}}(w, -iv),$$
and $-iv \in W$ still.
- Lattice: we claim that $W' \cap \Lambda$ is a lattice of W'. Certainly we have a $\mathbb{Z}$-subgroup, so it remains to compute the rank. We do this by an explicit construction of the basis. Let $\{w_1, \dots, w_{2\dim W}\}$ be a basis for $W \cap \Lambda$, and extend it by $\{v_1, \dots, v_{2\dim W'}\}$ to a basis of Λ. Now, for each v_i, we can subtract out something in W in order to land in W'; this factor is a rational number because it comes from dividing out by values of ψ on Λ, so we can then scale this element in order to land in $W' \cap \Lambda$. This process slowly produces a linearly independent subset of $W' \cap \Lambda$ of size $2 \dim W'$, which shows that $W' \cap \Lambda$ is a lattice of full rank in W'.
- Form: as before, we note that H restricts to a positive-definite Hermitian form on W' taking integral values on $W' \cap \Lambda$.

In total, we are able to conclude that $B' \coloneqq W'/(W' \cap \Lambda)$ is an abelian variety, and it is an abelian subvariety of $A = V/\Lambda$ via the inclusion. It remains to show that the induced map $B \times_{\mathbb{C}} B' \to A$ is an isogeny. Well, this map is given by taking the quotient of the isomorphism $W \oplus W' \twoheadrightarrow V$ of $\mathbb{C}$-vector spaces (by $(\Lambda \cap W) \oplus (\Lambda \cap W')$), which is an isogeny by Remark 1.48. ∎

Remark 1.50. On the homework, we are asked for an example of $B \subseteq A$ such that $B \cap B'$ is nontrivial for any $B' \subseteq A$ satisfying the conclusion.

In light of this decomposition, we can take the following definition.

Definition 1.51 (simple)**.** An abelian k-variety A is *k-simple* if and only if all abelian subvarieties of A are either $\{0_A\}$ or A.

Remark 1.52. It is possible to have an abelian variety be simple over k but not over $\overline{k}$.

Corollary 1.53. Fix an abelian k-variety A. Then there are simple abelian k-varieties $A_1, \dots, A_n$ such that
$$A \sim \prod_{i=1}^{n} A_i.$$

Proof. Apply Theorem 1.49, inducting on $\dim A$. Being explicit, note $\dim A = 0$ implies that A is simple because $A = \{e\}$. For the induction, note that if A is simple, there is nothing to do. Otherwise, there is an abelian subvariety $B \subseteq A$ of dimension strictly between 0 and $\dim A$. Then Theorem 1.49 provides us with $B' \subseteq A$ and an isogeny $B \times_k B' \to A$. Now, being surjective with finite kernel implies that $\dim$ is an isogney invariant, so
$$\dim A = \dim(B \times_k B') = \dim B + \dim B',$$
so $\dim B, \dim B' < \dim A$. So the induction applies to B and B', and we are done. ∎

1.3.2 Endomorphism Rings of Abelian Varieties

For uniqueness of the decomposition in Corollary 1.53, we will want to talk about morphisms between simple abelian varieties. It will be helpful to have some language for this.

Definition 1.54. Fix abelian k-varieties A and B. Then $\mathrm{Hom}_k(A,B)$ is the abelian group of homomorphisms $A \to B$, and $\mathrm{Hom}_k^0(A,B) \coloneqq \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Similarly, we define

$$\mathrm{End}_k(A) \coloneqq \mathrm{Hom}_k(A,A) \qquad \text{and} \qquad \mathrm{End}_k^0(A) \coloneqq \mathrm{Hom}_k^0(A,A).$$

Remark 1.55. Fix an abelian variety A (over $\mathbb{C}$). We show that $\mathrm{End}_k(A)$ is integral over $\mathbb{Z}$. Indeed, write $A = V/\Lambda$, and then an endomorphism $\varphi\colon A \to A$ is given by a $\mathbb{C}$-linear map $\widetilde{\varphi}\colon V \to V$ sending $\Lambda \to \Lambda$ by Proposition 1.43. To show φ is integral over $\mathbb{Z}$, it will be enough to show that the characteristic polynomial of $\widetilde{\varphi}$ has integral coefficients. Well, identify $\Lambda \cong \mathbb{Z}^{2n}$, and then we see that we induce a map $\widetilde{\varphi}\colon \mathbb{Z}^{2n} \to \mathbb{Z}^{2n}$, so $\widetilde{\varphi}$ can be written as a map with integer coefficients.

One can show that $\mathrm{Hom}_k^0(A,B)$ and $\mathrm{End}_k^0(A)$ only depend on the isogeny class of A and B. In fact, we will be able to use Corollary 1.53 to compute it.

Corollary 1.56. Fix a simple abelian k-variety A. Then $\mathrm{End}_k^0(A)$ is a division $\mathbb{Q}$-algebra.

Proof. Fix a nonzero element in $\mathrm{End}_k^0(A)$, and we will try to find an inverse for it. Because we only did a tensor product with $\mathbb{Q}$, we can create a common denominator to be able to write a generic element as $\frac{1}{d}\varphi$ for some positive integer d and nonzero k-endomorphism $\varphi\colon A \to A$. The inverse of $\frac{1}{d}$ is d, so it suffices to find an inverse to $\varphi\colon A \to A$.

The main point is the existence of "inverses" provided in Lemma 1.46. Namely, we are promised some $\psi\colon A \to A$ and a nonzero integer n such that $\varphi \circ \psi = \psi \circ \varphi = [n]_A$. Thus,

$$\varphi \circ \frac{1}{n}\psi = \frac{1}{n}\psi \circ \varphi = \mathrm{id}_A,$$

which is our inverse in A. ∎

Corollary 1.57. Fix non-isogenous simple abelian k-varieties A and B. Then the only k-homomorphism $\varphi\colon A \to B$ is the zero map.

Proof. Suppose A and B are simple abelian k-varieties, and suppose that we have a nonzero homomorphism $\varphi\colon A \to B$. We then claim that φ is actually an isogeny.

- Surjective: the image of φ (which is closed because A is proper) will be an abelian subvariety of B, and it cannot be $\{0_B\}$ because φ is nonzero, so $\mathrm{im}\,\varphi = B$.
- Finite kernel: the connected component of $\ker\varphi \subseteq A$ is an abelian subvariety of A, and it cannot be all of A because φ is nonzero, so $\ker\varphi = \{0_A\}$. Because $\ker\varphi$ is a group scheme, its connected components all have the same dimension, so $\ker\varphi$ must be zero-dimensional and hence finite. ∎

Corollary 1.58. Fix a field k and isogenous abelian k-varieties $A \sim A'$ and $B \sim B'$. Then $\mathrm{Hom}_k^0(A,B) \cong \mathrm{Hom}_k^0(A',B')$.

Proof. We use Lemma 1.46. Let $\varphi_A\colon A \to A'$ and $\varphi_B\colon B \to B'$ be the promised isogenies, and pick up $\psi_A\colon A' \to A$ and $\psi_B\colon B' \to B$ such that $\varphi_A \circ \psi_A$ and $\psi_A \circ \varphi_A$ is multiplication by n_A, and $\varphi_B \circ \psi_B$ and $\psi_B \circ \varphi_B$ is multiplication by n_B. Replacing ψ_A with $n_B\psi_A$ and replacing ψ_B with $n_A\psi_B$, we may assume that $n_A = n_B$. Anyway, we now can compute that the maps

$$\begin{aligned} \mathrm{Hom}_k^0(A,B) &\cong \mathrm{Hom}_k(A',B') \\ \alpha &\mapsto \tfrac{1}{n}\varphi_B \circ \alpha \circ \psi_A \\ \tfrac{1}{n}\psi_B \circ \alpha' \circ \varphi_A &\mapsfrom \alpha' \end{aligned}$$

are inverse homomorphisms, so we are done. ∎

Corollary 1.59. Fix sequences of pairwise non-isogenous simple abelian k-varieties denoted $\{A_i\}_{i=1}^m$ and $\{B_j\}_{j=1}^n$. Then for positive integers $\{r_i\}_{i=1}^m$ and $\{s_j\}_{j=1}^n$, we have

$$\mathrm{Hom}_k\left(\prod_{i=1}^m A_i^{r_i}, \prod_{j=1}^n B_j^{s_j}\right) \cong \prod_{\substack{i,j \\ A_i \sim B_j}} \mathrm{End}_k^0(A_i)^{r_i \times s_j}.$$

Proof. Moving out the products (which is legal because are living in an abelian category), we are looking at

$$\prod_{i,j} \mathrm{Hom}_k(A_i, B_j)^{r_i \times s_j},$$

but this term is zero unless $A_i \sim B_j$ by Corollary 1.57. In the event $A_i \sim B_j$, we can replace B_j by A_i by Corollary 1.58. ∎

Remark 1.60. Taking $A_i = B_j$ and $r_i = s_j$ in Corollary 1.59 shows that $\mathrm{End}_k^0(A)$ is a product of matrix division $\mathbb{Q}$-algebras. In particular, $\mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra.

Remark 1.61. If $\prod_{i=1}^m A_i^{r_i}$ and $\prod_{j=1}^n B_j^{s_j}$ are known to be isogenous already (to, say, an abelian variety A), then Corollary 1.59 forces $m = n$ and each i has some j such that $A_i \sim B_j$ (and vice versa). Up to permutation, we may as well force $A_i \sim B_i$ for each i. Now, having an invertible element in $\mathrm{End}_k^0(A)$ then forces having an invertible element in each $\mathrm{End}_k^0(A_i)$, so the relevant matrix algebra must have $r_i = s_i$ for each i. Thus, the decomposition of Corollary 1.53 is unique up to permutation and isogeny.

1.3.3 Complex Multiplication of Abelian Varieties

We are now ready to define complex multiplication for abelian varieties.

Definition 1.62 (complex multiplication)**.** Fix an abelian k-variety A. Then A has *complex multiplication* (or is *CM*) if and only if there is a CM algebra E (i.e., E is a finite product of CM fields) such that $[E : \mathbb{Q}] = 2 \dim A$, and there is an embedding $E \hookrightarrow \mathrm{End}_k^0(A)$.

Namely, A has "multiplication" by some CM fields.

Remark 1.63. It will turn out that this definition holds true for all abelian varieties over finite fields.

Remark 1.64. Suppose A is a simple abelian k-variety. Then A being CM is equivalent to $\mathrm{End}_k^0(A)$ being isomorphic to a CM field of degree $2 \dim A$. Certainly this condition is implied by being CM. In the other direction, over $\mathbb{C}$, one sees that $\mathrm{End}^0(A)$ acts faithfully on $H_1(A(\mathbb{C}), \mathbb{Q})$ by Proposition 1.43. Thus, $\mathrm{End}_k^0(A)$ is a division algebra of degree dividing $2 \dim A$.

Now, denoting the center of $D := \mathrm{End}_k^0(A)$ by F, it turns out that the largest field contained in D has degree (over $\mathbb{Q}$) is $[D : F]^{1/2}[F : \mathbb{Q}]$. To get this to be at most $2 \dim A$, we must have $F = D$ by a degree argument. (See [Mil20b, Section I.1] for the required facts on semisimple algebras.)

Remark 1.65. One can remove the requirement of being over $\mathbb{C}$ in the above argument by working with the "Tate module" $H^1_{\text{ét}}(A, \mathbb{Q}_\ell)$ for $\ell \neq \mathrm{char}\, k$ instead of $H^1(A(\mathbb{C}), \mathbb{Q})$. Concretely, the Tate module is

$$T_\ell A := \varprojlim_n A[\ell^n].$$

We will work more with Tate modules later in this course.

Here are some examples.

Example 1.66. Fix an imaginary quadratic field E. Then $\mathbb{C}/\mathcal{O}_E$ is a CM abelian $\mathbb{C}$-variety with complex multiplication by E; in particular, Proposition 1.43 tells us that the endomorphism ring is $\mathcal{O}_E$, so we get E upon taking $- \otimes_{\mathbb{Z}} \mathbb{Q}$. If E_1 and E_2 are distinct quadratic imaginary fields, then taking products reveals that $(\mathbb{C}/\mathcal{O}_{E_1}) \times (\mathbb{C}/\mathcal{O}_{E_2})$ has complex multiplication by $E_1 \times E_2$.

Example 1.67. Fix an imaginary quadratic field E. Then $(\mathbb{C}/\mathcal{O}_E)^2$ has endomorphism algebra given by

$$\operatorname{End}^0_{\mathbb{C}}\left((\mathbb{C}/\mathcal{O}_E)^2\right) \cong M_2(E).$$

Here, there is a lot of choice in the CM algebra embedding into $M_2(E)$. Notably, for any $D \in \mathbb{Z}$, we see

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

so $\mathbb{Q}(\sqrt{D})$ embeds into $M_2(\mathbb{Q})$ without tears.

Remark 1.68. One might be interested in understanding what abelian varieties look like in general, which leads to the notion of a moduli space. It turns out that abelian varieties with complex multiplication forms an interesting subset of the full moduli space of abelian varieties.

1.4 January 24

Here we go. Office hours begin today.

1.4.1 Classification of CM Abelian Varieties

Here is our definition. The point is that we would like to "recover" the complex multiplication of a field of CM type acting on a CM abelian variety.

Definition 1.69 (CM type)**.** Fix a CM field E, and let (A, i) be an abelian variety with complex multiplication by E by $i\colon E \to \operatorname{End}^0(A)$. Then E acts faithfully on $H_1(A(\mathbb{C}), \mathbb{Q})$. Hodge theory tells us that we can decompose

$$H^1(A(\mathbb{C}), \mathbb{C}) = H^{01} \oplus H^{10},$$

where $H^{10} = \overline{H^{01}}$; here $H^{01} = H^0(A(\mathbb{C}), \Omega^1)$ is the space of global sections 1-forms on $A(\mathbb{C})$. Dualizing, we see

$$H_1(A(\mathbb{C}), \mathbb{C}) = \operatorname{Lie} A(\mathbb{C}) \oplus \overline{\operatorname{Lie} A(\mathbb{C})},$$

and in fact E acts on $\operatorname{Lie} A(\mathbb{C})$. Decomposing $\operatorname{Lie} A(\mathbb{C})$ as an E-representation as $\bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$ where $\Phi \subseteq \operatorname{Hom}(E, \mathbb{C})$. (This decomposes into 1-dimensional representations because $E^\times$ is commutative.) Then Φ is the CM type.

Remark 1.70. The point of using the Hodge decomposition is to note that $\operatorname{Hom}(E, \mathbb{C}) = \Phi \sqcup \overline{\Phi}$ by taking the conjugation of the action. Thus, (E, Φ) is fact a CM type. Namely, we have a faithful action of $E \otimes_{\mathbb{Q}} \mathbb{C}$ on $H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = H_1(A(\mathbb{C}), \mathbb{C})$, and it decomposes into parts coming from $\operatorname{Lie} A(\mathbb{C})$ and parts coming from $\overline{\operatorname{Lie}(A(\mathbb{C}))}$. Irreducible components in $\operatorname{Lie} A(\mathbb{C})$ are $\bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$, and irreducible components in $\overline{\operatorname{Lie}(A(\mathbb{C}))}$ are then $\bigoplus_{\varphi \in \Phi} \mathbb{C}_{c\varphi}$, and in total everything must sum up to a faithful module over $E \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{\varphi \in \operatorname{Hom}(E,\mathbb{C})} \mathbb{C}_\varphi$ of rank 1, so we see $\Phi \sqcup c\Phi = \operatorname{Hom}(E, \mathbb{C})$, as needed.

Example 1.71. Fix a CM type (E, Φ), and set $A \coloneqq \mathbb{C}^\Phi/\mathcal{O}_E$. Then we claim that the CM type of A can be recovered as Φ. Namely, we certainly have an $\mathcal{O}_E$-action on A by construction, so we have an embedding $i\colon E \hookrightarrow \mathrm{End}^0(A)$ by $i(\alpha)(v_\varphi)_\varphi \coloneqq (\varphi(\alpha)v_\varphi)_\varphi$. As such, we see that the faithful action of E on the universal cover $\mathbb{C}^\Phi = H_1(A(\mathbb{C}), \mathbb{C})$ is exactly given by

$$\mathbb{C}^\Phi = \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi,$$

as needed.

We are going to classify isogeny and isomorphism classes of these abelian varieties. Quickly, we discuss our "inverse" map.

Lemma 1.72. Fix an abelian variety A with complex multiplication by $i\colon E \to \mathrm{End}^0(A)$, and let Φ be the CM type of A. Then there exists a fractional ideal $\mathfrak{a} \subseteq E$ such that $A \cong \mathbb{C}^\Phi/\mathfrak{a}$.

Proof. Set $V \coloneqq \mathrm{Lie}\, A$ so that we have a natural projection $\pi\colon V \twoheadrightarrow A$ with kernel $\Lambda \subseteq V$. By definition of the CM type, we may identify V with $\mathbb{C}^\Phi$ according to the E-action.

Now, by Proposition 1.43, E acts naturally on $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, but their ranks agree and E is a product of fields, so $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ must be isomorphic to E as a (semisimple) E-module. In particular, Λ is identified with a lattice $\mathfrak{a} \subseteq E$, as desired. ∎

The following definition will be useful.

Definition 1.73. Fix CM types (E, Φ) and (E', Φ'). An *isomorphism of CM types* is an isomorphism $\alpha\colon E \to E'$ such that

$$\Phi = \{\varphi' \circ \alpha : \varphi' \in \Phi'\}.$$

Here is the point of this definition.

Proposition 1.74. Fix a CM algebra E. Then the set of pairs (A, i) of abelian varieties with complex multiplication by i (up to isogeny commuting with i) is in bijection with CM types (E, Φ) up to isomorphism.

Proof. Here, an isogeny $\varphi\colon (A, i) \to (A', i')$ commuting with the complex multiplication is simply an isogeny $\varphi\colon A \to A'$ together with an automorphism $\alpha\colon E \to E$ such that the diagram

$$\begin{array}{ccc} E & \xrightarrow{i} & \mathrm{End}^0(A) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\varphi} \\ E & \xrightarrow{i'} & \mathrm{End}^0(A') \end{array} \tag{1.1}$$

commutes.

We now show that $(A, i) \mapsto (E, \Phi_A)$ (where Φ_A is the CM type of A) and $(E, \Phi) \mapsto \mathbb{C}^\Phi/\mathcal{O}_E$ are the needed forward and backward maps for our bijection.

- We claim that the construction of $(E, \Phi) \mapsto \mathbb{C}^\Phi/\mathcal{O}_E$ is well-defined. Well, suppose we have an isomorphism of CM types $\alpha\colon (E, \Phi) \to (E, \Phi')$. Then we get a commutative diagram as follows.

$$\begin{array}{ccccccc} \mathbb{C}^\Phi & & \dashrightarrow & & & & \mathbb{C}^{\Phi'} \\ {\scriptstyle\Phi}\uparrow & & & & & & \uparrow{\scriptstyle\Phi'} \\ \mathcal{O}_E & \longrightarrow & E & \xrightarrow{\alpha} & E' & \longleftarrow & \mathcal{O}_E \end{array}$$

Note that the bottom row becomes an isomorphism $\mathcal{O}_E \to \mathcal{O}_E$ because α and α^{-1} must carry algebraic integers to algebraic integers; this isomorphism on the bottom then extends to an isomorphism on the top because $\mathcal{O}_E$ is a full-rank lattice of our $\mathbb{C}$-vector spaces. In total, we produce an isomorphism of vector spaces $\mathbb{C}^\Phi \to \mathbb{C}^{\Phi'}$ carrying $\mathcal{O}_E$ to $\mathcal{O}_E$, which provides an isogeny $\varphi\colon \mathbb{C}^\Phi/\mathcal{O}_E \to \mathbb{C}^{\Phi'}/\mathcal{O}_E$ by Remark 1.48.

It remains to show that this isogeny φ produces an isogeny preserving the complex multiplication. Well, it is enough to note that the following diagram commutes.

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{End}^0\left(\mathbb{C}^\Phi/\mathcal{O}_E\right) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\varphi} \\ E & \longrightarrow & \mathrm{End}^0\left(\mathbb{C}^{\Phi'}/\mathcal{O}_E\right) \end{array} \qquad \begin{array}{ccc} x & \longmapsto & \left((v_\varphi) \mapsto (\varphi(x)v_\varphi)\right) \\ \downarrow & & \downarrow \\ \alpha x & \longmapsto & \left((v_\varphi) \mapsto (\varphi(\alpha x)v_\varphi)\right) \end{array}$$

- Remark 1.70 tells us that each (A, i) at least produces some CM type (E, Φ_A). We show that this is well-defined: let $\varphi\colon (A, i) \to (A', i')$ be an isogeny (with automorphism $\alpha\colon E \to E$), and we will show that we produce an isomorphism $\alpha\colon (E, \Phi_A) \to (E, \Phi_{A'})$ of CM types.

  Set $V := \mathrm{Lie}\, A(\mathbb{C})$ and $V' := \mathrm{Lie}\, A'(\mathbb{C})$, and recall that we have canonical isomorphisms $A = V/\Lambda$ and $A' = V'/\Lambda'$. By definition, Φ_A is the subset of $\mathrm{Hom}(E, \mathbb{C})$ so that $V = \bigoplus_{\varphi\in\Phi_A} \mathbb{C}_\varphi$ under the E-action, and $\Phi_{A'}$ is defined similarly. Now, Proposition 1.43 argues that the isogeny $\varphi\colon A \to A'$ lifts to an isomorphism of vector spaces $\widetilde{\varphi}\colon V \to V'$, and any element of $\mathrm{End}^0(A)$ or $\mathrm{End}^0(A')$ will also lift to an isomorphism of vector spaces. In particular, we produce a commutative diagram as follows.

$$\begin{array}{ccc} E & \xrightarrow{\ i\ } & \mathrm{End}_{\mathbb{C}}(V) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\widetilde{\varphi}} \\ E & \xrightarrow{\ i'\ } & \mathrm{End}_{\mathbb{C}}(V') \end{array}$$

  Thus, V is isomorphic to V' as an E-representation, and the decomposition $V \cong \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$ then forces V' to have a factor of $\mathbb{C}_{\varphi\circ\alpha^{-1}}$ for each $\varphi \in \Phi$, so we conclude that $\alpha\colon (E, \Phi_A) \to (E, \Phi_{A'})$ is in fact an isomorphism of CM types.

- For one inverse check, note that taking (E, Φ) to $A := \mathbb{C}^\Phi/\mathcal{O}_E$ has as its CM type just (E, Φ) back again by Example 1.71.

- For the other inverse check, we recall from Lemma 1.72 that we can write an abelian variety (A, i) with CM type (E, Φ) as $A = \mathbb{C}^\Phi/\Phi(\mathfrak{a})$ where $\mathfrak{a} \subseteq E$ is a lattice. We must show that A is isogenous to $\mathbb{C}^\Phi/\mathcal{O}_E$.

  To begin, fix a basis $\{\alpha_1, \ldots, \alpha_{2n}\}$ of $\mathfrak{a}$, and let $\mathfrak{b}_0$ be the $\mathcal{O}_E$-fractional ideal generated by these elements, and then (β) be a principal ideal containing $\mathfrak{b}_0$. There is a natural projection $\mathbb{C}^\Phi/\Phi(\mathfrak{a}) \twoheadrightarrow \mathbb{C}^\Phi/(\beta)$ given by expanding the kernel, and it is an isogeny by Remark 1.48. Now, $\beta\colon \mathcal{O}_E \to (\beta)$, so $\mathbb{C}^\Phi/(\beta) \cong \mathbb{C}^\Phi/\mathcal{O}_E$, so A is in fact isogenous to $\mathbb{C}^\Phi/\mathcal{O}_E$.

We won't bother to check that these functors are inverses of each other. ∎

Remark 1.75. We will eventually discuss the moduli space $\mathcal{A}_g$ of principally polarized g-dimensional abelian varieties. Then one can require that $\mathrm{End}(A)$ contains $\mathcal{O}_E$ for some CM field E as well as $[E : \mathbb{Q}] = 2\dim A$, and this will make finitely many points. (In fact, we produce a Shimura variety of PEL type by adding in Φ, which corresponds to a signature.) Dropping the condition that $[E : \mathbb{Q}] = 2\dim A$ could still desire a positive-dimensional subset of $\mathcal{A}_g$; in particular, we cannot expect that "just" (finite) combinatorics will be able to parameterize such abelian varieties.

Remark 1.76. We continue with a classification of the (A, i) with CM type (E, Φ). Letting $\mathcal{O} \subseteq E$ be the largest subring such that $\mathcal{O} \cdot \Lambda \subseteq \Lambda$, it turns out that $\mathrm{End}(A) = \mathcal{O}$ by Proposition 1.43. Thus, Λ is an $\mathcal{O}$-fractional ideal.

Corollary 1.77. Fix a CM algebra E and an order $\mathcal{O} \subseteq E$. Then the isomorphism classes of CM abelian varieties (A, i) with complex multiplication by $\mathcal{O} \subseteq E$ (namely, such that $i\colon \mathcal{O} \to \operatorname{End}(A)$) is in bijection with equivalence classes of triples $(E, \Phi, \mathfrak{a})$ where Φ is a CM type of E, and $\mathfrak{a} \subseteq \mathcal{O}$ is a fractional ideal. The equivalence class of triples is given by $(E, \Phi, \mathfrak{a}) \sim (E, \Phi', \mathfrak{a})$ if and only if there is an isomorphism $\alpha\colon E \to E$ carrying Φ to $\Phi' = \Phi \circ \alpha$ and $\alpha(\mathfrak{a}) = c\mathfrak{a}'$ for some $c \in E^\times$.

Proof. Use the functors of Proposition 1.74, but now we use Remark 1.76 at the end of the proof. ∎

Example 1.78. With $\mathcal{O} = \mathcal{O}_E$, we see that our abelian varieties are now in bijection with Cl_E.

Remark 1.79. Later in life, we will want to add a polarization to results such as Proposition 1.74. Additionally, we are somehow studying "geometric points" in the moduli space; there is a separate question of asking over what fields these points in the moduli space can be found over.

1.4.2 Classifying Simple CM Abelian Varieties

We would like to upgrade Proposition 1.74 to restrict to simple abelian varieties. This requires the notion of a "primitive" CM type.

Definition 1.80 (restriction, extension of CM types)**.** Fix an extension $E_0 \subseteq E$ of CM algebras.

- Given a CM type Φ_0 on E_0, we define its *extension* to E as
$$\Phi := \{\varphi \in \operatorname{Hom}(E, \mathbb{C}) : \varphi|_{E_0} \in \Phi_0\}.$$
- Suppose (E, Φ) is a CM type which is an extension of a CM type (E_0, Φ_0). Then we can recover the *restriction* to E_0 as
$$\Phi|_{E_0} := \{\varphi|_{E_0} : \varphi \in \Phi\}.$$

Remark 1.81. In fact, $\Phi|_{E_0}$ will succeed in being a CM type if and only if it is an extension. This explains the hypothesis in the definition.

Definition 1.82 (primitive)**.** Fix a CM algebra E. A CM type Φ on E is *primitive* if and only if Φ is not the extension of any CM type (E_0, Φ_0) for $E_0 \subseteq E$.

Here is a quick sanity check.

Lemma 1.83. Fix a CM type (E, Φ), where E is a field. Then there is a unique primitive CM type (E_0, Φ_0) extending to (E, Φ).

Proof. Omitted. The reference is [Mil20b, Proposition 1.9]. Basically, one may assume that E is Galois, and then one can restrict downwards via some kind of fixed field. ∎

And here is our result.

Proposition 1.84. Fix a CM field E. Then there is a bijection between simple abelian varieties A with complex multiplication by E (up to isogeny) and primitive CM types (E, Φ) up to isomorphism.

We will prove this next class.

1.5 January 26

Homework will be posted later today.

Remark 1.85. There are two notions of isogeny and isomorphism of CM abelian varieties (A, i) and (A', i') with complex multiplication by E, only one of which we used last class.

- Namely, we might want isomorphism/isogeny $f\colon A \to A'$ together with an isomorphism $\alpha\colon E \to E'$ making the following diagram commute.

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

- Alternatively, we can fix $\alpha = \mathrm{id}_E$ in the above definition.

Last class we used the second notion, despite my typos. This is needed to make isomorphisms $(E, \Phi) \cong (E', \Phi')$ make sense. Anyway, to recover the needed statements for the first notion, we need to mod out by some more isomorphisms.

1.5.1 Finishing Classification of Simple CM Abelian Varieties

Last class we were trying to show the following statement.

Proposition 1.84. Fix a CM field E. Then there is a bijection between simple abelian varieties A with complex multiplication by E (up to isogeny) and primitive CM types (E, Φ) up to isomorphism.

Proof. The point is to restrict Corollary 1.53 to simple abelian varieties. In one direction, if (E, Φ) is an extension of (E_0, Φ_0), then

$$\mathbb{C}^\Phi/\mathcal{O}_E \sim \left(\mathbb{C}^{\Phi_0}/\mathcal{O}_{E_0}\right)^{[E:E_0]}.$$

To see this, note that the right-hand side is isogenous to

$$\left(\mathbb{C}^{\Phi_0}/\mathcal{O}_{E_0}\right) \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E$$

by some sort of extension of scalars argument, and now the above abelian variety is just $\mathbb{C}^\Phi/\mathcal{O}_E$ by tracking through what it means to extend. The point is that the produced abelian variety is not simple.

In the other direction, suppose (E, Φ) is primitive, and we need to check that $\mathbb{C}^\Phi/\mathcal{O}_E$ is simple. We will sketch the idea and refer to [Mil20b, Proposition 3.6] for the full argument.

1. Suppose A has two pieces $A_1^{r_1}$ and $A_2^{r_2}$ in its decomposition into simple abelian varieties. Then we cannot find a CM field E embedding into $\mathrm{End}^0(A)$ of the required degree, due to some degree arguments.
2. Suppose A has the single piece A^r in its decomposition into simple abelian varieties. But then (E, Φ) would fail to be primitive by the above discussion unless $r = 1$, so we fall back to $r = 1$. ∎

1.5.2 A Jacobian Example

Let's do an example; see [Lan83, Section 1.7] for more.

Fix a prime p, and define the curve $C \subseteq \mathbb{P}^2_{\mathbb{C}}$ as cut out by the equation $X^p + Y^p = Z^p$. One can check that C is smooth, which tells us $g(C) = \frac{1}{2}(p-1)(p-2)$; alternatively, one can project this to $\mathbb{P}^1_{\mathbb{C}}$ and use the Riemann–Hurwitz formula directly. We will want to work with the Jacobian $\mathrm{Jac}(C)$, which is the group variety parameterized by the degree-0 divisor classes of C; one can check that $\mathrm{Jac}(C)$ is in fact an abelian variety, which we will do later in the course.

Remark 1.86. By some duality arguments, one finds that

$$J(C)(\mathbb{C}) = \frac{H^0(C,\Omega_1)^\vee}{H_1(C,\mathbb{Z})},$$

where the inclusion $H_1(C,\mathbb{Z}) \to H^0(C,\Omega_1)^\vee$ is given by integration of loops in C. Explicitly, one can take a degree-0 divisor class $\sum_{i=1}^n [P_i] - [Q_i]$ and produce an integration map

$$\omega \mapsto \sum_{i=1}^n \int_{P_i}^{Q_i} \omega,$$

which is well-defined up to the elements of $H_1(C,\mathbb{Z})$. Namely, the integral $\int_{P_i}^{Q_i}$ is not a well-defined complex number because there may be multiple paths, but this path is well-defined up to an element of $H_1(C,\mathbb{Z})$, so we are okay.

Remark 1.87. One might want to understand arithmetic objects attached to the geometric function $J(C)$, such as Galois representations or L-functions or periods. Having some CM structure grants us more information to answer these questions.

Let's see why $J(C)$ has complex multiplication.

Theorem 1.88. Fix everything as above. Then $J(C)$ has complex multiplication.

Proof. For brevity, define μ_p to be the multiplicative group of pth roots of unity. One can give μ_p a group scheme structure by viewing it as the kernel of the nth power map $(-)^n \colon \mathbb{G}_m \to \mathbb{G}_m$. Anyway, the point is that μ_p has an action on C by

$$\zeta_p \colon [X:Y:Z] \mapsto [\zeta_p X : Y : Z].$$

For example, when $p = 3$, we see that C itself will have complex multiplication by $\mathbb{Q}(\zeta_3)$, where the action by ζ_3 is given as above.

In general, we note $\mu_p \times \mu_p$ also has an action on C by

$$(\zeta_p^i, \zeta_p^j) \colon [\zeta_p^i X : \zeta_p^j Y : Z] \mapsto [\zeta_p X : Y : Z].$$

Now, the action on C provides an action on the Jacobian $J(C)$ by the degree-0 divisors viewpoint. (One can also see this by functoriality of the Jacobian construction, for example.)

To continue, we remark that one can check that our elements of $H^0(C,\Omega^1)$ have basis given by the 1-forms

$$\omega_{r,s} \coloneqq x^r y^s \cdot \frac{1}{p} \cdot \frac{dx^p}{x^p y^p},$$

where $1 \le r,s \le p-1$ when $r+s \le p-1$; here $x \coloneqq X/Z$ and $y \coloneqq Y/Z$ are coordinates on one of the standard affine charts of $\mathbb{P}^2_{\mathbb{C}}$. (We will not show this in detail.)

So we may note that $\mu_p \times \mu_p$ acts on $\omega_{r,s}$ by $(\zeta_p^i, \zeta_p^j) \colon \omega_{r,s} \mapsto \zeta_p^{ir+js}\omega_{r,s}$. For this action, we see there are $(p-2)$ orbits, each of size $\frac{1}{2}(p-1)$, where $(r,s) \sim (r',s')$ if and only if there is $m \in \mathbb{Z}/p\mathbb{Z}^\times$ such that $m(r,s) \equiv (r',s') \pmod p$.

Example 1.89. For example, at $p = 5$, we have orbits given by

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

Each of these classes will produce a simple abelian variety with complex multiplication by $\mathbb{Q}(\zeta_p)$. The point is that we can construct a curve $C_{r,s}$ with a map $C \to C_{r,s}$ via $(r,s) \mapsto (x^p, x^r y^s)$, and the holomorphic differentials of $C_{r,s}$ are the ones in the needed orbit of (r,s). So we get simple factors $J(C_{r,s}) \to J(C)$, each of which have complex multiplication by $\mathbb{Q}(\zeta_p)$, so we are done. ∎

Remark 1.90. This is not true for general curves C.

Remark 1.91. We will follow this recipe on the homework.

1.6 January 29

Homework has been posted. It looks hard. We have two weeks to do it.

1.6.1 The Rosati Involution

Here is our definition.

Definition 1.92 (Rosati involution)**.** Fix an abelian $\mathbb{C}$-variety $A = V/\Lambda$, and let $\psi\colon \Lambda\times\Lambda \to \mathbb{Z}$ be a Riemann form on A. Then we define the *Rosati involution* $(-)^\dagger\colon \operatorname{End}^0(A) \to \operatorname{End}^0(A)$ as follows: for each $\alpha \in \operatorname{End}^0(A)$, we define $\alpha^\dagger$ such that

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

for all $x, y \in \Lambda$.

Remark 1.93. Later on, we will view $(-)^\dagger$ from the lens of dual abelian varieties, as follows. Note that ψ provides an identification of Λ with its dual lattice $\Lambda^\vee$, and then $\alpha^\dagger$ is defined so that the following diagram commutes.

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

Namely, this shows that $\alpha^\dagger$ exists and is unique. Later on, we will have an analogous definition where Λs above are replaced with A itself (and $\Lambda^\vee$ is replaced with the dual abelian variety $A^\vee$).

Remark 1.94. One can check that $(\alpha^\dagger)^\dagger = \alpha$ via the above diagram.

Here is the main result.

Proposition 1.95. Fix an abelian $\mathbb{C}$-variety A with Riemann form $\psi\colon \Lambda \times \Lambda \to \mathbb{Z}$. The Rosati involution is positive: for all nonzero $\alpha \in \operatorname{End}^0(A)$, we have

$$\operatorname{Tr}(\alpha^\dagger\alpha) > 0.$$

Here, the trace map is defined by the trace in $\operatorname{End}^0(A) \subseteq \operatorname{End}(H_1(A, \mathbb{Q}))$.

Proof. Fix a $\mathbb{Q}$-basis B of $H_1(A, \mathbb{Q}) = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, by definition, we see that

$$\operatorname{Tr}(\alpha^\dagger\alpha) = \sum_{x\in B} \psi_{\mathbb{R}}(ix, \alpha^\dagger\alpha x) = \sum_{x\in B} \psi_{\mathbb{R}}(\alpha ix, \alpha x),$$

which is a sum of positive numbers because $\psi_{\mathbb{R}}$ is positive-definite by definition. ∎

Remark 1.96. There is a unique positive involution on any CM algebra E, namely its complex conjugation c. Thus, if A is a simple abelian variety with complex multiplication by $E = \mathrm{End}^0(A)$, we must have $\alpha^\dagger = c(\alpha)$, so

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

In general, if A is not simple, then one can show that there is a CM algebra $E \subseteq \mathrm{End}^0(A)$ of the correct degree and preserved by $(-)^\dagger$.

We now note that we have the following lemma.

Lemma 1.97. Fix an abelian variety $A = V/\Lambda$ with complex multiplication by $E \subseteq \mathrm{End}^0(A)$ fixed by the Rosati involution. Further, fix a non-degenerate skew-symmetric E-linear form $\psi\colon (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})^2 \to \mathbb{Q}$ such that $\psi(\alpha x, y) = \psi(x, c(\alpha y))$ for all $\alpha \in E$. Then

$$\psi(x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(\xi x c(y))$$

for all $x, y \in E$, were $\xi \in E$ and $c(\xi) - \xi$.

Proof. Do some linear algebra. ∎

And we may now give a classification of (polarized) abelian varieties.

Theorem 1.98. Fix a CM algebra E. We parameterize polarized abelian varieties with complex multiplication by E, up to isomorphism.

Proof. Here, an isomorphism $(A, i, \psi) \cong (A', i', \psi')$ is an isomorphism $f\colon A \to A'$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle i(\alpha)}\downarrow & & \downarrow{\scriptstyle i'(\alpha)} \\ A & \xrightarrow{f} & A' \end{array}$$

commutes for every $\alpha \in E$, and the diagram

$$\begin{array}{ccc} H_1(A, \mathbb{Z}) \times H_1(A, \mathbb{Z}) & \xrightarrow{\psi} & \mathbb{Z} \\ {\scriptstyle f}\downarrow & & \| \\ H_1(A', \mathbb{Z}) \times H_1(A', \mathbb{Z}) & \xrightarrow{\psi'} & \mathbb{Z} \end{array}$$

also commutes.

We now describe our constructions. Given (A, i, ψ), we build $(E, \Phi, \mathfrak{a})$ as before, where $\mathfrak{a}$ is constructor by taking the $\mathrm{End}(A)$-orbit of a chosen vector $v \in H_1(A, \mathbb{Q})$, and then we pick $\xi \in E^\times$ with $c(\xi) = -\xi$ from the above lemma. Notably, the choice of v is only defined up to multiplication by $E^\times$: replacing v with $a^{-1}v$ will adjust $\mathfrak{a}$ to $a\mathfrak{a}$, and we can see that $\xi \mapsto \xi/(a(c(a)))$. ∎

1.6.2 The Field of Definition: Abelian Varieties

We will now show that abelian varieties with complex multiplication are defined over $\overline{\mathbb{Q}}$.

Remark 1.99. One can show that $\mathrm{End}^0(A)$ is still defined over the reflex field. The same thing holds for Hodge cycles (from the perspective of the Shimura variety).

Anyway, our result will follow from the following, by taking $k = \overline{\mathbb{Q}}$.

Proposition 1.100. Fix an algebraically closed field $k \subseteq \mathbb{C}$. Then consider the base-change functor $(-)_{\mathbb{C}}$ taking abelian varieties defined over k to abelian varieties defined over $\mathbb{C}$. Then $(-)_{\mathbb{C}}$ is fully faithful and contains all CM abelian varieties in its (essential) image.

Proof. The key observation is that we have an injection $A(k) \subseteq A(\mathbb{C})$ (because $\mathbb{C}/k$ is a field extension), and we have an isomorphism $A(k)_{\text{tors}} = A(\mathbb{C})_{\text{tors}}$. Indeed, for any nonzero integer n, we see that $A(k)[n] = A[n](k)$, but $A[n](k)$ just consists of the solutions in k to some set of polynomial equations. So the solutions over k and over $\mathbb{C}$ will be the same because both these fields are algebraically closed.

Anyway, here are our checks. Fix abelian k-varieties A and A'.

- Faithful: fix $f, g\colon A \to A'$ such that $f_{\mathbb{C}} = g_{\mathbb{C}}$. Then we see that $f_{\mathbb{C}}$ and $g_{\mathbb{C}}$ are the same over $A(\mathbb{C})_{\text{tors}}$, so f and g are the same over $A(k)_{\text{tors}}$. Thus, it is enough to check that $A(k)_{\text{tors}}$ is Zariski dense in $A(k)$. Well, the Zariski closure $B \coloneqq \overline{A(k)_{\text{tors}}}$ is a smooth proper group subvariety of $A(k)$: smoothness is from $\operatorname{char} k = 0$ and $k = \overline{k}$, properness is because it is a closed subscheme of A, and being reduced follows by construction because we took the Zariski closure. So B° is an abelian subvariety with $B^\circ(k)[p] = A(k)[p]$ for all primes $p > \#\pi_0(B)$: having an element of order p outside B° would force there to be at least p connected components (one for each multiple of this element), so this can only happen for $p < \#\pi_0(B)$. Thus, we see $\dim A = \dim B^\circ$, so we must have $B^\circ = A$ because A is irreducible.

- Full: we use some descent theory. Fix a map $f\colon A_{\mathbb{C}} \to A'_{\mathbb{C}}$, which we must show is the base-change of a map $A \to A'$. Quickly, note that $k = \mathbb{C}^{\operatorname{Gal}(\mathbb{C}/k)}$ by some infinite Galois theory (or alternatively, a more direct argument via Zorn's lemma). Notably, for $\tau \in \operatorname{Gal}(\mathbb{C}/k)$, there is a map $\tau(f)\colon A_{\mathbb{C}} \to A'_{\mathbb{C}}$ given by applying τ to the coefficients of f viewed affine-locally; on $\mathbb{C}$-points, one sees that $\tau(f)$ is the composite $\left(\tau \circ f \circ \tau^{-1}\right) : A(\mathbb{C}) \to A'(\mathbb{C})$.

  Now, some descent theory shows that f is defined over k if and only if $f = \tau(f)$ for all $\tau \in \operatorname{Gal}(\mathbb{C}/k)$; approximately speaking, one can just see that the coordinates of f must all in fact be defined over k. Well, the point is that $\tau|_k = \mathrm{id}_k$, so f and $\tau(f)$ agree on $A(k)$ and hence on $A(\mathbb{C})$.

- Essential image: we will do this next class. Fix a CM abelian $\mathbb{C}$-variety A. By a spreading out argument that we will give next class (see Proposition 1.103), there is a finitely generated k-algebra $R \subseteq \mathbb{C}$ such that we have an abelian scheme $\mathcal{A}$ over $S \coloneqq \operatorname{Spec} R$ specializing to A.

  Now, $\mathcal{O} \coloneqq \operatorname{End}_{\mathbb{C}}(A)$ is finitely generated over $\mathbb{Z}$, so ensuring that these endomorphisms are all defined over R (perhaps by localizing more), we may assume that $\mathcal{O} \subseteq \operatorname{End}_R(\mathcal{A})$. In particular, $\mathcal{A}$ has complex multiplication. Choosing a geometric point of R given by $\operatorname{Spec} k \to R$ and pulling back $\mathcal{A}$ makes an abelian variety B over k.

  Quickly, note that the CM type of B is just the $\Phi \subseteq \operatorname{Hom}(E, \mathbb{C})$ appearing in the E-representation $\operatorname{Lie} B$, which is simply $\operatorname{Lie} A$. So $B_{\mathbb{C}}$ is at least isogenous with A, so there is a finite kernel $G_{\mathbb{C}} \subseteq B_{\mathbb{C}}$ such that $B_{\mathbb{C}}/G_{\mathbb{C}} \subseteq A$. But G is a finite group scheme, so it must be fully contained $B[n]$ for some n, so we can realize the quotient group scheme B/G back over k, and B/G is the required scheme.[1] ∎

Remark 1.101. Fix abelian varieties A and B defined over $\overline{\mathbb{Q}}$. Then Proposition 1.100 also tells us that a homomorphism $\varphi\colon A_{\mathbb{C}} \to B_{\mathbb{C}}$ is defined over $\overline{\mathbb{Q}}$.

1.7 January 31

We began class by finishing an argument of last class, so I have edited the argument there.

[1] Perhaps one should check that the quotient B/G makes sense as an abelian variety, but it all works out, so we won't bother.

1.7.1 Spreading Out Abelian Varieties

We quickly discuss a result on spreading out abelian varieties.

Proposition 1.102. Fix a K-variety A of finite type, and let $k \subseteq K$ be the prime field. Then there exists a finitely generated k-algebra R and an R-scheme $\mathcal{A}$ such that $\mathcal{A}_K = A$.

Proof. This follows from what it means to be finite type. ∎

Proposition 1.103. Fix an abelian K-variety A of finite type, and let $k \subseteq K$ be the prime field. Then there exists a finitely generated k-algebra R and an abelian R-scheme $\mathcal{A}$ such that $\mathcal{A}_K = A$.

Proof. We get some R and $\mathcal{A}$ by Proposition 1.102. We now spread out one condition on $\mathcal{A}$ at a time.

- Writing out equations, we may assume that the group law is well-defined by adding in enough denominators and other transcendental elements, making R larger if needed.
- For projectivity, we note that A is projective, and we can basically use the same equations to realize $\mathcal{A}$ as a closed subscheme of projective R-space.
- For smoothness, we pass to the smooth locus of $\operatorname{Spec} R$, which is nonempty because we are already smooth on the generic fiber. (Notably, we are smooth on, say, the identity section.)
- Lastly, for geometrically connected, we note that having a connected fiber is equivalent to the map $\mathcal{O}_{\operatorname{Spec} R} \to \pi_* \mathcal{O}_{\mathcal{A}}$ being an isomorphism on stalks. (Namely, we are asking for the local rings to fail to be products of R by properness.) This is an open condition, so we may again shrink $\operatorname{Spec} R$ enough to accommodate.

For a reference, Milne has an article on abelian varieties, where this argument is Remark 20.9. ∎

1.7.2 The Field of Definition: Endomorphisms

Quickly, we note that we can define a CM type as a collection $\Phi \subseteq \operatorname{Hom}(E, \overline{\mathbb{Q}})$ because E is finite étale over $\mathbb{Q}$ anyway. Notably, CM types of abelian varieties also still make sense because an abelian $\mathbb{Q}$-variety A will have its Lie algebra $\operatorname{Lie} A$ (now defined as the Zariski tangent space) continues to have the needed E-action, and we can decompose this is a representation into a $\overline{\mathbb{Q}}$-vector space.

Anyway, we now define the reflex field.

Definition 1.104 (reflex field)**.** Fix a CM type (E, Φ). Then the *reflex field* is the subfield $E^* \subseteq \overline{\mathbb{Q}}$ fixed by

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

where Φ is viewed as a subset of $\operatorname{Hom}(E, \mathbb{C})$.

Remark 1.105. If E is a field, then E^* is contained in the Galois closure of E (in $\overline{\mathbb{Q}}$).

Lemma 1.106 ([Mil20b, Proposition 1.16, 1.18]). Fix a CM type (E, Φ).

(a) E^* is generated by the elements

$$\sum_{\varphi \in \Phi} \varphi(\alpha),$$

where $\alpha \in E$.

(b) E^* a CM field.

(c) If $(E, \Phi) = \prod_{i=1}^m (E_i, \Phi_i)$, then $E^* = E_1^* \cdots E_m^*$.

(d) If (E', Φ') is an extension of (E, Φ), then $(E')^* = E^*$.

CM type? Milne, Ex 1.19. See also Lang Ch 1, S5.

Proof. Omitted. One does a little Galois theory to achieve the result. ∎

Example 1.107. If (E, Φ) is a primitive CM type with E a field, then $E = E^*$.

And now we can provide our definition field for endomorphisms.

Proposition 1.108. Fix an abelian k-variety, where $k \subseteq \mathbb{C}$. Further, suppose $A_{\overline{k}}$ is a CM abelian variety with CM type (E, Φ).

(a) If $E \subseteq \mathrm{End}_k^0(A)$, then $E^* \subseteq k$.

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

Proof. We prove one part at a time.

(a) We use (a) of Lemma 1.106. Quickly, we note that

$$\mathrm{Lie}\, A \otimes_k \mathbb{C} = \mathrm{Lie}\, A_{\mathbb{C}} = \bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi.$$

Thus, for each $\alpha \in E$, we see that the trace of α acting on $\mathrm{Lie}\, A$ is $\sum_{\varphi \in \Phi} \varphi(\alpha)$, but being defined over k requires that these endomorphisms have trace living in k. So the result follows.

Coherence of Lie?

(b) Being simple enforces $E = \mathrm{End}_{\overline{k}}^0(A_{\overline{k}})$. Now, $\mathrm{Gal}(\overline{k}/k)$ acts on $\mathrm{End}_{\overline{k}}^0(A_{\overline{k}})$, so notably we want it to act trivially on $E \subseteq \mathrm{End}_k^0(A)$ by some descent argument. Now, for each $\sigma \in \mathrm{Gal}(\overline{k}/k)$, we produce the following commutative diagram.

$$\begin{array}{ccc} \mathrm{Lie}\, A_{\overline{k}} & \xrightarrow{\sigma} & \mathrm{Lie}\, A_{\overline{k}} \\ \| & & \| \\ \bigoplus_{\varphi \in \Phi} \overline{k}_\varphi & \longrightarrow & \bigoplus_{\varphi \in \Phi} \overline{k}_\varphi \end{array}$$

In particular, σ induces an isomorphism of CM abelian varieties, so it must induce an isomorphism of CM types $\sigma \colon (E, \Phi) \to (E, \Phi)$. Thus, there is $\alpha \in \mathrm{Aut}(E)$ such that $\sigma \circ \Phi = \Phi \circ \alpha$. Because $E^* \subseteq k$, we can conclude that σ maps Φ to Φ, so actually $\Phi = \Phi \circ \alpha$. But then the primitivity of (E, Φ) forces $\alpha = \mathrm{id}_E$. ∎

Milne Prop. 1.9

Remark 1.109. This tells us that having CM makes our endomorphisms defined over $\overline{\mathbb{Q}}$.

1.8 February 2

Office hours next week will move to 2PM–4PM on Wednesday. I am pretty hopelessly behind catching up on adding details to these notes, but I will do my best to catch up over the weekend. Next week we start algebraic geometry.

1.8.1 The Shimura–Taniyama Formula

Fix an abelian variety A over a number field K. We want to "reduce A modulo" a prime $\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_K$.

Definition 1.110 (good reduction)**.** Fix an abelian variety A over a number field K. Given a prime $\mathfrak{P}$ of K, we say that A has *good reduction at* $\mathfrak{P}$ if and only if there is an abelian scheme $\mathcal{A}$ over $\mathcal{O}_{K_\mathfrak{P}}$ such that $\mathcal{A}_K = A$. By abuse of notation, we let $A_\mathfrak{P}$ denote $\mathcal{A}_{\mathcal{O}_K/\mathfrak{P}}$.

Remark 1.111. The theory of Néron models implies that the model $\mathcal{A}$ over $\mathcal{O}_{K_\mathfrak{P}}$ is unique. We will discuss this more later.

Remark 1.112. The theory of Néron models also tells us that

$$\operatorname{End}_K(A) \operatorname{End}_{\mathcal{O}_{K_\mathfrak{P}}}(\mathcal{A}) \subseteq \operatorname{End}(\mathcal{A}_\mathfrak{P}).$$

The last inclusion assumes complex multiplication of A.

Remark 1.113. It turns out that one can always extend K to have good reduction.

Definition 1.114 (Frobenius)**.** Fix a finite field $\mathbb{F}_q$. Given an $\mathbb{F}_q$-variety X, we define the *Frobenius morphism* $F_X \colon X \to X$ to be the identity on points and the q-power map on the sheaves $\mathcal{O}_X \to \mathcal{O}_X$.

Remark 1.115. On points, one can compute that the Frobenius map $F \colon \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ maps $(x_1, \dots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ to $(x_1^q, \dots, x_n^1) \in \mathbb{A}^n_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ because we are merely composing with the q-power map.

Definition 1.116 (Tate module)**.** Fix an abelian variety A over a number field K and a prime ℓ. Then we define the *Tate module* as

$$T_\ell A \coloneqq \varprojlim A\left[\ell^\bullet\right].$$

And now here is our result.

Theorem 1.117 (Shimura–Taniyama)**.** Fix an abelian variety A over a number field K of CM type (E, Φ) such that K contains all Galois conjugates of E (namely, E is a field) and $E \subseteq \operatorname{End}_K^0(A)$. If $\mathfrak{P}$ is a prime of good reduction, then the following hold.

(a) There is an element $\pi \in \mathcal{O}_E$ such that $\pi \in \operatorname{End}_K^0(A)$ is the Frobenius F_A.

(b) The ideal $(\pi) \subseteq \mathcal{O}_E$ is given by

$$\prod_{\varphi \in \Phi} \varphi^{-1}\left(\mathrm{N}_{K/\varphi(E)}\, \mathfrak{P}\right).$$

Here is another statement of Theorem 1.117.

Theorem 1.118 (Shimura–Taniyama). Fix an abelian variety A over a number field K of CM type (E, Φ), where $E \subseteq \operatorname{End}_K^0(A)$ is a field. If $\mathfrak{P}$ is a prime of good reduction, then the following hold.

(a) There is an element $\pi \in \mathcal{O}_E$ such that $\pi \in \operatorname{End}_K^0(A)$ is the Frobenius F_A.

(b) For each place $\mathfrak{p}$ of E lying over p, we have

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

where $H_v \coloneqq \operatorname{Hom}(E, \overline{\mathbb{Q}}_p) = \bigsqcup_{v|p} \operatorname{Hom}(E_v, \overline{\mathbb{Q}}_p)$.

Let's see an application.

Corollary 1.119. Fix an abelian variety A over a number field K of CM type (E, Φ), where $E \subseteq \operatorname{End}_K^0(A)$, and let $\mathfrak{P}$ be a prime of good reduction.

(a) Let P denote the characteristic polynomial of $F_{A_\mathfrak{P}}$ acting on $H_1(A(\mathbb{C}), \mathbb{Q})$. We have $P \in \mathbb{Z}[x]$.

(b) The q-adic valuation of the eigenvalues of $F_{A_\mathfrak{P}}$ given by

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

with multiplicities given by $H_v \coloneqq \operatorname{Hom}(E, \overline{\mathbb{Q}}_p)$ as before.

Proof. For (a), use Theorem 1.117 so that $\pi \in \mathcal{O}_E$ is the needed Frobenius element. Then the characteristic polynomial of π acting on $H_1(A(\mathbb{C}), \mathbb{Q})$ is simply π acting on E, so our characteristic polynomial has integer coefficients because $\pi \in \mathcal{O}_E$ is integral.

For (b), we note over $\mathbb{Q}_p$ we note that our characteristic polynomial is

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

but looping over all σ will have the same valuation as $\operatorname{ord}_v(\pi)/\operatorname{ord}_v(q)$, so normalizing with the valuation of q as 1 achieves the result directly from (b) of Theorem 1.118. ∎

Remark 1.120. Part (a) does not need Theorem 1.117; this is true without even having complex multiplication at all.

While we're here, let's see some examples.

Example 1.121. Fix an elliptic curve A with complex multiplication by an imaginary quadratic field $E/\mathbb{Q}$, and let Φ be the CM type. Fix a prime p. There are two cases.

- Ordinary: we can have $p = \mathfrak{p}_1\mathfrak{p}_2$ up in E. Then $\#H_{\mathfrak{p}_1} = \#H_{\mathfrak{p}_2}$, so the eigenvalues of the Frobenius will be 0 and 1 by looking at Theorem 1.118.
- Supersingular: we can have p inert or ramified so that $\#H_v = 2$, but then $\Phi \cap H_v$ will always have a single intersection with Φ, so our eigenvalues have valuation $1/2$ and $1/2$.

Example 1.122. Fix an abelian surface A with complex multiplication by $E \coloneqq \mathbb{Q}(\zeta_5)$. It turns out that all CM types are isomorphic to each other, so we will denote a random one by Φ. We have the following cases for an unramified prime p.

- If p splits completely, then $\#H_v = 1$ for any $v \mid p$, so the q-valuation of the eigenvalues will be 0 or 1.
- If p fails to split completely, then the q-valuations turn out to all be $1/2$. Quickly, one finds that all primes must be inert in the extension $E/\mathbb{Q}(\sqrt{5})$, and $c(H_v) = H_v$, so half of the elements will be in H_v and half not.

Remark 1.123. On the homework, we will compute the q-adic valuation of the Frobenius eigenvalues of $J(C)$ from section 1.5.2.

Remark 1.124. On the homework, we will compute an example of an abelian surface A with complex multiplication such that its q-valuations have Frobenius eigenvalues of q-valuation $\{0, 1/2, 1/2, 1\}$.

Remark 1.125. A presence of a Weil pairing on Tate modules explain why our eigenvalues of Frobenius appear "symmetric" (as in $\{0, 1/2, 1/2, 1\}$).

Anyway, let's sketch an argument for Theorem 1.118; we will do it in detail later in the class.

Warning 1.126. Today, we will discuss Theorem 1.117 under the additional assumptions that $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified, where p lies under $\mathfrak{P}$, and that $\mathrm{End}^0_K(A) \cap E = \mathcal{O}_E$.

Sketch of (a) in Theorem 1.118. For (a), we note that the action of $F_{A_{\mathfrak{P}}}$ on $\mathcal{O}_E$ commutes with the action of the larger $\mathrm{End}^0_{K_{\mathfrak{P}}}(A_{\mathfrak{P}})$, so it follows that it must live in $\mathcal{O}_E$ by an argument on semisimple modules. Namely, one does something with the Tate modules: one has $T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a rank 1 module over $\mathcal{O}_E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, so they must be the same. ■

Theme 2
Back to the Basics

Hold tight to your geometric motivation as you learn the formal structures which have proved to be so effective in studying fundamental questions.

—Ravi Vakil, [Vak17]

2.1 February 5

I did not do much over the weekend. Such is life.

2.1.1 The Rigidity Lemma

For this chapter, we will work over general fields, so we recall the following definition.

Definition 2.1 (abelian variety)**.** Fix a field k. Then an *abelian k-variety* is a group k-variety which is smooth, geometrically integral, and proper.

For example, we would like to show that the group law on A is abelian. We will want the following result.

Theorem 2.2 (Rigidity lemma)**.** Fix k-varieties X, Y, and Z. Suppose X and Y are geometrically integral, that X is proper, and that there is a point $x_0 \in X(k)$. Suppose a k-morphism $f\colon X \times_k Y \to Z$ has a point $y_0 \in Y(k)$ such that $f|_{X\times\{y\}}$ is constant, mapping to a point $z_0 \in Z(k)$. Then there is a morphism $g\colon Y \to Z$ such that $f = g \circ \mathrm{pr}_Y$ in the following diagram.

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

Proof. Plugging in $x = x_0$, we see that we must construct $g\colon Y \to Z$ by $g(y) \coloneqq f(x_0, y)$. More precisely, g is the composite

$$Y \xrightarrow{x_0} X \times_k Y \xrightarrow{f} Z.$$

We would like to show that $f = g \circ \mathrm{pr}_Y$. Now, the source is reduced, and the target is separated (everything is a variety), so it is enough to show that these maps agree on an open dense subset because then the equalizer of the two morphisms must be all of $X \times_k Y$. Well, because $X \times Y$ is irreducible (because X and Y are both geometrically integral), any nonempty open subset is dense.

Anyway, let $U \subseteq Z$ be any affine open subscheme containing x_0 so that $Z \setminus U$ is closed. Thus, $f^{-1}(Z \setminus U) \subseteq X \times Y$ continues to be closed, and because X is proper, the projection of this set to Y must still be closed. So define

$$V \coloneqq Y \setminus \mathrm{pr}_Y \left(f^{-1}(Z \setminus U) \right).$$

Quickly, note V is nonempty because $f(x_0, y_0) \in U$, implying that $y_0 \in V$. (Note we are abusing notation by identifying a geometric point with the point in its image.) So it is enough to show that

$$f|_{X \times_k V} \stackrel{?}{=} g \times \mathrm{pr}_Y|_{X \times_k V}.$$

It is enough to check this on $\overline{k}$-points because everything in sight is a variety: $\overline{k}$-points are dense because these schemes are finite type over k, so the equalizer scheme of these two morphisms would then be dense in $X \times Y$, as required.

Well, fix some $y \in V(\overline{k})$. Then f maps $X \times_k \{y\}$ to U, but $X \times_k \{y\}$ is proper, and U is affine, so f must be constant.[1] In particular, for any $x \in X(\overline{k})$, we see that

$$f(x, y) = f(x_0, y) = g(x, y),$$

as required. ∎

Let's see some applications.

Corollary 2.3. Fix abelian k-varieties A and B. Given a morphism $f \colon A \to B$, there exists a homomorphism $h \in \mathrm{Hom}_k(A, B)$ and a point $b \in B(k)$ such that $f = \tau_b \circ h$, where $\tau_b \colon B \to B$ is the translation map $b \mapsto m_B(x, b)$. In fact, if $f(e_A) = e_B$, then f is a homomorphism.

Proof. Define $b \coloneqq f(e_A)$ where $e_A \in A(k)$ is the identity. Then we see that $h \coloneqq \tau_b^{-1} \circ f$ sends $e_A \mapsto e_B$. We want to show that h is actually a group homomorphism. Well, define the map $\alpha \colon A \times A \to B$ by

$$\alpha(x_1, x_2) \coloneqq h(x_1 x_2) h(x_2)^{-1} h(x_1)^{-1}.$$

To verify that h is a homomorphism, it is enough to check that α is constantly e_B. For this, we use Theorem 2.2 on α. For example, we see that $e_A \in A(k)$ satisfies

$$\alpha(x, e_A) = h(x e_A) h(e_A)^{-1} h(x)^{-1} = h(x) e_B h(x)^{-1} = h(x) h(x)^{-1} = e_B,$$

so $\alpha(x, y) = \alpha(e_A, y)$ for all $x, y \in A(\overline{k})$ by Theorem 2.2. A symmetric argument shows that $\alpha(x, y) = \alpha(x, e_A)$ for all $x, y \in A(\overline{k})$, so we conclude that α must actually be constant. ∎

Corollary 2.4. Fix an abelian k-variety A. Then the group law on A is abelian.

Proof. The inverse map $i \colon A \to A$ maps $i(e_A) = e_A$, so i must be a homomorphism by Corollary 2.3, so

$$i(x_1 x_2) = i(x_1) i(x_2)$$

for all $x_1, x_2 \in A(\overline{k})$, so $x_1 x_2 = x_2 x_1$ for all $x_1, x_2 \in A(\overline{k})$, as required. ∎

[1] We can realize U is a closed subscheme of some affine space, so we get a morphism $X \times_k \{y\} \to \mathbb{A}^n_k$ for some $n > 0$. But then the projections of this map are all constant because maps $X \times_k \{y\} \to \mathbb{A}^1_k$ correspond to global sections of a proper integral k-scheme, which are just constants in k.

Remark 2.5. Note that we know that the group law on A is abelian, so the multiplication-by-n map $[n]\colon A \to A$ makes sense and is an endomorphism. In particular, we see $(x_1x_2)^n = x_1^n x_2^n$.

Notation 2.6. In light of Corollary 2.4, for the remainder of the course, we will denote the group law on an abelian variety additively.

2.1.2 Using The Theorem of the Cube

Here is our result. Again, the actual statement is in terms of varieties.

Theorem 2.7 (of the Cube)**.** Fix proper geometrically integral k-varieties X, Y, and Z. Given three k-points $x_0 \in X(k)$ and $y_0 \in Y(k)$ and $z_0 \in Z(k)$, suppose a line bundle $\mathcal{L}$ on $X \times Y \times Z$ has

$$\mathcal{L}|_{\{x_0\}\times Y\times Z} \quad \text{and} \quad \mathcal{L}|_{X\times\{y_0\}\times Z} \quad \text{and} \quad \mathcal{L}|_{X\times Y\times\{z_0\}}$$

all trivial. Then $\mathcal{L}$ is trivial.

Remark 2.8. In fact, Theorem 2.7 is even true if we have only two out of the three varieties being proper, but we will not need this.

We will prove Theorem 2.7 next lecture. For now, let's see how this is used.

Corollary 2.9. Fix an abelian k-variety A and a k-variety X. Given three morphisms $f, g, h\colon X \to A$ and a line bundle $\mathcal{L}$ on A, we have

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

For example, if $X = A \times A \times A$, where f, g, and h are the projections, then

$$m_{123}^*\mathcal{L} \otimes \mathrm{pr}_1^*\,\mathcal{L} \otimes \mathrm{pr}_2^*\,\mathcal{L} \otimes \mathrm{pr}_3^*\,\mathcal{L} = m_{12}^*\mathcal{L} \otimes m_{23}^*\mathcal{L} \otimes m_{31}^*\mathcal{L}.$$

Here, $m_\bullet$ denotes summing the relevant coordinates.

Proof. Pulling back the second equality along the map $(f, g, h)\colon X \to A \times A \times A$ produces the first equality, so it suffices to focus on the second equality. Well, define

$$\mathcal{K} \coloneqq m_{123}^*\mathcal{L} \otimes \mathrm{pr}_1^*\,\mathcal{L} \otimes \mathrm{pr}_2^*\,\mathcal{L} \otimes \mathrm{pr}_3^*\,\mathcal{L} \otimes m_{12}^*\mathcal{L}^{-1} \otimes m_{23}^*\mathcal{L}^{-1} \otimes m_{31}^*\mathcal{L}^{-1}.$$

It suffices to show that $\mathcal{K}$ is trivial. For this, we use Theorem 2.7. By symmetry, we will just show that $\mathcal{K}|_{\{e_A\}\times A\times A}$ is trivial, which will complete the proof. Well, upon doing this restriction, we find

$$\mathcal{K}|_{\{e_A\}\times A\times A} \cong m_{23}^*\mathcal{L} \otimes \mathrm{pr}_1^*\,\mathcal{L} \otimes \mathrm{pr}_2^*\,\mathcal{L} \otimes \mathrm{pr}_3^*\,\mathcal{L} \otimes \mathrm{pr}_2^*\,\mathcal{L}^{-1} \otimes m_{23}^*\mathcal{L}^{-1} \otimes \mathrm{pr}_3^*\,\mathcal{L}^{-1}$$

is manifestly trivial. Notably, restriction commutes with taking tensor products by construction of the tensor product. ∎

Remark 2.10. Of course, an induction can extend past three projections.

In particular, we will use Corollary 2.9 in order to compute $[n]^*\mathcal{L}$.

Corollary 2.11. Fix a line bundle $\mathcal{L}$ on an abelian k-variety A. Then, for any $n \in \mathbb{Z}$,

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

In particular, if $\mathcal{L} = [-1]^*\mathcal{L}$, then $[n]^*\mathcal{L} = \mathcal{L}^{\otimes n^2}$.

Proof. Induct on n using Corollary 2.9 for the inductive step. Namely, $n = 0$ and $n = -1$ have no content, and then one can induct upwards and downwards from there. ■

Remark 2.12. The quadratic relation here is what is used in the construction of the Néron–Tate height.

2.2 February 7

We continue.

2.2.1 Preparing The Theorem of the Cube

Let's give another application of Theorem 2.7.

Corollary 2.13. Fix an abelian k-variety A and two points $x, y \in A$. Given a line bundle $\mathcal{L}$, we have

$$t_{x+y}^*\mathcal{L} \cong t_x^*\mathcal{L} \otimes t_y^*\mathcal{L}.$$

Proof. Apply Corollary 2.9 to the maps $f \equiv x$ and $g \equiv y$ and $h := \mathrm{id}_A$. ■

Remark 2.14. Fix a finite field extension k'/k. Then given a line bundle $\mathcal{L}$, we produce a group homomorphism $A(k') \to \operatorname{Pic} A_{k'}$ given by $x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$.

We will now prove Theorem 2.7. We will prove under the hypothesis where k is algebraically closed. The following lemma tells us that this is fine most of the time.

Lemma 2.15. Fix a proper geometrically integral k-scheme V. Then $\Gamma(V, \mathcal{O}_V) = k$.

Proof. This is [SP, Lemma 0BUG]. ■

Lemma 2.16. Fix a proper geometrically integral k-scheme V. Given a line bundle $\mathcal{L}$ on V, if $\mathcal{L}_{\overline{k}}$ over $V_{\overline{k}}$ is trivial, then $\mathcal{L} \cong \mathcal{O}_V$ over k.

Proof. Quickly, we claim that $\mathcal{L}$ is trivial if and only if $\Gamma(V, \mathcal{L}) \neq 0$ and $\Gamma\left(V, \mathcal{L}^{-1}\right) \neq 0$. Certainly if $\mathcal{L}$ is trivial, then those are $\mathcal{O}_V(V) \neq 0$. Conversely, suppose we have nonzero elements $s \in \Gamma(V, \mathcal{L})$ and $t \in \Gamma(V, \mathcal{L}^{-1})$, which correspond to maps $s \colon \mathcal{O}_V \to \mathcal{L}$ and $t \in \mathcal{L} \to \mathcal{O}_V$. But now the composite

$$\mathcal{O}_V \xrightarrow{s} \mathcal{L} \xrightarrow{t} \mathcal{O}_V$$

is given by a global section $ts \in \mathcal{O}_V(V)$, which is a field and hence invertible, so we see that the above composite is invertible, so both s and t must be isomorphisms (e.g., by looking at stalks).

Thus, to complete the proof, we note that

$$\Gamma(V_{\overline{k}}, \mathcal{L}'_{\overline{k}}) = \Gamma(V, \mathcal{L}) \otimes_k \overline{k}$$

because cohomology commutes with faithfully flat base-change, so the left-hand is nonzero if and only if $\Gamma(V, \mathcal{L})$ is nonzero. ■

In particular, Theorem 2.7 follows from the algebraically closed case.

2.2.2 Review of Cohomology

We quickly review some cohomology; we refer to [Har77, Chapter III] for proofs.

Fix a morphism $f\colon X \to Y$ of Noetherian schemes. Sheaf cohomology is usually given by taking the right-derived functors $H^\bullet(X, -) \coloneqq R^\bullet\Gamma(X, -)$. We also a pushforward of f, which becomes a left-exact functor $f_*\colon \mathrm{QCoh}(X) \to \mathrm{QCoh}(Y)$, so we can consider its right-derived functors $R^\bullet f_*$. Further, if f is proper, then $R^\bullet f_*$ sends coherent sheaves to coherent. Being right-derived functors, we have the following properties.

- $R^0 f_* = f_*$.
- Given an exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ of quasicoherent sheaves on X, we have a long exact sequence
$$0 \to R^0 f_* \mathcal{F}' \to R^0 f_* \mathcal{F} \to R^0 f_* \mathcal{F}'' \xrightarrow{\delta^1} R^1 f_* \mathcal{F}' \to \cdots.$$
- If Y is affine, then $R^\bullet f_* \mathcal{F} = \widetilde{H^\bullet(X, \mathcal{F})}$. Indeed, the point is that $\widetilde{\cdot}$ is exact, so we can just check that we have an isomorphism of δ-functors by hand.
- If $Y = \operatorname{Spec} R$ is affine, and X is separated, we can compute $H^\bullet(X, \mathcal{F})$ via Čech cohomology as follows: let $\mathcal{U}$ be an open cover of X by affine open subschemes, and we define the Čech complex $C^\bullet(\mathcal{U}, \mathcal{F})$ of R-modules as follows: define
$$C^n(\mathcal{U}, \mathcal{F}) \coloneqq \prod_{i_0 < \cdots < i_n} \Gamma(U_{i_0} \cap \cdots \cap U_{i_n}, \mathcal{F})$$
and $d^n\colon C^n(\mathcal{U}, \mathcal{F}) \to C^{n+1}(\mathcal{U}, \mathcal{F})$ by
$$(d^n\sigma)_{i_0 < \cdots < i_{n+1}} \coloneqq \sum_{j=0}^{n+1} (-1)^j (\sigma_{i_0 < \cdots < \widehat{j} < \ldots < i_{n+1}})|_{U_{i_0} \cap \cdots \cap U_{i_{n+1}}}.$$
Then $H^n(X, \mathcal{F})$ agrees with the cohomology of the Čech complex.

We will also want the following two big results.

Theorem 2.17 (Semicontinuity)**.** Fix a proper morphism $f\colon X \to Y$ of Noetherian schemes. Suppose that a coherent sheaf $\mathcal{F}$ is flat over Y; i.e., $\mathcal{F}_x$ is flat over $\mathcal{O}_{Y, f(x)}$ for each $x \in X$. Then for each $n \geq 0$, the function $Y \to \mathbb{Z}$ given by
$$y \mapsto \dim_{k(y)} H^n(X_y, \mathcal{F}|_{X_y})$$
is upper semi-continuous. In particular,
$$\left\{y \in Y : \dim_{k(y)} H^n(X_y, \mathcal{F}|_{X_y}) \leq a\right\} \subseteq Y$$
is closed for all $a \in \mathbb{Z}$.

We may be interested in equality.

Theorem 2.18 (Grauert)**.** Fix a proper morphism $f\colon X \to Y$ of Noetherian schemes. Suppose that a coherent sheaf $\mathcal{F}$ is flat over Y; i.e., $\mathcal{F}_x$ is flat over $\mathcal{O}_{Y,f(x)}$ for each $x \in X$. The following are equivalent for some $n \geq 0$.

(i) The function $y \mapsto \dim_{k(y)} H^n(X_y, \mathcal{F}|_{X_y})$ is constant.

(ii) $R^n f_* \mathcal{F}$ is locally free of finite rank, and

$$R^n f_* \mathcal{F} \otimes k(y) \simeq H^n(X_y, \mathcal{F}|_{X_y}).$$

2.2.3 The Seesaw Principle

Anyway, our proof of Theorem 2.7 will come from the following result.

Proposition 2.19 (Seesaw principle)**.** Fix a proper geometrically integral k-scheme X and a k-variety T. Fix a line bundle $\mathcal{L}$ on $X \times T$.

(a) The set $T_1 \coloneqq \{\text{closed } t \in T : \mathcal{L}|_{X\times\{t\}} \text{ is trivial}\}$ is closed.

(b) There is a line bundle $\mathcal{M}$ on T_1 such that $\mathcal{L}|_{X\times T_1} \cong \mathrm{pr}_{T_1}^*(\mathcal{M})$.

Intuitively, what's going on here is that we are trying to bring a line bundle on the product to come from a subscheme of our test scheme T.

Proof of Proposition 2.19. We use our cohomology results. Note that $\mathcal{L}|_{X\times\{t\}}$ trivializing is equivalent to having $\Gamma(X \times \{t\}, \mathcal{L}^{\pm 1}|_{X\times\{t\}})$ failing to be trivial. But applying this to $n = 0$ in Theorem 2.17, we see that these are closed subsets of T, so (a) follows.

For (b), we note that we are achieving equality with

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

always, so Theorem 2.18 tells us that $\mathcal{M} \coloneqq \mathrm{pr}_{T_1 *}\,\mathcal{L}$ is a locally free sheaf of finite rank of rank 1. Now, we have an adjunction map

$$\mathrm{pr}_{T_1}^*\,\mathcal{M} = \mathrm{pr}_{T_1}^*\,\mathrm{pr}_{T_1 *}\,\mathcal{L} \to \mathcal{L},$$

which we can check is an isomorphism on stalks over T_1. By Nakayama, we may check that this is an isomorphism actually on fibers, so we may check that the result is merely nonzero on fibers (because these are just fields on the fibers), but then it's nonzero on the other side of the adjunction, so the above map must continue to be an adjunction. ∎

Remark 2.20. Take $k = \mathbb{C}$, and we will argue for Theorem 2.7. For $W \coloneqq X \times Y \times Z$, we note that we have the exact sequence

$$0 \to \underline{\mathbb{Z}} \to \mathcal{O}_W \xrightarrow{\exp} \mathcal{O}_W^\times \to 1,$$

which produces the long exact sequence

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

We have a line bundle $\mathcal{L}$ on W which we would like to check is trivial, so with $H^1(W, \mathcal{O}_W^\times) = \operatorname{Pic} W$, we may as well check triviality through the sequence. Note the Künneth formula allows us to decompose $H^2(W, \underline{\mathbb{Z}})$ into smaller factors, and we see $\mathcal{L}$ trivializes in all those factors by the hypothesis on $\mathcal{L}$. So we see that our line bundle must come from $H^1(W, \mathcal{O}_W)$, but it must come from something trivial there by doing a similar Künneth formula computation. So $\mathcal{L}$ will trivialize; note that this argument actually works on arbitrary products bigger than 3.

We will prove Theorem 2.7 next class. The point is to reduce to curves, where cohomology is understood.

2.3 February 9

Today we will prove the Theorem of the Cube.

2.3.1 Proof of The Theorem of the Cube

We prove Theorem 2.7. The strategy is to reduce to the case of curves.

Theorem 2.7 (of the Cube)**.** Fix proper geometrically integral k-varieties X, Y, and Z. Given three k-points $x_0 \in X(k)$ and $y_0 \in Y(k)$ and $z_0 \in Z(k)$, suppose a line bundle $\mathcal{L}$ on $X \times Y \times Z$ has

$$\mathcal{L}|_{\{x_0\}\times Y\times Z} \quad \text{and} \quad \mathcal{L}|_{X\times\{y_0\}\times Z} \quad \text{and} \quad \mathcal{L}|_{X\times Y\times\{z_0\}}$$

all trivial. Then $\mathcal{L}$ is trivial.

We have two steps. To begin, we reduce to the case where X is a curve. We will want the following tools.

Theorem 2.21 (Chow's lemma)**.** Fix a proper A-scheme $\pi\colon X \to \operatorname{Spec} A$. Then there is an A-scheme map $\mu\colon X' \to X$ such that μ is surjective and projective, X' is projective, and there is an open dense subscheme $U \subseteq X$ such that $\mu\colon \mu^{-1}U \to U$ is an isomorphism.

Proof. See [Vak17, Vakil 19.9.2]. ∎

Theorem 2.22 (Bertini)**.** Fix an infinite field k and a geometrically integral projective k-scheme $X \subseteq \mathbb{P}^N_k$. Then there is a hyperplane $H \subseteq \mathbb{P}^N_k$ such that $H \cap X$ is geometrically integral. In fact, the collection of $H \in \left(\mathbb{P}^N_k\right)^\vee$ with $H \cap X$ geometrically integral is Zariski dense.

Remark 2.23. One can add adjectives to X and then to the conclusion, like smoothness.

Remark 2.24. One can allow finite fields by working with hypersurfaces instead of hyperplanes; see [CP14].

This allows us to prove the following geometric fact.

Lemma 2.25. Fix a proper, geometrically integral k-variety X. For any two closed points $x_0, x_1 \in X$, there is a closed 1-dimensional k-subvariety $C \subseteq X$ containing x_0 and x_1.

Proof. By Chow's lemma (Theorem 2.21), we may assume that X is projective, basically by pulling back along our map $\mu\colon X' \to X$; getting back to X, one needs to project back along μ.

Explicitly, one can use Theorem 2.22 to the blow-up $\operatorname{Bl}_{\{x_0,x_1\}} X \to X$. Then x_0 and x_1 become codimension-1 closed subvarieties of the blow-up, so we can get them to intersect with a hypersurface (see Remark 2.24). So we may induct downwards. ∎

Remark 2.26. This statement is still true for any finite set of points.

Let's now do the reduction.

Reduction to the curve case. It is enough to show that $\mathcal{L}|_{\{x\}\times Y\times\{z\}}$ is trivial for all (x, z). Indeed, by Proposition 2.19, one finds that $\mathcal{L} = \operatorname{pr}_{13}^* \mathcal{M}$ for some line bundle $\mathcal{M}$ on $X \times Z$. Then the hypothesis tells us that $\mathcal{L}|_{X\times\{y_0\}\times Z}$ is trivial (replace X with a curve connecting x with x_0), so $\mathcal{M}$ will trivialize, so $\mathcal{L}$ will trivialize. ∎

Warning 2.27. I did not really follow the below proof during class.

Proof in the curve case. Fix $g := g(X)$. Then we claim that there is a divisor $E \subseteq X$ of degree g such that $\Gamma(X, \Omega_X(-E)) = 0$. Well, we are looking for global differentials on X which vanish on E, so we choose points one at a time.

Now, define $\mathcal{M} := \mathrm{pr}_1^* \mathcal{O}_X(E) \otimes \mathcal{L}$, and let W denote the support of $R^1 \mathrm{pr}_{23*} \mathcal{M}$, which is a closed subscheme of $Y \times Z$ by definition. Now, for all $y \in Y$, we know that $\mathcal{L}|_{X\times\{y\}\times\{z_0\}}$ is trivial, so $\mathcal{M}|_{\{x\}\times\{y\}\times\{z_0\}} \cong \mathcal{O}_E$. But then

$$H^1(X \times \{y\} \times \{z_0\}, M|_{X\times\{y\}\times\{z_0\}}) = H^1(X, \mathcal{O}_X(E)) \cong H^0(X, \Omega_X(-E)),$$

where the last isomorphism is by Serre duality. But now $H^0(X, \Omega_X(-E)) = 0$ by construction of E, so the point is that $W \cap (Y \times \{z_0\})$ is empty.

Now, because Y is proper, we see $\mathrm{pr}_Z(W) \subseteq Z$ is closed and avoiding z_0, so we can find an open $Z' \subseteq Z$ around z_0 such that $W \cap (Y \times Z') = 0$. As such, we claim that $\mathcal{L}|_{X\times Y\times Z'}$ trivializes, which will be enough by Proposition 2.19. Now, $R^1 \mathrm{pr}_{23*} \mathcal{M}$ is locally free of rank 1 on $Y \times Z'$: it is enough to check that the Euler is constantly 1, but being locally constant allows us to compute it on z_0, so

$$\chi(M|_{X\times\{y\}\times\{z_0\}}) = \chi(\mathcal{M}|_{X\times\{y\}\times\{z_0\}}) = \chi(\mathcal{O}_X(E)),$$

and we know $\chi(\mathcal{O}_X(E)) = 1$ by a Riemann–Roch computation.

Being a line bundle now produces a divisor $D \subseteq X \times Y \times Z'$. Namely, on an affine open cover $\{U_i\}$ on $Y \times Z$, one has isomorphisms $\alpha_i \colon \mathcal{O}_{U_i} \to \mathcal{N}|_{U_i}$, and we let D_i denote the zero set of $\alpha_i(1)$ in $X \times U_i$, and we can glue these D_i together. Namely, on the intersections, one can check gluing data from $\mathcal{N}$. The point is that $\mathcal{O}(D)|_{X\times\{y\}\times\{z\}} \cong \mathcal{M}|_{X\times\{y\}\times\{z\}}$ for all $(y, z) \in Y \times Z$, essentially by construction.

Quickly, we claim that $D = E \times Y \times Z$. Well, find some $p \in X$ not in the support of E, and we will show that $D \cap (\{p\} \times Y \times Z)$ is empty, which will imply the claim because then we will find that D is the needed sum of points in E's support times $Y \times Z$. So we will be able to complete the proof by restricting computing $\mathcal{L}$ on D by its restriction to $X \times \{y_0\} \times \{z_0\}$, which we know to be trivial already.

Well, to show the claim, we (sub)claim

$$(D \cap (\{p\} \times Y \times Z)) \cap ((\{p\} \times Y \times \{z_0\}) \cup (\{p\} \times \{y_0\} \times Z)) \stackrel{?}{=} \varnothing.$$

Well, $\mathcal{L}$ trivializes on $X \times \{y_0\} \times Z$ and $X \times Y \times \{z_0\}$ already, so $\mathcal{M}$ on this restriction is $\mathcal{O}_X(E)$, so this intersection must then be empty.

We now upgrade using that Y is proper. The projection $\mathrm{pr}_Z(D \cap (\{p\} \times Y \times Z))$ is a closed subset of Z, so $D \cap (\{p\} \times Y \times Z)$ must just be $\{p\} \times Y \times Z''$ for a codimension-1 subscheme $Z'' \subseteq Z$. But the previous subclaim now requires everything to be empty.

We now complete the proof. Right now we know that $\mathcal{O}(D)|_{X\times\{y\}\times\{z\}}$ must be $\mathrm{pr}_1^* \mathcal{O}(E)|_{X\times\{y\}\times\{z\}}$ by the claim of the previous paragraphs. But $\mathcal{O}(D)$ is just $\mathcal{M}$, so we are being told that $\mathcal{L}|_{X\times\{y\}\times\{z\}}$ is trivial, so Proposition 2.19 along with the trivialization of $\mathcal{L}|_{\{x_0\}\times Y\times Z}$ completes the argument that $\mathcal{L}$ is trivial. ∎

2.4 February 12

The homework is due today.

2.4.1 Ample Line Bundles on Abelian Varieties

Today we will show that abelian varieties are projective. The point is to exhibit an ample line bundle, so we want to understand ample line bundles.

As a corollary to Theorem 2.7, we have the following result.

Theorem 2.28 (of the Square)**.** Fix a line bundle $\mathcal{L}$ on an abelian k-variety A. For any $a \in A(\overline{k})$, let $t_a \colon A \to A$ denote the translation. Then for any $x, y \in A(\overline{k})$, we have

$$t_{x+y}^* \mathcal{L} \cong t_x^* \mathcal{L} \otimes t_y^* \mathcal{L}.$$

Thus, the map $\varphi_{\mathcal{L}} \colon A(\overline{k}) \to \operatorname{Pic}(A_{\overline{k}})$ given by $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ is a group homomorphism.

Proof. For the first claim, take $f \colon \{x\} \to A$ and $g \colon \{y\} \to A$ and $h \colon \{0_A\} \to A$ and apply Corollary 2.9. For the second claim, we simply expand $\varphi_{\mathcal{L}}(x+y) = \varphi_{\mathcal{L}}(x) \otimes \varphi_{\mathcal{L}}(y)$ directly. ■

Remark 2.29. In fact, $\varphi_\bullet \colon \operatorname{Pic} A \to \operatorname{Hom}(A(\overline{k}), \operatorname{Pic}(A_{\overline{k}}))$ is a group homomorphism, which we can see by expanding out the definitions directly.

So we may make the following definition.

Definition 2.30. Fix an abelian k-variety A. Then we define the subgroup $\operatorname{Pic}^0(A) \subseteq \operatorname{Pic}(A)$ as $\ker \varphi_\bullet$. In other words, $\varphi \in \operatorname{Pic}^0(A)$ if and only if $\varphi_{\mathcal{L}}$ is trivial.

Example 2.31. For an elliptic curve A, one can identify A with $\operatorname{Pic}^0(A)$, so we get an exact sequence

$$0 \to \operatorname{Pic}^0(A) \to \operatorname{Pic}(A) \to \mathbb{Z} \to 0,$$

where the last map is the degree map.

Let's describe Pic^0 in a better way.

Lemma 2.32. Fix an abelian k-variety A. Then $\mathcal{L} \in \operatorname{Pic}^0(A)$ if and only if $m^* \mathcal{L} \cong \operatorname{pr}_1^* \mathcal{L} \otimes \operatorname{pr}_2^* \mathcal{L}$.

Proof. We have two implications to show.

- Suppose $m^* \mathcal{L} \cong \operatorname{pr}_1^* \mathcal{L} \otimes \operatorname{pr}_2^* \mathcal{L}$. We must show that $\varphi_{\mathcal{L}}$ is trivial. Well, fix some point $x \in A(\overline{k})$, and let $i_x \colon \{x\} \to A$ be the closed embedding. By definition, one sees
$$t_x^* \mathcal{L} = i_x^* m^* \mathcal{L} = i^* \left(\operatorname{pr}_1^* \mathcal{L} \otimes \operatorname{pr}_2^* \mathcal{L} \right) = \mathcal{O}_A \otimes \mathcal{L}$$
by some projections. So $\varphi_{\mathcal{L}}(x) = \mathcal{O}_A$ is trivial.
- Suppose $\mathcal{L} \in \operatorname{Pic}^0(A)$. Define $\mathcal{M} \coloneqq m^* \mathcal{L} \otimes \operatorname{pr}_1^* \mathcal{L}^{-1} \otimes \operatorname{pr}_2^* \mathcal{L}^{-1}$, which we want to show is trivial. Now, for each $x \in A(\overline{k})$, we see that
$$M|_{A \times \{x\}} \cong \mathcal{O}_A,$$
so Proposition 2.19 means that $\mathcal{M}$ must pull back to a trivial line bundle on both factors, so $\mathcal{M}$ is actually trivial. ■

We now pick up some notation.

Definition 2.33. Fix an abelian k-variety A. For a line bundle $\mathcal{L}$ on A, we define $K(\mathcal{L}) \coloneqq \ker \varphi_{\mathcal{L}}$, which by definition is

$$\{x \in A(\overline{k}) : t_x^* \mathcal{L} \cong \mathcal{L}\}.$$

Remark 2.34. Once we upgrade Pic to a scheme, we can view $K(\mathcal{L})$ as the closed subscheme $\ker \varphi_{\mathcal{L}}$. For today, it will be enough to realize that $K(\mathcal{L})$ is Zariski closed and then view it as a reduced closed subscheme of A.

Remark 2.35. One has $K(\mathcal{L}) = A$ if and only if $\mathcal{L} \in \mathrm{Pic}^0(A)$.

Let's check that $K(L)$ is Zariski closed.

Lemma 2.36. Fix an abelian k-variety A. For a line bundle $\mathcal{L}$ on A, the subset $K(\mathcal{L}) \subseteq A$ is Zariski closed.

Proof. By definition, we see

$$K(\mathcal{L}) = \left\{x \in A(\overline{k}) : m^*\mathcal{L} \otimes \mathrm{pr}_2^*\, \mathcal{L}^{-1}|_{A\times\{x\}} \cong \mathcal{O}_A\right\}.$$

However, a computation with Proposition 2.19 shows that $K(\mathcal{L})$ is closed. ∎

Lemma 2.37. Fix an abelian k-variety A. For a line bundle $\mathcal{L}$ on A, we have $K\left(\mathcal{L}^{-1}\right) = K(\mathcal{L})$.

Proof. Direct from the definition. ∎

Notably, the above lemma tells us that we cannot tell if a line bundle is ample just from looking at $K(\mathcal{L})$: if $\mathcal{L}$ is ample, then $\mathcal{L}^{-1}$ is almost never ample. So we will need some notion of effectivity in the following result.

Theorem 2.38. Fix an abelian k-variety A. For an effective divisor D on A, set $\mathcal{L} \coloneqq \mathcal{O}(D)$. Then the following are equivalent.

(a) $\mathcal{L}$ is ample.

(b) $K(\mathcal{L})$ is finite.

(c) $H(D) \coloneqq \{\text{closed } x \in A : x + D = D\}$ is finite.

(d) The linear system $|2D| \coloneqq \Gamma(X, \mathcal{O}_A(2D))/k^\times$ (or equivalently, the collection of effective divisors linearly equivalent to $2D$) is base-point free, and the map $A \to \mathbb{P}_k^{|2D|}$ is finite.

Note $x + D = D$ is literal equality, not linear equivalence of divisors. Also, the addition by x is a translation.

Proof. The equivalence of (a) and (d) is algebraic geometry not arising from abelian varieties.

- We show (a) implies (b). Certainly $K(\mathcal{L})$ is a closed k-subgroup of A. In particular, $B \coloneqq K(\mathcal{L})^\circ$ will be connected (hence geometrically integral), reduced (hence smooth), and proper, so B is an abelian variety. But by definition of B, we know $t_x^*\mathcal{L}|_B \cong \mathcal{L}|_B$, so $\mathcal{L}|_B \in \mathrm{Pic}^0(B)$, so Lemma 2.32 implies

  $$m^*\mathcal{L}|_B \cong \mathrm{pr}_1^*\, \mathcal{L}|_B \otimes \mathrm{pr}_2^*\, \mathcal{L}|_B$$

  as line bundles on $B \times B$. Now $([1], [-1])\colon B \to B \times B$ has both $[1]\colon B \to B$ and $[-1]\colon B \to B$ being isomorphisms, by $m \circ ([-1], [1]) = [0]$, so pulling back along $([1], [-1])$ implies

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

  But then $\mathcal{L}|_B$ is ample, and $[-1]$ is an isomorphism, so $[-1]^*\mathcal{L}|_B$ is ample, so $\mathcal{O}_B$ is ample. But then B must have dimension 0, meaning that B is finite, so $K(\mathcal{L})$ is also finite.

- We show (b) implies (c). Indeed, $x \in H(D)$ with $x + D = D$ then implies $t_x^* \mathcal{L} \cong \mathcal{L}$, so $H(D) \subseteq K(\mathcal{L})$, which is enough.

- We sketch (d) implies (a). It suffices to show that $\mathcal{L}^{\otimes 2}$ is ample. We claim that the pullback of an ample line bundle by a finite morphism is ample. Well, $\mathcal{L}^{\otimes 2}$ is ample if and only if

$$H^i\left(X, \mathcal{F} \otimes \mathcal{L}^{\otimes 2n}\right) = 0$$

for all coherent sheaves $\mathcal{F}$ and indices $i > 0$. (The forward implication is just by a cohomology computation, noting that $\mathcal{L}$ to a sufficiently high power will simply induce an embedding to projective space, allowing us to compute the cohomology in projective space.)

- We show (c) implies (d). Quickly, we note that $(x + D) + (-x + D) \sim 2D$ by translating around, via Theorem 2.28.

  Now, to be base-point free, we want to show that each point $p \in A$ has some section x such that $(x + D) + (-x + D)$ fails to vanish on y; equivalently, we are asking for $x \notin (-y + D)$ and $x \notin y + D$. But $-y + D$ and $y + D$ are both of codimension 1 in A, so these two divisors cannot cover A.

  Lastly, we need to show that the associated map $\varphi \colon A \to \mathbb{P}_k^N$ is finite. Well, because A is proper, it follows that φ is proper, so it suffices to show that φ is quasifinite. Well, suppose for the sake of contradiction that we have a closed point $y \in \mathbb{P}_k^N$ with infinite fiber; surely the fiber is quasicompact, so the fiber must actually have positive dimension. Namely, there will be an irreducible proper curve $C \subseteq A$ such that $\varphi(C)$ is a point; notably, proper curves are projective, so we may as well say that C is projective.

  Well, for any effective divisor $E \in |2D|$, we either have $E \cap C = C$ or $E \cap C = \varnothing$. For this, we will use Lemma 2.40, proven next class. Indeed, setting $E' \coloneqq x + D$ for some $x \in C$, one must have $(x+D) \cup (-x+D) \cap C \neq \varnothing$, so any $x, y \in C$ will have $(x - y + x) + D = x + D$, meaning $x - y \in H(D)$. But we have put too many points in $H(D)$, so we have achieved our contradiction. ∎

Corollary 2.39. Fix an abelian k-variety A. Then A is a projective k-scheme.

Proof. It suffices to produce an ample line bundle $\mathcal{L}$. By Theorem 2.38, it suffices to produce an effective divisor D such that $H(D) \coloneqq \{\text{closed } x \in A : x + D = D\}$ is finite.

For our construction, let $U \subseteq A$ be an affine open neighborhood of e. Then $D \coloneqq A \setminus U$ is an effective divisor (it is a fact that D is pure of codimension 1!). We will show our finiteness in two claims.

- We claim $H(D) \subseteq U$. Indeed, if $x \in H(D)$, then $x + D = D$, so $x + U = U$ by taking complements, so $x \in U$.

- We claim $H(D) \subseteq A$ is closed. Indeed, note there is a map $m \colon A \times D \to A$, and $H(D)$ by definition is $\operatorname{pr}_A\left(m^{-1}(D)\right)$. But $D \subseteq A$ is closed, and A is proper, so $H(D)$ is thus closed.

The above two claims imply that $H(D)$ is finite: giving $H(D)$ the reduced closed subscheme structure, we see that $H(D) \subseteq A$ is a proper k-variety, but it is contained in the affine k-variety U, so $H(D)$ must be zero-dimensional. (For example, to show finiteness, we may as well assume irreducibility, but then if we have positive dimension, then we will get non-constant global sections from U, so $\dim H(D) = 0$ is forced.) ∎

2.5 February 14

We began class by completing the proof of Theorem 2.38, which I have edited into directly.

2.5.1 Finishing Up Ample Line Bundles

From last class, we needed the following lemma.

Lemma 2.40. Fix an irreducible projective curve C sitting inside an abelian k-variety A. Given an effective divisor E with $E \cap C = \varnothing$, we will have $(x-y)+E = E$ for any $x, y \in C$.

Proof. Fix $\mathcal{L} \coloneqq \mathcal{O}_A(E)$; the hypothesis is that $\mathcal{L}|_C = \mathcal{O}_C$. Note there is a (restricted) multiplication map $m\colon C \times A \to A$, so we may look at the line bundle $m^*\mathcal{L}$ on $C \times A$. For example, for $a \in A$, we may compute

$$\chi\left(m^*\mathcal{L}|_{C\times\{x\}}\right) = \chi\left(t_x^*\mathcal{L}|_C\right).$$

On the other hand, the Euler characteristic needs to be constant in our family, so we can compute this at $x = 0_A$ as $\chi(t_0^*\mathcal{L}|_C) = \chi(\mathcal{O}_C)$. From here, Riemann–Roch implies $\deg t_x^*\mathcal{L}|_C = \deg \mathcal{O}_C = 0$. But E being an effective divisor requires that $t_x^*\mathcal{L}|_C$ to fully trivialize, so either $(x+E)$ cannot intersect C at all. Thus, for any $x, y \in C$ and $z \in E$, one has $z \in (z-y+C) \cap E$, so actually $z - y + C \subseteq E$, so $z - y + x \in E$, so $z \in (y-x) + E$. Looping over all $z \in E$ completes the proof. ∎

Here is a nice application.

Corollary 2.41. Fix an abelian k-variety A. For any nonzero integer n, the map $[n]_A\colon A \to A$ is an isogeny.

Proof. Because the dimension of the target and source are the same, it is enough to check that $[n]_A$ is surjective or finite kernel; see [Mil08, Proposition 7.1]. The point is that the dimension of the fiber needs plus the dimension of the image needs to be the dimension of the target.

As such, we will show that $[n]_A$ has finite kernel. Well, fix an ample line bundle $\mathcal{L}$ on A, which exists by Corollary 2.39. In fact, we may replace $\mathcal{L}$ by $\mathcal{L} \otimes [-1]^*\mathcal{L}$, which is still ample because pulling back by an automorphism $[-1]$ preserves being ample. So $[-1]^*\mathcal{L} = \mathcal{L}$, and then we can compute $[n]^*\mathcal{L} = \mathcal{L}^{\otimes n^2}$.

Let $A[n]$ be the kernel of $[n]\colon A \to A$. We want to show that $A[n]$ is finite, and because A is quasicompact, it will be enough to show that $A[n]$ is zero-dimensional. Now, $A[n]^\circ$ is an abelian variety, so we want to show that $A[n]^\circ = \{0_A\}$. But

$$[n]^*\mathcal{L}|_{A[n]^\circ} \cong \mathcal{O}_{A[n]^\circ},$$

so the trivial line bundle on $\mathcal{O}_{A[n]^\circ}$ is ample, forcing $A[n]^\circ$ to be zero-dimensional. ∎

2.5.2 Degree

We will want to understand the degree of isogenies. Let's go ahead and give the general definition of degree.

Definition 2.42 (degree)**.** Fix a dominant morphism of $f\colon X \to Y$ of integral k-schemes such that $\dim X = \dim Y$. Then $\deg f \coloneqq [K(X) : K(Y)]$ is the *degree* of f; we define the *separable degree* and *inseparable degree* accordingly. We say that f is *separable* if and only if $f\colon K(Y) \to K(X)$ is separable.

Here is another way to think about degree.

Definition 2.43 (degree)**.** Fix a proper k-variety X and a line bundle $\mathcal{L}$ on X. For a coherent sheaf $\mathcal{F}$ on X, we define $P_L : \mathbb{Z} \to \mathbb{Z}$ by

$$P_{\mathcal{L}}(\mathcal{F}, n) \coloneqq \chi\left(\mathcal{F} \otimes \mathcal{L}^{\otimes n}\right).$$

It turns out that P_L is a polynomial of degree bounded above by $\dim X$, by [Vak17, Theorem 19.6.1]. Then the *degree* of $\mathcal{F}$ with respect to $\mathcal{L}$ is the number $d_{\mathcal{L}}(\mathcal{F})$ making the leading term of $P_L(\mathcal{F}, n)$, in the sense that

$$\lim_{n\to\infty} \frac{P_{\mathcal{L}}(\mathcal{F}, n)}{d_{\mathcal{L}}(\mathcal{F}) n^{\dim X}/(\dim X)!}.$$

Then we define the *degree* as $\deg \mathcal{L} \coloneqq d_{\mathcal{L}}(\mathcal{O}_X)$.

Let's see how these align.

Proposition 2.44. Fix a finite dominant morphism of $f : X \to Y$ of proper integral k-schemes such that $\dim X = \dim Y$. Then

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

Example 2.45. Fix an abelian k-variety A. Then we claim $\deg[n]_A = n^{2\dim A}$. As in Corollary 2.41, choose an ample line bundle $\mathcal{L}$ with $\mathcal{L} = [-1]^*\mathcal{L}$. Being ample implies $\deg \mathcal{L} > 0$: by taking powers, we may assume that $\mathcal{L}$ is very ample, and then one can do an explicit computation. (Alternatively, do intersection theory to realize the degree as an intersection number, which is positive.) But we showed

$$[n]^*\mathcal{L} = \mathcal{L}^{\otimes n^2},$$

so the result follows from Proposition 2.44.

2.6 February 16

Today we continue discussing degree.

2.6.1 More on Degree

Let's just get going.

Lemma 2.46. Fix a proper integral k-scheme X with generic point η. For a line bundle $\mathcal{L}$ on X and a coherent sheaf $\mathcal{F}$ on X, we have

$$d_\ell(\mathcal{F}) = (\operatorname{rank} \mathcal{F}_\eta)(\deg \mathcal{L}).$$

Proof. This is a standard "dèvissage" argument. Because χ is additive in short exact sequences, it is enough to check that there is a coherent sheaf of ideals $\mathcal{I} \subseteq \mathcal{O}_X$ fitting in the exact sequence

$$0 \to \mathcal{I}^{\operatorname{rank} \mathcal{F}_\eta} \to \mathcal{F} \to \mathcal{Q} \to 0,$$

where $\mathcal{Q}$ is a torsion sheaf where $\operatorname{supp} \mathcal{Q}$ is a closed subscheme of X of positive codimension, and $\operatorname{supp} \mathcal{O}_X/\mathcal{I}$ is also a closed subscheme of X of positive codimension. Indeed, this will imply that

$$d_\ell(\mathcal{F}) = \operatorname{rank} \mathcal{F}_\eta \cdot d_\ell(\mathcal{I}) = \operatorname{rank} \mathcal{F}_\eta \cdot \deg \mathcal{L}$$

by staring at our short exact sequences.

So it remains to find $\mathcal{I}$. Well, $\mathcal{F}$ is coherent with rank r, so a spreading out argument promises that we can find an open subscheme $U \subseteq X$ such that $\mathcal{F}|_U = \mathcal{O}_U^{\oplus r}$. Then we can view $X \setminus U$ as a divisor and take the line bundle associated to it given by $\mathcal{I}$. Because U is dense, the quotient $\mathcal{J}$ will end up being torsion, which is enough. ∎

Proposition 2.44 will follow from this.

Proposition 2.44. Fix a finite dominant morphism of $f\colon X \to Y$ of proper integral k-schemes such that $\dim X = \dim Y$. Then

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

Proof. Exactness of f allows us to see

$$H^i\left(X, f^*\mathcal{L}^{\otimes n}\right) = H^i\left(Y, f_*f^*\mathcal{L}^{\otimes n}\right).$$

Now, the adjunction formula tells us that this is $H^i(Y, f_*\mathcal{O}_X \otimes \mathcal{L}^{\otimes n})$, so unwinding our characteristic polynomial reveals that

$$\deg f^*\mathcal{L} = d_{\mathcal{L}}(f_*\mathcal{O}_X) = (\deg f)(\deg \mathcal{L}),$$

where the last equality has used Lemma 2.46. ∎

Remark 2.47. One can weaken f from being finite to dominant by passing to an open subscheme where we are finite.

This allows us to understand $[n]_A$.

Theorem 2.48. Fix an abelian k-variety A. For any nonzero integer n, the map $[n]_A\colon A \to A$ is an isogeny of degree $n^{2\dim A}$.

(a) $[n]_A$ is separable if and only if $\operatorname{char} k \nmid n$.

(b) If $p \coloneqq \operatorname{char} k$, then the inseparable degree of $[p]_A$ is at least $p^{\dim A}$.

Proof. The degree computation is immediate from Proposition 2.44 and the computation $[n]_A^*\mathcal{L} = \mathcal{L}^{\otimes n^2}$ for an ample symmetric line bundle $\mathcal{L}$.

For (a), we note that $[n]_A$ is separable if and only if it is étale (indeed, $[n]_A$ is already flat by miracle flatness), so it is enough to check smoothness. But being a group scheme means that we may as well check smoothness only at $0_A \in A$. Well, an induction on n shows that $d[n]_A|_{0_A}\colon \operatorname{Lie} A \to \operatorname{Lie} A$ is multiplication-by-n,[2] and this map is invertible if and only if $\operatorname{char} k \nmid n$.

Now, for (b), we note that $d[p]|_{0_A}\colon \operatorname{Lie} A \to \operatorname{Lie} A$ is the zero map. However, $[p]\colon A \to A$ produces a map by pullback in the opposite direction given by $[p]^*\Omega^1_A \to \Omega^1_A$. This map on the stalk at 0 is dual to the map on $\operatorname{Lie} A$, which is the zero map, so homogeneity now requires that $[p]^*\Omega^1_A \to \Omega^1_A$ is fully the zero map. In other words, for any $f \in K(A)$, we have $[p]^*df = 0$ in $\Omega^1_{K(A)/k}$, which upon unwinding definitions (in the differentials) implies

$$[p]^*f \in K(A)^p.$$

The moral of the story is that $[p]^*K(A) \to K(A)$ factors through $k \cdot K(A)^p$. But $K(A)^p$ has transcendence degree $\dim A$ over k, so this extension has inseparable degree at least $p^{\dim A}$. ∎

Corollary 2.49. Fix an abelian k-variety A.

(a) If $\operatorname{char} k \nmid n$, then $A[n](\overline{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$.

(b) If $n = p^\nu$ where $p \coloneqq \operatorname{char} k > 0$, then $A[p](\overline{k}) \cong (\mathbb{Z}/p^\nu\mathbb{Z})^i$ for some $i \le \dim A$.

[2] The main thing to check is that $dm(t_1, t_2) = t_1 + t_2$. This is computed in [Mum08, p. 40].

Proof. For (a), the point is that $[n]_A$ being separable implies that $A(\overline{k})[n] = \deg[n]_A$, so we know that $A(\overline{k})[n]$ at least has the correct size by Theorem 2.48. Now, for $n = \ell^\nu$ a prime power, one can induct on the power and use the fact that it has a quotient of the form $\mathbb{Z}/\ell^{\nu-1}\mathbb{Z}$ given by multiplication-by-ℓ, so the sharper result holds. If n is not a prime power, then we decompose into prime powers to conclude.

The argument for (b) is similar. Note $\deg[p] = p^{2\dim A}$ still, but we have at least $\dim A$ stuck in inseparable degree, so

$$\#A(\overline{k})[p] = \deg_{\text{sep}}[p] = \frac{p^{2\dim A}}{\deg_{\text{insep}}[p]} = p^i$$

for some $0 \le i \le g$. But the group is p-torsion, so we get $(\mathbb{Z}/p\mathbb{Z})^i$, and the same induction on n achieves the result for p^ν in general. More explicitly, we write out the exact sequence

$$0 \to A(\overline{k})[p] \to A(\overline{k})[p^\nu] \xrightarrow{p} A(\overline{k})\left[p^{\nu-1}\right] \to 0,$$

which forces the middle by induction. ∎

Remark 2.50. The i in the above result is usually called the "p-rank" of A. It is an isomorphism invariant, so for example it can produce a stratification of the moduli space. As an example of this being interesting, it is known that having maximal p-rank implies that A is "ordinary," which relates to the Frobenius action.

This permits the following definition.

Definition 2.51 (Tate module)**.** Fix an abelian k-variety A and a prime ℓ coprime to $\operatorname{char} k$. Then

$$T_\ell A \coloneqq \varprojlim A[\ell^\bullet].$$

The point is that $T_\ell A = \mathbb{Z}_\ell^{2\dim A}$ by taking limits over Corollary 2.49.

Remark 2.52. To define a Tate module for $\ell = \operatorname{char} k$, one needs to define a p-divisible group.

2.6.2 The Picard Scheme

We will need a little moduli theory but not too much. In particular, we need the Picard functor.

Definition 2.53 (Picard)**.** Fix a k-scheme X. Then the *Picard functor* takes k-schemes T to $\operatorname{Pic}_{X/k}(T)$ of isomorphism classes of line bundles on $X \times_k T$. Given a k-rational point $x \in X(k)$, this is in bijection with "rigidified" line bundles $(\mathcal{L}, \alpha)$ on $X \times_k T$, where $\alpha\colon \mathcal{L}|_{\{x\}\times T} \cong \mathcal{O}_T$ is a choice of trivialization.

Here is the theorem.

Theorem 2.54 (Grothendieck)**.** The functor $\operatorname{Pic}_{X/k}$ is representable by a separated k-scheme locally of finite type. In fact, $\operatorname{Pic}^\circ_{X/k}$ is quasi-projective and is projective if X is smooth.

We will not need to know any part of this proof, but we do need to use that this scheme exists.

Remark 2.55. One can check directly that $\operatorname{Pic}_{X/k} \otimes \overline{k} = \operatorname{Pic}_{X_{\overline{k}}/\overline{k}}$ by some base-change like argument.

2.7 February 21

Today we begin our discussion of duality in earnest. Homework will be posted next week.

2.7.1 The Picard Scheme of an Abelian Variety

Note that an abelian k-variety A has a k-rational point $0_A \in A(k)$ and is smooth, projective, and so on. Thus, $\mathrm{Pic}^\circ_{A/k} A$ exists. Because A is smooth, this scheme is projective. We would like this to agree with our construction of $\mathrm{Pic}^0 A$ from earlier.

Theorem 2.56. Fix an abelian k-variety A. Then $\mathrm{Pic}^\circ_{A/k}(k) = \mathrm{Pic}^0(A)$.

Namely, our goal is to make sense of the following definition.

Definition 2.57 (dual abelian variety)**.** For an abelian k-variety A, we set $A^\vee := \mathrm{Pic}^\circ_{A/k}$ to be the *dual abelian variety*.

We know that $\mathrm{Pic}^\circ_{A/k}$ is a connected (and hence irreducible) group scheme, but we do not yet know if it is smooth; Theorem 2.56 will help with this. For example, we do know that $A^\vee_{\mathrm{red}}$ is in fact an abelian variety.

It will help to have the following notion.

Definition 2.58 (Poincaré line bundle)**.** Fix a k-scheme X for which $\mathrm{Pic}_{X/k}$ exists. Then there is a universal *Poincaré (rigidified) line bundle* $(\mathcal{P}, \alpha_{\mathcal{P}})$ on $X \times_k \mathrm{Pic}_{X/k}$ where $\alpha\colon \mathcal{P}|_{\{x\}\times \mathrm{Pic}_{X/k}} \cong \mathcal{O}_{\mathrm{Pic}_{X/k}}$. Namely, $(\mathcal{P}, \alpha)$ corresponds to $\mathrm{id}_{\mathrm{Pic}_{X/k}} \in h_{\mathrm{Pic}_{X/k}}(\mathrm{Pic}_{X/k})$.

Remark 2.59. Unwinding via the Yoneda lemma, any T-point $\varphi\colon T \to \mathrm{Pic}_{X/k}$ corresponds to the rigidified line bundle $(\mathcal{L}, \alpha) = \varphi^*(\mathcal{P}, \alpha_{\mathcal{P}})$. For example, if k'/k is a field extension, then a k'-point $\lambda \in \mathrm{Pic}_{X/k}$ corresponds to the rigidified line bundle $\mathcal{P}|_{X\times\{\lambda\}}$.

It will be useful to have some notion of equivalence.

Definition 2.60 (algebraically equivalent)**.** Fix line bundles $\mathcal{M}$ and $\mathcal{N}$ over a k-scheme X, where k is algebraically closed. Then $\mathcal{M}$ and $\mathcal{N}$ are *algebraically equivalent* if and only if there is a connected k-variety T and a line bundle $\mathcal{L}$ over $X_k \times T$ and $t_1, t_2 \in T(k)$ such that

$$\mathcal{M} \cong \mathcal{L}|_{X\times\{t_1\}} \qquad \text{and} \qquad \mathcal{N} \cong \mathcal{L}|_{X\times\{t_2\}}.$$

Remark 2.61. One may restrict T to just being a curve by finding a curve between t_1 and t_2.

Remark 2.62. Rational equivalence basically amounts to taking $T = \mathbb{P}^1_k$.

Algebraic equivalence is in fact a weaker condition.

Lemma 2.63. Fix a line bundle $\mathcal{L}'$ on a k-scheme X (with marked point $e \in X(k)$) coming from some $\lambda \in \mathrm{Pic}_{X/k}(k)$ (where we assume $\mathrm{Pic}_{X/k}$ exists). Then $\lambda \in \mathrm{Pic}^\circ_{X/k}(k)$ if and only if $\mathcal{L}'_{\overline{k}}$ and $\mathcal{O}_{X_{\overline{k}}}$ are algebraically equivalent.

Proof. In the forward direction, we take $T := \left(\mathrm{Pic}^\circ_{X/k}\right)_{\overline{k},\mathrm{red}}$, which is a connected variety. (For connectivity, we see) Then the universal line bundle $\mathcal{P}$ restricts to $\mathcal{L}'$ on $X \times \{\lambda\}$ (by definition of λ) and restricts to $\mathcal{O}_X$ on $X \times \{e\}$ (by definition of $\mathcal{P}$).

In the reverse direction, pick up our k-scheme T and the provided line bundle $\mathcal{L}$ over $X \times T$ with points $t_1, t_2 \in T$, and let $\{U_i\}_{i\in I}$ be a trivializing open cover, and we assume that the U_i are connected. Notably,

being a trivializing open cover means that we have equipped ourselves with morphisms $U_i \to \mathrm{Pic}_{X/k}$. Now, we know

$$\mathcal{L}|_{X_{\overline{k}}\times\{t_1\}} \cong \mathcal{L}'_{\overline{k}} \qquad \text{and} \qquad \mathcal{L}|_{X_{\overline{k}}\times\{t_2\}} \cong \mathcal{O}_{X_{\overline{k}}}.$$

Now, the marked point t_2 lives in some U_i, and this U_i goes to $\mathrm{Pic}^\circ_{X/k}$ by the above trivialization, so because T is connected, actually is all maps to $\mathrm{Pic}^\circ_{X/k}$. Thus, we can specialize to t_1 to get $\mathcal{L}$ in $\mathrm{Pic}^\circ_{X/k}$. ■

What?

This allows us to prove part of Theorem 2.56.

Lemma 2.64. Fix an abelian k-variety A. Then $\mathrm{Pic}^\circ_{A/k}(k) \subseteq \mathrm{Pic}^0(A)$.

Proof. Let $\mathcal{P}$ be the universal line bundle on $A \times A^\vee_{\mathrm{red}}$, which is legal because we're only ever going to work with k-points anyway. Now, pick up some $\mathcal{L} \in \mathrm{Pic}^\circ_{A/k}(k)$, and we need to show that

$$m^*\mathcal{L} \cong \mathrm{pr}_1^*\,\mathcal{L} \otimes \mathrm{pr}_2^\circ\,\mathcal{L}.$$

By pullback, it suffices to show this for $\mathcal{P}$, so define

$$\mathcal{M} \coloneqq (m \otimes \mathrm{id}_{A^\vee})^*\mathcal{P} \otimes (\mathrm{pr}_1 \otimes \mathrm{id}_{A^\vee})^*\mathcal{P}^{-1} \otimes (\mathrm{pr}_2 \otimes \mathrm{id}_{A^\vee})^*\mathcal{P}^{-1},$$

which we want to show is trivial. Well, the above is a line bundle on $A \times A \times A^\vee$, so we use Theorem 2.7. For this, note $\mathcal{P}|_{\{0_A\}\times A^\vee_{\mathrm{red}}} \cong \mathcal{O}_{A^\vee_{\mathrm{red}}}$ by construction of the universal line bundle, and $\mathcal{P}|_{A\times\{0_{A^\vee}\}} \cong \mathcal{O}_A$ again by construction. Now,

$$\mathcal{M}|_{\{0_A\}\times A\times A^\vee_{\mathrm{red}}} \cong \mathrm{pr}_1^*\left(\mathcal{P}|_{\{0_A\}\times A^\vee_{\mathrm{red}}}\right)$$

because the first and last terms cancel, and the above line bundle trivializes as discussed; the argument is similar for $A \times \{0_A\} \times A^\vee$. Lastly, we see

$$\mathcal{M}|_{A\times A\times\{0_{A^\vee_{\mathrm{red}}}\}} = \left(m^* \otimes (\mathrm{pr}_1^*)^{-1} \otimes (\mathrm{pr}_2^*)^{-1}\right)\left(\mathcal{P}|_{A\times\{0_A\}}\right)$$

vanishes because now we're just over $A \times A$. ■

Before showing the other inclusion, we make some remarks. Well, given some line bundle $\mathcal{L}$, we build $\varphi_{\mathcal{L}} \colon A(\overline{k}) \to \mathrm{Pic}^0(A_{\overline{k}})$, which we claim actually factors through $\mathrm{Pic}^\circ_{A/k}(\overline{k})$. Indeed, for $x \in A(\overline{k})$, we want to know that $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is algebraically equivalent to $\mathcal{O}_{A_{\overline{k}}}$ by Lemma 2.63. But then $A_{\overline{k}} \times A_{\overline{k}}$ itself witnesses the algebraic equivalence because you can write down a line bundle which specializes to both $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ and $t_e^*\mathcal{L} \otimes \mathcal{L}^{-1}$ (the latter of which is trivial).

So we are going to want to show the following.

Proposition 2.65. Fix an abelian k-variety A and an ample line bundle $\mathcal{L}$ on A. Then the map $\varphi_{\mathcal{L}} \colon A(\overline{k}) \to \mathrm{Pic}^0(A_{\overline{k}})$ is surjective.

It will help to prove the following lemma.

Lemma 2.66. Fix an abelian k-variety A and a nontrivial line bundle $\mathcal{L} \in \mathrm{Pic}^0(A)$. Then $H^i(A, \mathcal{L}) = 0$ for all i.

Proof. We begin by showing $H^0(A, \mathcal{L}) = 0$. Well, if this is not the case, then we may find an effective divisor $D \subseteq A$ such that $\mathcal{L} \cong \mathcal{O}_A(D)$ by viewing $\Gamma(A, \mathcal{L})$ as parameterizing linear systems. Now, we compute

$$\mathcal{O}_A = 0_A^*\mathcal{L} = ([1]_A \times [-1]_A)^* m^*\mathcal{L} = ([1]_A \times [-1]_A)(\mathrm{pr}_1^*\,\mathcal{L} \otimes \mathrm{pr}_2^*\,\mathcal{L}) = \mathcal{L} \otimes [-1]^*\mathcal{L}.$$

But then we are being told that $D + [-1]^*D$ is rationally equivalent to 0, which forces $\mathcal{L}$ to be trivial.

For the second part, we use the Künneth formula. Let k be the smallest positive integer where $H^k(A, \mathcal{L})$ is nonzero; note $k > 0$ by the above paragraph. Now, we note that we have the commutative diagram.

$$\begin{array}{ccc} H^k(A,\mathcal{L}) & \xrightarrow{m^*} & H^k(A\times A, m^*\mathcal{L}) \\ & \searrow & \downarrow{\scriptstyle (0_A\times \mathrm{id}_A)^*} \\ & & H^k(A,\mathcal{L}) \end{array}$$

Thus, $H^k(A \times A, m^*\mathcal{L})$ is nonzero, but the Künneth formula tells us that

$$H^k(A\times A, \mathrm{pr}_1^*\mathcal{L}\otimes \mathrm{pr}_2^*\mathcal{L}) = \bigoplus_{i+j=k} H^i(A,\mathcal{L})\otimes H^j(A,\mathcal{L}).$$

The left-hand side is nonzero, but then some term on the right-hand side must be nonzero, which is a contradiction because we cannot have $i = 0$ or $j = 0$. ∎

2.8 February 23

Today we are joined by a peach and a crab.

2.8.1 More on the Picard Scheme

Recall we were in the middle of proving Proposition 2.65. Morally, we are saying that A is isogenous to its dual.

Proposition 2.65. Fix an abelian k-variety A and an ample line bundle $\mathcal{L}$ on A. Then the map $\varphi_{\mathcal{L}}\colon A(\overline{k}) \to \mathrm{Pic}^0(A_{\overline{k}})$ is surjective.

Proof. We may take k to be algebraically closed. Assume for the sake of contradiction that there is a line bundle $\mathcal{M} \in \mathrm{Pic}^\circ(A_{\overline{k}})$ which is not of the form $\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$, so we set

$$\mathcal{N} \coloneqq m^*\mathcal{L}\otimes \mathrm{pr}_1^*\mathcal{L}^{-1}\otimes \mathrm{pr}_2^*\left(\mathcal{L}^{-1}\otimes\mathcal{M}^{-1}\right),$$

which is a line bundle on $A \times A$.

We now use the Leray spectral sequence.

Theorem 2.67 (Leray spectral sequence)**.** Fix a morphism $f\colon X \to Y$ of schemes and a quasicoherent sheaf $\mathcal{F}$ on X. Then there is a spectral sequence

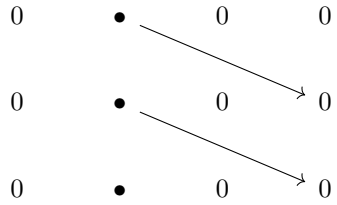
$$E_2^{pq} = H^p(Y, R^q f_*\mathcal{F}) \Rightarrow H^{p+q}(X,\mathcal{F}).$$

We will apply this to $\mathcal{N}$ on $A \times A$ with the two projections $\mathrm{pr}_1, \mathrm{pr}_2\colon A \times A \to A$.

- For example, $\mathcal{N}|_{\{x\}\times A} = t_x^*\mathcal{L}\otimes\mathcal{L}^{-1}\otimes\mathcal{M}^{-1}$ (which is nontrivial), so its cohomology vanishes by Lemma 2.66. Thus, we see that $R^j\,\mathrm{pr}_{1*}\mathcal{N} = 0$ by computation of higher direct images via Theorem 2.18, so its cohomology vanishes.
- On the other hand, $\mathcal{N}|_{A\times\{x\}} = t_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$ is trivial if and only if $x \in K(\mathcal{L})$ using the notation of Theorem 2.38, which is a finite set by that theorem, so $H^j(A, \mathcal{N}|_{A\times\{x\}}) = 0$ for $x \in A \setminus K(\mathcal{L})$, meaning that the higher direct images on $A \times K(\mathcal{L})$ need to vanish via Theorem 2.18.

  In other words, $R^j\,\mathrm{pr}_{2*}\mathcal{N}$ is a coherent sheaf supported in the finite set $K(\mathcal{L})$. In particular, dimension arguments mean that $H^i(A, R^j\,\mathrm{pr}_{2*}\mathcal{N}) = 0$ for positive i. So our spectral sequence looks like the

following diagram.



Because our spectral sequence is converging on this E_2 page, we are able to conclude that

$$H^n(A \times A, \mathcal{N}) = H^0(A, R^n \operatorname{pr}_{2*} \mathcal{N}).$$

Our previous point tells us that the left group vanishes, but then the right-hand sheaf is just supported on finitely many points and so will have global sections unless we actually have $R^n \operatorname{pr}_{2*} \mathcal{N} = 0$ for all n. However, $\mathcal{N}|_{A \times \{0_A\}} \cong \mathcal{O}_A$ by construction, so the vanishing of our higher direct images provides contradiction because $H^0(A, \mathcal{O}_A) \neq 0$. ∎

This concludes the proof of Theorem 2.56. Notably, we are now able to upgrade $\varphi_{\mathcal{L}}$ to a full morphism $A \to \operatorname{Pic}^\circ_{A/k}$ sending rigidified line bundles to what we expect them to be. (Explicitly, $\varphi_{\mathcal{L}}$ is realized on the level of the moduli spaces.) We factor through Pic° because A is connected, meaning that the image of $\varphi_{\mathcal{L}}$ needs to actually land in the connected component.

Remark 2.68. Notably, if $\mathcal{L}$ is an ample line bundle, we get a surjective map $\varphi_{\mathcal{L}} \colon A \to \operatorname{Pic}^\circ_{A/k}$, so $\dim A = \dim A^\vee$.

2.8.2 Smoothness of the Dual Abelian Variety

Here is the desired result.

Theorem 2.69. Fix an abelian k-variety A. Then $A^\vee = \operatorname{Pic}^\circ_{A/k}$ is smooth.

Notably, it will be enough to show that $A^\vee$ is smooth somewhere (because we are a group), so it is enough to show that $\dim T_0 A^\vee = \dim A$.

It will help to provide a cohomological description of the tangent space.

Lemma 2.70. Fix an abelian k-variety A. Then $T_0 A^\vee \cong H^1(A, \mathcal{O}_A)$.

Proof. By definition,

$$T_0 A^\vee \coloneqq \ker\left(A^\vee(\Lambda) \to A^\vee(k)\right),$$

where $\Lambda \coloneqq \operatorname{Spec} k[\varepsilon]/\left(\varepsilon^2\right)$ is the ring of dual numbers. Unwinding the definition of $A^\vee$, we are looking at

$$T_0 A^\vee \coloneqq \ker\left(\operatorname{Pic}_{A/k}(\Lambda) \to \operatorname{Pic}_{A/k}(k)\right),$$

where we may replace Pic° with Pic because $0 \in \operatorname{Pic}^\circ_{A/k}$ anyway. As a moduli description, we see that Pic classifies line bundles up to some suitable equivalence, but this equivalence vanishes over the affine scheme Λ, so we are going to want to have an exact sequence

$$0 \to T_0 A^\vee \to \operatorname{Pic}(A \times \Lambda) \to \operatorname{Pic} A.$$

On the other side of things, we know $\operatorname{Pic}(X) = H^1(X, \mathcal{O}_X^\times)$ for any scheme X, which explains how cohomology is going to appear. Notably, one has the "exponential" exact sequence

$$0 \to \mathcal{O}_A \to \mathcal{O}_{A \times \Lambda}^\times \to \mathcal{O}_A^\times \to 1,$$

of quasicoherent sheaves on A, where the first map sends $f \mapsto 1 + \varepsilon f$, and the second map comes from the inclusion $A \to A \times \Lambda$. Notably, the inclusion $A \to A \times \Lambda$ has a splitting given by the projection, so the above exact sequence will also split. Because we split, we will remain exact upon applying global sections, so long exact sequence may read

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

(Here, $H^1(A \times \Lambda, \mathcal{O}_{A\times\Lambda}^\times) = H^1(A, \mathcal{O}_{A\times\Lambda}^\times)$ because the inclusion is a closed embedding.) The point is that we get the following morphism of left exact sequences.

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_0 A^\vee & \longrightarrow & \operatorname{Pic}(A \times \Lambda) & \longrightarrow & \operatorname{Pic} A \\ & & \vdots & & \| & & \| \\ 0 & \longrightarrow & H^1(A, \mathcal{O}_A) & \longrightarrow & H^1(A \times \Lambda, \mathcal{O}_{A\times\Lambda}^\times) & \longrightarrow & H^1(A, \mathcal{O}_A^\times) \end{array}$$

The dashed arrow is induced an isomorphism, so we are done. ■

Theorem 2.69 will now follow from the following proposition.

Proposition 2.71. Let k be an algebraically closed field, and fix an abelian k-variety A, and set $g \coloneqq \dim A$. Then $\dim H^1(A, \mathcal{O}_A) = g$, and

$$\bigwedge H^1(A, \mathcal{O}_A) \cong \bigoplus_{i=0}^{g} H^i(A, \mathcal{O}_A)$$

of graded k-vector spaces.

Remark 2.72. A similar statement holds for étale cohomology and other Weil cohomology theories.

Remark 2.73. In fact, we will be able to upgrade the isomorphism in Proposition 2.71 to an isomorphism of Hopf k-algebras, where the Hopf algebra structure is provided by the cup product.

Notably, Theorem 2.69 follows from the above two results because we are directly told that $\dim T_0 A^\vee = \dim A = \dim A^\vee$.

2.9 February 26

We continue.

2.9.1 Cohomology Rings as Hopf Algebras

Last class we stated the following result.

Proposition 2.71. Let k be an algebraically closed field, and fix an abelian k-variety A, and set $g \coloneqq \dim A$. Then $\dim H^1(A, \mathcal{O}_A) = g$, and

$$\bigwedge H^1(A, \mathcal{O}_A) \cong \bigoplus_{i=0}^{g} H^i(A, \mathcal{O}_A)$$

of graded k-vector spaces.

In fact, we will use the classification of Hopf algebras to show that both sides here are Hopf algebras and that they are isomorphic. For example,

$$H_A := \bigoplus_{i=0}^{g} H^i(A, \mathcal{O}_A)$$

is a graded k-algebra with product given by the cup product. To see this cup product, one can define it by

$$H_A \otimes_k H_A \xrightarrow{\Delta^*} H_{A\times A} \to H_A$$

where the first map is the Künneth formula, and the last map is given by pullback along the diagonal $\Delta\colon A \to A \times A$. In fact, there is some extra structure of a cocommutative coalgebra. Indeed, there is a map

$$H_A \xrightarrow{m^*} H_{A\times A} \cong H_A \otimes_k H_A,$$

where again the second map is the Künneth formula. We also have an inversion $[-1]^*\colon H_A \to H_A$. All of this structure can be put into a Hopf algebra.

Definition 2.74 (Hopf algebra)**.** Fix a field k. Then a *Hopf algebra* is a graded k-vector space equipped with a product $m\colon H \otimes H \to H$, a comultiplication $\Delta\colon H \to H \otimes H$, an inversion $s\colon H \to H$, an identity $\varepsilon H \to k$, and a coidentity $\delta\colon k \to H$, satisfying the following.

- (m, δ) makes H into a k-algebra.
- (Δ, ε) makes H into a k-coalgebra, meaning that the following diagrams commute.

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

- The maps Δ and m are algebra and coalgebra homomorphisms, respectively.
- The map s

Remark 2.75. We can see that commutative Hopf k-algebras A are equivalent to affine group k-schemes. Indeed, one can just unwind the definition of an affine group k-scheme to see that they are just schemes of the form $\operatorname{Spec} A$ where A is a commutative Hopf k-algebra.

We will also want some notion of commutativity in our graded setting.

Definition 2.76 (graded commutative)**.** A k-algebra H is *graded commutative* if and only if any homogeneous elements $a, b \in H$ have

$$ab = (-1)^{(\deg a)(\deg b)} ba.$$

Example 2.77. Fix an abelian k-variety A. Then our work above tells us that H_A is a finite dimensional graded commutative Hopf k-algebra. In fact, we see that $H^0 = k$ by taking global sections. We also note that we can compute

$$m^*(h) = (1 \otimes h) + (h \otimes 1) + \sum_{i>j>0} (h_i \otimes h_j)$$

for some unknown h_i and h_j. One can see this because m maps $1 \otimes h$ and $h \otimes 1$ to h.

Why?

The above data will be enough for our classification result.

Lemma 2.78. Fix a perfect field k. Suppose that H is a graded commutative Hopf k-algebra such that $H^0 = k$ and $H^r = 0$ for $r > g$ and any $h \in H$ has

$$m^*(h) = (1 \otimes h) + (h \otimes 1) + \sum_{i>j>0} (h_i \otimes h_j)$$

for some unknown h_i and h_j. Then $\dim H^1 \leq g$; in fact, if $\dim H^1 = g$, then $H \cong \bigwedge H^1$ as graded commutative Hopf k-algebras.

Sketch. One can show (and it is due to Borel) that such an H is generated by finitely many homogeneous elements, generated essentially freely by these elements (i.e., the only relations are given by the graded commutativity and nilpotent), so let these generators be $x_1, \dots, x_m$. Notably,

$$\deg \prod_{i=1}^{m} x_i = \sum_{i=1}^{m} \deg x_i \leq g,$$

where the inequality at the end is because the product must be nonzero, so we see that $\dim H_1 \leq g$ because $\dim H_1$ is upper-bounded by the number of x_i with $\deg x_i = 1$. But if we have $\dim H_1 = g$, then the above degree computation must achieve equality, so all the generators must have degree exactly 1, and there must be g of them. Furthermore, we claim that $x_j^2 = 0$ for each generator x_j, which holds because $x_j^2 \neq 0$ means that the product $x_j \prod_i x_i$ is still nonzero but has degree larger than g, which is a contradiction. ∎

One can then feed the above lemma into Proposition 2.71 to show that $\dim H^1(A, \mathcal{O}_A) \leq g$, which is enough for our purposes because the quasifinite surjection $A \twoheadrightarrow A^\vee$ promises that $\dim A^\vee \geq \dim A$. So in fact we get the isomorphism claimed in Proposition 2.71. This in turn completes the proof of Theorem 2.69.

2.9.2 Polarizations

We now discuss some special isogenies.

Definition 2.79 (polarization)**.** Fix an abelian k-variety A. An isogeny $\lambda \colon A \to A^\vee$ is a *polarization* if and only if $\lambda_{\overline{k}} = \varphi_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$ on $A_{\overline{k}}$. A polarization λ is *principal* if and only if $\deg \lambda = 1$; i.e., λ is an isomorphism.

Remark 2.80. Each line bundle $\mathcal{L}' \in \mathrm{Pic}^\circ_{A/k}(A)$ will have $\varphi_{\mathcal{L}} = \varphi_{\mathcal{L} \otimes \mathcal{L}'}$, and in fact the converse still holds by unwinding the definition of Pic^0. As such, we can think about polarizations as being a subset of

$$\frac{\mathrm{Pic}(A_{\overline{k}})}{\mathrm{Pic}^0(A_{\overline{k}})}.$$

Definition 2.81 (Néron–Severi group)**.** Fix an abelian k-variety A. Then the *Néron–Severi group* is

$$\mathrm{NS}(A) \coloneqq \frac{\mathrm{Pic}_{A/k}(A_{\overline{k}})}{\mathrm{Pic}^\circ_{A/k}(A_{\overline{k}})}.$$

Approximately speaking, the Néron–Serveri group measures polarizations.

Remark 2.82. Take $k = \mathbb{C}$. Then the exponential short exact sequence $0 \to \mathbb{Z} \to \mathcal{O}_A \to \mathcal{O}_A^\times \to 1$ produces a long exact sequence

$$H^1(A, \mathbb{Z}) \to H^1(A, \mathcal{O}_A) \to H^1(A, \mathcal{O}_A^\times) \to H^2(A, \mathbb{Z}).$$

Now, $H^1(A, \mathcal{O}_A)/H^1(A, \mathbb{Z}) \cong \mathrm{Pic}^0(A)$ as discussed earlier, so we note that we have the exact sequence

$$H^1(A, \mathbb{Z}) \to H^1(A, \mathcal{O}_A) \to \underbrace{H^1(A, \mathcal{O}_A^\times)}_{\mathrm{Pic}\, A} \to \mathrm{NS}(A) \to 0.$$

Thus, $\mathrm{NS}(A)$ is a finitely generated $\mathbb{Z}$-module because it embeds into $H^2(A, \mathbb{Z})$.

Remark 2.83. More generally, $\mathrm{NS}(A)$ is a free $\mathbb{Z}$-module of finite rank for any abelian k-variety A, for any field k. The point is that viewing $\mathrm{NS}(A)$ as polarizations will embed into

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

by $\varphi_\bullet$, and the target is a free $\mathbb{Z}$-module of finite rank because one can show that any prime ℓ with $\mathrm{char}\, k \nmid \ell$ builds an injection

$$T_\ell \colon \mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, A^\vee_{\overline{k}}) \to \mathrm{Hom}(T_\ell(A_{\overline{k}}), T_\ell(A^\vee_{\overline{k}})),$$

and the target is a free $\mathbb{Z}_\ell$-module of finite rank, and the proof of this inclusion is able to show that the source is thus free of finite rank (over $\mathbb{Z}$!).

Remark 2.84. Just because λ is a polarization does not mean that there is a line bundle $\mathcal{L}$ on A such that $\lambda = \varphi_{\mathcal{L}}$. Take k to be perfect so that we can use Galois descent by $G \coloneqq \mathrm{Gal}(\overline{k}/k)$. By definition of $\mathrm{NS}(A)$, we have an exact sequence

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

so we get a long exact sequence

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

As such, we are asking if every $\lambda \in \mathrm{NS}(A)^G$ comes from $\mathrm{Pic}_{A/k}(k)$, which might be false if $H^1(G, A^\vee(\overline{k}))$ fails to vanish. However, it turns out that this is not the case if k is finite.

Remark 2.85. Fix a projective k-curve X and some k-rational point $x_0 \in X(k)$. One can show that $J(X) \coloneqq \mathrm{Pic}^\circ_{X/k}$ is a smooth group scheme and hence an abelian variety. Now, each $d > 0$ produces a map $X^d \to J(X)$ by sending $(x_1, \dots, x_d)$ to the line bundle $\mathcal{O}_X(x_1) \otimes \cdots \otimes \mathcal{O}_X(x_d) \otimes \mathcal{O}_X(-x_0)^{\otimes d}$. In particular, it turns out that the image of $X^{g-1} \to J(X)$ gives rise to an ample line bundle $\mathcal{L}$ and hence a polarization $\varphi_{\mathcal{L}}$. In fact, this is a principal polarization.

2.10 February 28

We now move into a discussion of quotients, so we will want to understand some descent. Homework will be posted over the weekend.

2.10.1 Cartier Duals

Our end goal is the following result.

Theorem 2.86 ([Mum08, Theorem 15.1]). Fix an isogeny $f\colon A \to B$ of abelian k-varieties. Then there is a dual isogeny $f^\vee\colon B^\vee \to A^\vee$ defined by sending $(\mathcal{L}, \alpha) \in \operatorname{Pic}^\circ_{B/k}(T)$ to $(f^{\mathcal{L}}, f^*\alpha) \in \operatorname{Pic}^\circ_{A/k}(T)$. In fact, $\ker f^\vee = (\ker f)^\vee$.

Remark 2.87. For definition of $f^\vee$ to make sense, f merely needs to be a homomorphism.

Wait, how does one define $(\ker f)^\vee$? Well, we will use the Cartier dual [Mum08, §14].

Definition 2.88. Fix a finite commutative group k-scheme G given by the commutative (and cocommutative) Hopf k-algebra H. Then we define the dual $H^\vee \coloneqq \operatorname{Hom}_k(H, k)$, which is still a Hopf k-algebra, so the *Cartier dual* $G^\vee$ of G is the finite commutative group k-scheme

$$G^\vee \coloneqq \operatorname{Spec} H^\vee.$$

Remark 2.89. Let's explain how $H^\vee$ is a Hopf k-algebra. For example, the unit is a map $k \to H$ dualizes to a map $H^\vee \to k$, which is the counit; similarly, the multiplication is a map $H \otimes_k H \to H$, which dualizes to a map $H^\vee \to H^\vee \otimes H^\vee$, which is the comultiplication.

Remark 2.90. We can see on the level of Hopf algebras that $G^{\vee\vee} = G$.

More generally, one can discuss the Hopf algebra of morphisms.

Definition 2.91 (Hom scheme). Fix commutative groups S-schemes G and H. Then we define the functor $\underline{\operatorname{Hom}_S(G, H)}\colon \operatorname{Sch}_S \to \operatorname{Ab}$ by

$$\underline{\operatorname{Hom}_S(G, H)}(T) \coloneqq \operatorname{Hom}_T(G_T, H_T)$$

is in fact represented by an S-scheme frequently.

Let's see an example of this, which provides another way to think about the Cartier dual.

Proposition 2.92. Fix a finite commutative group k-scheme G. Then $G^\vee$ represents $\underline{\operatorname{Hom}_k(G, \mathbb{G}_m)}$.

Proof. It suffices to check the result on affine schemes. Namely, given a k-algebra R, we need a (natural) isomorphism between $G^\vee(R)$ and $\operatorname{Hom}_R(G_R, \mathbb{G}_{m,R})$. On one hand, we compute

$$G^\vee(R) = \operatorname{Hom}_k(H^\vee, R) = \operatorname{Hom}_R(H^\vee \otimes_k R, R).$$

Notably, this is a subset of R-linear maps $H^\vee \otimes_k R \to R$, which is H_R after taking another dual. Well, $\varphi \in H_R$ if and only if $\varphi(1) = 1$ and $\varphi(ab) = \varphi(a)\varphi(b)$. Explicitly, letting $\Delta\colon H \to H \otimes_k H$ denote the comultiplication and letting $\varepsilon\colon H \to k$ denote the counit, we find that we are asking for $\Delta_R(\varphi) = \varphi \otimes \varphi$ and $\varepsilon_R(\varphi) = 1$.

On the other hand,

$$\operatorname{Hom}_R(G_R, \mathbb{G}_{m,R}) = \operatorname{Hom}_{\operatorname{Hopf}_R}\left(R[t, t^{-1}], H_R\right).$$

Thus, we see that we are in bijection with invertible elements of H_R such that the relevant map preserves the Hopf algebra structure. In particular, preserving the comultiplication map $t \mapsto t \otimes t$ is asking for $\varphi \in H_R$ to be invertible as well as $\Delta_R(\varphi) = \varphi \otimes \varphi$.

So in total, we need to relate units in H_R to having $\varepsilon_R(\varphi) = 1$, which is a general fact. Certainly $\varepsilon_R(\varphi) = 1$ implies that φ is a unit by using the comultiplication. In the reverse direction, we note $1 \cdot 1 = 1$ rewrites as $(\varepsilon \otimes \varepsilon) \circ \Delta = \varepsilon$, meaning that $\varepsilon_R(\varphi)^2 = \varepsilon_R(\varphi)$ always, so φ being invertible requires $\varepsilon_R(\varphi) = 1$. ∎

Remark 2.93. Fix a finite commutative group k-scheme G with $G = \operatorname{Spec} H$ for Hopf k-algebra H. Then $k[G] \cong H^\vee$, where we send $g \in G$ to the map $H \to k$ corresponding to evaluation at g. (Notably, we are viewing H as global sections of G, so evaluation makes sense.)

Example 2.94. Take $G = (\mathbb{Z}/n\mathbb{Z})_k$, which we note is an étale reduced group scheme with n (closed) points. We claim that $G^\vee = \mu_n$. Set H to be the Hopf k-algebra corresponding to G. Using the previous remark, we find that

$$H^\vee = k[G] = \frac{k[x]}{(x^n - 1)}$$

at least as k-algebras. It remains to check that comultiplication structure is the same on both. On μ_n, the comultiplication structure is given by $x \mapsto (x \otimes x)$, so we just have to track it through on the dual. Well, for global sections $f, g \in H$, we evaluate

$$(fg)([1]_n) = f([1]_n)g([1]_n) = (f \otimes g)([1]_n \otimes [1]_n),$$

so we have the correct comultiplication.

2.10.2 fpqc Descent

We take a short intermission to discuss fpqc descent. There are lots of references; for example, see [Con15, §6]. We will work with relatively light hypotheses.

Definition 2.95 (fpqc)**.** A morphism $f\colon X \to Y$ of schemes is *fpqc* if and only if it is faithfully flat and quasicompact.

Remark 2.96. Somehow we are generalizing the discussion for gluing on Zariski opens.

Let's discuss what gluing looks like. Fix a map $f\colon S_0 \to S$ which is fpqc; then we set $S_1 \coloneqq S_0 \times_S S_0$ and $S_2 \coloneqq S_0 \times_S S_0 \times_S S_0$, and we let $p_{12}, p_{23}, p_{13}\colon S_2 \to S_1$ and $p_1, p_2\colon S_1 \to S_0$ be the projections. We would like to discuss when we can lift quasicoherent sheaves.

Definition 2.97 (descent datum)**.** Fix everything as above. Given a quasicoherent sheaf $\mathcal{F}$ on S_0, a *descent datum* on $\mathcal{F}$ is an isomorphism $\theta\colon p_1^*\mathcal{F} \to p_2^*\mathcal{F}$ of quasicoherent sheaves on S_1 satisfying the "cocycle condition" that

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

A morphism of descent datum $h\colon (\mathcal{F}, \theta) \to (\mathcal{G}, \psi)$ is a morphism of the quasicoherent sheaves commuting with the isomorphisms. In other words, the following diagram commutes.

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

More explicitly, the equality to define the descent datum is asking for the following diagram to commute.

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

with the bottom arrow labeled $p_{13}^*\theta$.

The equalities listed above are really natural isomorphisms induced by equalities of projections; for example, $p_1 \circ p_{12} = p_1 \circ p_{13}$.

Here is our result.

Theorem 2.98. Fix a map $f\colon S_0 \to S$ which is fpqc. Then $\mathrm{QCoh}(S)$ is equivalent to the category of descent data $(\mathcal{F}, \theta)$.

Proof. The forward map takes a quasicoherent sheaf $\mathcal{F}$ on S to the pair $(f^*\mathcal{F}, \theta_{\mathcal{F}})$ where $\theta_{\mathcal{F}}$ is the composite

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

It remains to discuss the inverse functor. The proof reduces to the affine case, where we are talking about modules, and one can attempt to recover the original model from the descent datum by taking some kernel. ■

One can even discuss descent datum on schemes.

Definition 2.99 (descent datum)**.** Fix an S_0-scheme X. Build S_1 and S_2 and the projections as above. Then a *descent datum* is an isomorphism $\theta\colon X \times_{S_0,p_1} S_1 \cong X \times_{S_0,p_2} S_1$ such that

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

Remark 2.100. In general, we do not expect to be able to actually get a scheme from descent datum, but we will be okay for affine schemes because these are basically understood by their global sections.

2.11 March 1

Here we go.

2.11.1 The Dual Isogeny

Let's prove Theorem 2.86.

Theorem 2.86 ([Mum08, Theorem 15.1])**.** Fix an isogeny $f\colon A \to B$ of abelian k-varieties. Then there is a dual isogeny $f^\vee\colon B^\vee \to A^\vee$ defined by sending $(\mathcal{L}, \alpha) \in \mathrm{Pic}^\circ_{B/k}(T)$ to $(f^{\mathcal{L}}, f^*\alpha) \in \mathrm{Pic}^\circ_{A/k}(T)$. In fact, $\ker f^\vee = (\ker f)^\vee$.

Proof. Fix a k-scheme T. Then $(\ker f^\vee)(T)$ by definition consists of rigidified line bundles $(\mathcal{L}, A) \in \mathrm{Pic}^\circ_{B/k}(T)$ such that $f^*(\mathcal{L}, \alpha)$ is trivial in $A^\vee$. It turns out that we can show that asserting we are in $\mathrm{Pic}^\circ_{B/k}$ already: one can show that $t_y^*\mathcal{L} \cong \mathcal{L}$ directly for all $y \in B$. Explicitly, for $x \in A$, we note that $t_x^* f^*\mathcal{L} \cong f^*\mathcal{L}$ because we know that $f^*\mathcal{L} \cong \mathcal{O}_{A\times T}$. As such, $\varphi_{f^*\mathcal{L}}$ is the zero map. But now we note that

$$\varphi_{f^*\mathcal{L}}(x) = f^\vee(\varphi_{\mathcal{L}}(f(x)))$$

because $t_x^* f^* \mathcal{L} = f^* t_{f(x)}^* \mathcal{L}$ and some rearranging. So because the left-hand side vanishes, the right-hand side will need to vanish; in particular, surjectivity of f requires the composite $f^\vee \circ \varphi_{\mathcal{L}}$ to vanish. We will shortly see that $f^\vee$ has finite kernel as a map $\mathrm{Pic}_{B/k} \to \mathrm{Pic}_{A/k}$, so $f^\vee$ is essentially an isogeny, so $\varphi_{\mathcal{L}}$ must itself vanish. (Formally, one should argue on connected components to make sure everything is okay.)

We claim that this set is in bijection with just line bundles $\mathcal{L}$ on $B \times T$ such that $f^*\mathcal{L} \cong \mathcal{O}_{A\times T}$. Indeed, for any such line bundle $\mathcal{L}$, having $f^*\mathcal{L} \cong \mathcal{O}_{A\times T}$ pins it down in the target, and then this actually fixes the isomorphism α.

To continue, we will use fpqc descent to the map $A \times T \to B \times T$, which is fpqc because $f\colon A \to B$ is an isogeny (flat, for example, by miracle flatness). The point is that Theorem 2.98 tells us line bundles on $B \times T$ are equivalent to line bundles on $A \times T$ together with descent data. Let's unwind the descent data; set $G \coloneqq \ker f$.

- We take $S_0 \coloneqq A \times T$ and $S \coloneqq B \times T$.
- Then $S_1 \coloneqq S_0 \times_S S_0$ is $(A \times T)_{B\times T}(A \times T)$. Pairs in S_1 can be written as $(a, a+g)$ for some $g \in \ker f$ (notably, the coordinates must agree down in $B \times T$), so this is just $A \times T \times G$.
- Analogously, we see that $S_2 = A \times T \times G \times g$.

Now, the line bundles $\mathcal{L}$ of interest need to be $\mathcal{O}_{A\times T}$ after pulling back by f, so $\theta\colon \operatorname{pr}_1^* \mathcal{O}_{A\times T} \to \operatorname{pr}_2^* \mathcal{O}_{A\times T}$ can be turned into an invertible global section $\mathcal{O}_{A\times T\times G} \to \mathcal{O}_{A\times T\times G}$. Namely, $\theta \in \Gamma(A \times T \times G, \mathcal{O}^\times_{A\times T\times G})$. Because A is proper over k, this really amounts to having $\theta \in \Gamma(T \times G, \mathcal{O}^\times_{T\times G})$. Also note that we are asking to satisfy a cocycle condition

$$\operatorname{pr}_{13}^* \theta = \operatorname{pr}_2^* \theta \circ \operatorname{pr}_{12}^* \theta.$$

Let's compare what we have with $G^\vee(T)$, which is supposed to be $f \in \operatorname{Hom}(G_T, \mathbb{G}_{m,T})$. In other words, f is a global section of $\Gamma(T \times G, \mathcal{O}^\times_{T\times G})$ such that $\Delta_T(f) = f \otimes f$ (to be a group homomorphism).

So it remains to show that the cocycle condition on θ corresponds to the homomorphism condition on f. Well, tracking through all the identifications, we see that we are asking for

$$\theta(a, g_1 + g_2) = \theta(a, g_1)\theta(a + g_1, g_2),$$

which unwinds to $\Delta_T(\theta) = \theta \otimes \theta$ upon staring out how the Hopf algebra comultiplication behaves. ∎

Remark 2.101. Because $\ker f$ is a finite group scheme, we see that $(\ker f)^\vee$ is finite. Because f being an isogeny requires $\dim A = \dim B$, we are able to conclude that $f^\vee$ is also an isogeny. In fact, $\deg f = \deg f^\vee$ by plugging Theorem 2.86 into

$$\deg f = \dim_k \Gamma(\ker f, \mathcal{O}_{\ker f}).$$

Let's run some other checks on duality.

Proposition 2.102. Given two morphisms $f, g\colon A \to B$ of abelian k-varieties, we have $(f+g)^\vee = f^\vee + g^\vee$.

Proof. It is enough to check this on $B^\vee(\overline{k})$. By unwinding the definitions, it is enough to show that

$$(f+g)^* \mathcal{L} \overset{?}{\cong} f^* \mathcal{L} \otimes g^* \mathcal{L}.$$

But in fact $\mathcal{L} \in B^\vee(\overline{k})$ implies that $m^* \mathcal{L} \cong \operatorname{pr}_1^* \mathcal{L} \otimes \operatorname{pr}_2^* \mathcal{L}$ on $B \times B$, which we can then pull back along $(f, g)\colon A \to B \times B$ to achieve the desired equality. ∎

Corollary 2.103. Fix any abelian k-variety A. Then for any integer $n \in \mathbb{Z}$, we have $[n]_{A^\vee} = [n]_A^\vee$.

Proof. Note $\operatorname{id}_A^\vee = \operatorname{id}_{A^\vee}$ by unwinding definitions. Then for $n \geq 0$, write $[n]_A = [1]_A + \cdots + [1]_A$ and apply Proposition 2.102. For $n \leq 0$, one notes that $[n] + [-n] = [0]$ to derive this from the positive case. ∎

Remark 2.104. For example, we are able to say that $A[n]^\vee$ is $A^\vee[n]$ after identifying duals suitably.

2.11.2 Quotients

We will want quotients. For the correct references, see SGA 3, exposé 6, 3.2.

Theorem 2.105. Fix a closed normal group k-subscheme $A \subseteq B$, where A and B are fppf group k-schemes. (Here, fppf means faithfully flat of finite presentation.) Then there is a unique fppf group scheme C such that

$$1 \to A \to B \to C \to 1$$

is exact in the category of fppf sheaves. In fact, C is the fppf sheafification of the fppf presheaf $T \mapsto B(T)/A(T)$.

In life, A will typically be affine and in fact finite (such as the kernel of an isogeny). If B is also affine, then one can take the ring of A-invariants to do the job. In general, because A is finite, one may work locally on A to complete the argument. Perhaps the gluing wants to glue along the fppf topology, for which one needs to do descent.

Theorem 2.106 ([BLR90, Theorem 6.1.5])**.** Fix a map $f\colon S_0 \to S$ which is fpqc. Then the functor from Sch_S to S_0-schemes with descent data is fully faithful. In fact, this upgrades to an equivalence if one works with quasi-affine schemes.

This is enough to do our gluing because we only need uniqueness. The point of the above result is to reduce this discussion to sheaves on the fpqc topology.

Remark 2.107. There is a general theory trying to build a quotient scheme modulo some proper and flat equivalence relation; one essentially uses the Hilbert scheme to encode everything.

For our purposes, we are only ever going to take quotients by finite group schemes, but understanding quotients in general can be helpful because, for example, this allows us to construction the Picard scheme by taking a quotient of divisors by an equivalence relation to get line bundles.

2.12 March 4

Homework has been posted. It is due shortly before spring break. There will be another homework assigned over spring break.

Remark 2.108. Any surjective group homomorphism $f\colon A \to B$ of abelian k-varieties will be fpqc automatically: quasicompactness has no content, and flatness follows by Miracle flatness.

2.12.1 Construction of the Dual Abelian Variety

For completeness, we provide a construction of $\mathrm{Pic}^\circ_{A/k}$; see [Mum08, §II.8, §III.13]. The point is to use the surjection $\varphi_{\mathcal{L}}\colon A \to \mathrm{Pic}^\circ_{A/k}$ (which we know exists on the functor of points), so one can recover $\mathrm{Pic}^\circ_{A/k}$ as a quotient group scheme by $K(\mathcal{L}) \coloneqq \ker \varphi_{\mathcal{L}}$. For example, in characteristic 0, our finite group scheme must be smooth, so we should use the reduced scheme structure.

Quickly, we provide a moduli interpretation for $A^\vee$.

Definition 2.109 (Poincaré line bundle)**.** Fix an abelian k-variety A. The *Poincaré line bundle* $\mathcal{P}$ on $A \times A^\vee$ is the line bundle satisfying $\mathcal{P}|_{0_A \times A^\vee}$ and $\mathcal{P}|_{A \times \lambda} \cong \lambda$ for any (rigidified) line bundle $\lambda \in A^\vee$.

Remark 2.110. The line bundle $\mathcal{P}$ is unique by Proposition 2.19.

To see that it exists, for given very ample line bundle $\mathcal{L}$ on A, define

$$\mathcal{M} \coloneqq m^*\mathcal{L} \otimes \mathrm{pr}_1^*\,\mathcal{L}^{-1} \otimes \mathrm{pr}_2^*\,\mathcal{L}^{-1}$$

on $A \times A$. Notably, $\mathcal{M}|_{0_A \times A} \cong \mathcal{O}_A$ and $\mathcal{M}|_{A\times\{x\}} = \varphi_{\mathcal{L}}(x)$ by some computation, so we expect to have $(\mathrm{id}_A \times \varphi_{\mathcal{L}})^*\mathcal{P} = \mathcal{M}$. So we will be able to construct $\mathcal{P}$ by some suitable descent.

Let's now give $K(\mathcal{L})$ a scheme structure: we let it be the maximal subscheme of A such that $\mathcal{M}|_{K(\mathcal{L})\times A}$ is trivial; we won't bother to check that this exists. It turns out that this is the correct scheme structure for $\mathrm{Pic}^\circ_{A/k}$ by some checking. So to finish our construction of the Poincaré line bundle as providing descent data on

$$A \times A \times A \times K(\mathcal{L}) = (A \times A) \times_{A\times A^\vee} (A \times A) \to A \times A^\vee.$$

The descent data now amounts to providing an isomorphism $\mathcal{M} \cong (1 \times t_x)^*\mathcal{M}$ for $x \in K(\mathcal{L})$, which can be done by staring at the group law.

2.12.2 Symmetry of Duality

We defined $A^\vee$ as a dual, so one should expect that A and $A^{\vee\vee}$ are canonically isogenous. In general, a line bundle $\mathcal{Q}$ (living in the connected component) on $A \times B$ produces a homomorphism $\kappa_{\mathcal{Q}} \colon B \to A^\vee$ by. For example, $\mathcal{P}$ on $A \times A^\vee$ corresponds to $\mathrm{id} \colon A^\vee \to A^\vee$. However, swapping coordinates produces an isomorphism $\sigma \colon A \times A^\vee \to A^\vee \times A$ will then produce a morphism $\kappa_{\sigma^*\mathcal{P}} \colon A \to (A^\vee)^\vee$, which we claim is an isomorphism.

Proposition 2.111. Fix an abelian k-variety A with Poincaré line bundle $\mathcal{P}$. Then swapping coordinates produces an isomorphism $\sigma \colon A \times A^\vee \to A^\vee \times A$ will then produce a canonical isomorphism $\kappa_{\sigma^*\mathcal{P}} \colon A \to (A^\vee)^\vee$. In fact, the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{\kappa_{\sigma^*\mathcal{P}}} & (A^\vee)^\vee \\ {\scriptstyle \varphi_{\mathcal{L}}}\downarrow & \swarrow_{\varphi_{\mathcal{L}}^\vee} & \\ A & & \end{array}$$

Proof. To see that $\kappa_{\sigma^*\mathcal{P}}$ is an isomorphism, we let $\mathcal{L}$ be ample so that $\varphi_{\mathcal{L}}$ and $\varphi_{\mathcal{L}}^\vee$ is an isogeny, and both of these covers of $A^\vee$ have the same kernel by Theorem 2.86. Now, $\kappa_{\sigma^*\mathcal{P}}$ is an isogeny because everything in sight is an isogeny (for example, everything has the same dimension, and finite kernel is forced because its composite with $\varphi_{\mathcal{L}}^\vee$ has finite kernel), and we are able to conclude that $\kappa_{\sigma^*\mathcal{P}}$ is an isomorphism because it has degree 1 (indeed, $\deg \varphi_{\mathcal{L}} = \deg \varphi_{\mathcal{L}}^\vee$).

We now show the commutativity of the given triangle by hand on closed points. In one direction, $\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ for $x \in A(\overline{k})$. In other direction, we begin by computing

$$\kappa_{\sigma^*\mathcal{P}}(x) = \mathcal{P}|_{\{x\}\times A^\vee}$$

by definition of κ, and

$$\varphi_{\mathcal{L}}^\vee\left(\kappa_{\sigma^*\mathcal{P}}(x)\right) = \varphi_{\mathcal{L}}^\vee\left(\mathcal{P}|_{\{x\}\times A^\vee}\right) = (\mathrm{id} \times \varphi_{\mathcal{L}})^*\mathcal{P}|_{\{x\}\times A} = \left(m^*\mathcal{L} \otimes \mathrm{pr}_1^*\,\mathcal{L}^{-1} \otimes \mathrm{pr}_2^*\,\mathcal{L}^{-1}\right)|_{\{x\}\times A},$$

which agrees with the other side. ∎

Remark 2.112. For an abelian k-variety A, we will let $\mathcal{P}_A$ be its Poincaré line bundle in this remark. Then it turns out that $\mathcal{P}_{A^\vee}$ on $A^\vee \times (A^\vee)^\vee$ is $\sigma^*\mathcal{P}_A$ pulled back along $\kappa^{-1}_{\sigma^*\mathcal{P}_A} \colon A^\vee \times (A^\vee)^\vee \to A^\vee \times A$. To see this, I think one can use a moduli interpretation or the commutativity of the above diagram for some uniqueness.

Proposition 2.111 motivates the following definition.

Definition 2.113. Fix an abelian k-variety A. A homomorphism $\lambda\colon A \to A^\vee$ is *symmetric* if and only if $\lambda^\vee = \lambda$ up to the identification of A with $A^{\vee\vee}$.

Example 2.114. A polarization $\varphi_{\mathcal{L}}$ is symmetric by Proposition 2.111 (perhaps needing to check on $\overline{k}$-points due to the definition of polarization).

Remark 2.115. Fix a morphism of abelian k-varieties $f\colon A \to B$. Given a line bundle $\mathcal{L}$ on B, tracking through moduli interpretations produces the following commutative diagram.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \varphi_{f^*\mathcal{L}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathcal{L}}} \\ A^\vee & \xrightarrow{f^\vee} & B^\vee \end{array}$$

This symmetry allows us to construct the "dual" isogeny.

Theorem 2.116. Fix an isogeny $f\colon A \to B$ of abelian k-varieties. Then there is an isogney $g\colon B \to A$ such that $g \circ f = [\deg f]_A$.

Remark 2.117. It also turns out that $f \circ g = [\deg f]_B$ and so $\deg g = \deg f$ (where f and g are as above). This is essentially by doing cancellation on isogenies via quotients.

The proof of Theorem 2.116 is surprisingly technical in its group theory. For example, one needs the following result.

Theorem 2.118 (Deligne)**.** Fix a commutative finite flat k-group scheme G of order $m := \dim \Gamma(G, \mathcal{O}_G)$. Then G is killed by $[m]_G$.

Proof. Omitted. We will show this later. ∎

We now prove Theorem 2.116.

Proof of Theorem 2.116. Note f is fpqc, so descent tells us that a k-scheme X makes $X(B)$ an equalizer of $\mathrm{pr}_1, \mathrm{pr}_2\colon X(A) \to X(A \times_B A)$ by viewing X as a quasicoherent sheaf. (See [Con15, Theorem 6.2.14].) For example, the composite

$$A \times \ker f \cong A \times_B A \xrightarrow{\mathrm{pr}} A \xrightarrow{[m]} A$$

vanishes for each projection, where $m := \deg f = \dim \ker f$. So $[m] \circ \mathrm{pr}_1 = [m] \circ \mathrm{pr}_2$, so descent tells us that $[m]$ factors through f, which is what promises the existence of g. ∎

2.13 March 6

Here we go.

2.13.1 Poincaré Reducibility

Now that we have a notion of inverse isogeny, we are able to establish the following result.

Theorem 2.119 (Poincaré reducibility)**.** Fix an abelian k-subvariety B of A. Then there exists an abelian k-subvariety B' such that $m\colon B \times B' \to A$ is an isogeny.

Proof. Let $i\colon B \hookrightarrow A$ denote the inclusion. We want to build a complement for B, which is essentially going to be a quotient of $A^\vee$ (by duality). Explicitly, there is a dual morphism $i^\vee\colon A^\vee \to B^\vee$, and pick an ample line bundle $\mathcal{L}$ on A to provide a polarization $\varphi_{\mathcal{L}}\colon A \to A^\vee$. Notably, we have the following commutative diagram.

$$\begin{array}{ccc} B & \xrightarrow{\ i\ } & A \\ {\scriptstyle \varphi_{i^*\mathcal{L}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathcal{L}}} \\ B^\vee & \xleftarrow{\ i^\vee\ } & A^\vee \end{array}$$

As such, we consider the kernel of $(i^\vee \circ \varphi_{\mathcal{L}})\colon A \to B^\vee$, and we let B' be the reduced scheme structure on the connected component so that B' is in fact an abelian k-variety.

It remains to check that B' works. Note that the kernel of the addition map $B \times B' \to A$ is contained in $B \cap B'$ (on k-points), which is contained in the kernel of $\varphi_{i^*\mathcal{L}}$ by the commutativity of the above diagram, which is finite because $\varphi_{i^*\mathcal{L}}$ is finite. So it is enough to just check that

$$\dim B + \dim B' \stackrel{?}{=} \dim A.$$

Well, finiteness of $B \cap B'$ at least gives $\dim B + \dim B' \le \dim A$, so we only need the other inequality. The main difficulty arises from understanding $\dim B'$. Well, abelian varieties have pure dimension, so

$$\dim B' = \dim \ker(i^\vee \circ \varphi_{\mathcal{L}}) = \dim \ker i^\vee.$$

(The second equality holds because $\varphi_{\mathcal{L}}$ has finite kernel, so it cannot adjust the dimension of the fiber.) Now, $i^\vee\colon B^\vee \to A^\vee$ is a group homomorphism, so all its fibers have the same dimension, and generically the dimension must be upper-bounded by $\dim A^\vee - \dim B^\vee$, which is $\dim A - \dim B$. ∎

2.13.2 Finite Group Schemes

We are morally studying finite flat group schemes G over a base scheme S, but we will ignore flatness and just work over a field k (where everything is flat). We would like to move towards a classification.

Definition 2.120 (connected)**.** Fix a finite group k-scheme G. Then G is *local* or *connected* if and only if G is connected; i.e., $G = G^\circ$.

Example 2.121. Fix a field k of characteristic p (possibly 0), and let μ_n be the kernel of $[n]\colon \mathbb{G}_m \to \mathbb{G}_m$. Then

$$\mu_n = \operatorname{Spec} \frac{k[x]}{(x^n - 1)}$$

is only connected when n is a power of p, and μ_n is étale if and only if $p \nmid n$.

Unique?

Here is our main result.

Proposition 2.122. Fix a finite group k-scheme G. Then there is a connected group k-scheme G_{loc} and étale group k-scheme $G_{\text{ét}}$ such that

$$1 \to G_{\text{loc}} \to G \to G_{\text{ét}} \to 1$$

is exact (as fppf sheaves, for example). In fact, if k is perfect, then this splits naturally in G.

Morally, one should have $G_{\text{loc}} = G^\circ$ and $G_{\text{ét}}$ to be the quotient given the reduced scheme structure. We begin with a lemma.

Lemma 2.123. Fix a field k. There is an equivalence of categories between finite étale k-algebras and finite étale k-schemes. Explicitly, one sends a finite étale k-scheme X to $\Gamma(X, \mathcal{O}_X)$ and goes in the opposite direction

Proof. Everything is affine, so we are just moving the words étale and finite back and forth. ∎

Lemma 2.124. Fix a field k. There is an equivalence of categories between finite étale k-schemes X and finite sets with continuous $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-action.

Proof. Send a scheme X to the set $X(k^{\mathrm{sep}})$; one can see that this is fully faithful, so it is enough to show that we are essentially surjective. We will just give a functor from sets with action by $G := \mathrm{Gal}(k^{\mathrm{sep}}/k)$ to a finite étale k-algebra. Well, we just take

$$\left(\prod_{s\in S} k^{\mathrm{sep}}\right)^G,$$

where G acts by permuting the coordinates and component-wise at the same time. This produces a finite étale k-algebra. ∎

Example 2.125. Fix a field k of characteristic $p := \mathrm{char}\, k$, and choose an integer n coprime to p. Then μ_n is an étale group scheme, and it corresponds to the set $\mu_n(k^{\mathrm{sep}})$, which is the set of nth roots of unity (equipped with Galois action).

We now add in group structure.

Lemma 2.126. Fix a field k. Then the category of finite étale k-group schemes is equivalent to the category of finite groups with continuous action by $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Proof. Set $G := \mathrm{Gal}(k^{\mathrm{sep}}/k)$ for brevity. Then use the previous lemma and add in group structure everywhere. ∎

Example 2.127. Let k be algebraically closed. The category of group k-schemes G is just the category of groups because we are looking for sets with action by the trivial group.

To continue, we will want an understanding of étale morphisms. In particular, we want the notion of "formally étale."

Proposition 2.128. Fix a field k and a finite type k-scheme X. Then there is a finite étale k-scheme $\pi_0(X)$ and map $q\colon X \to \pi_0(X)$ with the following universal property: any map $q'\colon X \to Y'$ such that Y' is finite étale factors uniquely through q.

Morally, we should think about $\pi_0(X)$ as (geometrically) connected components.

Proof. The main point is the construction of $\pi_0(X)$, for which it is enough to give a set $\pi_0(X)(k^{\mathrm{sep}})$ with continuous action by $G := \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Well, just take our set to be $\pi_0(X_{k^{\mathrm{sep}}})$ to be the collection of geometrically connected components. Then note that G acts on $X_{k^{\mathrm{sep}}}$ continuously, so it will also permute the connected components, so our action descends to $\pi_0(X_{k^{\mathrm{sep}}})$. Thus, we have indeed constructed some finite étale k-scheme X.

Note that there is a natural map $X(k^{\mathrm{sep}}) \to \pi_0(X)(k^{\mathrm{sep}})$ given by sending a point to its connected component, so we get to lift this to a map $q\colon X_{k^{\mathrm{sep}}} \to \pi_0(X)_{k^{\mathrm{sep}}}$. This map is G-invariant, so Galois descent provides

a map $X \to \pi_0(X)$. (For example, one can even use Theorem 2.98.) We will not bother to check the universal property, but this can be seen by construction because any $q' \colon X \to Y'$ is essentially determined by where it sends the connected components of X, all of whose information is given by $\pi_0(X)$. ■

Remark 2.129. One can also check that q is faithfully flat, and its fibers are the connected components of q. Indeed, the fibers are the connected components by construction, so flatness follows by miracle flatness, and q is faithful because q is geometrically surjective.

Remark 2.130. As usual, if X is a group k-scheme, then we can force $\pi_0(X)$ to be a group k-scheme too.

We are now ready to prove Proposition 2.122.

Proof of Proposition 2.122. Take $G_{\text{ét}} \coloneqq \pi_0(G)$, which we know to be a finite étale group $k$scheme. Then the exact sequence is essentially immediate. For k perfect, the point is that $G_{\text{red}} \subseteq G$ is a smooth subgroup k-scheme, and the splitting is given by

$$G_{\text{red}} \to G \to \pi_0(G),$$

Why? whose composite we can find to be an isomorphism. ■

We are now equipped to give the following definition.

Definition 2.131 (étale-local)**.** Fix a commutative group k-scheme G. Then G is *étale-local* if and only if G is étale and its Cartier dual is connected.

Remark 2.132. One finds that G is the sum of four pieces which are étale-étale, étale-local, local-étale, and local-local. In fact, this decomposition is unique: any map to any other component must be the zero map (a map from something local to something étale must be trivial and vice versa, essentially because étale must reduce our scheme structure, but when connected, this must then just go to the identity).

Example 2.133. Fix a field k of characteristic $p \coloneqq \operatorname{char} k$, where $p > 0$.

- If n is coprime to p, then μ_n is étale-étale (in fact, it is self-dual).
- The group $\mathbb{Z}/p\mathbb{Z}$ is dual to μ_p, so $\mathbb{Z}/p\mathbb{Z}$ is étale-local, and μ_p is local-étale.
- There is a group α_p is self-dual and local, so it is local-local.

In fact, one has the following remark.

Remark 2.134. Fix an algebraically closed field k of characteristic $p > 0$.

- The only étale-étale commutative group k-schemes G are products of μ_n where n is coprime to p. Indeed, being étale means that G is a sum of cyclic groups $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, and we can only have n coprime to p in order for the dual of μ_ns to be étale.
- A similar point holds for étale-local as being products of $\mathbb{Z}/p^\bullet\mathbb{Z}$. Essentially the same argument works, but now we need n to be a power of p in order for the dual factors μ_ns to be local.
- Lastly, a similar point holds for local-étale as being products of $\mu_{p^\bullet}$. Indeed, the dual is étale-local, and then we go to the previous point.

However, there can be lots of local-local commutative k-group schemes.

Remark 2.135. Fix a field k of characteristic 0. Then every group k-scheme is smooth so every finite commutative group k-scheme is étale-étale.

Here is an application.

Remark 2.136. Fix a field k of characteristic $p > 0$. Given an abelian k-variety A and positive integer n coprime to p, one has

$$A[n] \oplus A\left[p^\nu\right] \cong A\left[np^\nu\right]$$

by the natural map. Note that $A[n]$ is étale, and its dual is $A^\vee[n]$, which continues to be étale. On the other hand, one finds that $A[p^\nu]$ has no étale-étale part: one could take a decomposition, and any étale-étale part remains that way after passing to k^{sep}, whereupon Remark 2.134 tells us that we can only have factors of μ_m with $\gcd(m, p) = 1$, but $A[p^\nu]$ has order which is a power of p.

2.14 March 8

Here we go.

2.14.1 Torsion as Finite Flat Group Scheme

The finite group k-schemes of interest to us are of the form $A[n]$ where n is an integer. Remark 2.136 tells us that the particularly bad case is $A[p^\nu]_{\overline{k}}$ where $p := \operatorname{char} k$ is positive. We know that this will have no étale-étale part, so it remains to find the remaining parts. Let's use Remark 2.134 to take care of some of these.

- We know that there will be some étale-local part of the form $(\mathbb{Z}/p^m\mathbb{Z})^r$ (one needs to induct on m). Here, r is the p-rank.
- By duality, we have some local-étale part of the form $\mu_{p^m}^s$ (again, one needs to induct on m).

We would like for $r = s$. This requires the following result.

Proposition 2.137. Fix abelian k-varieties A and B of p-rank r_A and r_B. If A and B are isogenous, then $r_A = r_B$.

Proof. Let $f\colon A \to B$ be an isogeny, and let n be the order of $\ker f$. Now, we see that f restricts to a group homomorphism $A[p^m](\overline{k}) \to B[p^m](\overline{k})$ with kernel of size at most n, so in light of our kernel having order n, we see that

$$p^{mr_A} \le np^{mr_B}$$

for all integers m. Sending $m \to \infty$ forces $r_A \le r_B$; by symmetry, we get the other inequality, so we are done. ∎

So we see that $r = s$ because A and $A^\vee$ are isogenous.

2.14.2 Local Finite Flat Group Schemes

It remains to study the local-local piece. This is harder. We pick up the following definition.

Definition 2.138 (height one)**.** Fix a field k of characteristic $p > 0$. A finite commutative local k-group scheme G is of *height one* if and only if $x^p = 0$ for all $x \in \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal at $e_G \in G$.

The point of being height one is that its Lie algebra. To understand the Lie algebra, we need to discuss differentials.

Definition 2.139 (differential)**.** Fix an S-group scheme G of finite type. Then $\Omega^1_{G/S}$ is the *sheaf of differentials* defined so that

$$\mathrm{Hom}_{\mathcal{O}_G}\left(\Omega^1_{G/S}, \mathcal{F}\right) = \mathrm{Der}_S(\mathcal{O}_G, \mathcal{F})$$

for any quasicoherent sheaf $\mathcal{F}$ on S. Here, $\mathrm{Der}_S(\mathcal{O}_G, \mathcal{F})$ refers to the $\mathcal{O}_S$-differentials $\delta\colon \mathcal{O}_G \to \mathcal{F}$, which are additive maps vanishing on $f^{-1}\mathcal{O}_S \subseteq \mathcal{O}_G$ and satisfying the Leibniz rule.

And here is our Lie algebra.

Definition 2.140 (Lie algebra)**.** Fix an S-group scheme G of finite type. Then the *Lie algebra* is the set of left-invariant differentials in $\mathrm{Der}_S(\mathcal{O}_G, \mathcal{O}_G)$, which is canonically identified with $\mathrm{Hom}_{\mathcal{O}_G}(\Omega_{G/S}, \mathcal{O}_G)$.

Remark 2.141. Fix an S-group scheme G of finite type. Then there is a natural isomorphism $\mathrm{Lie}\, G \cong T_e G$ given by sending a differential D to its restricted vector $D|_e$. We refer to [Mum08, pp. 92–94] for the proof; the idea is to construct an inverse map by using right translates of $D|_e$ to build D.

Anyway, here is our "classification" result, which at least gives us the coordinate ring.

Lemma 2.142. Fix a field k of characteristic $p > 0$. Fix a finite local k-group scheme G of height 1 with coordinate ring R. Then

$$R \cong \frac{k[x_1, \dots, x_n]}{(x_1^p, \dots, x_n^p)}$$

for some n. In particular, $\dim_k R$ is a power of p.

Proof. Fix $x_1, \dots, x_n \in \mathfrak{m}$ which form a k-basis of $\mathfrak{m}/\mathfrak{m}^2$. Because G is local, this extends to a surjection $k[x_1, \dots, x_r] \to R$. Being height one tells us that we now get a surjection

$$\frac{k[x_1, \dots, x_n]}{(x_1^p, \dots, x_n^p)} \to R.$$

We would like this to be an isomorphism. For this, we will want to show that no monomial with powers less than p vanishes in R. (This is enough because any polynomial relation among the variables can multiply through by various $x_\bullet$s in order to derive that a monomial must equal zero; we are crucially using that $x_\bullet^p = 0$ already.)

We now use the Lie algebra. Let $D_1, \dots, D_n \in \mathrm{Lie}\, G$ be differentials providing a dual basis for $\overline{x}_1, \dots, \overline{x}_n \in \mathfrak{m}/\mathfrak{m}^2$. Lifting this back up to R tells us that

$$D_j \prod_{i=0} x_i^{n_i} \neq 0$$

where $0 \leq n_i < p$ and $n_j \neq 0$. But now any monomial being zero must have all exponents equal zero by applying the various $D_\bullet$s, so it remains to see that $1 \neq 0$. ∎

Remark 2.143. Without the hypothesis on height, one needs to allow modding out by terms of the form $x_i^{p^\bullet}$.

Let's continue discussing the Lie algebra.

Definition 2.144 (Lie bracket)**.** Fix an S-group scheme G of finite type. Then there is a *Lie bracket* given by

$$[D_1, D_2] \coloneqq D_1 D_2 - D_2 D_1$$

for any derivations $D_1, D_2 \in \mathrm{Lie}\, G$.

Remark 2.145. If G is a k-group scheme of finite type, then if $p \coloneqq \operatorname{char} k$ is positive, then

$$D^{\circ p} = \underbrace{D \circ \cdots \circ D}_{p}$$

still lives in $\operatorname{Lie} G$. Certainly this is additive and G-linear and vanishes on k, so it remains to check the Leibniz rule. The point is that one can expand out the Leibniz rule p times as

$$D^{\circ p}(ab) = \sum_{i+j=p} \binom{p}{i} D^{\circ i}(a) D^{\circ j}(b),$$

but with $p = \operatorname{char} k$, all terms except the ending ones vanish, giving the Leibniz rule.

The above remark motivates the following definition.

Definition 2.146. Fix a field k of positive characteristic $p > 0$. Then a *p-Lie algebra* is a Lie algebra $\mathfrak{g}$ equipped with bracket $[\cdot,\cdot]$ as well as an endomorphism $(-)^{(p)} \colon \mathfrak{g} \to \mathfrak{g}$ satisfying the following.

- $(\lambda x)^{(p)} = \lambda^p x^{(p)}$.
- The adjoint map $(\operatorname{ad} x) \colon y \mapsto [x,y]$ satisfies $\operatorname{ad} x^{(p)} = (\operatorname{ad} x)^{(p)}$.
- One has $(x+y)^{(p)} = x^{(p)} + y^{(p)} + F_p(\operatorname{ad} x, \operatorname{ad} y)y$, where F_p is some non-commutative polynomial which we will not write down.

We feel okay not writing down the polynomial F_p because, in our setting, everything is commutative, so the Lie bracket vanishes, and it will be enough to remark that the relevant term always vanishes.

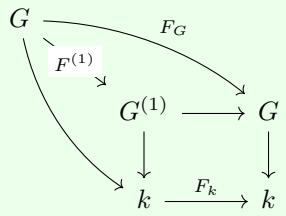
At long last, we note that we have the following result, explaining our remark earlier that height one means that it is enough to study the Lie algebra.

Theorem 2.147. The category of finite local k-group schemes of height one is equivalent to the category of p-Lie algebras over k.

Proof. See [Mum08, p. III.14]. Morally, the point is to recover the group G from its p-Lie algebra $\mathfrak{g}$. Well, one simply takes the universal enveloping algebra and quotients out by some extra relations arising from being a p-Lie algebra. ∎

For our application, we will want the following morphism.

Definition 2.148 (relative Frobenius)**.** Fix a group k-scheme G of finite type, and let $F_G \colon G \to G$ be the absolute Frobenius given by taking pth powers. Then we define the *relative Frobenius* $F_{G/\operatorname{Spec} k} \colon G \to G^{(1)}$ as the map of k-schemes making the following diagram commute, where the square is a pullback.



Example 2.149. Take $G \coloneqq \mathbb{G}_{a,k}$. Then $\alpha_p = \ker F^{(1)}$.

Remark 2.150. We note that $F^{(1)}$ is a group homomorphism by just writing out the relevant diagrams and noting that uniqueness of everything must make our diagrams commute. In fact, $\ker F^{(1)}$ is a finite local k-group scheme of height 1! Indeed, the point is that $F^{(1)}$ is purely inseparable (by construction), making $\ker F^{(1)}$ local, and then we know

$$\Gamma(\ker F^{(1)}, \mathcal{O}_{\ker F^{(1)}}) = \frac{\mathcal{O}_{G,e}}{\{x^p : x \in \mathfrak{m}_{G,e}\}}.$$

Corollary 2.151. Fix a commutative finite group k-scheme G of height 1. Then the map $[p]\colon G \to G$ is the zero map.

Proof. Note that p vanishes on $\operatorname{Lie} G$, from which the result follows from using the inverse functor of Theorem 2.147. ∎

Why is Lie faithful?

Corollary 2.152. Fix a commutative finite group k-scheme G of order m. Then $[m]\colon G \to G$ is the zero map.

Proof. It suffices to check the result on $\overline{k}$. Group theory will give the result for any étale part of G, so we may assume that G is local and in particular has order p^n. Now, we note that we can build the composite of relative Frobenius maps

$$G \to G^{(1)} \to G^{(2)} \to \cdots \to G^{(n)}.$$

This produces injections $\ker F^{(1)} \subseteq \ker F^{(2)} \subseteq \cdots$ until $\ker F^{(n)} = G$. (Namely, one can see that if any two kernels are the same, then they must stabilize, but if they are all supposed to be distinct up until G, so we get this result.) But each quotient becomes a finite group k-scheme killed by $[p]$, so $\ker F^{(n)}$ will be killed by $[p^n]$, and we are done. ∎

What?

2.15 March 11

Here we go.

2.15.1 Degree of Isogenies

Today we are going to discuss degrees of isogenies. The point is that we are going to show that the degree map $\deg\colon \operatorname{End} A \to \mathbb{Z}$ is polynomial. Let's define what this means

Definition 2.153. Fix a k-vector space V. Then a function $f\colon V \to k$ is a *homogeneous polynomial of degree* n if and only if $f|_W$ is a homogeneous polynomial of degree n for any finite-dimensional subspace $W \subseteq V$. In other words, for any finite set of linearly independent vectors $\{v_1, \ldots, v_n\}$, the function

$$(a_1, \ldots, a_n) \mapsto f(a_1 v_1 + \cdots + a_n v_n)$$

is a homogeneous polynomial of degree n. (The point here is that change of basis does not adjust the fact that f is a homogeneous polynomial of degree n.)

Remark 2.154. An induction tells us that it suffices to check the result for sets of linearly independent vectors of size 2.

So we are actually going to show that $\deg \operatorname{End} A \to \mathbb{Z}$ is a polynomial map of degree $2g$. For isogenies, we know how to make sense of degree, but we should probably make a convention if not an isogeny.

Definition 2.155. Given a homomorphism $f\colon A \to B$ of abelian k-varieties, we define $\deg f = 0$ if f is not an isogeny. For a general map $\frac{1}{n}f \in \mathrm{End}^0(A)$ where $g \coloneqq \dim A$, we define

$$\deg\left(\frac{1}{n}f\right) \coloneqq \frac{\deg f}{n^{2g}}.$$

Remark 2.156. One can check that $\frac{1}{m}f = \frac{1}{n}g$ implies that

$$\frac{\deg f}{m^{2g}} = \frac{\deg g}{n^{2g}}.$$

Indeed, by Theorem 2.48, we see that $\deg[n] = n^{2g}$ for any integer n, so $[m]\circ f = [n]\circ g$ yields the above equality after rearranging.

So in fact we will aim to show that $\deg\colon \mathrm{End}^0(A) \to \mathbb{Q}$ is a homogeneous polynomial of degree $2g$.

Here is a starting lemma.

Lemma 2.157. Fix an isogeny $g\colon A \to B$ of abelian k-varieties. For all line bundles $\mathcal{L}$ on B, one has

$$\chi(g^*\mathcal{L}) = (\deg g)\chi(\mathcal{L}).$$

Proof. See [Mum08, Theorem 12.2]. Note that this result is similar to Proposition 2.44. We will have more context for this result when we discuss Riemann–Roch for abelian varieties in more detail. The main point is to reduce to the elliptic curve case, where one can use the Riemann–Hurwitz formula; notable, the map g is a group homomorphism and hence unramified. ∎

Remark 2.158. One can upgrade this result so that one needs to make the target of g into a torsor over the source.

And here is our result.

Theorem 2.159. Fix a simple abelian k-variety A of dimension g. Then $\deg\colon \mathrm{End}^0(A) \to \mathbb{Q}$ is a homogeneous polynomial of degree $2g$.

Proof. Once we know that we have a polynomial, the fact that $\deg(nf) = n^{2g}\deg f$ will enforce homogeneity. So it suffices to show that we are just polynomial, so by Remark 2.154, it suffices to show that the map $\deg(nf_1 + f_2)$ is a polynomial map in n, where $f_1, f_2\colon A \to A$ are isogenies.

Choose an ample line bundle $\mathcal{L}$ on A. By Serre's criterion for ampleness, we may replace $\mathcal{L}$ with a power of itself so that $\mathcal{L}$ has no higher cohomology. But $\mathcal{L}$ must be globally generated (it's ample), so $\mathcal{L}$ has some global sections, so $\chi(\mathcal{L}) \neq 0$. Now, Lemma 2.157 tells us

$$\deg(nf_1 + f_2) = \frac{\chi((nf_1 + f_2)^*\mathcal{L})}{\chi(\mathcal{L})},$$

so it remains to work with the numerator. We would like to evaluate $\mathcal{L}_n \coloneqq (nf_1 + f_2)^*\mathcal{L}$ inductively, for which we must use Theorem 2.7. In particular, Theorem 2.7 tells us that

$$\mathcal{L}_{n+2} = (f_1 + f_1 + (nf_1 + f_2))^*\mathcal{L} \cong \mathcal{L}_{n+1} \otimes \mathcal{L}_{n+1} \otimes (2f_1)^*\mathcal{L} \otimes \mathcal{L}_n^{-1} \otimes L_n^{-1} \otimes f_1^*\mathcal{L}^{\otimes -2}.$$

An induction is now able to show that

$$\mathcal{L}_n = \mathcal{M}^{\otimes n(n-1)/2} \otimes \mathcal{N}^{\otimes n} \otimes Q$$

for some line bundles $\mathcal{M}$ and $\mathcal{N}$ and $\mathcal{Q}$ (which do not depend on n).

Now, the same argument which shows that the Hilbert polynomial is a polynomial shows that the map

$$(n_1, \dots, n_r) \mapsto \chi\left(\mathcal{L}_1^{\otimes n_1} \otimes \cdots \otimes \mathcal{L}_r^{\otimes n_r}\right)$$

is always a polynomial in $\mathbb{Q}[n_1, \dots, n_r]$, so we are done. ■

2.15.2 Riemann–Roch for Abelian Varieties

Let's study the Euler characteristic of line bundles in more detail.

Proposition 2.160. Fix a line bundle $\mathcal{L}$ on an abelian k-variety A.

(a) Then $n \mapsto \chi\left(\mathcal{L}^{\otimes n}\right)$ is a homogeneous polynomial of degree $2g$.

(b) If $\mathcal{L} = \mathcal{O}_A(D)$ for a divisor D, then $\chi(\mathcal{L}) = (D, \dots, D)/g!$, where $(D, \dots, D)$ is the intersection number.

Remark 2.161. Note that (c) of the above tells us that indeed $\mathcal{L}$ being ample means $\varphi_{\mathcal{L}}$ is an isogeny, so $\chi(\mathcal{L})^2$ must be nonzero, so $\chi(\mathcal{L})$ is nonzero.

Proof. We may assume that k is algebraically closed because we are just computing dimensions of cohomology, which is preserved by flat base change (such as a field extension).

For (a), we proceed in steps. The point is to reduce to the case of $\mathcal{L}$ being symmetric or in $A^\vee$, which can be attacked separately.

1. We claim that $\mathcal{L}_1 \otimes \mathcal{L}_2^{-1} \in A^\vee$ implies that $\chi(\mathcal{L}_1) = \chi(\mathcal{L}_2)$. Indeed, $\mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$ being in $A^\vee$ implies that $\mathcal{L}_1$ and $\mathcal{L}_2$ are algebraically equivalent, so they arise as restrictions of a larger line bundle $\mathcal{L}$ on $A \times S$. However, the Euler characteristic χ is locally constant, so we conclude $\chi(\mathcal{L}_1) = \chi(\mathcal{L}_2)$.

2. We claim that any line bundle $\mathcal{L}$ on A has line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ such that $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$ such that $\mathcal{L}_1$ is symmetric and $\mathcal{L}_2 \in A^\vee$.

   The main point is the construction of $\mathcal{L}_2$. We would like to set $\mathcal{L}_1$ to be $\mathcal{L} \otimes [-1]^*\mathcal{L}$, and take $\mathcal{L}_2$ to be $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}$, but this does not actually multiply to $\mathcal{L}$. So we will want to take some square-roots, which requires a more careful argument.

   To begin, we claim that $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1} \in A^\vee$. Indeed, it suffices to show that the line bundle is translation-invariant, so we compute

   $$t_x\left(\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}\right) \otimes \mathcal{L}^{-1} \otimes [-1]^*\mathcal{L} = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \otimes [-1]^*\left(t_{-x}^*\mathcal{L}^{-1} \otimes \mathcal{L}\right).$$

   Now, $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is certainly in $A^\vee$ because it is just in the image of $\varphi_{\mathcal{L}}$, and pulling back along $[-1]^*$ stays in $A^\vee$ because this map is just $[-1]_{A^\vee} : A^\vee \to A^\vee$. In fact, $[-1]$ corresponds to inverting the line bundle, so our line bundle now looks like

   $$t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \otimes \left(t_{-x}^*\mathcal{L} \otimes \mathcal{L}^{-1}\right),$$

   which vanishes by Theorem 2.28.

   We now use the fact that we are over $\overline{k}$, so we may find $\mathcal{L}_2 \in A^\vee(\overline{k})$ with $\mathcal{L}_2^{\otimes 2} = \mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}$. Now, we define $\mathcal{L}_1 \coloneqq \mathcal{L} \otimes \mathcal{L}_2^{-1}$ so that

   $$[-1]^*\mathcal{L}_1 = [-1]^*\mathcal{L} \otimes [-1]^*\mathcal{L}_2^{-1} = [-1]^*\mathcal{L} \otimes \mathcal{L}_2^{\otimes 2} \otimes \mathcal{L}_2^{-1} = [-1]^*\mathcal{L} \otimes \mathcal{L} \otimes [-1]^*\mathcal{L}^{-1} \otimes \mathcal{L}_2^{-1} = \mathcal{L}_1,$$

   so $\mathcal{L}_1$ is in fact symmetric, as needed.

3. We now prove (a). As remarked in the previous proof, this function is certainly polynomial, so it is enough to compute the degree. The result is true for $\mathcal{L} \in A^\vee$ by an inductive argument via $m^*\mathcal{L} = \mathrm{pr}_1^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}$, so it remains to handle the case where $\mathcal{L}$ is symmetric. Here, an induction with Theorem 2.7 shows that
$$\chi\left(\mathcal{L}^{\otimes m^2 n}\right) = \chi\left([m]^*\mathcal{L}^{\otimes n}\right) \overset{*}{=} \deg[m] \cdot \chi\left(\mathcal{L}^{\otimes n}\right) = m^{2g}\chi(\mathcal{L}^{\otimes n}),$$
where $\overset{*}{=}$ has used Lemma 2.157. This completes the homogeneity check.

We now hand-wave the proof of (b) and leave the details for [Mum08, Theorem III.16]. Any line bundle can be written as the difference of two very ample line bundles, so it is enough to check the result for very ample line bundles. If $\mathcal{L}$ is very ample, then intersection theory provides the result: a choice of generic global sections of $\mathcal{L}$ as $\sigma_0, \dots, \sigma_g$ so that they have no common zeroes and the $\operatorname{div}\sigma_\bullet$ intersect transversally; as such,
$$D^g = (\operatorname{div}\sigma_0, \dots, \operatorname{div}\sigma_g)$$
is literally the number of points in the intersection of the $\operatorname{div}\sigma_\bullet$s. Now, our choice of global sections induces a closed embedding $\varphi\colon A \to \mathbb{P}^g$, and the above intersection number is the pre-image of the point $[1:0:\cdots:0]$, so we see that $D^g = \deg\varphi$. On the other hand, $\deg(\mathcal{L}) = (\deg\varphi)\deg(\mathcal{O}_{\mathbb{P}^g}(1))$, which completes the proof upon a computation. ∎

2.16 March 13

Office hours are from 3PM to 5PM today.

2.16.1 More on Riemann–Roch

Here is our statement.

Proposition 2.162. Fix a line bundle $\mathcal{L}$ on an abelian k-variety A. Then if $\#K(\mathcal{L})$ is finite, then $\deg\varphi_{\mathcal{L}} = c\chi(\mathcal{L})^2$ for some absolute constant c depending only on A.

Proof. Note that $\mathcal{M} \coloneqq m^*\mathcal{L} \otimes \mathrm{pr}_1^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}$ is just $(\mathrm{id} \times \varphi_{\mathcal{L}})^*\mathcal{P}$, where $\mathcal{P}$ is the Poincaré line bundle. We now use Lemma 2.157 so that
$$\chi(\mathcal{M}) = (\deg\varphi_{\mathcal{L}})\chi(\mathcal{P}).$$
Recall from the proof of Proposition 2.65 that $R^\bullet \mathrm{pr}_{1*}\mathcal{M}$ is supported on $K(\mathcal{L})$, which is still finite, so the Leray spectral sequence continues to yield
$$H^i(A \times A, \mathcal{M}) = \Gamma\left(A, R^i \mathrm{pr}_{1*}\mathcal{M}\right).$$
Now, the projection formula tells us that
$$R^\bullet \mathrm{pr}_{1*}\left(m^*\mathcal{L} \otimes \mathrm{pr}_1^*\mathcal{L}^{-1} \otimes \mathrm{pr}_2^*\mathcal{L}^{-1}\right) = R^i \mathrm{pr}_{1*}\left(m^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}\right) \otimes \mathcal{L}^{-1},$$
but because this is supposed to be supported on the finite scheme $K(\mathcal{L})$, the line bundle $\mathcal{L}^{-1}$ will trivialize. So
$$H^i(A \times A, \mathcal{M}) = \Gamma\left(A, R^i \mathrm{pr}_{1*}(m^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}^{-1})\right) = H^i\left(A \times A, m^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}^{-1}\right).$$
This right-hand side is basically a line bundle on $A \times A$ because $(m, \mathrm{pr}_2)\colon A \times A \to A \times A$, so the Künneth formula tells us
$$\chi(\mathcal{M}) = \chi\left(m^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}^{-1}\right) = \chi(\mathcal{L})\chi\left(\mathcal{L}^{-1}\right).$$
However, (a) of Proposition 2.160 lets us write $\chi\left(\mathcal{L}^{-1}\right) = (-1)^g\chi(\mathcal{L})$, so we conclude. ∎

Remark 2.163. One can actually show that the degree of the map $\varphi_{\mathcal{L}}\colon A \to A^\vee$ is $\chi(\mathcal{L})^2$, but we will not need this. To show this, one needs to compute $\chi(\mathcal{P}) = (-1)^g$, which is done in [Mum08, Part III].

2.16.2 The Tate Functor Is Faithful

We now shift gears to talk about homomorphisms.

Theorem 2.164. Fix abelian k-varieties A and B. Then $\mathrm{Hom}_k(A,B)$ is a finitely generated abelian group. In fact, for primes ℓ not divisible by $\mathrm{char}\, k$, the functor T_ℓ is fully faithful: explicitly, we have an injection

$$T_\ell \colon \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathrm{Gal}(k^{\mathrm{sep}}/k)}(T_\ell A, T_\ell B)$$

This result is essentially due to Weil; our exposition will follow [Mum08, Theorem IV.19.3].

Remark 2.165. It is an easy mistake to make to claim that $\mathrm{Hom}_k(A,B)$ is finitely generated because the T_ℓ are injective, and the target is a finitely generated $\mathbb{Z}_\ell$-module. However, one can have infinitely generated abelian groups which become finitely generated upon tensoring with $\mathbb{Z}_\ell$; for example, $\mathbb{Z}_\ell$ itself will do.

Remark 2.166. Theorem 2.164 produces a bound of the form

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \le 4(\dim A)(\dim B)$$

by bounding the $\mathbb{Z}_\ell$-rank when passing to Tate modules. This bound is not sharp in characteristic zero, but supersingular abelian varieties of positive characteristic are able to show that this bound is sharp.

Remark 2.167. It is a conjecture of Tate that, if k is finitely generated over its prime field, then T_ℓ is actually full. (The hypothesis on k is necessary: if $k = \mathbb{Q}_p$, then the Galois action is unramified, so one basically only has Frobenius action, which is not enough to cut down morphisms on the Tate modules.) If k is finite, the result is due to Tate; if k has positive characteristic, the result is known to Zarhin. Lastly, $\mathrm{char}\, k = 0$ was shown by Faltings.

Anyway, let's prove Theorem 2.164.

Proof. By working through the isogeny class, we may assume that A and B are simple. Explicitly, given isogenies $\prod_i A_i \to A$ and $B \to \prod_j B_j$, we get an injection

$$\mathrm{Hom}_k(A,B) \otimes \mathbb{Z}_\ell \to \prod_{i,j} \mathrm{Hom}_k(A_i, B_j) \otimes \mathbb{Z}_\ell,$$

and a symmetric argument produces a map in the reverse direction. Notably, if A and B are simple, then there are no homomorphisms; otherwise, $\mathrm{Hom}_k(A,B)$ embeds in $\mathrm{End}(A)$. Thus, we may even assume that A and B are isogenous and hence equal.

Now, Theorem 2.159 kicks in to tell us that $\deg \colon \mathrm{End}(A) \to \mathbb{Z}$ is a homogeneous polynomial of degree $2\dim A$, so $\mathrm{End}(A)$ is torsion-free because isogenies are always going to have nonzero degree.

To continue, we want the following geometric claim. Suppose that $M \subseteq \mathrm{End}(A)$ is a finitely generated subgroup. Then we claim that

$$\mathbb{Q}M \cap \mathrm{End}(A) \coloneqq \{f \in \mathrm{End}(A) : nf \in M \text{ for nonzero } n \in \mathbb{Z}\}$$

is a finitely generated abelian group. Indeed, $\mathbb{Q}M$ is a finite-dimensional $\mathbb{Q}$-vector space by assumption, so $\deg|_{\mathbb{Q}M}$ is a homogeneous polynomial of degree $2g$, so it is going to extend continuously to a map $\mathbb{R}M \to \mathbb{R}$. As such,

$$U \coloneqq \{x \in \mathbb{R}M : |\deg x| < 1\}$$

is an open neighborhood of 0 in $\mathbb{R}M$, but $U \cap \mathrm{End}(A) = \{0\}$ because all isogenies have positive integer degree. Thus, $\mathbb{Q}M \cap \mathrm{End}(A)$ is a discrete subgroup of $\mathbb{R}M$, meaning that $\mathbb{Q}M \cap \mathrm{End}(A)$ is a lattice and in particular free of finite rank.

We now complete the proof.

- We show the injectivity. Because elements of $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is made of finite sums of the form $f \otimes \alpha$, it is enough to show that T_ℓ is injective when restricted to arbitrary finitely generated submodules $M \subseteq \mathrm{End}\, A$. Now, M is finitely generated and torsion-free, so it is free of finite rank, so give it a $\mathbb{Z}$-basis $f_1, \dots, f_r$; note that this continues to be a $\mathbb{Z}_\ell$-basis of $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. We now go ahead and enlarge M to $\mathbb{Q}M \cap \mathrm{End}(A)$, which we know continues to be finitely generated by the above claim. For our proof, we now suppose that
$$T_\ell\left(\sum_{i=1}^{r} a_i f_i\right) = 0$$
where $a_i \in \mathbb{Z}_\ell$ for each i, and we want to show that the sum vanishes.

  This is done by an approximation argument. For example, we can find an r-tuple of integers $(a_1', \dots, a_r')$ equivalent to $(a_1, \dots, a_r)$ to arbitrary precision ℓ^N, meaning
$$T_\ell\left(\sum_{i=1}^{r} a_i' f_i\right) \equiv 0 \pmod{\ell^N},$$
  so this endomorphism $\varphi := \sum_i a_i' f_i$ will take $T_\ell A$ to $\ell^N T_\ell A$, so its kernel contains $A\left[\ell^N\right]$. But then the nature of our isogenies means that we have some f' such that $\varphi = f' \circ \left[\ell^N\right]$, meaning ℓ^N divides each of the a_i' (by using that the $f_\bullet$ forms a basis!). Sending $N \to \infty$ forces the $a_\bullet'$ to vanish.
- We show that $\mathrm{End}(A)$ is finitely generated. Because T_ℓ is injective for infinitely many primes ℓ, we see that $\mathrm{End}^0(A)$ must be a finite-dimensional $\mathbb{Q}$-vector space. Thus, we get some finitely generated subgroup $M \subseteq \mathrm{End}(A)$ such that $\mathbb{Q}M = \mathrm{End}^0(A)$, so $\mathrm{End}(A) = \mathbb{Q}M \cap \mathrm{End}^0(A)$ is finitely generated by the claim. ∎

Remark 2.168. As another application, we note that the Néron–Severi group $\mathrm{NS}(A)$ is contained in $\mathrm{Hom}_k(A, A^\vee)$, which is finitely generated, so $\mathrm{NS}(A)$ is still finitely generated.

Remark 2.169. It will turn out that the degree of an isogeny $f\colon A \to B$ can be computed on the level of Tate modules.

Corollary 2.170. Fix an abelian k-variety A. Then $\mathrm{End}^0(A)$ is a finite-dimensional semisimple algebra.

Proof. Indeed, $\mathrm{End}^0(A)$ for simple abelian varieties A is a field of finite dimension over $\mathbb{Q}$ by Theorem 2.164, so it is a number field. So we are just looking at some summation of number fields, which is semisimple. ∎

We close class by stating a lemma from linear algebra.

Definition 2.171. Fix a finite-dimensional simple $\mathbb{Q}$-algebra B. Then a *trace form* is a $\mathbb{Q}$-linear map $T\colon B \to \mathbb{Q}$ such that $T(ab) = T(b)T(a)$. Similarly, a *norm form* is a polynomial map $N\colon B \to \mathbb{Q}$ such that $N(ab) = N(a)N(b)$.

Proposition 2.172. Fix a finite-dimensional simple $\mathbb{Q}$-algebra B with center K. Then there is a trace form $\mathrm{Tr}^\circ_{B/k}$ with $\mathrm{Tr}^\circ(1) = 1$ such that any trace form T on B has the form $T = \varphi \circ \mathrm{Tr}^\circ$. Similarly, there is a norm form $\mathrm{Nm}_{B/k}$ with $\mathrm{Nm}^\circ(1) = 1$ such that any trace form T on B has the form $\left(\mathrm{Nm}_{K/\mathbb{Q}} \circ \mathrm{Nm}^\circ\right)^i$ for positive integer i.

Proof. Omitted. ∎

We remark that a similar statement works for $\mathbb{Q}_\ell$.

2.17 March 15

Here we go.

2.17.1 Degree via Tate Modules

Here is our next result: characteristic polynomials can be computed on the Tate module.

Theorem 2.173. Fix an endomorphism $f \in \operatorname{End}^0(A)$.

(a) We have $\deg f = \det V_\ell f$, where V_ℓ is the functor $A \mapsto (T_\ell A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Thus, the characteristic polynomial $P_\ell(x)$ of $V_\ell f$ satisfies, for any $n \in \mathbb{Z}$,

$$P_\ell(n) = \deg([n]_A - f).$$

(b) The characteristic polynomial $P(x)$ of $T_\ell f$ has integral coefficients.

For (b), note that (a) actually tells us that $P(n) = \deg([n]_A - f)$ for all integers n.

It will be helpful to have the following lemma.

Lemma 2.174. Fix an isogeny $f\colon A \to B$ of abelian k-varieties. Then the sequence

$$0 \to T_\ell A \to T_\ell B \to (\ker f)(k^{\text{sep}})_\ell \to 0$$

is exact, where, where $(\cdot)_\ell$ denotes taking the ℓ-primary part.

Proof. See [EGM, pp. 10.5–10.6]. Let's sketch the idea. The point is to use cohomology, so we begin by writing

$$T_\ell A = \varprojlim A[\ell^\bullet](k^{\text{sep}}) = \varprojlim \operatorname{Hom}\left(\mathbb{Z}/\ell^\bullet\mathbb{Z}, A(k^{\text{sep}})\right) = \operatorname{Hom}\left(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^{\text{sep}})\right).$$

Now, setting $N := \ker f$, we have an exact sequence

$$0 \to N \to A \xrightarrow{f} B \to 0$$

of fppf sheaves, which gives an exact sequence

$$0 \to N(k^{\text{sep}}) \to A(k^{\text{sep}}) \xrightarrow{f} B(k^{\text{sep}}) \to 0,$$

which is exact on the right by the surjectivity of f. Now, applying the functor $\operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, -)$, we note that $N(k^{\text{sep}})$ is finite anyway, so it will vanish under the functor, leaving us with the exact sequence

$$0 \to T_\ell A \to T_\ell B \to \operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^{\text{sep}})) \to \operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^{\text{sep}})).$$

Notably, if k is perfect, then $k^{\text{sep}} = \overline{k}$, so $A(\overline{k})$ being divisible makes the last term vanish; in the general case, one still gets that the map into that term vanishes because we are looking at ℓ-torsion, where $A(k^{\text{sep}})$ is going to be sufficiently divisible.

So it remains to compute the Ext^1 term. To begin, note that

$$\operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^{\text{sep}})) = \operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^{\text{sep}})_\ell)$$

because $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ works to kill out anything other than ℓ-torsion. (Namely, multiplication by something coprime to ℓ is an isomorphism on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ but will kill out what happens in N.) Now, to compute this last term, we take the exact sequence

$$0 \to \mathbb{Z}_\ell \to \mathbb{Q}_\ell \to \mathbb{Q}_\ell/\mathbb{Z}_\ell \to 0$$

and apply $\operatorname{Hom}(-, N(k^{\text{sep}})_\ell)$ to get

$$\operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k^{\text{sep}})_\ell) = \operatorname{Hom}(\mathbb{Z}_\ell, N(k^{\text{sep}})_\ell),$$

after some argument in the long exact sequence, which is what we wanted. ∎

We are now ready to prove Theorem 2.173.

Proof of Theorem 2.173. We focus on (a) for now; the second claim is immediate from the first and the definition of the characteristic polynomial, so we focus on the first claim. It suffices to prove the results for bona fide endomorphisms $f\colon A \to A$. Indeed, once we have the result here, scaling produces the result for $\mathbb{Q}$, and then a density argument for $\mathbb{Q} \subseteq \mathbb{Q}_\ell$ achieves the full result for $\mathbb{Q}_\ell$. Then we see that

$$|\deg f|_\ell = |\#(\ker f)_\ell(k^{\mathrm{sep}})|_\ell\,.$$

Now, the above lemma tells us that this is $|\det T_\ell f|_\ell$. This equality extends to $f \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$ via the aforementioned density argument.

We now apply Proposition 2.172. Now, write $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ as a product of simple $\mathbb{Q}_\ell$-algebras $\prod_i D_i$ (notably, this algebra is semisimple because it is the base-change of a semisimple algebra). Now, $\deg$ and $\det$ agree on ℓ-adic valuation as above, so the classification Proposition 2.172 forces them to be actually equal. More formally, one should write $f \mapsto |\deg f|_\ell$ as some product

$$\prod_i \left(\mathrm{Nm}_{K_i/\mathbb{Q}_\ell} \circ \mathrm{Nm}^{\circ}_{D_i/K_i}\right)^{v_i}$$

where $K_i = Z(D_i)$ and the $v_\bullet$s are some integers. Doing similar for $\det$ and then plugging in various $f \in \prod_i D_i$ (forming a basis) reveals the desired equality.

We now show (b). Define $P(n) \coloneqq \deg([n]_A - f)$, which we know is a polynomial (because $\deg$ is polynomial Theorem 2.159), meaning we can view P as an element of $\mathbb{Q}[x]$; thus, $P_\ell = P$ has rational coefficients. It remains to show that the coefficients are integral. Well, because $\mathrm{End}(A)$ is free of finite rank over $\mathbb{Z}$, our f is going to have some monic minimal polynomial $q \in \mathbb{Z}[x]$.[3] Thus, $q(V_\ell f) = 0$, so the roots of P_ℓ must all be algebraic integers, meaning that $P(x) \in \overline{\mathbb{Z}}[x]$, meaning that $P(x) \in \mathbb{Z}[x]$, as desired. ∎

2.17.2 Weil Pairing

We now use duality for fun and profit.

Definition 2.175 (Tate twist)**.** Fix a field k and a prime ℓ not divisible by $\mathrm{char}\, k$. We define the *Tate twist* $\mathbb{Z}_\ell(1)$ as $T_\ell(\mathbb{G}_m)$. Notably, $\mathbb{Z}_\ell(1)$ is a free $\mathbb{Z}_\ell$-module of rank 1 with Galois action from $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ acting via the cyclotomic character, where the point is that

$$T_\ell(\mathbb{G}_m) = \varprojlim \mu_{\ell^\bullet}.$$

More generally, given a free $\mathbb{Z}_\ell$-module M of finite rank, we define $M(n) \coloneqq M \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1)^{\otimes n}$, where n is an integer.

To motive our Weil pairing, we note that $A^\vee[\ell^\bullet] \cong A[\ell^\bullet]^\vee$ by Theorem 2.86, where the second dual is a Cartier dual. Thus, using our Cartier duality, we induce a map

$$A[\ell^\bullet] \times A^\vee[\ell^\bullet] \to \mu_{\ell^\bullet}.$$

We would like to take limits over $\ell^\bullet$, but to do this, we need the following diagram to commute.

$$\begin{array}{ccc} A[\ell^n] \times A^\vee[\ell^n] & \longrightarrow & \mu_{\ell^n} \\ {\scriptstyle (\ell,\ell)}\uparrow & & \uparrow{\scriptstyle \ell} \\ A\left[\ell^{n+1}\right] \times A^\vee\left[\ell^{n+1}\right] & \longrightarrow & \mu_{\ell^{n+1}} \end{array}$$

To check the commutativity here, we need to recall the isomorphism $A^\vee[\ell^\bullet] \cong A[\ell^\bullet]^\vee$.

[3] This can be checked by base-changing to $\mathbb{C}$ and thinking about the minimal polynomial for a morphism on the level of lattices.

Namely, given an endomorphism $f\colon A \to A$, we need to recall why $(\ker f)^\vee \cong \ker f^\vee$. Well, fix a $\overline{k}$-point x of $\ker f$ and some line bundle $\mathcal{L}$ on $\ker f$. Then we may choose some $\beta\colon f^*\mathcal{L} \to \mathcal{O}_A$ (unique up to scalar), and we note that we have the following large diagram.

$$\begin{array}{ccc} t_x^* f^*\mathcal{L} & \xrightarrow{t_x^*\beta} & t_x^*\mathcal{O}_A \\ \| & & \\ f^* t_{f(x)}^*\mathcal{L} & & \downarrow \\ \| & & \\ f^*\mathcal{L} & \xrightarrow[t_x^*\beta]{} & \mathcal{O}_A \end{array}$$

Then our Weil pairing $e_f\colon (\ker f)(\overline{k}) \times (\ker f^\vee)(\overline{k}) \to \mathbb{G}_m$ is just given by

$$e_f(x, \mathfrak{L}) \coloneqq t_x^*\beta \circ \beta^{-1},$$

which is an isomorphism $\mathcal{O}_A \to \mathcal{O}_A$ and hence provides a global section and hence an element of $\overline{k}^\times$, as needed. Note that this does not change if we adjust β by a scalar, so it notably does not depend on the choice of β.

Let's now do our computation.

Lemma 2.176. Fix an abelian k-variety A and positive integers n and m. Given $\mathcal{L} \in A^\vee[m](\overline{k})$ and $x \in A[mn](\overline{k})$, we have $e_{mn}(x, \mathcal{L}) = e_m(nx, \mathcal{L})$.

Proof. We do the explicit computation. Pick an isomorphism $\beta\colon [m]^*\mathcal{L} \to \mathcal{O}_A$, which induces the isomorphism $[n]^*\beta\colon [mn]^*\mathcal{L} \to \mathcal{O}_A$. Now, we compute

$$e_{mn}(x, \mathcal{L}) = t_x^*([n]^*\beta) \circ ([n]^*\beta)^{-1} = [n]^*\left(t_{nx}^*\beta \circ \beta^{-1}\right) = [n]^* e_m(nx, \mathcal{L}) = e_m(nx, \mathcal{L}).$$

Here, this last equality comes about because we're just pulling back a full isomorphism $\mathcal{O}_A \to \mathcal{O}_A$, which does not change the produced global section. ∎

Remark 2.177. On the homework, we will show that a homomorphism $f\colon A \to B$ reveals

$$e_{\ell^\infty}((T_\ell f)x, y) = e_{\ell^\infty}(x, T_\ell(f^\vee)y),$$

again by a reasonably explicit computation.

As a corollary, we compute

$$e_{\ell^n}(\ell x, \ell\mathcal{L}) = e_{\ell^{n+1}}(x, \ell\mathcal{L}) = e_{\ell^{n+1}}(x, \mathcal{L})^\ell,$$

where the first equality is by the lemma, and the second equality is by using the explicit description for the pairing provided above. (More precisely, we can see that taking a power of ℓ induces a power at the end.) So we may take limits to produce the following definition.

Definition 2.178 (Weil pairing)**.** Fix an abelian k-variety A. Then we define the *Weil pairing* as $e_\bullet\colon T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ defined above.

Remark 2.179. A choice of polarization $A \to A^\vee$ grants us a skew-symmetric form

$$T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(1)$$

induced by the Weil pairing.

2.18 March 18

Here we go.

2.18.1 More on the Weil Pairing

We quickly provide a more explicit description of the Weil pairing. As before, choose geometric points $x \in A[n](\bar{k})$ and $\mathcal{L} \in A^\vee[n](\bar{k})$. Smoothness of our abelian k-variety A allows us to realize any line bundle $\mathcal{L} \in A^\vee$ as $\mathcal{O}_A(D)$ for some Weil divisor D. Note that $\mathcal{O}_A(D) \subseteq \mathcal{K}_A$, where $\mathcal{K}_A$ is the sheaf of rational functions on A.

Now, computation of the Weil pairing requires us to choose an isomorphism $\beta\colon [n]^*\mathcal{L} \to \mathcal{O}_A$. Well, we note that $[n]^*\mathcal{L}$ embeds into $[n]^*\mathcal{K}_A$, which is isomorphic to $\mathcal{K}_A$, so we choose the rational function $g := [n]^*i \circ \beta^{-1}(1)$ so that $\operatorname{div} g^{-1} = [n]^{-1}D$ by tracking through what a pole or zero could be. Then we can compute

Why?

$$e_n(x, \mathcal{L}) = t_x^*\beta \circ \beta^{-1} = \frac{g(z+x)}{g(z)},$$

which is a number independent of the choice of z.

We now use this computation for some fun and profit.

Proposition 2.180. Fix an abelian k-variety A. For any line bundle $\mathcal{L}$ on A, the composite map

$$T_\ell A \times T_\ell A \xrightarrow{\mathrm{id}\times\varphi_{\mathcal{L}}} T_\ell A \times T_\ell A^\vee \xrightarrow{e_{\ell^\infty}} \mathbb{Z}_\ell(1)$$

is skew-symmetric. In particular, if $\varphi_{\mathcal{L}}$ is a polarization, then this pairing is symplectic.

Proof. We already know that the pairing is non-degenerate by a direct computation, so it remains to show that (x, x) goes to 0. Namely, we want to show that

Why?

$$e_{\ell^\infty}(x, T_\ell(\varphi_{\mathcal{L}})x) = 0$$

for each x. It suffices to show this result for all $x \in A[\ell^n]$ for any n by taking the limit as $n \to \infty$.

For this, we use our prior explicit description of the Weil pairing. Well, write $\mathcal{L} = \mathcal{O}_A(D)$ for some Weil divisor D, and we compute

$$\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} = \mathcal{O}_A(t_{-x}D - D).$$

We now choose g as in the explicit description as above so that $\operatorname{div} g^{-1} = [\ell^n]^{-1}(t_{-x}D - D)$. Now, to show that our Weil pairing vanishes, we want to show that $g(z+x) = g(z)$ for any given z. Well, for any $y \in A(\bar{k})$ such that $\ell^n y = x$ (which exists by divisibility), we note

$$\operatorname{div} g^{-1} = t_{-y}\left([\ell^n]^{-1}D\right) - [\ell^n]^{-1}D,$$

so telescoping implies

$$\operatorname{div} \prod_{i=0}^{\ell^n - 1} t_{iy}^*\left(g^{-1}\right) = t_{-x}\left([\ell^n]^{-1}D\right) - [\ell^n]^{-1}D,$$

but this vanishes because x is ℓ^n-torsion. Thus, our left-hand side is a function h with no zeroes or poles, so it must be a constant function. For example, $h(z+y) = h(z)$, which unwinds to $g(z+x) = g(z)$ by another telescoping argument. ∎

Remark 2.181. In fact, the above argument works for any polarization $\varphi\colon A \to A^\vee$. The passage to the algebraic closure is not so bad because.

We now pick up the following result.

Theorem 2.182. Fix a homomorphism $\varphi\colon A \to A^\vee$ of abelian k-varieties. Then the following are equivalent.

(i) φ is symmetric.

(ii) The pairing E^φ induced by

$$T_\ell A \times T_\ell A \xrightarrow{\mathrm{id}\times\varphi} T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$$

is skew-symmetric.

(iii) $2\varphi = \varphi_{\mathcal{L}}$ for some line bundle $\mathcal{L}$.

(iv) If k is algebraically closed, then $\varphi = \varphi_{\mathcal{L}}$ for some line bundle $\mathcal{L}$.

Proof. We will only prove part of this. In particular, we will not show the implication (iii) implies (iv); see [Mum08, p. 214]. Our argument will use Remark 2.177. Additionally, we note that the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \varphi_{f^*\mathcal{L}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathcal{L}}} \\ A^\vee & \xleftarrow[f^\vee]{} & B^\vee \end{array} \tag{2.1}$$

commutes. Unwinding definitions now implies that

$$E^{f^*\mathcal{L}}(x,y) = E^{\mathcal{L}}(T_\ell f(x), T_\ell f(y)).$$

We also quickly recall that $(A\times B)^\vee \cong A^\vee \times B^\vee$ essentially by restriction of line bundles; this result is on the homework. In particular, $A \times A^\vee$ is self-dual.

Now, let $\mathcal{P}$ denote the Poincaré line bundle. We now execute the following computation.

Lemma 2.183. Let $\mathcal{P}$ be the Poincaré line bundle of an abelian k-variety A. Then

$$E^{\mathcal{P}}((x,x^\vee),(y,y^\vee)) = e_{\ell\infty}(x,y^\vee) - e_{\ell\infty}(y,x^\vee).$$

Here, $x,y \in T_\ell A$ and $x^\vee, y^\vee \in T_\ell A^\vee$.

Proof. By bilinearity and skew-symmetry, it is enough to verify the equalities on the pairs $((x,0),(y,0))$ and $((x,0),(0,y^\vee))$.

- We verify on $((x,0),(y,0))$, where our pairing should vanish. Pulling back along $(\mathrm{id},0)\colon A \to A\times A^\vee$, we see $\mathcal{P}$ trivializes (it's from Pic), so

$$E^{\mathcal{P}}((x,0),(y,0)) = E^{\mathcal{O}_A}(x,y) = e_{\ell\infty}(x,0) = 0.$$

- We verify on $((x,0),(0,y^\vee))$. We pull back along $(0,\mathrm{id})\times A^\vee \to A\times A^\vee$, where the main point is to figure out where $\mathcal{P}$ goes. Well, one has the composite map

$$A \times A^\vee \to (A\times A^\vee)^\vee = A^\vee \times A,$$

where the last map is given by restriction of line bundles. In particular, the pair $(x,x^\vee)$ goes to the line bundle $t^*_{(x,x^\vee)}(\mathcal{P}\otimes\mathcal{P}^{-1})$, which then goes to $(t_x^* x^\vee, x)$ by a computation with the Poincaré line bundle, but $x^\vee \in A^\vee$ is translation invariant, so we are just going to $(x^\vee,x)$. So we can compute that

$$E^{\mathcal{P}}((x,0),(0,y^\vee)) = e_{\ell\infty}((x,0),(y^\vee,0)) = e_{\ell\infty}(x,y^\vee),$$

as desired. ∎

We now proceed with the proof. We already know that (iv) implies (i) and (ii) from earlier statements involving polarizations. To see that (i) implies (iii), we set $\mathcal{L} := (\mathrm{id} \times \varphi)^* \mathcal{P}$. Using (2.1), we see

$$\begin{aligned} \varphi_{\mathcal{L}}(x) &= (1 \times \varphi)^\vee \circ \varphi_{\mathcal{P}} \circ (1 \times \varphi)(x) \\ &= (1 \times \varphi)^\vee (\varphi(x), x) \\ &\overset{*}{=} (1 \times \varphi)(\varphi(x), x) \\ &= 2\varphi(x), \end{aligned}$$

where we have used symmetry of φ at $\overset{*}{=}$. (Note $\varphi_{\mathcal{P}}$ swaps coordinates as shown in the previous proof.)

We now show (ii) implies (iii). Continuing with the same $\mathcal{L}$ as in the previous paragraph, we use the lemma to see

$$\begin{aligned} E^{\mathcal{L}}(x,y) &= E^{\mathcal{P}}(T_\ell(1 \times \varphi)(x), T_\ell(1 \times \varphi)(y)) \\ &= e_{\ell^\infty}(x, T_\ell \varphi(y)) - e_{\ell^\infty}(y, T_\ell \varphi(x)) \\ &= E^{\varphi}(x,y) - E^{\varphi}(y,x) \\ &= 2E^{\varphi}(x,y), \end{aligned}$$

where the last equality has used skew-symmetry. Non-degeneracy of our pairing now forces $2\varphi = \varphi_{\mathcal{L}}$, so we are done. ∎

Remark 2.184. This result shows that $\mathrm{NS}(A) = \mathrm{NS}(A_{\overline{k}})$ is exactly the $\mathbb{Z}$-submodule of symmetric homomorphisms $A \to A^\vee$.

2.18.2 The Rosati Involution

Here is our definition.

Definition 2.185 (Rosati involution)**.** Fix a polarization $\lambda \colon A \to A^\vee$ of abelian k-variety A. Then the *Rosati involution* $(-)^\dagger$ on $\mathrm{End}^0(A)$ sends φ to the map $\varphi^\dagger$ making the following diagram commute.

$$\begin{array}{ccc} A & \xleftarrow{\varphi^\dagger} & A \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda} \\ A^\vee & \xleftarrow{\varphi^\vee} & A^\vee \end{array}$$

Explicitly,

$$\varphi^\dagger := \lambda^{-1} \circ \varphi^\vee \circ \lambda.$$

Remark 2.186. We are working with $\mathrm{End}^0(A)$ so that we can write down λ^{-1} in general. However, if A is principally polarized, then this inverse already exists in $\mathrm{End}(A)$, so we can still write down the Rosati involution even on $\mathrm{End}(A)$.

Remark 2.187. The Rosati involution depends on λ, but this dependence is not too bad. Namely, if λ_1 and λ_2 are two polarizations (in particular, isogenies), then we get an isogeny such that $\lambda_1 = \lambda_2 \circ f$, so

$$\lambda_1^{-1} \circ \varphi \circ \lambda_1 = f^{-1} \circ \lambda_2^{-1} \circ \varphi \circ \lambda_2 \circ f,$$

so we at least have the same conjugacy class in $\mathrm{End}^0(A)$.

2.19 March 20

Today we use the Rosati involution for fun and profit.

2.19.1 Positivity of the Rosati Involution

Manipulation with definitions verify the following.

Proposition 2.188. Fix a polarization $\lambda\colon A \to A^\vee$ of an abelian k-variety A.

(a) $(-)^\dagger$ is linear.

(b) $(-)^\dagger$ anti-commutes: $(\varphi \circ \psi)^\dagger = \psi^\dagger \circ \varphi^\dagger$.

(c) For the Weil pairing, $E^\lambda(T_\ell\varphi(x), y) = E^\lambda(x, T_\ell\varphi^\dagger(y))$.

Proof. For (a), note that composition is linear. For (b), proceed directly from the definitions and use the duality of $(-)^\vee$. Lastly, for (c), use Remark 2.177 and then pass through λ everywhere as needed. ■

Now here is our main result on the Rosati involution.

Theorem 2.189 (Positivity)**.** Fix a polarization $\lambda\colon A \to A^\vee$ of an abelian k-variety A. Then for any nonzero $\varphi \in \operatorname{End}^0(A)$, one has that

$$\operatorname{tr}(\varphi \circ \varphi^\dagger) = \operatorname{tr}(\varphi^\dagger \circ \varphi) > 0.$$

Here, tr refers to the reduced trace on the semisimple algebra $\operatorname{End}^0(A)$. More precisely, for a semisimple $\mathbb{Q}$-algebra D, let K be its center, and then base-change to $\overline{K}$ and compute the trace as a matrix algebra because $D \otimes_K \overline{K}$ is a matrix algebra. Working with the characteristic polynomial allows us to compute the trace on the level of $V_\ell A$ via Theorem 2.173, or equivalently via the characteristic polynomial.

Proof. By base-changing our morphisms (which does not adjust the reduced trace here), we may assume that k is algebraically closed. As such, $\lambda = \varphi_{\mathcal{L}}$ for an ample line bundle $\mathcal{L}$; taking powers of $\mathcal{L}$ adjusts $\varphi_{\mathcal{L}}$ by multiplication by this power, but this does not change the Rosati involution, so we may actually assume that $\mathcal{L}$ is very ample, so say $\mathcal{L} = \mathcal{O}_A(D)$ where D is an effective Weil divisor (in fact, a hyperplane intersection).

Now, let $g \coloneqq \dim A$, and the main claim is that

$$\operatorname{tr}(\varphi \circ \varphi^\dagger) \overset{?}{=} 2g \cdot \frac{(D^{g-1}, \varphi^{-1}D)}{(D^g)}.$$

This will complete the proof because $\varphi^{-1}(D)$ continues to be an effective Weil divisor, and then we are just computing some intersection numbers, which is positive.

So it remains to prove the claim. We will use Proposition 2.160. Note that $\varphi_{\varphi^*\mathcal{L}^{-1}\otimes\mathcal{L}^{\otimes n}}\colon A \to A^\vee$ is an isogeny, and this map is equal to $[n] \circ \varphi_{\mathcal{L}} - \varphi_{\varphi^*\mathcal{L}}$. The moral is that we can compute the degree

$$\begin{aligned}
\deg\left([n] \circ \varphi_{\mathcal{L}} - \varphi_{\varphi^*\mathcal{L}}\right) &= \deg\left([n] \circ \varphi_{\mathcal{L}} - \varphi^\vee \circ \varphi_{\mathcal{L}} \circ \varphi\right) \\
&= \deg\left(\varphi_{\mathcal{L}} \circ \left([n] - \varphi_{\mathcal{L}}^{-1} \circ \varphi^\vee \circ \varphi_{\mathcal{L}} \circ \varphi\right)\right) \\
&= \deg \varphi_{\mathcal{L}} \cdot \deg\left([n]\varphi^\dagger \circ \varphi\right).
\end{aligned}$$

This last quantity is now the characteristic polynomial $P(n)$ of $\varphi^\dagger \circ \varphi$. Thus,

$$P(n) = \frac{\deg\left([n] \circ \varphi_{\mathcal{L}} - \varphi_{\varphi^*\mathcal{L}}\right)}{\deg \varphi_{\mathcal{L}}},$$

which by Proposition 2.162 is

$$P(n) = \frac{\chi\left(\varphi^*\mathcal{L}^{-1} \otimes \mathcal{L}^{\otimes n}\right)}{\chi(\mathcal{L})^2}.$$

Now, Proposition 2.160 implies

$$P(n) = \left(\frac{(nD - \varphi^{-1}D)^g}{(D^g)} \right)^2.$$

We would like the term after the leading term of this polynomial, which by linearity looks like

$$P(n) = \frac{1}{(D^g)^2} \left(n^g(D^g) - gn^{g-1} \left(D^{g-1}, \varphi^{-1}D \right) + \cdots \right)^2,$$

whose term after the leading term is exactly what we claimed it would be. ■

2.19.2 The Albert Classification

We now see that the positivity of the Rosati involution now gives us some tools to classify algebras.

Lemma 2.190. Fix a division $\mathbb{Q}$-algebra D equipped with a positive anti-involution $(-)^\dagger$ on D. Further, set $K \coloneqq Z(D)$ and $K^+ \coloneqq \left\{ x \in K : x = x^\dagger \right\}$ with $e \coloneqq [K : \mathbb{Q}]$ and $e^+ \coloneqq [K^+ : \mathbb{Q}]$. Then K_0 is totally real, and either $K = K^+$ or K/K^+ is a totally imaginary quadratic extension.

Proof. We begin by trying to prove that K^+ is totally real. Well, we can write

$$K_0 \otimes \mathbb{R} = \mathbb{R}^r \otimes \mathbb{C}^s$$

for some nonnegative integers $r, s \geq 0$. Notably, the quadratic form $x \mapsto \operatorname{tr}(xx^\dagger)$ is a quadratic form $q(x)$ on K^+ (note $x^\dagger = x$ here), which extends by continuity to a quadratic form $q_{\mathbb{R}}$ on $\mathbb{R}^r \times \mathbb{C}^s$. Now, q itself was defined over $\mathbb{Q}$, so its null space will be defined over $\mathbb{Q}$, but positivity of $(-)^\dagger$ tells us that this null space must vanish. So actually $q_{\mathbb{R}}$ is positive-definite, but then there can be no copies of $\mathbb{C}$ in $K^+ \otimes \mathbb{R}$ because one can always solve these quadratic equations over the complex numbers.

We now complete the proof. Notably, by definition $[K : K^+] \in \{1, 2\}$: indeed, K^+ is defined as being a subfield of K fixed by a group of order 2 (namely, generated by the automorphism $\alpha \mapsto \alpha^\dagger$). It remains to show that K/K^+ is a totally imaginary quadratic extension if nontrivial. Well, if nontrivial, we can write $K = K^+(\sqrt{\alpha})$ for some $\alpha \in K^+$. Now, $(\sqrt{\alpha})^2 = \alpha$ must be fixed by $(-)^\dagger$, but $\sqrt{\alpha}$ is not, so we must have $(\sqrt{\alpha})^\dagger = -\sqrt{\alpha}$.

Continuing, suppose for the sake of contradiction that we have a real place $i \colon K \to \mathbb{R}$. Then $i^\dagger \colon K \to \mathbb{R}$ continues to be a real place but now has $i(\sqrt{\alpha}) = -i^\dagger(\sqrt{\alpha})$. To derive contradiction, we work with the pieces $\mathbb{R} \times \mathbb{R}$ inside $K \otimes \mathbb{R}$ corresponding to i and $i^\dagger$, where we see that

$$\operatorname{tr}\left((x, y) \cdot (x, y)^\dagger \right) = \operatorname{tr}((x, y), (y, x)) = 2xy$$

now fails to be positive-definite. ■

There is now a full classification of division algebras with positive anti-involution.

Theorem 2.191 (Albert)**.** Fix a division $\mathbb{Q}$-algebra D equipped with a positive anti-involution $(-)^\dagger$ on D. Further, set $K \coloneqq Z(D)$ and $K^+ \coloneqq \left\{ x \in K : x = x^\dagger \right\}$ with $e \coloneqq [K : \mathbb{Q}]$ and $e^+ \coloneqq [K^+ : \mathbb{Q}]$. Then (D, K, K^+) satisfies one of the following.

- Type I: $D = K = K^+$, and $(-)^\dagger = \mathrm{id}_D$.
- Type II: $K = K^+$, but D is a quaternion K-algebra $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i \colon K \hookrightarrow \mathbb{R}} M_2(\mathbb{R})$ split as the matrix algebra at all archimedean places of K (which are necessarily real), where $(-)^\dagger$ (up to isomorphism) is given by transposition of matrices. Explicitly, we have $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i \colon K \hookrightarrow \mathbb{R}} M_2(\mathbb{R})$.
- Type III: $K = K^+$, but D is a quaternion K-algebra $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i \colon K \hookrightarrow \mathbb{R}} \mathbb{H}$ ramified at all places, and $(-)^\dagger$ is the standard involution on the quaternions.
- Type IV: K/K^+ is a totally imaginary extension with complex conjugation c, and D is a division K-algebra such that $\operatorname{inv}_v(D) + \operatorname{inv}_{c(v)} D = 0$ if $v \neq c(v)$, and $\operatorname{inv}_v(D) = 0$ if $v = c(v)$; $(-)^\dagger$ is conjugate transpose.

Remark 2.192. In the final case, one finds that

$$D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{\substack{i\colon K \to \mathbb{C} \\ \text{up to } c}} M_d(\mathbb{C})$$

where $d \coloneqq \sqrt{[D:K]}$ is the reduced degree.

2.20 March 22

Today we continue discussing endomorphism algebras.

2.20.1 More on the Albert Classification

We begin by discussing Theorem 2.191. For our notation, D is a simple algebra with center K and positive involution $(\cdot)^\dagger$ so that $K^+ = K^\dagger$. We also set $d \coloneqq \sqrt{[D:K]}$ and $e \coloneqq [K:\mathbb{Q}]$ and $e_0 \coloneqq [K^+:\mathbb{Q}]$.

Remark 2.193. In the case of a simple abelian k-variety A of dimension g with $D \coloneqq \operatorname{End}^0(A)$, then we get the following data.

Type	$[K^+:\mathbb{Q}]$	$\sqrt{[D:K]}$	$\operatorname{char} = 0$	$\operatorname{char} k > 0$	$\dim_{\mathbb{Q}} \mathrm{NS}(A_{\overline{k}})_{\mathbb{Q}} / \dim_{\mathbb{Q}} \operatorname{End}(A_{\overline{k}})_{\mathbb{Q}}$
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	$2e \mid g$	$e \mid g$	$1/3$
IV	$2e_0$	d	$e_0 d^2 \mid g$	$e_0 d \mid g$	$1/2$

We will explain where these restrictions come from later. Do note that we do not if all possible simple algebras D with positive involution $(\cdot)^\dagger$ come from simple abelian varieties. In characteristic 0, we know exactly what occurs, due to Albert and Shimura. (Shimura, notably, used the geometry of the moduli space $\mathcal{A}_g$.)

Remark 2.194. Let's explain what's going on with the Néron–Severi group. This is occurring when k is algebraically closed, and we pick a polarization $\lambda\colon A \to A^\vee$. Now, we have our embedding

$$\mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \to \operatorname{Hom}(A, A^\vee) \otimes_{\mathbb{Z}} \mathbb{Q} \to \operatorname{End}^0(A),$$

where $\mathrm{NS}(A)$ consists of the symmetric homomorphisms. Notably, being a symmetric homomorphism $\lambda'\colon A \to A^\vee$ means that $f = f^\dagger$, where $f \in \operatorname{End}^0(A)$ is the isogeny such that $\lambda' = \lambda \circ f$. Indeed, we are asking for $\lambda \circ f = f^\vee \circ \lambda$ in order to be symmetric, which amounts to $f = f^\dagger$. So the point is that

$$\mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \operatorname{End}^0(A)^\dagger.$$

Let's see an example of a dimension restriction.

Lemma 2.195. Fix a simple abelian k-variety A, where $\operatorname{char} k = 0$. Then set notation as above with $D \coloneqq \operatorname{End}^0(A)$. Then $d^2 e \mid 2g$.

Proof. In characteristic zero, the Lefschetz principle allows us to assume that $k \subseteq \mathbb{C}$. Then we are granted that $\operatorname{End}^0(A) \subseteq \operatorname{End}^0(A_{\mathbb{C}})$ will act faithfully on $H^1(A(\mathbb{C}), \mathbb{Q})$, meaning that $d^2 e \mid 2g$ in order for the dimensions to check on. ∎

This provides the dimension restrictions in types II–IV.

Lemma 2.196. Fix a simple abelian k-variety A for any field k. Then set notation as above with $D \coloneqq \mathrm{End}^0(A)$. Then $de \mid 2g$.

Proof. The point is that $\deg\colon \mathrm{End}^0(A) \to \mathbb{Q}$ is a polynomial of degree $2g$, and in fact we showed earlier that $\deg$ is a norm form. But Proposition 2.172 tells us that

$$\deg = \left(\mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{N}^{\circ}_{D/K}\right)^i$$

for some integer i. Computing the degree of the polynomials everywhere, we get that $dei = 2g$ for some integer i, which is what we needed. ∎

This provides the dimension restrictions in types III–IV.

Proposition 2.197. Fix a simple abelian k-variety A for any field k. Then set notation as above with $D \coloneqq \mathrm{End}^0(A)$. Further, suppose that L is a subfield of D fixed by $(\cdot)^\dagger$. Then $[L:\mathbb{Q}] \mid g$.

Proof. The point is that $L \subseteq \mathrm{NS}(A_{\overline{k}})$ as discussed before. Now, choose a polarization $\lambda\colon A \to A^\vee$ so that $\lambda = \varphi_{\mathcal{L}}$; we also define $f\colon \mathrm{NS}(A_{\overline{k}})_{\mathbb{Q}} \to \mathbb{Q}$ by

$$f(\varphi_{\mathcal{M}}) \coloneqq \frac{\chi(\mathcal{M})}{\chi(\mathcal{L})},$$

so Proposition 2.162 tells us f^2 is a norm form. Namely, we know that $f(ab) = \pm f(a)f(b)$; an argument on the coefficients of our polynomial is able to show that we either have $f(ab) = +f(a)f(b)$ always or $f(ab) = -f(a)f(b)$ always. However, taking $\mathcal{M} = \mathcal{L}$, we see that the sign $+$ is forced, so f is a norm form on L of degree g! Arguing as in Lemma 2.196 completes. ∎

In the Type I case, one is able to take $L = K(\alpha)$ for suitable choice of α makes $K(\alpha)/K$ a degree-2 extension, providing the needed bounds for Type I. We won't discuss this in more detail.

Anyway, let's provide some examples.

Example 2.198. Fix an elliptic curve E so that $g = 1$. We work in characteristic 0. We see we may only have Type I with $e = 1$ or Type IV with $d = e_0 = 1$, meaning that $\mathrm{End}^0(E)$ is an imaginary quadratic extension of $\mathbb{Q}$ so that E has complex multiplication.

Example 2.199. Fix an elliptic curve E so that $g = 1$ in characteristic $p > 0$.

- It looks like we might be able to have Type I, which forces $e = 1$; however, this does not happen over $\mathbb{F}_q$ or even $\overline{\mathbb{F}_q}$ by Remark 2.167. (This does happen over $\mathbb{F}_p(t)$.)
- We can still have Type IV, meaning that $e_0 = d = 1$, so $\mathrm{End}^0(E)$ is an imaginary quadratic field; one can achieve this by finding an elliptic curve over $\mathbb{Q}$ with ordinary reduction at some prime p so that the Frobenius endomorphism Frob fails to be in $\mathbb{Z}$.
- Lastly, it is possible to have Type III, which means that $e = e_0 = 1$, but we still must have $d \mid 2g$, and $d = 1$ is already considered above, so we actually have $d = 2$ here. This means that $D \coloneqq \mathrm{End}^0(\mathbb{Q})$ is a central simple $\mathbb{Q}$-algebra, and Theorem 2.191 requires it to be $\mathbb{H}$ at ∞. For finite $\ell \neq p$, we also see
$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subseteq \mathrm{End}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell A \otimes_{\mathbb{Z}} \mathbb{Q}_\ell).$$
But both sides here have dimension 4, so we must have $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$, meaning that D splits at all these finite primes ℓ. The fundamental exact sequence now forces ramification at p.

Example 2.200. Fix an abelian surface A so that $g = 2$. We work in characteristic 0.

- Type I is possible; an open subset of the moduli space has $e = 1$ so that $\mathrm{End}^0(A) = \mathbb{Q}$, but it is still possible to have $e = 2$ so that $\mathrm{End}^0(A)$ is a real quadratic field.
- Type II is possible, but this forces $e = 1$ so that D is a quaternion $\mathbb{Q}$-algebra. Theorem 2.191 requires D to split at ∞; every quaternion algebra appears.
- Type III forces $e = 1$, and Shimura shows that this never happens.
- For Type IV, one can have $e_0 = 2$ so that A is an abelian surface with complex multiplication. Otherwise, $e_0 = 1$, this does not happen when k is algebraically closed: we may take $k = \mathbb{C}$, but then $\mathrm{End}^0(A)$ contains a product of two imaginary quadratic fields, which forces A to be isogenous to a product of elliptic curves, meaning that A it not simple. However, it is possible that $e_0 = 1$ in general; for example, the Jacobian of $y^8 = x(x-1)$ modulo the Jacobian of $y^4 = x(x-1)$ over $\mathbb{Q}$ will work.

THEME 3

BACK TO COMPLEX MULTIPLICATION

3.1 April 1

We now return to discussing complex multiplication.

3.1.1 Néron Models

We will not discuss constructions too much, but we will say something. For today, R is a discrete valuation ring with fraction field K and residue field κ. Here is our definition.

Definition 3.1 (Néron model)**.** Fix a discrete valuation ring $(R, \mathfrak{m}, \kappa)$ with fraction field K. Then a *Néron model* of some K-scheme A such that $\mathcal{A}$ is a smooth separated R-scheme of finite type satisfying the following.

- $\mathcal{A}_K = A$
- Néron mapping property: if $\mathcal{X}$ is a smooth R-scheme with $X \coloneqq \mathcal{X}_K$, then any map $u\colon X \to U$ is the base-change of a unique map $\mathcal{X} \to \mathcal{A}$.

Remark 3.2. The Néron mapping property immediately implies uniqueness up to unique isomorphism.

Remark 3.3. Additionally, the universal property implies that formation of Néron models commutes with étale base-change. Namely, if $\operatorname{Spec} R' \to \operatorname{Spec} R$ is étale, then $\mathcal{A}_{R'}$ continues to be smooth over R', and drawing out the Cartesian square

Here is our result.

Proposition 3.4. Fix a discrete valuation ring $(R, \mathfrak{m}, \kappa)$ with fraction field K. If $\mathcal{A}$ is an abelian R-scheme, then $\mathcal{A}$ is a Néron model of $\mathcal{A}_K$.

Group structure upgrades?

Proof. The point is to use the valuative criterion of properness. Let $\mathcal{X}$ be a smooth R-scheme, and set $X \coloneqq \mathcal{X}_K$. To apply the valuative criterion for properness, we let η be the generic point of $\mathcal{X}_\kappa$, so $\mathcal{O}_{\mathcal{X},\eta}$ is a discrete valuation ring. Thus, the map $\operatorname{Frac} \mathcal{O}_{\mathcal{X},\eta} \to A$ produces a unique lift $\operatorname{Spec} \mathcal{O}_{\mathcal{X},\eta} to \mathcal{A}$. (Note the valuative criterion is legal because everything in sight is finite type.)

Continuing, by spreading out, we note that we get an R-scheme $\mathcal{Y} \subseteq \mathcal{X}$ such that $\mathcal{Y}_K = X$ and $\mathcal{Y}_\kappa \subseteq \mathcal{X}_\kappa$ is open, and we have our unique map $\mathcal{Y} \to \mathcal{A}$. However, $\mathcal{X} \setminus \mathcal{Y}$ can be taken to be codimension at least 2 (in

Why?

the spreading out) because we are including the generic point. Now, [BLR90, Theorem 4.4.1] tells us that the group structure (and smoothness) of $\mathcal{A}$ tells us that the rational map $\mathcal{Y} \to \mathcal{A}$ can be uniquely extended to all $\mathcal{X}$. Here is the precise citation.

Proposition 3.5. Fix a discrete valuation ring R, and let G be a smooth separated group R-scheme such that we have some rational map $f\colon Z \to G$ where Z is smooth, and f is defined outside a set of codimension at least 2. Then f extends uniquely to a map $Z \to G$.

Proof. To use the group structure, we define the rational map $F\colon Z \times_R Z \to G$ given by

$$F(x,y) \coloneqq f(x)f(y)^{-1}.$$

Then f being defined at x means that F is defined at the element (x,x); in fact, the converse is also true: F being defined on (x,x) means we can define it an open neighborhood (x,U), and then we can shrink U so that f is also defined on U, so one can write $f(x) = F(x,u)f(u)$ for $u \in U$ to promise that f is defined at x.

From here, we see that f is defined in codimension 1, so F is defined codimension 1, so an argument with algebraic Hartog's lemma tells us that F can just be defined globally, so f can be defined globally. To be more explicit, we note that F is defined at some (x,x) provided that the map $\mathcal{O}_{G,e} \to K(Z \times Z)$ factors through $\mathcal{O}_{Z\times Z,(x,x)}$, where the application of algebraic Hartog's is valid because we can now to pass to a sufficiently small open (affine) open neighborhood of (x,x) going to $e \in G$. (Namely, this factoring happens in codimension 1, so our elements are actually in the ring, so we are okay.) ■

This completes the proof. ■

Corollary 3.6. Fix abelian schemes $\mathcal{A}$ and $\mathcal{B}$ over the discrete valuation ring $(R,\mathfrak{m},\kappa)$ with fraction field K. Then the map

$$\mathrm{Hom}_R(\mathcal{A},\mathcal{B}) \to \mathrm{Hom}_K(\mathcal{A}_K,\mathcal{B}_K)$$

is an isomorphism.

Proof. Examining the squares to be a homomorphism and using the Néron model property tells us that the backward map is well-defined both as a morphism and in fact a homomorphism. (Namely, squares commuting can be encoded in uniqueness of our morphisms.) ■

We now state our theorem for existence, but we will not prove it.

Theorem 3.7. Fix a discrete valuation ring $(R,\mathfrak{m},\kappa)$ with fraction field K. Then any abelian K-variety A has a Néron model $\mathcal{A}$. In fact, $\mathcal{A}$ is a smooth group scheme, and there is a finite extension L of K such that $\mathcal{A}_L$ has semi-abelian identity component.

3.1.2 The Shimura–Taniyama Formula

We now return to prove (a special case of) the Shimura–Taniyama formula. It will help to have the following lemma.

Lemma 3.8. Let A be an abelian variety of good reduction. Fix everything as above, and let m be an integer coprime to p. Then

$$A(\overline{K})[m] = A(K_{\mathfrak{P}}^{\mathrm{unr}})[m] = \mathcal{A}_\kappa(\overline{\kappa})[m].$$

Proof. This only uses that A has good reduction. The second equality is not so bad because $A(K_{\mathfrak{P}}^{\mathrm{unr}}) = \mathcal{A}(\mathcal{O}_{K_{\mathfrak{P}}^{\mathrm{unr}}})$ by the Néron mapping property (even as groups), which then reduces to $\mathcal{A}_\kappa(\overline{\kappa})$. But we are looking at kernels of $[m]$, which is finite étale, so Hensel's lemma applies to provide that reduction is a bijection.

We now address the first equality. The cardinality of $A(K_{\mathfrak{P}}^{\mathrm{unr}})[m]$ is the correct number $m^{2\dim A}$, so all torsion from $\overline{K_{\mathfrak{P}}}$ is defined over $K_{\mathfrak{P}}^{\mathrm{unr}}$. In fact, all this torsion must be defined over the smaller algebraically closed field $\overline{K}$, so the first equality follows as well. ∎

In particular, we see that making m a prime-power tells us that

$$T_\ell A = T_\ell \mathcal{A}_\kappa,$$

where we have compatibility with Galois action, where the "Galois action" by $\mathrm{Gal}(\overline{K}/K)$ on the right is via the decomposition group. So Theorem 2.164 does the job.

3.2 April 3

Today we prove our special case of the Shimura–Taniyama formula.

3.2.1 Proving the Shimura–Taniyama Formula

Here is our statement.

Theorem 3.9. Fix a number field K, and let A be an abelian K-variety with complex multiplication by the CM algebra (E, Φ). Further, we take the following extra assumptions.

- K contains the Galois closure of E.
- A has good reduction at some prime $\mathfrak{P}$ of K, meaning that $\mathcal{A}$ is an abelian scheme.
- $K_{\mathfrak{P}}$ is unramified over $\mathbb{Q}_p$ where p. Set $\kappa \coloneqq \mathcal{O}_K/\mathfrak{P}$.
- $\mathrm{End}(A) \cap E = \mathcal{O}_E$.

Then there is some unique $\pi \in \mathcal{O}_E$ such that the reduction of π from $\mathcal{O}_E \subseteq \mathrm{End}\, A = \mathrm{End}\, \mathcal{A}$ to $\mathrm{End}\, \mathcal{A}_\kappa$ is Frob. In fact, (π) is

$$\prod_{\varphi \in \Phi} \varphi^{-1}\left(\mathrm{Nm}_{K/\varphi(E)}\, \mathfrak{P}\right).$$

Proof. We begin by discussing how to get $\pi \in \mathcal{O}_E$. Recall that the Néron mapping property yields $\mathrm{End}\, A = \mathrm{End}\, \mathcal{A}$, which embeds in $\mathrm{End}\mathcal{A}_\kappa$ because we can check the equality of two endomorphisms $\varphi, \psi \colon \mathcal{A} \to \mathcal{A}$ on the Zariski dense subset of prime-to-p torsion of $\mathcal{A}$, which is already found in $\mathcal{A}_\kappa$ by Lemma 3.8.

Now, we know $E \subseteq \mathrm{End}^0(A) \subseteq \mathrm{End}\, \mathcal{A}_\kappa$, and there is some Frob element. In fact, Frob will commute with anything from E, which means that it must live in E, which can be seen directly from the Albert classification or more directly as follows: it suffices to check the commutativity on the Tate module. But then $V_\ell \mathcal{A}_\kappa$, but $\dim(E \otimes \mathbb{Q}_\ell) = 2 \dim A$ (because E is our CM algebra), and $V_\ell A_\kappa$ also has dimension $2 \dim A$, and the relevant action is faithful on A and hence faithful on $\mathcal{A}$ and hence faithful on $\mathcal{A}_\kappa$, so $V_\ell \mathcal{A}_\kappa$ is a faithful $(E \otimes \mathbb{Q}_\ell)$-module of rank 1. Thus, Frob will have to live in $E \otimes \mathbb{Q}_\ell$ and in $\mathrm{End}\, \mathcal{A}_\kappa$, so it comes from $E \cap \mathrm{End}\, A$, which is $\mathcal{O}_E$. So Frob comes from a unique element $\pi \in \mathcal{O}_E$.

We now turn to the second claim. Note the relative Frobenius $F \colon A \to A^{(1)}$ factors through $[p]$ (we showed this when discussing finite flat group schemes), so the full Frobenius Frob factors through $[q]$. In fact, we can see this more explicitly via the following lemma.

Lemma 3.10. Fix everything as above. Then

$$\mathrm{Frob} \circ \mathrm{Frob}^\dagger \stackrel{?}{=} [q]$$

for any Rosati involution $(\cdot)^\dagger$.

Proof. This is a matter of unraveling the definition. It will be enough to show that $\mathrm{Frob}^\dagger \circ \mathrm{Frob} = [q]$ by duality. Well, let $\lambda\colon A \to A^\vee$ be our polarization providing the Rosati involution, and then we see that

$$\mathrm{Frob}_A{}^\dagger \circ \mathrm{Frob}_A = \lambda^{-1} \circ \mathrm{Frob}_A{}^\vee \circ \lambda \circ \mathrm{Frob}_A\,.$$

This being equal to $[q]$, by rearranging, is equivalent to showing that

$$\mathrm{Frob}_A^\vee \circ \mathrm{Frob}_{A^\vee} = [q].$$

We will do this by hand. Fix a test T-scheme, and a rigidified line bundle $\mathcal{L}$ on $A \times T$ living in $A^\vee(T)$. We pass $\mathcal{L}$ through. For example,

$$\mathrm{Frob}_{A^\vee}(\mathcal{L}) = (\mathrm{id} \times F_T^{(m)})^*\mathcal{L},$$

where $F_T^{(m)}$ means the relative Frobenius, and then applying the dual morphism $\mathrm{Frob}_A^\vee$ leaves us with

$$(\mathrm{Frob}_A \times \mathrm{id})^*(\mathrm{id} \times F_T^{(m)})^*\mathcal{L}.$$

So we see that we are just taking qth powers on both coordinates, which does indeed produce $\mathcal{L}^{\otimes q}$, as desired. ∎

The point is that (π) is supported on $p\mathcal{O}_E$, so we can write

$$\pi = \prod_{v \mid p} \mathfrak{p}_v^{m_v}$$

for some nonnegative integers m_v. To make things principal, set $h \coloneqq \#\operatorname{Cl} E$ so that $\mathfrak{p}_v^{m_v h}$ can be said to be generated by some $\gamma_v \in \mathcal{O}_E$. We will compute $\deg \gamma_v$ in two ways.

Lemma 3.11. Fix everything as above. For any $\alpha \in \mathcal{O}_E$, the degree of α as an endomorphism $A \to A$ is $\mathrm{Nm}_{E/\mathbb{Q}}\,\alpha$.

Proof. We may let α act on the Tate module $V_\ell \mathcal{A}_\kappa$, as discussed above. Then we previously showed that

$$\deg \alpha = \det(\alpha|_{V_\ell \mathcal{A}_\kappa}),$$

but we know $V_\ell \mathcal{A}_\kappa$ is just $E \otimes \mathbb{Q}_\ell$, and multiplication by α then becomes the usual multiplication by α map $E \to E$. Thus, the determinant is indeed $\mathrm{Nm}_{E/\mathbb{Q}}\,\alpha$, as desired. ∎

The point is that

$$\deg \gamma_v = \mathrm{Nm}_{E/\mathbb{Q}}\,\gamma_v = \mathrm{Nm}_{E/\mathbb{Q}}\,\mathfrak{p}_v^{m_v h}.$$

We now compute this $\deg \gamma_v$ differently. Because we are only interested in the degree, we may as well take $\kappa = \overline{\kappa}$.

Lemma 3.12. Fix an algebraically closed field k of positive characteristic p, and set $q \coloneqq p^m$. Then any isogeny $f\colon A \to B$ of abelian k-varieties such that $f^*K(B)$ contains $K(A)^q$ has

$$\deg f \le q^d,$$

where $d = \dim \ker \mathrm{Lie}\, f$.

Sketch. We will use [Mil17, Theorem 11.27]. Note that $\ker f$ is a local finite group k-scheme because f factors through multiplication-by-q, from which one can see that

$$\ker f = \operatorname{Spec} \frac{k[x_1, \dots, x_n]}{\left(x_1^{p^{r_1}}, \dots, x_n^{p^{r_n}}\right)}$$

with $r_i \le m$ for each i and $n = \dim T_e \ker f$ by the proof of this result. Then one computes

$$\deg f = \prod_{i=1}^{m} p^{r_i} \le p^{mn} = q^n,$$

but $n = \dim T_e \ker f$ is $\dim \ker \operatorname{Lie} f$. ∎

We are actually pretty happy that Lie has appeared because we need to relate everything back to the CM type. In particular, we know that $\operatorname{Lie} A$ admits a K-basis $(e_\varphi)_{\varphi \in \Phi}$, where $a \in E$ acts on e_φ by $\varphi(a)$.

Now, because $K_{\mathfrak{P}}/\mathcal{O}_p$ is unramified, we know that $\operatorname{Lie} \mathcal{A}$ will admit an $\mathcal{O}_{K_{\mathfrak{P}}}$-basis by $(e_\varphi)_{\varphi \in \Phi}$ again. Indeed, the point is that

$$\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{K_{\mathfrak{P}}} = \bigoplus_{\sigma \colon E \subseteq K_{\mathfrak{P}}} \mathcal{O}_{K_{\mathfrak{P}}}$$

because we are unramified.[1] This basis then goes down to a basis $\{\overline{e}_\varphi\}_{\varphi \in \Phi}$ of $\operatorname{Lie} \mathcal{A}_\kappa$ by reduction. Thus,

$$\ker(\operatorname{Lie} \gamma_v \colon \operatorname{Lie} \mathcal{A}_\kappa \to \operatorname{Lie} \mathcal{A}_\kappa) = \operatorname{span}\{\overline{e}_\varphi : \varphi(\gamma_v) \in \mathfrak{P}\}$$

because our multiplication is basically coordinate-wise.

To continue, we recall that

$$H_v \coloneqq \left\{\tau \in \operatorname{Hom}(E, K) : \tau^{-1}\mathfrak{P} = \mathfrak{p}_v\right\} \qquad \text{and} \qquad \Phi_v \coloneqq \Phi \cap H_v.$$

The point is that we know $\dim \ker(\operatorname{Lie} \gamma_v)$ is exactly $\#\Phi_v$, meaning $\deg \gamma_v \le q^{h\#\Phi_v}$ by the previous lemma.

Comparing our two expressions for the degree, we see that

$$\operatorname{Nm}_{E/\mathbb{Q}} \mathfrak{p}_v^{m_v} \le q^{\#\Phi_v}.$$

We claim that we have equality. Well, using (3.10), we see

$$\operatorname{Nm}_{E/\mathbb{Q}} \pi = \deg \operatorname{Frob} = q^{\dim A}$$

because $\deg \operatorname{Frob} = \deg \operatorname{Frob}^\dagger$. On the other hand,

$$\operatorname{Nm}_{E/\mathbb{Q}} \pi = \operatorname{Nm}_{E/\mathbb{Q}} \prod_{v \mid p} \mathfrak{p}_v^{m_v} \le \prod_{v \mid p} q^{\#\Phi_v} = q^{\#\Phi} = q^{\dim A},$$

so the inequality here sharpens to an equality.

Thus, we achieve $(\operatorname{Nm}_{K/\mathbb{Q}} \mathfrak{P})^{\#\Phi_v} = \operatorname{Nm}_{E/\mathbb{Q}} \mathfrak{p}_v^{m_v}$. On the other hand, decomposing the norm as a product of conjugates, we see

$$\operatorname{Nm}_{E/\mathbb{Q}} \left(\prod_{\varphi \in \Phi_v} \varphi^{-1}(\operatorname{Nm}_{K/\varphi(E)} \mathfrak{P}) \right) = \prod_{\varphi \in \Phi} \operatorname{Nm}_{K/\mathbb{Q}} \mathfrak{P},$$

so comparing our norms implies that

$$\mathfrak{p}_v^{m_v} = \prod_{\varphi \in \Phi_v} \varphi^{-1}(\operatorname{Nm}_{K/\varphi(E)} \mathfrak{P}).$$

(In particular, both sides are powers of $\mathfrak{p}_v$ by construction, so one only needs to compare exponents.) Looping over all φ completes the proof. ∎

[1] If we want to remove this unramified assumption, then we must work with more theory of p-divisible groups to make this sort of thing go through.

Remark 3.13. The bulleted assumptions can essentially be removed, but we will not do so.

Remark 3.14. In fact, one can show that there is an explicit formula of $(\pi) \subseteq \mathcal{O}_E$, which we will show next class.

3.3 April 5

Today we would like to state the Main theorem of complex multiplication.

3.3.1 The Reflex Norm

We need to discuss the reflex norm. To describe our definition, fix a CM type (E, Φ), and let E^* be the reflex field. Recall that we may view Φ as a subset of $\mathrm{Hom}(E, \overline{\mathbb{Q}})$. Note that

$$E \otimes_{\mathbb{Q}} K \cong \prod_{\sigma \in \mathrm{Hom}(E,\overline{\mathbb{Q}})} K_\sigma$$

for any field K containing all embeddings of E into $\overline{\mathbb{Q}}$. Then Galois descent provides an $E \otimes_{\mathbb{Q}} E^*$ module V_Φ such that

$$V_\Phi \otimes_{E^*} K \cong \prod_{\varphi \in \Phi} K_\varphi$$

simply by definition of E^* as being fixed by automorphisms $\sigma \colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ permuting Φ.

Definition 3.15 (reflex norm)**.** Fix a CM type (E, Φ), and define V_Φ as above. Then we define $\mathrm{N}_\Phi \colon (E^\times)^* \to E^\times$ by

$$\mathrm{N}_\Phi(\alpha) \coloneqq \det(\alpha \mid V_\Phi).$$

In fact, for any K containing E^*, one can define $\mathrm{N}_{K,\Phi} \colon K^\times \to K^\times$ by

$$\mathrm{N}_{K,\Phi}(\alpha) \coloneqq \det(\alpha \mid V_\Phi \otimes_{E^*} K).$$

Remark 3.16. Because of transitivity of norms, we see that

$$\mathrm{N}_{K,\Phi} = \mathrm{N}_\Phi \circ \mathrm{N}_{K/E^*}.$$

This definition work well with Theorem 3.9.

Proposition 3.17. Fix a field K containing the all images of E in $\overline{\mathbb{Q}}$. Then any $a \in K^\times$ has

$$\mathrm{N}_{K,\Phi}(a) = \prod_{\varphi \in \Phi} \varphi^{-1}\left(\mathrm{N}_{K/\varphi(E)}\, a\right)$$

Proof. Omitted. See [Mil20b, Proposition 1.26]. The point is to expand out the definitions and stratify along Φ. ∎

Remark 3.18. By tensoring with local fields suitably, we see that $\mathrm{N}_{K,\Phi}$ provides a map $\mathbb{A}_K^\times \to \mathbb{A}_E^\times$ and also a map on the fractional ideals.

3.3.2 The Main Theorem

Now, for our set-up, let A be an abelian $\overline{\mathbb{Q}}$-variety with CM type (E, Φ). Let E^* be the reflex field. From here, note that $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ lets us define

$$A^\sigma := A \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}},$$

which has CM type given by $\sigma\Phi$; thus, if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$, then $\sigma\Phi = \Phi$ by definition of E^*, meaning that our CM type is preserved! This observation will simplify matters, though it is possible to work with more general σ if one is willing to put in more work.

Continuing, note that pointwise application of σ provides a map $\sigma\colon A \to A^\sigma$, and this isomorphism is compatible with the E-action on both sides. Continuing, we are granted an isogney $\alpha\colon A \to A^\sigma$ which is compatible with the E-action and unique up to multiplication by $E^\times$; this is because A and A^σ are both CM abelian varieties with the same CM type.[2] We would like to understand our Galois representations, so we define

$$\widehat{T}(A) := \prod_\ell T_\ell A \qquad \text{and} \qquad \widehat{V}(A) := \widehat{T}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

So we get our isomorphism $\widehat{V}(\sigma)\colon \widehat{V}(A) \to \widehat{V}(A^\sigma)$ and similarly get some $\widehat{V}(\alpha)$. These maps are both going to be $E \otimes \mathbb{A}_f$ linearly, where $\mathbb{A}_f := \mathbb{A}_{E,f}$ is denoting the finite adéles. Comparing our two morphisms, we get some $\eta(\sigma) \in \mathbb{A}_{E,f}^\times$ such that

$$\alpha(\eta(\sigma)x) = \sigma(x)$$

for all $x \in \widehat{V}(A)$; this is simply because we have provided two isomorphisms between Galois representations, which must be unique up to some multiplication. In total, we have gotten a group homomorphism

$$\eta\colon \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) \to \mathbb{A}_{E,f}^\times/E^\times.$$

We now get the feeling that global class field theory should come up. Because the target is abelian, the above map actually factors through the abelianization, so it factors through $\mathrm{Gal}(E^{*,\mathrm{ab}}, E) \to \mathbb{A}_{f,E}^\times/E^\times$. On the other hand, we know from the next subsection that there is a global Artin map

$$\mathbb{A}_{E^*,f}^\times/E^* \to \mathrm{Gal}(E^{*,\mathrm{ab}}/E^*).$$

The statement of our Main theorem is then the following.

Theorem 3.19 (Main)**.** Fix everything as above. Then the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/E^*) & \xrightarrow{\eta} & \mathbb{A}_{E,f}^\times/E^\times \\ \downarrow & & \uparrow{\scriptstyle \mathrm{N}_\Phi} \\ \mathrm{Gal}(E^{*,\mathrm{ab}}/E^*) & \xleftarrow[\mathrm{Art}]{} & \mathbb{A}_{E^*,f}/(E^*)^\times \end{array}$$

In particular, we are granted essentially total understanding of the Galois action on the Tate module.

Remark 3.20. Later, we will use this fine understanding of the Galois representation in order to compute the L-function of a CM abelian variety.

[2] An easy way to see the uniqueness up to $E^\times$ is to use the Albert classification: it suffices to show that $\beta \in \mathrm{End}^0(A)$ commuting with the E-action must be in E, which can be seen by looking at the cases individually.

Remark 3.21. Fix a polarization $\lambda\colon A \to A^\vee$ such that $(\cdot)^\dagger$ is complex conjugation on E. Then one has a Weil pairing $\psi\colon \widehat{V}(A) \times \widehat{V}(A) \to \mathbb{A}_f(1)$ given by gluing together the local Weil pairings. We now define ψ^σ on A^σ by $\psi^\sigma(\sigma x, \sigma y) \coloneqq \sigma(\psi(x,y))$, which by definition of $\mathbb{A}_f(1)$ is just $\chi(\sigma)\psi(x,y)$ where χ is the cyclotomic character. Applying Theorem 3.19 to our situation, we get some s such that

$$\begin{aligned}\psi^\sigma(\sigma x, \sigma y) &= \psi^\sigma(\alpha(\mathrm{N}_\Phi(s)x), \alpha(\mathrm{N}_\Phi(s)y)) \\ &= \psi^\sigma(\mathrm{N}_\Phi(s)\overline{\mathrm{N}_\Phi(s)}\alpha x, \alpha y) \\ &= \mathrm{N}_\Phi(s)\overline{\mathrm{N}_\Phi(s)}\psi^\sigma(\alpha x, \alpha y).\end{aligned}$$

(Note that we get complex conjugation on the $\mathrm{N}_\Phi(s)$ because $(\cdot)^\dagger$ is complex conjugation.) So we are able to compare ψ^σ with χ_{cyc} by comparing our two expressions.

3.3.3 A Little Global Class Field Theory

We quickly review the statement of global class field theory. Fix a number field K, and let K^{ab} be its abelian closure.

Definition 3.22 (Artin map)**.** Fix a number field K. Then there is a canonical homomorphism

$$\mathrm{Art}_K\colon \mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

satisfying the following: for any finite place v, of K and $w \mid v$, the following diagram commutes.

$$\begin{array}{ccc} K_v & \xrightarrow{\quad\mathrm{Art}_{L_w/K_v}\quad} & \mathrm{Gal}(L_w/K_v) \\ {\scriptstyle i_v}\downarrow & & \downarrow \\ \mathbb{A}_K^\times/K^\times & \xrightarrow[\mathrm{Art}_K]{} \mathrm{Gal}(K^{\mathrm{ab}}/K) & \twoheadrightarrow \mathrm{Gal}(L/K) \end{array}$$

Here, Art_v is the local Artin map; it is also an isomorphism.

Remark 3.23. Let's describe some properties of the local Artin map.

- If L_w/K_v is unramified and nonarchimedean, then
$$\mathrm{Art}_{L_w/K_v}(\alpha) = \mathrm{Frob}_{L_w/K_v}^{-v(\alpha)},$$
where the $-$ in the exponent is a rather annoying convention.
- If L_w/K_v is the extension $\mathbb{C}/\mathbb{R}$, then we are looking at the sign map $\mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Remark 3.24. One can take a quotient suitably to provide an Artin isomorphism

$$\mathrm{Art}_{L/K}\colon \frac{\mathbb{A}_K^\times}{K^\times \,\mathrm{N}(\mathbb{A}_L^\times)} \to \mathrm{Gal}(L/K).$$

Remark 3.25. If K is CM, one may basically ignore the infinite places because they all start out as $\mathbb{C}$.

3.4 April 8

We begin to talk about L-functions.

3.4.1 Hecke Characters from Abelian Varieties

Fix an abelian variety A over a number field $K \subseteq \overline{\mathbb{Q}}$ with complex multiplication by $E \subseteq \operatorname{End}^0(A)$. For simplicity, we will assume that $E^* \subseteq K$. Recall we built a Galois representation

$$\rho_A \colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}_{\mathbb{A}_{E,f}}(\widehat{V}A),$$

but because A has complex multiplication, this right-hand side is $\operatorname{Aut}^{\times}_{E,f}$, so in fact ρ will factor as

$$\overline{\rho}_A \colon \operatorname{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{A}^{\times}_{E,f}.$$

It turns out that Theorem 3.19 implies that

$$\rho(\operatorname{Art}_K(s)) = \mathrm{N}_{\Phi}(\mathrm{N}_{K/E^*}(s)) \cdot \lambda_s^{-1}$$

for some unique $\lambda_s \in E^{\times}$. Indeed, we know that

$$\begin{array}{ccc} \operatorname{Gal}(\overline{\mathbb{Q}}/E^*) & \xrightarrow{\eta} & \mathbb{A}^{\times}_{E,f}/E^{\times} \\ \downarrow & & \uparrow{\scriptstyle \mathrm{N}_{\Phi}} \\ \operatorname{Gal}(E^{*,\mathrm{ab}}/E^*) & \xleftarrow[\mathrm{Art}]{} & \mathbb{A}_{E^*,f}/(E^*)^{\times} \end{array}$$

commutes, so we combine this with the functoriality of the global Artin map, which says that

$$\begin{array}{ccc} \mathbb{A}^{\times}_K/K^{\times} & \xrightarrow{\mathrm{Art}_K} & \operatorname{Gal}(\overline{\mathbb{Q}}/K)^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{K/E^*}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbb{A}^{\times}_{E^*}/(E^*)^{\times} & \xrightarrow{\mathrm{Art}_{E^*}} & \operatorname{Gal}(\overline{\mathbb{Q}}/E^*)^{\mathrm{ab}} \end{array}$$

commutes. Combining the two diagrams is able to produce our result.

To continue, we have the following result.

Proposition 3.26. The map $\lambda_{\bullet} \colon \mathbb{A}^{\times}_{K,f} \to E^{\times}$ is continuous, where E has been given the discrete topology.

We are going to take a roundabout way to this result. We begin with the following result, which will also be a key input to our proof of the Weil conjectures for abelian varieties.

Remark 3.27. Fix a polarized abelian variety (A, φ). Then for any $m \geq 3$, it turns out that

$$\operatorname{Aut}((A,\varphi)) \to \operatorname{Aut} A[m]$$

is injective.

To prove the remark, we will want

Proposition 3.28. Fix an abelian k-variety A. Further, fix any endomorphism α such that $\alpha^{\dagger} \circ \alpha = [n]$ for some nonzero $n \in \mathbb{Z}$. Then the following are true.

(a) Then $\mathbb{Q}(\alpha) \subseteq \operatorname{End}^0(A)$ is semisimple.

(b) The multiset $\{\omega_i\}$ of roots of the characteristic polynomial all have absolute value $\sqrt{|n|}$.

(c) The multiset $\{\omega_i\}$ is stable under $\omega \mapsto n/\omega$.

Proof. We begin with (a). Here, we find $\alpha^\dagger = n \circ \alpha^{-1}$, so $\mathbb{Q}(\alpha)$ is preserved under $(\cdot)^\dagger$. The point is that $x \mapsto \operatorname{tr}(xx^\dagger)$ can now be defined to be a positive-definite quadratic form on $\mathbb{Q}(\alpha)$.

We now show that $\mathbb{Q}(\alpha)$ is semisimple. Let $\mathfrak{a} \subseteq \mathbb{Q}(\alpha)$ be an ideal, then having our quadratic form lets us define $\mathfrak{a}^\perp$ and see that $\mathbb{Q}(\alpha) = \mathfrak{a} \oplus \mathfrak{a}^\perp$ because everything in sight is finite-dimensional. Thus, we can decompose $\mathbb{Q}(\alpha)$ into simple algebras inductively, meaning that $\mathbb{Q}(\alpha)$ is semisimple.

We now handle (b) and (c). We can write

$$\mathbb{Q}(\alpha) = K_1 \times K_2 \times \cdots \times K_m$$

for some m. Because $(\cdot)^\dagger$ is positive-definite, it cannot swap any of these fields, so in fact $(\cdot)^\dagger$ must preserve all these fields, meaning that each is either totally real or has complex multiplication (by some argument from the Albert classification). Now, we see that the ω_j are the images of α via the various embeddings

$$\mathbb{Q}(\alpha) \to K_i \to \mathbb{C},$$

but $(\cdot)^\dagger$ becomes complex conjugation in $\mathbb{C}$, so we see that the image of α will have magnitude $\sqrt{|n|}$ by direct computation passing through $\alpha^\dagger \alpha = [n]$. Additionally, we see that we can exchange α with $\alpha^\dagger$ to send ω_i to n/ω_i, which yields (c). ∎

Remark 3.29. One recovers the Riemann hypothesis part of the Weil conjectures for abelian varieties by applying this result to the fact that

$$\operatorname{Frob}^\dagger \circ \operatorname{Frob} = [q].$$

One gets the other parts of the Weil conjectures by formally unraveling everything into the other parts; for example, (b) will give rise to the functional equation.

We next pick up [Mum08, Theorem 21.5].

Theorem 3.30. Fix a polarized abelian variety (A, φ). Then for any $m \geq 3$, the map

$$\operatorname{Aut}((A, \varphi)) \to \operatorname{Aut} A[m]$$

is injective.

Proof. Suppose that α is an automorphism of $\operatorname{Aut}((A, \varphi))$. Then $\alpha^\dagger \circ \alpha = 1$ because we are an isomorphism of the polarized abelian variety. (This is a matter of writing down the corresponding commuting square for an isomorphism of polarized abelian varieties.) It follows that all eigenvalues of α are algebraic integers with norm 1, so they are all roots of unity.

We are now ready to complete the proof. It is enough to show that the map has trivial kernel. But then we see that $\alpha = 1 + Mx$ for some x where $M > 3$, so $\omega_i = 1 + Mx_i$ for some x_i where $M > 3$, from which some algebraic number theory is able to enforce that $\omega_i = 1$ for each i. ∎

Remark 3.31. The point of this is to show that the isomorphism class of our polarized abelian varieties is finite. The reason we must have the word "polarized" is that it is possible to provide abelian varieties with infinitely many automorphisms; for example, take an abelian variety with complex multiplication by $\mathbb{Q}(\sqrt{-1}, \sqrt{-2})$, which then will have endomorphisms in an order of $\mathbb{Q}(\sqrt{2})$, which has infinitely many units.

We are now ready to prove Proposition 3.26.

Proof of Proposition 3.26. Because everything in sight is a group, it is enough to show that $s \to 1$ in $\mathbb{A}_{K,f}^\times$ implies that $\lambda_s = 1$. Well, for m large enough and s close enough to 1, we can achieve $\lambda_s \in \mathcal{O}_E^\times$ (namely, force s to be a unit at all finite places), $\lambda_s \equiv 1 \pmod{M}$ for large M (which is finitely many congruence

How?

conditions), and $\lambda_s \in \mathrm{End}(A_{\overline{\mathbb{Q}}})$. In particular, we know that $\lambda_s^{\pm 1}$ lives in $\mathcal{O}_E \cap \mathrm{Aut}\, A_{\overline{\mathbb{Q}}}$ and acts trivially on $A_{\overline{\mathbb{Q}}}[M]$.

Continuing, we are given that there is a polarization $\varphi\colon A_{\overline{\mathbb{Q}}} \to A_{\overline{\mathbb{Q}}}^\vee$ which is compatible with the E-action, and we are able to descend this polarization to its field of definition as $\varphi\colon A_L \to A_L^\vee$. The point is that we will be able to see that λ_s preserves φ, from which $\lambda_s = 1$ will follow from Theorem 3.30. To see that we preserve φ, we recall the ideas and notations from Remark 3.21, which grants a rational number c such that

$$c\psi(x,y) = \psi^\sigma\left(\lambda_s^{-1}x, \lambda_s^{-1}y\right)$$

With s close enough to 1, we will get $\psi^\sigma = \psi$ because $\sigma = \mathrm{Art}\, s$ (so s close enough to 1 will make σ trivial over the field of definition L). Continuing, unwinding definitions, we see

$$c^{-1}\psi(x,y) = \psi(\lambda_s x, \lambda_s y) = \psi(\lambda_s\overline{\lambda_s}x, y),$$

from which the non-degeneracy of the Weil pairing forces $\lambda_s\overline{\lambda_s} \in \mathbb{Q}$. Thus, for degree reasons (and positivity reasons), we see that $\lambda_s \cdot \overline{\lambda_s}$ is a positive integer but also invertible, so it must be 1, so indeed λ_s preserves φ by staring at the above computation. ∎

We are now ready to define Hecke characters and check that we've built one.

Definition 3.32 (Hecke character)**.** Fix a number field K. A *Hecke character* is a continuous homomorphism $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$. If $\mathrm{im}\,\chi \subseteq S^1$, we say that χ is *unitary*.

Remark 3.33. For any Hecke character $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$, one has a unique decomposition $\chi = \chi_0\,|\cdot|^\sigma$ for some $\sigma \in \mathbb{R}$ where χ_0 is unitary and $|\cdot|$ is the norm. Indeed, the main point is to define σ as $|\chi|$; then the image of $\chi\,|\cdot|^{-\sigma}$ lands in S^1.

Thus, we see that we need $\lambda_\bullet$ to be trivial on $K^\times$.

Let's describe this construction. Fix everything as before, and choose an embedding $\tau\colon E \hookrightarrow \mathbb{C}$. Then one can define a map α^τ via the composite

$$\mathbb{A}_K^\times \to \prod_{v|\infty} E_v^\times \twoheadrightarrow E_\tau \xrightarrow{\tau} \mathbb{C}^\times.$$

Here, the first map is given by $s \mapsto \mathrm{N}_{K,\Phi,\infty}^{-1}(s)\lambda(s)$; here, $\mathrm{N}_{K,\Phi,\infty}$ is given by taking the infinite components of the local reflex norms $\mathrm{N}_{K,\Phi}\colon \mathbb{A}_K^\times \to \mathbb{A}_E^\times$. The continuity of α^τ is basically by definition (everything involved in the definition is continuous), so it remains to check that α^τ vanishes on $K^\times$.

3.5 April 10

Today we continue towards our discussion of L-functions.

3.5.1 L-functions for Abelian Varieties

We begin by checking that we have actually defined a Hecke character.

Lemma 3.34. Fix everything as previously discussed. Then $\alpha^\tau(K^\times) = 1$.

Proof. Quickly, for $s \in \mathbb{A}_K^\times$, let $s_f \in \mathbb{A}_{K,f}^\times$ be the finite part, and we recall that

$$\lambda(s)\,\mathrm{N}_\Phi^{-1}\left(\mathrm{N}_{K/E^*}\, s_f\right) = \lambda(s)\,\mathrm{N}_{K,\Phi}(s_f) = \rho\left(\mathrm{Art}_K^{-1}(s)\right)$$

from Theorem 3.19. Now, the right-hand side is trivial for $s \in K^\times$, and we are able to compute that the left-hand norm is

$$\mathrm{N}_{K,\Phi}^{-1}(s_f) = \mathrm{N}_{K,\Phi,\infty}^{-1}(s)$$

basically by definition of s, so we are able to conclude. ∎

To continue, we note that our Hecke character is actually algebraic.

Definition 3.35 (algebraic)**.** Fix a number field K. A Hecke character $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ is *algebraic* if and only if its archimedean part $\chi_\infty \coloneqq \chi|_{K_\infty^\times}$ is of the form

$$\chi_\infty(x_\infty) = \prod_{v \text{ real}} x_v^{n_v} \cdot \prod_{v \text{ complex}} x_v^{n_v}\overline{x}_v^{n_{\overline{v}}}$$

for integers $n_\bullet \in \mathbb{Z}$.

Remark 3.36. Approximately speaking, we are asking for this to come from morphism $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m \to \mathbb{G}_m$. In particular, a priori, χ_∞ can have exponents which are any integers, so we are placing a fairly strong algebraic limitation.

Unwinding the definition of $\mathrm{N}_{K,\Phi,\infty}$ reveals that $\mathrm{N}_{K,\Phi,\infty}^{-1}\lambda$ is an algebraic Hecke character.

We are now able to define our L-function on the level of the Hecke character.

Definition 3.37 (conductor)**.** Fix a number field K. The *conductor* $\mathfrak{m}$ of a Hecke character $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ is a finite ideal $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}}$ chosen to be the smallest possible so that χ is trivial on $\prod_{\mathfrak{p}} (1+\mathfrak{p}^{m_\mathfrak{p}})$.

Note that $\mathfrak{m}$ conductor exists by continuity of χ.

Outside these factors?

Definition 3.38. Fix a number field K. A Hecke character $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ of conductor $\mathfrak{m}$ has associated L-function given by

$$L(\chi, s) \coloneqq \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi_\mathfrak{p}(\varpi_\mathfrak{p})\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

where $\varpi_\mathfrak{p} \in \mathfrak{p}$ is a uniformizer.

We now recall the following result on these L-functions.

Theorem 3.39 (Hecke, Tate's thesis)**.** Fix a number field K and a Hecke character $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$. Then $L(s,\chi)$ admits a functional equation and a meromorphic continuation to all $\mathbb{C}$.

On the other hand, we can build an L-function for A.

Definition 3.40. Fix an abelian variety A over a number field K. Then the *L-function of A* is

$$L(A,s) \coloneqq \prod_{\mathfrak{p}} \frac{1}{\det\left(1-\mathrm{Frob}_\mathfrak{p}(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s} \mid V_\ell A\right)},$$

where the Euler factor written is correct when A has good reduction at $\mathfrak{p}$, but at bad reduction we must look at the part of $V_\ell A$ fixed by inertia.

It turns out that for $\mathrm{Re}\,s$ large enough, the Euler product will converge; this is essentially by the Weil conjectures. In more words, we may only look at primes of good reduction (there are only finitely many primes of bad reduction), and the eigenvalues of $\mathrm{Frob}_\mathfrak{p}$ have magnitude $|\mathrm{N}\,\mathfrak{p}|^{1/2}$, so we should expect convergence after $\mathrm{Re}\,s > 3/2$.

We now have the following result.

Theorem 3.41. Fix an abelian variety A over a number field K, and assume that A has complex multiplication by the CM algebra E. Then

$$L(A,s) = \prod_{\tau\colon E\to\mathbb{C}} L(\alpha^\tau, s).$$

In particular, $L(A,s)$ admits a functional equation and meromorphic continuation.

Basically, what is happening is that the Galois representation attached to A is abelian, so we should be able to decompose it into characters. The theorem will follow from the following result.

Proposition 3.42. Fix an abelian variety A over a number field K, and assume that A has complex multiplication by the CM algebra E. Fix a prime $\mathfrak{p}$ of K. We will basically have two steps.

1. If A has good reduction at $\mathfrak{p}$, then the restricted character $\chi_\mathfrak{p} \coloneqq \lambda|_{K_\mathfrak{p}^\times}$ is trivial on $\mathcal{O}_{K_\mathfrak{p}}^\times$. (In fact, the converse is true, which we will show next lecture.)
2. $\lambda_\mathfrak{p}(\varpi_\mathfrak{p}) \in \mathcal{O}_E$ acts on $\mathcal{A}_{\kappa(\mathfrak{p})}$ as $\mathrm{Frob}_\mathfrak{p}$.

We now prove Theorem 3.41.

Proof of Theorem 3.41 assuming Proposition 3.42. We compare the Euler factors by hand. Note $V_\ell A$ is a rank-1 module over $E\otimes_\mathbb{Q}\mathbb{Q}_\ell$, so

$$\det\left(1-\mathrm{Frob}_\mathfrak{p} T \mid V_\ell A\right) = \mathrm{N}_{E/\mathbb{Q}}(1-\mathrm{Frob}_\mathfrak{p} T).$$

Now, Proposition 3.42 implies that this equals

$$\mathrm{N}_{E/\mathbb{Q}}(1-\lambda_\mathfrak{p}(\varpi_\mathfrak{p})T) = \prod_{\tau\colon E\to\mathbb{C}} \left(1-\alpha_\mathfrak{p}^\tau(\varpi_\mathfrak{p})T\right),$$

as desired. ∎

We now move towards a proof of Proposition 3.42.

Proof of Proposition 3.42. We begin with (a). Fix $\mathfrak{p}$, and choose ℓ not divisible by $\mathfrak{p}$. By local class field theory, the inertia subgroup $I_\mathfrak{p} \subseteq \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the image of $\mathcal{O}_{K_\mathfrak{p}}^\times$ under the Artin map, which means that

$$\rho(\mathrm{Art}_K(s))_\ell = 1$$

for $s\in\mathcal{O}_{K_\mathfrak{p}}^\times \subseteq \mathbb{A}_K^\times$. So $\mathrm{Art}_K(s)$ acts trivially on $T_\ell A$, but then we see that $\lambda(s)^{-1}\mathrm{N}_{K,\Phi}^{-1}(s)$ vanishes on $T_\ell A$. Similarly, $\mathrm{N}_{K,\Phi}^{-1}(s)_\ell = 1$ because $\mathfrak{p}$ does not divide ℓ, so we are forced to conclude that $\lambda(s)$ acts trivially, as desired.

We now turn to (b). Here, the point is that $\lambda_\mathfrak{p}(\varpi_\mathfrak{p})$ acts on $T_\ell A = T_\ell \mathcal{A}_{\kappa(\mathfrak{p})}$ as $\rho\left(\mathrm{Art}_{K_\mathfrak{p}}(\varpi_\mathfrak{p})^{-1}\right)$, which is $\rho(\mathrm{Frob}_\mathfrak{p})$, as desired. ∎

3.6 April 12

Today we discuss the fact that an abelian variety with complex multiplication has potentially good reduction everywhere.

3.6.1 Potentially Good Reduction Everywhere

The following definition is our main character.

Definition 3.43 (potentially good reduction)**.** Fix an abelian variety A over a number field L. For a prime $\mathfrak{p}$ of K, we say that A has *potentially good reduction at* $\mathfrak{p}$ if and only if there is a some prime $\mathfrak{P}$ over $\mathfrak{p}$ from a finite extension $L_{\mathfrak{P}}$ of $K_{\mathfrak{p}}$ such that $A_{L_{\mathfrak{P}}}$ has good reduction at $\mathfrak{P}$.

Remark 3.44. We already know that A has good reduction at all but finitely many primes of K. So if A has potentially good reduction at all primes, we can find a suitably large finite extension L/K such that A_L has good reduction everywhere. Indeed, simply take a single extension L which is okay for one prime $\mathfrak{P}$ over each prime $\mathfrak{p}$ of K which originally had bad reduction. Then one may make L larger without losing our good reduction at those primes, but then we can replace L with its Galois closure, and then the primes are permuted transitively by the Galois group, so we will get good reduction over every prime $\mathfrak{P}'$ over a prime $\mathfrak{p}$ of K which originally has bad reduction.

Here is our main result for today.

Proposition 3.45. Fix an abelian variety A over a number field K with complex multiplication. Then A has potentially good reduction everywhere.

For this, we will use the following criterion for good reduction.

Theorem 3.46 (Néron–Ogg–Shafarevich criterion)**.** Fix a discrete valuation ring $(R, \mathfrak{p}, \kappa)$ with fraction field K. Then an abelian variety A over K has good reduction if and only if the inertia subgroup $I \subseteq \mathrm{Gal}(\overline{K}/K)$ acts trivially on $T_\ell A$ for some ℓ not dividing $\operatorname{char} \kappa$.

Proof. We will only sketch the proof because we don't want to get bogged down with the theory of affine algebraic groups.

For the converse direction, let $\mathcal{A}$ (over R) be the Néron denote the Néron model of A over K. Then the Néron mapping property implies that

$$\mathcal{A}(K^{\mathrm{unr}})[\ell^\bullet] \cong \mathcal{A}\left(\mathcal{O}_{K^{\mathrm{unr}}}\right)[\ell^\bullet] \twoheadrightarrow \mathcal{A}(\kappa)[\ell^\bullet].$$

Note that the last map is an isomorphism by Hensel's lemma, namely by our smoothness. This now implies the forward direction: good reduction means that we are proper in the target, so the end becomes $T_\ell A$, but inertia acts trivially on the left, so it must act trivially on the right.

We now focus on the harder converse direction. Because inertia acts trivially on $T_\ell A$, our left-hand side is just $A(\overline{K})[\ell^\bullet]$. (A priori, this would only be the submodule of $A(\overline{K})[\ell^\bullet]$ fixed by inertia because we are only looking at the unramified part.) This is somehow "too big" for $\mathcal{A}$ to be anything other than an abelian variety. Let's explain this. Note $\mathcal{A}_\kappa$ is a smooth commutative finite type group scheme over κ, so it lives in a short exact sequence

$$0 \to \mathcal{A}_\kappa^\circ \to \mathcal{A}_\kappa \to \mathcal{A}_\kappa/\mathcal{A}_\kappa^\circ \to 0,$$

where the target is finite, and $\mathcal{A}_\kappa^\circ$ lives in some short exact sequence

$$1 \to U \to \mathcal{A}_\kappa^\circ \to G \to 0,$$

where U is unipotent and G is semi-abelian (i.e., an extension of an abelian variety B by a torus T). (This last clause follows by some structure theory of algebraic groups.) Notably, we see that $\dim A = \dim \mathcal{A}_\kappa = \dim U + \dim T + \dim B$. We now examine the torsion everywhere.

- $\#B(\overline{\kappa})[\ell^n]$ is $\ell^{n \cdot 2 \dim B}$.
- $\#T(\overline{\kappa})[\ell^n]$ is $\ell^{n \dim T}$ because over the algebraically closed field, this will split into $\mathbb{G}_m^{\dim T}$, which has torsion given by $\mu_{\ell^n}^{\dim T}$.
- $\#U(\overline{\kappa})[\ell^n]$ is one because unipotent groups are torsion-free.

Now, sending $n \to \infty$ forces that

$$2 \dim A = 2 \dim B + \dim T,$$

so $\dim T = 0$ and $\dim B = \dim A$, so $\dim U = 0$ as well. Thus, $\mathcal{A}_\kappa$ is proper, which can then be lifted to show that $\mathcal{A}$ is proper and hence an abelian scheme. ■

How?

We are now ready to prove Proposition 3.45.

Proof of Proposition 3.45. We may extend K immediately so that the endomorphisms promised by complex multiplication are all defined. We are going to use a little local class field theory and the fact that the Galois representation $\rho_\ell \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell A)$ is abelian.

Fix some prime $\mathfrak{p}$ of K which we would like to show that A has potentially good reduction at $\mathfrak{p}$ (and choose ℓ not divisible by $\mathfrak{p}$). Then we note that

$$\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}) \subseteq \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, T_\ell A$$

has abelian image and hence must factor as

$$\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}) \to \mathrm{Aut}\, T_\ell A.$$

Let $I_\mathfrak{p}$ be the corresponding inertia subgroup so that we want $\rho_\ell(I_\mathfrak{p})$ to be trivial after some extension.

Now, by Local class field theory, $I_\mathfrak{p}$ contains $\mathcal{O}_{K_\mathfrak{p}}^\times$ and hence contains a finite-index subgroup of the form $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. Further, $\mathrm{Aut}\, T_\ell A$ has an ℓ-adic topology, and we see that it has $1 + \ell \,\mathrm{End}\, T_\ell A$ as a finite-index subgroup, which is a pro-ℓ group. Now, taking the pre-image of $\mathrm{Aut}(T_\ell A)$'s finite-index neighborhood of the identity and then intersecting with $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ produces a map from a finite-index pro-p subgroup of $I_\mathfrak{p}$ to a finite-index pro-ℓ subgroup of $\mathrm{Aut}\, T_\ell A$. But such a thing must have finite image, so $\rho_\ell(I_\mathfrak{p})$ must still have finite image by going back up the finite index subgroups. However, we can kill this finite image by passing to a finite extension of K, so we are done. (Namely, the pre-image of the identity is an open finite index subgroup of $I_\mathfrak{p}$, so we just extend K enough so that the new inertia subgroup goes in there.) ■

3.6.2 Honda–Tate Theory

As a fun application of some of the theory we've built so far will be to classify isogeny classes of abelian varieties over finite fields. Let's state our theorem, which requires the notion of a "q-Weil number."

Definition 3.47 (Weil numbers)**.** Fix a prime-power q. Then a *q-Weil number* is an algebraic integer π such that $|\sigma(\pi)|^2 = q$ for any embedding $\sigma \colon \mathbb{Q}(\pi) \to \mathbb{C}$. Two q-Weil numbers π and π' are *conjugate*, written $\pi \sim \pi'$, if and only if there is an isomorphism $\mathbb{Q}(\pi) \to \mathbb{Q}(\pi')$ sending $\pi \mapsto \pi'$. (In other words, π and π' have the same minimal polynomial, which is equivalent to π and π' being Galois conjugates.)

Remark 3.48. Let's explain where this notion is coming from. Well, fix an abelian $\mathbb{F}_q$-variety A. Then we know that

$$\mathrm{Frob}_A^\dagger \circ \mathrm{Frob}_A = [q],$$

so $\pi_A \coloneqq \mathrm{Frob}_A$ has that $\mathbb{Q}(\pi_A)$ is semisimple (and hence a field when A is simple), so the Albert classification explaining how to embed this into $\mathbb{C}$ tells us that π_A is a q-Weil number.

Here is our result.

Theorem 3.49 (Honda–Tate)**.** Fix a prime power q. There is a bijection between isogeny classes of simple abelian $\mathbb{F}_q$-variety A and conjugacy classes of q-Weil numbers π given by sending $A \mapsto \mathrm{Frob}_A$.

The injectivity of the map $A \mapsto \mathrm{Frob}_A$ is due to Tate. We will not prove this, but here is the precise statement which Tate proved.

Theorem 3.50 (Tate)**.** Fix a prime power q and a prime ℓ not dividing q. Then the Tate functor T_ℓ is fully faithful.

We already know that T_ℓ is faithful, so the main content is showing that this functor is full. This turns out to be rather difficult, though it is not too far outside the scope of the current course. The main point here is that we will be able to construct morphisms of abelian varieties only by providing morphisms of the Tate modules.

Corollary 3.51. Fix a prime power q and a prime ℓ not dividing q. Then the following are equivalent.

(a) A and B are $\mathbb{F}_q$-isogenous.

(b) $V_\ell A \cong V_\ell B$ (as Galois representations) for some prime ℓ not dividing q.

(c) $V_\ell A \cong V_\ell B$ (as Galois representations) for all primes ℓ not dividing q.

(d) $P_A(t) = P_B(t)$, where the P_A and P_B are the characteristic polynomials of the Frobenius.

Proof. We already know that (a) implies (c) (the isogeny provides the isomorphism of the Tate modules), which implies (b) (with no content), which implies (d) by taking the characteristic polynomial on both sides and seeing that the isomorphism forces them to agree.

We now show the harder implications. To see that (d) implies (c), we note that Frob is semisimple, so having $P_A = P_B$ implies that $V_\ell(A) = V_\ell(B)$, where the equality even preserves the Frobenius action, and this Frobenius action is the same as the total Galois action because we are over a finite field. Explicitly, $P_A = P_B$ implies that Frob_A and Frob_B are conjugate on the Tate module (base-changed to $\overline{\mathbb{Q}}$) because they have the same eigenvalues; this then descends to an isomorphism to $V_\ell A \cong V_\ell B$ preserving Frobenius by Hilbert's theorem 90 by Galois descent for representations. (Namely, any obstruction to descent would be a 1-cocycle in a vanishing cohomology group.)[3]

It remains to show that (c) implies (a), which will follow from Theorem 3.50. Namely, having two isomorphic Galois representations provides inverse maps on the level of Tate modules, which can then be lifted to inverse maps of the abelian varieties (up to multiplication by an integer, which is an isogeny), which is what we wanted. ∎

Remark 3.52. Without much more work, we can upgrade this to state that the following are equivalent.

(a) There is an isogeny of A onto an abelian subvariety of B.

(b) $V_\ell A$ is a Galois sub-representation of $V_\ell B$.

(c) P_A divides P_B.

We now see that the equivalence of (a) and (d) implies that the map sending A to the conjugacy class of q-Weil numbers given by Frob_A will be injective, which is the injectivity required in Theorem 3.49. Let's be more explicit about this: if $\pi_A = \pi_B$, then they have the same minimal polynomial, so one of P_A will have to divide P_B (using the remark), so one of A or B is isogenous to an abelian subvariety of the other, but then simplicity forces full isomorphism.

3.7 April 15

Today we continue discussing Honda–Tate theory.

[3] Here is another argument: $P_A = P_B$ implies that one can explicitly write down what $V_\ell A$ and $V_\ell B$ should be and then show that they are isomorphic.

3.7.1 Building a CM Field

It remains to see the surjectivity of Theorem 3.49. For this, we will start with a q-Weil number π and actually construct an abelian variety A over a number field K with complex multiplication and then reduce it by some $\mathfrak{p} \in V(K)$ (making K large enough to ensure that the reduction is okay). This A will be required to have $A_{\kappa(\mathfrak{p})}$ with the correct q-Weil number. The point is that our proof shows that we can lift any abelian variety over a finite field (up to finite extension) to an abelian variety with complex multiplication!

Remark 3.53. It is in general an interesting question when one can add requirements to our lifting. For example, perhaps we want to avoid passing to the isogeny class or removing the finite extension or with some extra Hodge cycles or endomorphisms.

As such, we need to construct a CM type for our q-Weil number π. Let's begin with building the CM field. It will be helpful to have a better understanding of q-Weil numbers.

Lemma 3.54. Fix a q-Weil number π. Then exactly one of the following is true.

(i) q is a square, and $\pi = \pm\sqrt{q}$, meaning $\mathbb{Q}(\pi) = \mathbb{Q}$.

(ii) q is not a square, and $\pi = \pm\sqrt{q}$, meaning $\mathbb{Q}(\pi)$ is a real quadratic extension of $\mathbb{Q}$.

(iii) $\mathbb{Q}(\pi)$ is CM.

Proof. For (i) and (ii), suppose we have some real embedding $\rho\colon \mathbb{Q}(\pi) \to \mathbb{R}$. Then $\rho(\pi)$ has magnitude $\sqrt{q}$, so $\rho(\pi)$ is one of $\pm\sqrt{q}$. If q is a square, we get (i); if q is not a square, we get (ii).

Otherwise, π is totally imaginary, so we claim that $\mathbb{Q}(\pi)$ is CM. We claim that $\mathbb{Q}(\pi + q/\pi)$ is totally real, but then $\mathbb{Q}(\pi)$ has degree at most 2 over $\mathbb{Q}(\pi + q/\pi)$ while having no real embeddings, so this extension must be quadratic and totally imaginary, which will complete the proof. So to check that $\pi + q/\pi$ is totally real, pick up some embedding $\tau\colon \mathbb{Q}(\pi) \to \mathbb{C}$, and then we see that

$$\tau\left(\pi + \frac{q}{\pi}\right) = \tau(\pi) + \overline{\tau(\pi)}$$

because $|\tau(\pi)|^2 = q$. Now, the above quantity is always real, so we are done. ∎

We now construct our CM field.

Theorem 3.55. Fix a simple abelian $\mathbb{F}_q$-variety A where $\mathbb{F}_q$ has characteristic p. Then set $D \coloneqq \mathrm{End}^0(A)$ and $K \coloneqq Z(D)$ and $d \coloneqq \sqrt{[D : K]}$ and $e \coloneqq [K : \mathbb{Q}]$. Then the following hold.

(a) $K = \mathbb{Q}(\pi_A)$.

(b) $de = 2 \dim A$.

(c) For each place $v \in V(K)$, we have

$$\mathrm{inv}_v(D \otimes_K K_v) = \begin{cases} 1/2 & \text{if } v \text{ is real,} \\ \frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)}[K_v : \mathbb{Q}_p] & \text{if } v \mid p, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We will show (a) and (b) and only sketch (c).

(a) By Theorem 3.50, we know that

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}_{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(V_\ell A) = \mathrm{End}_{\mathbb{Q}(\pi_A)}(V_\ell A).$$

We now apply the double–centralizer theorem [Mil20a, Theorem IV.1.14]. Let's recall the statement: fix a field k. Given a finite-dimensional k-algebra B and some faithful semisimple B-module V, we have

$$Z(Z(B)) = B,$$

where centralizers are taken in $\mathrm{End}_k(V)$.

Applying the theorem to $k \coloneqq \mathbb{Q}_\ell$ and $B \coloneqq \mathbb{Q}(\pi_A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $V \coloneqq V_\ell A$, we see that $Z(B) = D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ because everything commutes with Frobenius, so

$$Z(D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Intersecting everything with D, we are done.

(b) By the Albert classification, we already know that $ed \mid 2 \dim A$, so we only need to show the equality. Note that

$$K \otimes \mathbb{Q}_\ell = K_{v_1} \times \cdots \times K_{v_r}$$

where $v_1, \dots, v_r$ are the places of K above ℓ. Now, $K \otimes \mathbb{Q}_\ell$ acts faithfully on $V_\ell A$, so we can split up $V_\ell A$ into

$$V_1 \oplus \cdots \oplus V_r$$

where K_{v_i} acts on V_i for each i. We now do some careful dimension-counting. Note

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}_K(V_\ell A) = \prod_{i=1}^{r} \mathrm{End}_{K_{v_i}}(V_i),$$

which by computing $\mathbb{Q}_\ell$-dimensions provides

$$d^2 e = \sum_{i=1}^{r} e_i d_i^2,$$

where $e_i \coloneqq [K_{v_i} : \mathbb{Q}_\ell]$ and $d_i \coloneqq \dim_{K_{v_i}} V_i$. Now, we see that

$$(2g)^2 \geq (de)^2 = d^2 e \cdot e = \left(\sum_{i=1}^{r} e_i d_i^2 \right) \left(\sum_{i=1}^{r} e_i \right) \overset{*}{\geq} \left(\sum_{i=1}^{r} e_i d_i \right)^2 = (2g)^2,$$

where we have used Cauchy–Schwartz at $\overset{*}{\geq}$. So our inequalities get upgraded to equalities, so we are okay.

(c) We postpone the case of $v \mid p$ until much later. For finite $v_i \mid \ell$ where ℓ is a rational prime not dividing p, we note that the proof of (b) above tells us that

$$D \otimes_{v_i} K_{v_i} = \mathrm{End}_{K_{v_i}}(V_i) = M_d(K_{v_i}),$$

so our invariant vanishes.

For infinite places v, note that there is nothing to say if v is complex, so we only focus on the real case. Looking at our Albert classification, we note that types I and II cannot occur because $ed = 2g$, and type IV poses no threat because there are no real places anyway. So it remains to run type III, where the Albert classification tells us that $D \otimes \mathbb{R}$ is non-split. ∎

Remark 3.56. By definition, we see that A has complex multiplication. Namely, we are able to find some subfield of D with degree $2 \dim A$, which does provide CM by its technical definition.

Remark 3.57. Using the above, we see that P_A is the minimal polynomial of π_A (which has degree e) to the power of d. But by facts about central simple algebras from class field theory, d is the least common multiple of the local invariants. This enables us to pin down D by global class field theory because we know that it is a division algebra.

Remark 3.58. It is worth noting that our proof of (b) shows that we achieve the equality case in Cauchy–Schwartz, which implies that the dimensions of the $V_\bullet$ must all be equal to each other.

We now begin our construction.

Lemma 3.59. Fix a q-Weil number π. Then there is a division algebra D over $K \coloneqq \mathbb{Q}(\pi)$ such that it satisfies the local conditions of Theorem 3.55(c).

Proof. By the fundamental exact sequence of global class field theory, it suffices to show that the required D exists provided that

$$\sum_v \operatorname{inv}_v(D \otimes_K K_v) = 0.$$

If D is totally real, we leave this for homework. It remains to deal with the case where K is CM. Here, there are no infinite places to worry about, so it remains to study the places over $p = \operatorname{char} \mathbb{F}_q$. Being CM means that $\pi\overline{\pi} = q$ for our complex conjugation automorphism $\bar{\cdot}$. We have two cases for a place v over p.

- If $v \neq \overline{v}$, then pairing off $\operatorname{inv}_v(D \otimes K_v)$ and $\operatorname{inv}_v(D \otimes K_v)$ will sum to zero because

$$\operatorname{ord}_v(\pi) + \operatorname{ord}_v(\overline{\pi}) = \operatorname{ord}_v(q).$$

- If $v = \overline{v}$, then we get $\frac{1}{2}$ times the degree, but the number of cases where $v = \overline{v}$ must be even anyway because our total extension has even degree. So looping over all v, we get

$$\frac{1}{2} \sum_{\substack{v \mid p \\ v = \overline{v}}} [K_v : \mathbb{Q}_p],$$

  but the sum must be even because it is $[K : \mathbb{Q}]$ (which is even) minus the contributions of the degrees from the previous case (which is even by the same sort of pairing with $[K_v : \mathbb{Q}_p] = [K_{\overline{v}} : \mathbb{Q}_p]$), as needed. ∎

3.8 April 17

Today we complete the proof of the surjectivity of Honda–Tate theory.

3.8.1 Finishing Honda–Tate Theory

We continue our construction of the required CM field.

Proposition 3.60. Fix a q-Weil number π, and set $K \coloneqq \mathbb{Q}(\pi)$. Let D be a K-division algebra satisfying the local conditions of Theorem 3.55(c). Then there is a CM field L such that $D \otimes_K L$ splits at all places of L, and $[L : K] = \sqrt{[D : K]}$.

Proof. Once again, we leave the case where K is totally real to homework. As a quick sketch, one takes $L \coloneqq K(\sqrt{-p})$ where $p \coloneqq \operatorname{char} \mathbb{F}_q$.

Otherwise, K is CM with totally real subfield $K^+ \coloneqq \mathbb{Q}(\pi + q/\pi)$. Set $d \coloneqq \sqrt{[D:K]}$ to be our reduced degree. Now, there exists a totally real extension L^+ of K^+ of degree d such that each place v_0 of K^+ above p remains inert in L^+: simply construct an irreducible polynomial (with real roots) which remains irreducible over all our finitely many places, which comes down to some explicit construction. Then $L \coloneqq KL^+$ is CM over L^+ and has the correct degree.

It remains to check that $D \otimes_K L$ splits at all places of L. Note D already splits at all places not above p, so we just need to check that we split at the places above p. Well, for each $w \in V(L)$ above $v \in V(K)$ above p, we see

$$\operatorname{inv}_w(D \otimes_K L) = [L_w : K_v] \operatorname{inv}_v(D),$$

which vanishes because $\operatorname{inv}_v(D)$ vanishes once multiplied by d by some facts of central simply algebras. ∎

Remark 3.61. We quickly recall [Mil20a, Corollary IV.3.7]. Under the assumption $[L:K] = \sqrt{[D:K]}$, then one knows that $D \otimes_K L$ splitting everywhere locally implies splitting globally (by the fundamental exact sequence), which is equivalent to having a K-algebra embedding $L \subseteq D$.

We now produce our abelian variety.

Proposition 3.62. Fix a q-Weil number π, and set $p \coloneqq \operatorname{char} \mathbb{F}_q$ and $K \coloneqq \mathbb{Q}(\pi)$. Then there is an abelian scheme $\mathcal{A}$ over $\mathcal{O}_{K'}$ where K' is a finite extension of $\mathbb{Q}_p$ such that $\mathcal{A}_{K'}$ admits CM by the L constructed in the previous proposition and $\mathcal{A}_\kappa$ (where κ is the residue field) has Frobenius conjugate to π^N for some positive integer N.

Proof. By the complex theory, it is enough to construct the required CM type (L, Φ). Then we can take K' large enough so that $\mathcal{A}$ has good reduction everywhere, and we will use the Shimura–Taniyama formula to check what's going on with the Frobenius. Well, let's recall from Theorem 1.117 that $\Phi \subseteq \operatorname{Hom}(L, \overline{\mathbb{Q}}_p)$, so we define $\Phi_w \coloneqq \Phi \cap H_w$, and we would like

$$\frac{\operatorname{ord}_w(\pi_{\mathcal{A}_\kappa})}{\operatorname{ord}_w(\#\kappa)} \overset{?}{=} \frac{\#\Phi_w}{\#H_w}.$$

To continue, we want the following lemma, which explains why we need π^N in our construction if we are only ever going to use the above condition from Φ.

Lemma 3.63. Fix a Weil q-number π and q'-Weil number π', where $p \coloneqq \operatorname{char} \mathbb{F}_q = \operatorname{char} \mathbb{F}_{q'}$. If K is a field containing $\mathbb{Q}(\pi, \pi')$ and

$$\frac{\operatorname{ord}_w(\pi)}{\operatorname{ord}_w(q)} = \frac{\operatorname{ord}_w(\pi')}{\operatorname{ord}_w(q')}$$

for any place $w \in V(K)$ above p, then $(\pi')^{a'} = \pi^a$ for some positive integers a and a'.

Proof. By taking powers of π and π' (which continue to be Weil numbers), we may assume that $\pi\overline{\pi} = \pi'\overline{\pi'}$, meaning $q = q'$. We now want to show that π/π' is a root of unity (so that they will become equal after taking more powers). But we know that

$$|\tau\pi| = |\tau\pi'|$$

for any embedding $\tau : \mathbb{Q}(\pi) \to \mathbb{C}$, so it will be enough to check that π/π' is an algebraic integer. Well, for any place w not above p, we know that $w(\pi) = w(\pi') = 0$ because $\pi\overline{\pi} = \pi'\overline{\pi'}$ are powers of p. And for any place w of p, the hypothesis tells us that $w(\pi) = w(\pi')$ still. Thus, we are able to conclude that π/π' is an algebraic integer, all of whose archimedean norms are 1, so it is a root of unity. ∎

We now continue with the proof with the above lemma in mind. Let's quickly explain how to construct Φ so that

$$\#\Phi_w \overset{?}{=} H_w \cdot \frac{\operatorname{ord}_w(\pi_{\mathcal{A}_\kappa})}{\operatorname{ord}_w(\#\kappa)} = [L_w : K_v] \cdot [K_v : \mathbb{Q}_p] \cdot \frac{\operatorname{ord}_v(\pi)}{\operatorname{ord}_v(q)}.$$

Note the product of the central and right factors on the rightmost side is $\mathrm{inv}_v(D)$, which we know becomes an integer after multiplying by $[L_w : K_v]$ by construction of L at this place. So we may choose $\Phi_w \subseteq H_w$ somewhat randomly to have the right number of elements. The only extra constraint on Φ is to have $\Phi \sqcup \overline{\Phi}$ to be the full $\mathrm{Hom}(L, \overline{\mathbb{Q}}_p)$, which amounts to requiring

$$\#\Phi_w + \#\Phi_{\overline{w}} \overset{?}{=} \#H_w = \#H_{\overline{w}}$$

after rearranging our chosen Φ_w appropriately. But comparing what we are requiring about $\#\Phi_w$, we see we are asking for $\mathrm{ord}_v(\pi) + \mathrm{ord}_{\overline{v}}(\pi) = \mathrm{ord}_v(q)$, which is true because $\mathrm{ord}_{\overline{v}}(\pi) = \mathrm{ord}_v(\overline{\pi})$.

So in total, we have constructed a special CM type (L, Φ), which produces an abelian variety over some number field with the correct CM type by our Galois descent arguments from much earlier, and then the theory of Néron models provides us with our CM abelian scheme $\mathcal{A}$ with CM type (L, Φ). Then Theorem 1.117 grants

$$\frac{\mathrm{ord}_w(\pi_{\mathcal{A}_\kappa})}{\mathrm{ord}_w(\#\kappa)} = \frac{\#\Phi_w}{\#H_w} = \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)}$$

for any prime $w \in V(L)$ above p, and then the lemma tells us that π is realized up to a power as the Frobenius $\pi_{\mathcal{A}_\kappa}$. Note we can base-change $\mathcal{A}$ a little further in order to replace $\pi_{\mathcal{A}_\kappa}$ with a higher power, so we are done. ∎

We are now ready to prove the surjectivity of Theorem 3.49. Thus far, for our q-Weil number π, we have produced an abelian variety A over a large finite field κ such that $\pi^N = \pi_A$. Note that we must have $\#\kappa = q^N$ because $\pi_A \overline{\pi_A} = |\#\kappa|$. To complete the proof, we use Weil restriction, and we will leave some details to the homework.

Definition 3.64 (Weil restriction)**.** Fix a finite field extension L/K. Given an L-group G, we define the *Weil restriction* $\mathrm{Res}_{L/K} G$ on R-points (for $R \in \mathrm{Alg}_K$) by

$$\mathrm{Res}_{L/K} G(R) \coloneqq G(R \otimes_K L).$$

Remark 3.65. On the homework, we will show that

$$V_\ell(\mathrm{Res}_{L/K} A) \cong \mathrm{Ind}_{\mathrm{Gal}(\overline{K}/K)}^{\mathrm{Gal}(\overline{L}/L)} V_\ell A$$

for any finite extension L/K of fields.

Using the previous remark, we set $B \coloneqq \mathrm{Res}_{\kappa/\mathbb{F}_q} A$ and see that the action of $\mathrm{Frob}_{A,\mathbb{F}_q}^N$ on $\mathrm{Res}_{\kappa/\mathbb{F}_q} A$ is going to be $\mathrm{Frob}_{A,\kappa}$, which then splits up as conjugation by cosets on the induction on each piece of the induction $V_\ell B = \mathrm{Ind}\, V_\ell A$, so we see that $\pi_B^N = \pi_A$ and $P_B(t) = P_A\left(t^N\right)$, meaning π is a root of P_B, so π_B is conjugate to π, completing our surjectivity construction.

What?

3.9 April 19

Today we go back to the main theorem of complex multiplication.

3.9.1 A Little Dieudonné Theory

Recall that the proof of Theorem 3.55 avoided the computation in the case where $v \mid p$. Quickly, let's recall our set-up: let A be a simple abelian k-variety (where k is perfect), and set $D \coloneqq \mathrm{End}^0(A)$.

We might be interested in the "p-divisible group" $A[p^\infty]$, which is the inductive system of groups $A[p^n]$ equipped with the embeddings $A[p^n] \subseteq A\left[p^{n+1}\right]$. Here is our precise definition.

Definition 3.66 (p-divisible group)**.** Fix a prime p and an integer h. A *p-divisible group* is a system of finite group schemes $\{X_n\}_{n\in\mathbb{N}}$ of order p^{nh} equipped with closed embeddings $\iota_n\colon X_n \hookrightarrow X)n+1$ such that $[p]\colon X_{n+1}\to X_n$ factors through $[p]$ as $[p]=\pi_n\circ\iota_{n-1}$, and π_n is faithfully flat.

Do note that we can forget about being faithfully flat if we work over a field.

We now note that Tate's theorem extends to this setting.

Theorem 3.67. Fix abelian $\mathbb{F}_q$-varieties A and B. Then the restriction map

$$\operatorname{Hom}(A,B)\otimes\mathbb{Z}_p\to\operatorname{Hom}(A[p^\infty],B[p^\infty])$$

is an isomorphism.

One concern here is that $A\,[p^\infty]$ does not immediately look like it has any attached linear algebra. Let's remedy this, which is the point of Dieudonné theory; see [CCO14, Appendix A.1] for more details.

Theorem 3.68 (Dieudonné)**.** Fix a perfect field k of characteristic $p>0$, and let $W(k)$ be the Witt ring. Then there is an anti-equivalence of categories sending a p-divisible group to Dieudonné modules, which are free $W(k)$-modules of finite rank with specified action by two endomorphisms F and V satisfying some explicit relations. Explicitly, let $\sigma\colon W(k)\to W(k)$ be the lift of the Frobenius map $k\to k$, and then we require F to be σ-linear, V to be σ^{-1}-linear, and $FV=VF=p$. We label this functor as taking the p-divisible group G to the Dieudonné module $\mathbb{D}(G)$.

Here, F is intended to be a "Frobenius." In our context, we expect $\operatorname{Frob}_A\colon A\to A^{(1)}$, which then will descend to a map on the p-divisible group $A\,[p^\infty]$. Then we know that Frob_A factors through $[p]$ via map $V\colon A^{(1)}\to A$ we call the "Verschiebung."

Remark 3.69. If we want to consider isogeny classes, then we end up inverting p in our Homs, so the conditions $FV=VF=p$ end up fully specifying V; for example, this condition implies that V is σ^{-1}-linear by the linearity of the condition $FV=p$.

As one might expect, our equivalence of categories sends a p-divisible group $\{X_n\}_{n\in\mathbb{N}}$ basically to its crystalline cohomology, in analogy with the Tate module being étale cohomology.

3.9.2 Loose End of Honda–Tate Theory

We now return to the setting of Theorem 3.55. Recall that we have $K:=\mathbb{Q}(\pi)$ equal to $Z(D)$, where $D:=\operatorname{End}^0(A)$. Also, set $W:=W(\mathbb{F}_q)$ for brevity. Now, the equivalence of our categories tells us that

$$D\otimes_{\mathbb{Q}}\mathbb{Q}_p=(\operatorname{End}\mathbb{D}(A[p^\infty]))^{\mathrm{op}}\otimes W[1/p],$$

so the decomposition $K\otimes_{\mathbb{Q}}\mathbb{Q}_p=\prod_{v|p}K_v$ gives rise to a decomposition

$$A[p^\infty]\sim\prod_{v|p}G_v$$

in the isogeny category of p-divisible groups. As such, we get a decomposition of $\mathbb{D}(A[p^\infty])$ as

$$\mathbb{D}(A[p^\infty])\otimes_W W[1/p]=\bigoplus_{v|p}\mathbb{D}(G_v)\otimes_W W[1/p].$$

We now set $D_v:=D\otimes_K K_v$ to be the v-component, which is going to be the endomorphism algebra $(\operatorname{End}\mathbb{D}(G_v))^{\mathrm{op}}\otimes_W W[1/p]$. (Here, endomorphism means that we are taking a $W[1/p]$-linear map compatible with the action by Frobenius.)

There is some way to track through the Frobenius action on everything. Approximately speaking, if $g(t)$ is the minimal polynomial for π_A, then a factorization $g = \prod_{v|p} g_v$ in $\mathbb{Q}_p[T]$ will make π_A act on $\mathbb{D}(A[p^\infty])$ as F^r (with $q = p^r$), and then the polynomials g_v explicate how Frobenius should end up acting on each of the v-components. With some effort, one can compute $\operatorname{inv} D_v$ as

$$\frac{W[1/p][F]}{g_v(F^r)},$$

which yields the correct answer.

Remark 3.70. One can run a similar computation to prove Theorem 1.117 without all of our extra assumptions.

3.9.3 Reduction Step for the Main Theorem

We now begin the proof of Theorem 3.19. We quickly recall the set-up. Fix our abelian variety A over a number field K with complex multiplication by (E, Φ), and we will assume that K contains the reflex field E^*. For some $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/E^*)$, we can reduce this down to the abelianization, so Artin reciprocity grants a unique $s \in \mathbb{A}_{E,f}^\times / E^{*,\times}$ such that

$$\operatorname{Art}_{E^*}(s) = \sigma|_{E^{*,\mathrm{ab}}}.$$

Further, $\eta(\sigma)$ is some finite idéle in $\mathbb{A}_{E,f}^\times$, and we know $\mathrm{N}_\Phi(s) \in \mathbb{A}_{E,f}^\times / E^\times$. We would like to know that these elements agree in the idéle class group.

We begin with some notation.

Notation 3.71. Let K be a number field, and set $T^K := \operatorname{Res}_{K/\mathbb{Q}} \mathbb{G}_m$ to be an algebraic $\mathbb{Q}$-group. Now, for our CM field E, set $F := E^+$. Note that there is a norm map $\mathrm{N}_{E/F} \colon T_E \to T_F$ for any extension of numbers fields E/F, so we go ahead and define

$$T := \mathbb{G}_m \times_{T^F} T^E,$$

where the embedding $\mathbb{G}_m \to T^F$ is given on $\mathbb{Q}$-points by the inclusion $\mathbb{Q}^\times \subseteq F^\times$.

For example, we see that

$$T(\mathbb{Q}) = \mathbb{Q}^\times \times_{F^\times} E^\times = \left\{ a \in E^\times : \mathrm{N}_{E/F}(a) \in \mathbb{Q}^\times \right\}.$$

More generally, for a $\mathbb{Q}$-algebra R, we have

$$T(R) = R^\times \times_{(R \otimes_{\mathbb{Q}} F)^\times} (R \otimes_{\mathbb{Q}} E)^\times = \{ r \in (R \otimes_{\mathbb{Q}} E)^\times : \mathrm{N}_{E/F}(r) \in (R \otimes_{\mathbb{Q}} F)^\times \},$$

so $T(\mathbb{A}_f) = \left\{ a \in \mathbb{A}_{E,F}^\times : \mathrm{N}_{E/F}(a) \in \mathbb{A}_{\mathbb{Q}}^\times \right\}$.

Lemma 3.72. Fix everything as above.

(a) If $T \subseteq T^E$, then $T(\mathbb{A}_f)/T(\mathbb{Q}) \subseteq T^E(\mathbb{A}_f)/T^E(\mathbb{Q})$ is a topological embedding.

(b) The space $T(\mathbb{A}_f)/T(\mathbb{Q})$ is Hausdorff.

The point for (b) is to show that we will be able to compare two elements via open subsets, which we understand in $\mathbb{A}_{E,f}^\times$ already. Importantly, $\mathbb{A}_{E,f}^\times / E^\times$ fails to be Hausdorff because $E^\times$ is dense in $\mathbb{A}_{E,f}^\times$ (even though the embedding $E^\times \to \mathbb{A}_E^\times$ is discrete and cocompact!).

Proof. For (a), the inclusion $T \subseteq T^E$ is defined on the level of algebraic groups, so it is defined using polynomials over $\mathbb{Q}$. Thus, if $x \in T(\mathbb{A}_f)$ goes down to $T^E(\mathbb{Q})$, then we can actually show that $x \in T(\mathbb{Q})$ by some algebra. The rest of the check for (a) is similar.

For (b), we will actually check that $T(\mathbb{Q}) \subseteq T(\mathbb{A}_f)$ is discrete. For this, we need to find an open neighborhood of the identity which intersects $T(\mathbb{A}_f)$ at only finitely many points. Well, $T(\mathbb{Q}) \cap \mathcal{O}_E^\times$ is an open subset of $T(\mathbb{Q})$ in the restricted topology. By the Dirichlet unit theorem, we know that $\mathcal{O}_F^\times$ is a finite-index subgroup of $\mathcal{O}_E^\times$, so we may pass to $T(\mathbb{Q}) \cap \mathcal{O}_F^\times$.

Now, $a \in T(\mathbb{Q}) \cap \mathcal{O}_F^\times$ consists of elements $a \in \mathcal{O}_F^\times$ such that $\mathrm{N}_{E/F}\, a = a^2$, and this value is rational. But then this requires that $a^2 = \pm 1$, so being totally real requires $a^2 = 1$, so we see that $T(\mathbb{Q}) \cap \mathcal{O}_F^\times$ is a finite set. ∎

3.10 April 22

Today we continue discussing the main theorem of complex multiplication.

3.10.1 Continuing the Reduction Step

We continue with the notations and notions from last lecture.

Lemma 3.73. Fix some $\sigma \in \mathrm{Gal}(E^{*,\mathrm{ab}}/E^*)$, and select $s \in \mathbb{A}_{E^*,f}^\times/(E^*)^\times$ so that $\mathrm{Art}(s) = \sigma$. Further, choose an isogeny $\alpha\colon A \to A^\sigma$, and we recall that we have some $\eta\colon \widehat{V}A \to \widehat{V}A$ such that $\widehat{V}\alpha \circ \eta = \widehat{V}\sigma$. Then we claim that

$$\frac{\eta(\sigma)}{\mathrm{N}_\Phi(s)} \in \frac{T(\mathbb{A}_f)}{T(\mathbb{Q})}.$$

The point of this lemma is to reduce everything to the finite setting over $\mathbb{Q}$, allowing us to transition to an ideal-theoretic statement.

Proof. Fix a polarization λ giving rise to the Weil pairing $\psi\colon \widehat{V}(A) \times \widehat{V}(A) \to \mathbb{A}_f(1)$. Then recall from Remark 3.21 that

$$\begin{aligned}
\chi_{\mathrm{cyclo}}(\sigma)\psi(x,y) &= \psi^\sigma(\sigma x, \sigma y) \\
&= \psi^\sigma(\alpha(\eta(x)), \alpha(\eta(y))) \\
&= \psi^\sigma(\alpha x, \alpha y) \\
&= \eta(\sigma)\overline{\eta(\sigma)}\psi^\sigma(\alpha x, \alpha y).
\end{aligned}$$

Now, note that ψ and $\psi^\sigma \circ \alpha^2$ are both Weil pairings compatible with the E-action (by an explicit check: everything in sight commutes with the E-action), so the classification of Riemann forms over $\mathbb{C}$ allows us to say that they are of the form $\mathrm{tr}_{E/\mathbb{Q}}(\xi x \overline{y})$ where ξ is totally negative. The point is that any two Weil pairings will differ by a totally positive element in $F = E^+$, so

$$\eta(\sigma)\overline{\eta(\sigma)} = \chi_{\mathrm{cyclo}}(\sigma)c$$

for some totally positive $c \in F$.

On the other hand, compatibility of global class field theory requires

$$\begin{aligned}
\mathrm{N}_\Phi(s)\overline{\mathrm{N}_\phi(s)} &= \mathrm{Nm}_{\mathbb{A}_{E^\times,f}/\mathbb{A}_f}(s) \\
&= \mathrm{Art}_{\mathbb{Q}}(\sigma|_{\mathbb{Q}^{\mathrm{ab}}}) \\
&= \chi_{\mathrm{cyclo}}(\sigma)
\end{aligned}$$

up to multiplication by $\mathbb{Q}^\times$. Our norm must be positive, so the "multiplication by $\mathbb{Q}^\times$" must upgrade to "multiplication by $\mathbb{Q}^+$."

Why?

Now, define $t := \eta(\sigma)/\mathrm{N}_\Phi(s)$ so that $t\bar{t}$ must be a totally positive element in E^+ too (notably, the cyclotomic character cancels out), so checking the Hasse norm principle allows us to conclude that we have some $e \in E$ such that $e\bar{e} = t\bar{t}$. Then $(t/e)\overline{(t/e)} = 1$, so we are able to conclude $t \pmod{E^\times}$ lives in $T(\mathbb{A}_f)/T(\mathbb{Q})$. ∎

Why?

3.10.2 Ideal-Theoretic Class Field Theory

We are working with CM fields, so we will take our number fields to be totally imaginary.

Definition 3.74 (modulus)**.** Fix a totally imaginary number field K. Then a *modulus* is a formal product of the form

$$\mathfrak{m} \coloneqq \prod_{\mathfrak{p} \in V(K)} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$$

where $\mathfrak{m}(\mathfrak{p}) \geq 0$ always, $\mathfrak{m}(\mathfrak{p}) = 0$ for infinite places, and $\mathfrak{m}(\mathfrak{p}) > 0$ for only finitely many $\mathfrak{p}$.

Here is some more notation we will want to state ideal-theoretic global class field theory.

Definition 3.75 (ray class group)**.** Fix a modulus $\mathfrak{m}$ of a totally imaginary number field K. We let $S(\mathfrak{m}) \coloneqq \{\mathfrak{p} : \mathfrak{m}(\mathfrak{p}) \neq 0\}$ be the *support* of $\mathfrak{m}$, and we define $I^{S(\mathfrak{m})}$ to be the subgroup of fractional ideals freely generated by $S(\mathfrak{m})$. Then we define

$$\mathrm{Cl}_K^{\mathfrak{m}} \coloneqq I^{S(\mathfrak{m})} / K_{\mathfrak{m},1},$$

where $K_{\mathfrak{m},1} \coloneqq \{\alpha \in K^\times : \alpha \equiv 1 \pmod{\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}} \text{ for } \mathfrak{p} \in S(\mathfrak{m})\}$.

Definition 3.76. Fix a modulus $\mathfrak{m}$ of a totally imaginary number field K. Then we define

$$\begin{aligned}
\mathbb{A}_{K,\mathfrak{m}}^\times &\coloneqq \prod_{v \nmid \mathfrak{m}} (K_v^\times, \mathcal{O}_v^\times) \times \prod_{v \mid \mathfrak{m}} \left(1 + \mathfrak{p}_v^{\mathfrak{m}(\mathfrak{p}_v)} \mathcal{O}_v\right), \\
U_{\mathfrak{m}} &\coloneqq \prod_{v \mid \mathfrak{m}} \left(1 + \mathfrak{p}_v^{\mathfrak{m}(\mathfrak{p}_v)} \mathcal{O}_V\right) \times \prod_{v \nmid \mathfrak{m}\infty} \mathcal{O}_v^\times, \\
W_{\mathfrak{m}} &\coloneqq \prod_{\substack{v \nmid \mathfrak{m} \\ v \mid \infty}} K_v^\times U_{\mathfrak{m}}, \\
C_{\mathfrak{m}} &\coloneqq \mathbb{A}_{E,\mathfrak{m}}^\times / K_{\mathfrak{m},1} W_{\mathfrak{m}}.
\end{aligned}$$

Remark 3.77. One can see that the $U_{\mathfrak{m}}$s form an open neighborhood basis of 1 in $\mathbb{A}_{f,E}^\times / E^\times$, so it forms an open neighborhood basis of 1 in $T(\mathbb{A}_f)/T(\mathbb{Q})$ upon intersection. Now, η and N_Φ are both continuous, essentially by their definition, so we are granted a modulus $\mathfrak{m}$ such that N_Φ actors as $\mathrm{Cl}_{E^*}^{\mathfrak{m}} \to C_{\mathfrak{m}}(E)$.

We now state a version of Theorem 3.9 which will help us with our ideal-theoretic main theorem of complex multiplication.

Theorem 3.78. Fix an abelian variety A over $\overline{\mathbb{Q}}$ with CM type (E, Φ). Let E^* be the reflex field, and fix $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$, and choose a nonnegative integer m. We will assume that $\mathrm{End}\, A \cap E = \mathcal{O}_E$. Then the following are true.

(a) There is an ideal $\mathfrak{a}(\sigma) \subseteq \mathcal{O}_E$ and isogeny $\alpha \colon A \to A^\sigma$ such that $\alpha(x) = \sigma(x)$ for $x \in A[m]$ and α is an $\mathfrak{a}(\sigma)$-multiplication. In fact, the ideal class $[\mathfrak{a}(\sigma)]$ in Cl_E^m is uniquely determined by σ.

(b) For sufficiently large modulus $\mathfrak{m}$ of E^*, the class $[\mathfrak{a}(\sigma)]$ only depends on the action σ on the ray class field $L_{\mathfrak{m}}$ of $\mathfrak{m}$, and $[\mathfrak{a}(\sigma)] = [\mathrm{N}_\Phi(\mathfrak{a}^*)]$ where $\mathfrak{a}^* \in C_{\mathfrak{m}}$ corresponds to σ via the reciprocity map $\mathrm{Gal}(L_{\mathfrak{m}}/E) \cong \mathrm{Cl}_E^{\mathfrak{m}}$.

Wait what does $\mathfrak{a}(\sigma)$-multiplication mean?

Definition 3.79. Fix an abelian variety A with complex multiplication by E such that $\mathcal{O}_E \subseteq \operatorname{End} A$. Fix an ideal $\mathfrak{a}$ of $\mathcal{O}_E$. A surjective homomorphism $\lambda\colon A \to B$ is an $\mathfrak{a}$-multiplication if and only if each $a \in \mathfrak{a}$ has the map $a\colon A \to A$ factor through B, and λ is in fact universal with respect to this factoring. (Namely, any other $\lambda'\colon A \to B'$ similarly factoring has a unique map $B' \to B$ commuting with everything in sight.)

Remark 3.80. If E is not a field but instead merely a CM algebra, then we must make $\mathfrak{a}$ into a lattice instead of an ideal.

Remark 3.81. For any lattice $\mathfrak{a} \subseteq E$, there is some (B, λ) satisfying the required universal property. Indeed, simply take $B \coloneqq A/\ker \mathfrak{a}$, where

$$\ker \mathfrak{a} \coloneqq \bigcap_{a \in \mathfrak{a}} \ker a,$$

which we note is actually a finite intersection because $\mathfrak{a}$ is finitely generated.

Remark 3.82. One expects to have $\operatorname{Art}(s) = \sigma$ yielding $\eta(\sigma)$ corresponding to the class $[\mathfrak{a}(\sigma)]^{-1}$, which will be able to provide the required result.

3.11 April 24

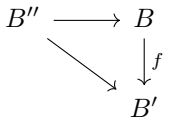
Today we complete the proof of the main theorem of complex multiplication.

3.11.1 More on $\mathfrak{a}$-Multiplication

For our set-up, we have a homomorphism $\lambda\colon A \to B$, where A has CM type (E, Φ). Then let $\mathfrak{a}$ be a lattice in E, and we assume that B is an $\mathfrak{a}$-multiplication. On $\mathbb{C}$, we can think of A as $\mathbb{C}^g/\Phi(\Lambda)$, and then it turns out that

Proposition 3.83. Fix an abelian variety A with CM type (E, Φ). With lattices $\mathfrak{a}, \mathfrak{a}' \subseteq E$, let $\lambda\colon A \to B$ and $\lambda A \to B'$ be an $\mathfrak{a}$-multiplication and an $\mathfrak{a}'$-multiplication, respectively. Then there exists an isogeny $f\colon B \to B'$ such that $\lambda' = f\lambda$ if and only if $\mathfrak{a} \supseteq \mathfrak{a}'$.

Proof. If $\mathfrak{a} \supseteq \mathfrak{a}'$, one can build f via the universal property of $\mathfrak{a}$-multiplication. For the converse, we want to show that $\mathfrak{a} = \mathfrak{a} + \mathfrak{a}'$. Let $\lambda'' \to A \to B''$ be an $(\mathfrak{a} + \mathfrak{a}')$-multiplication so that the universal properties everywhere induce maps as follows.



Thus,

$$\frac{\ker \mathfrak{a}}{\ker(\mathfrak{a} + \mathfrak{a}')} = \ker(B'' \to B) \subseteq \ker(B'' \to B) = \frac{\ker \mathfrak{a}'}{\ker(\mathfrak{a} + \mathfrak{a}')}.$$

Because $\ker \mathfrak{a} \cap \ker \mathfrak{a}' = \ker(\mathfrak{a} + \mathfrak{a}'')$, we see from the above computation that $B'' \to B$ is injective, so $\mathfrak{a} + \mathfrak{a}' = \mathfrak{a}$, as required. ∎

Proposition 3.84. Fix an abelian variety A with CM type (E,Φ). With lattices $\mathfrak{a},\mathfrak{a}'\subseteq E$, let $\lambda\colon A\to A'$ and $\lambda A'\to A''$ be an $\mathfrak{a}$-multiplication and an $\mathfrak{a}'$-multiplication, respectively. Then $\lambda'\lambda\colon A\to A''$ is an $\mathfrak{a}\mathfrak{a}'$-multiplication.

Proof. One can just use the explicit construction of our $\mathfrak{a}$-multiplications. For example, one can note that $A'=A/\ker\mathfrak{a}=A\otimes_{\mathcal{O}_E}\mathfrak{a}^{-1}$ and then iterate this tensor product. ∎

Proposition 3.85. Fix an abelian variety A with CM type (E,Φ). With lattice $\mathfrak{a}\subseteq\mathcal{O}_E$, let $\lambda\colon A\to A'$ be an $\mathfrak{a}$-multiplication. Then $\deg\lambda=[\mathcal{O}_E:\mathfrak{a}]$.

Proof. Over $\mathbb{C}$, write $A=\mathbb{C}^g/\Lambda$, so $\deg\lambda=\left[\mathfrak{a}^{-1}\Lambda:\Lambda\right]=[\mathcal{O}_E:\mathfrak{a}]$ immediately.

We now work over an arbitrary field. If $\mathfrak{a}=(a)$ is principal with integral generator, then $[a]\colon A\to A$ is the required a-multiplication, which has the correct degree. In general, by using the previous proposition, we can find λ' so that $\lambda'\lambda=[\alpha]$ for $\alpha\in\mathcal{O}_E$, and we can further require that λ' and λ have coprime degree, and now we can finish. ∎

Proposition 3.86. Fix abelian $\overline{\mathbb{Q}}$-varieties A and B with CM by E, and assume $\mathcal{O}_E\subseteq\operatorname{End}A$ and $\mathcal{O}_E\subseteq\operatorname{End}B$. If there is an isogeny $f\colon A\to B$ preserving the E-action, then there is a lattice $\mathfrak{a}\subseteq E$ and isogeny $\lambda\colon A\to B$ which is an $\mathfrak{a}$-multiplication.

Proof. By Galois descent, we'll be able to work over $\mathbb{C}$. Then $A(\mathbb{C})=\mathbb{C}^g/\Phi(\mathfrak{b}_1)$ and $B(\mathbb{C})=\mathbb{C}^g/\Phi(\mathfrak{b}_2)$ for fractional ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$, where (E,Φ) is the CM type. (The existence of the isogeny basically allows us to assume that A and B have the same CM type, which is why we used the same Φ.) Then the point is that we can adjust our two abelian varieties up to isogeny to make our projection into a $\mathfrak{b}_1\mathfrak{b}_2^{-1}$-multiplication. ∎

We are now ready to prove Theorem 3.78.

Proof. We begin with the proof of (a). By Proposition 3.86, we can an isogeny $\lambda\colon A\to A^\sigma$ compatible with the E-action which is an $\mathfrak{a}$-multiplication, where $\mathfrak{a}\subseteq\mathcal{O}_E$ is some ideal. By Proposition 3.85, we see that $\deg f=[\mathcal{O}_E:\mathfrak{a}]$.

Now, looking at our integer m, we may select some $a\in E^\times$ such that $a\mathfrak{a}\subseteq\mathcal{O}_E$ and $[\mathcal{O}_E:a\mathfrak{a}]$ is coprime to m; this is basically done by looking at the prime factorization of m and of $\mathfrak{a}$ and "fixing" the prime factorization to avoid the various primes. Replacing λ by $a\lambda$ and $\mathfrak{a}$ by $a\mathfrak{a}$, we now know that $\lambda\colon A\to\mathfrak{A}^\sigma$ is still an $\mathfrak{a}$-multipication, but now it has degree coprime to m.

The point is that $\lambda\colon A[m]\to A^\sigma[m]$ factors through $[\deg f]_A$, which is an isomorphism on m-torsion, so f is an isomorphism on m-torsion. Because $\sigma\colon A[m]\to A^\sigma[m]$ is also an isomorphism, and everything is compatible with the E-action, we are granted $\beta\in\mathcal{O}_E$ such that

Why?

$$\beta\equiv f^{-1}\circ\sigma\pmod m.$$

As such, we finally define $\alpha\colon A\to A^\sigma$ as $f\circ\beta$ so that $\alpha|_{A[m]}=\sigma|_{A[m]}$, and we know α is now an $\mathfrak{a}(\sigma)$-multiplication for some ideal $\mathfrak{a}(\sigma)$. Looking at our construction, f is unique up to an element of $E^\times$, and because we are only looking at m-torsion, we only get uniqueness up to $E_{m,1}$. So $[\mathfrak{a}(\sigma)]$ is really an ideal class in $I^{S(\mathfrak{m})}/E_{m,1}$, which is Cl_E^m, as required.

What?

We now turn to (b). Suppose $\alpha\colon A\to A^\sigma$ is an $\mathfrak{a}(\sigma)$-multiplication, and $\alpha'\colon A\to A^{\sigma'}$ is an $\mathfrak{a}(\sigma')$-multiplication. Then $(\alpha')^\sigma\alpha\colon A\to A^{\sigma\sigma'}$ is an $\mathfrak{a}(\sigma)\mathfrak{a}(\sigma')$-multiplication by Proposition 3.84, so we have produced a group homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/E^\times)\to\mathrm{Cl}_E^m$$

given by $\sigma\mapsto[\mathfrak{a}(\sigma)]$. By continuity, this must factor through some $\mathrm{Gal}(L_{\mathfrak{m}}/E^*)$ for sufficiently large $\mathfrak{m}$ (as restriction), so (b) follows. ∎

3.12 April 26

Today we complete the proof, for real this time.

3.12.1 Completing the Proof

We are going to combine the Shimura–Taniyama formula with Theorem 3.78 to conclude our proof. Fix an abelian variety A over a number field K with CM type (E, Φ), and suppose that K is Galois and contains all Galois conjugates of E. Fix a prime p, and let $\mathfrak{p}$ be a prime of E^* above p, and let $\mathfrak{P}$ be a prime of K above $\mathfrak{p}$. We will further assume that $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified and that $\mathcal{O}_E \subseteq \operatorname{End} A$.

Corollary 3.87. Fix everything as above.

(a) There exists an $\mathfrak{a}$-multiplication $\alpha\colon A \to A^\sigma$ (defined over a finite extension of K) where $\sigma \in \operatorname{Gal}(K/E^*)$ reduces to the Frobenius automorphism of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$.

(b) In fact, $\mathfrak{a} = \mathrm{N}_\Phi(\mathfrak{p})$.

Proof. From Theorem 3.78, we get some $f\colon A \to A^\sigma$ which is a $\mathfrak{b}$-multiplication, so the same is true after passing to the reductions A_0 and A_0^σ over $\kappa(\mathfrak{P})$, for example by considering the construction of $\mathfrak{b}$-multiplications as a tensor product. Now, because we have $\mathfrak{b}$-multiplications, we see

$$\operatorname{Hom}_E(A, A^\sigma) = \mathfrak{b}^{-1} = \mathfrak{b}^{-1} = \operatorname{Hom}_E(A, A^\sigma),$$

so our Frobenius $A_0 \to A_0^\sigma$ lifts to $\alpha\colon A \to A^\sigma$ (where we are implicitly using the Néron mapping property).

Now, for (b), the point is that we will be able to take powers to recover the Frobenius. Namely, we know from Theorem 1.117 that there is $\pi \in \mathcal{O}_E$ which is a lift of the endomorphism $x \mapsto x^{\#\kappa(\mathfrak{P})}$ on the reduction A_0. Now, we know that (π) is $\mathrm{N}_{K,\Phi}(\mathfrak{P})$ be a valuation computation (and everything in sight being unramified). Continuing, we compute

$$\mathrm{N}_{K,\Phi}(\mathfrak{P}) = \mathrm{N}_\Phi\left(\mathrm{N}_{K/E^*}\mathfrak{P}\right) = \mathrm{N}_\Phi(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}.$$

Now, we note that we can write $\pi = \alpha \cdot \sigma\alpha \cdots \sigma^{f(\mathfrak{P}/\mathfrak{p})-1}\alpha$, where σ is the relative $\#\kappa(\mathfrak{p})$-power Frobenius, but this twisting does not adjust which ideal we are going to live in, so $(\pi) = \mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})}$. The equality in (b) follows. ∎

We now show the main theorem. Reciprocity tells us that σ corresponding to the Frobenius element corresponds to $\mathfrak{p} \in \mathrm{Cl}^{\mathfrak{m}}(E^*)$. Thus, the above result shows the result for all Frobenius corresponding to $\mathfrak{p}$ in the case where $\mathfrak{p}$ is unramified in K/E^* and where $\mathfrak{p}$ is unramified in $E^*/\mathbb{Q}$. However, such $\mathfrak{p}$ have their Frobenius elements are dense in the Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/E^*)$, so we are okay because everything in sight is continuous.

Remark 3.88. To recover the adélic statement, one finds that $\eta(\sigma)$ in $\mathrm{Cl}^{\mathfrak{m}}(E^*)$ is $\mathfrak{a}(\sigma)^{-1}$ by unwinding the definition of the corresponding $\alpha\colon A \to A^\sigma$ in the adélic language.

3.12.2 A Little on the André–Oort Conjecture

Here is our result.

Theorem 3.89. Fix an irreducible polynomial $P \in \mathbb{C}[j, j']$. If P uses both variables, and P is not divisible by P_N (which is the defining equation for the subscheme $Y_0(N) \subseteq \mathbb{A}^1 \times \mathbb{A}^1$ of pairs (E_1, E_2) for which there is a cyclic N-isogeny $E_1 \to E_2$), then there are only finitely many pairs (j_n, j_n') corresponding to points with complex multiplication such that $P(j_n, j_n') = 0$.

Geometrically, we should imagine P as cutting out an irreducible curve in $\mathbb{A}^2$, which is being viewed as a coarse moduli space for elliptic curves. Essentially, we are saying that if $C(\mathbb{C})$ has infinitely many CM points, then either C is $X_0(N)$, vertical, or horizontal.

Remark 3.90. The André–Oort conjecture is about this story for general Shimura variety, which was recently proved.

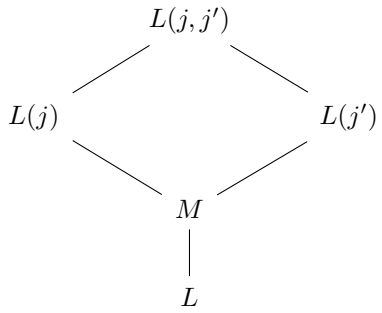
Anyway, here is our proof.

Proof. Suppose for the sake of contradiction that we have an infinite sequence of points (j_n, j_n') on which P vanishes.

1. We reduce to the case where P has rational coefficients, and P is irreducible over $\mathbb{Q}$. Well, the points (j_n, j_n') all live in $\overline{\mathbb{Q}}$ because these points have complex multiplication, so P being irreducible with all these roots requires P to have coefficients in $\overline{\mathbb{Q}}$. However, P has only finitely many coefficients, so say they live in a number field F. By replacing P with an irreducible factor of
$$\prod_{\sigma\colon F\to\overline{\mathbb{Q}}} \sigma(P) \in \mathbb{Q}[j, j']$$
divisible by P, we maintain all of our roots but now live in our reduced case.

2. We set some notation. Let E_n and E_n' be the elliptic curves with j-invariant j_n and j_n'. Then we set $\mathcal{O}_n \coloneqq \operatorname{End}((E_n)_{\overline{\mathbb{Q}}})$ and $K_n \coloneqq \operatorname{Frac}\mathcal{O}_n$ and $d_n \coloneqq \operatorname{disc} K_n$ and $D_n \coloneqq \operatorname{disc} D_n$, which is $f_n^2 d_n$ for some f_n. We also set $h_n \coloneqq \#\operatorname{Cl}\mathcal{O}_n$.

   Now, for n very large, we claim that $K_n = K_n'$ and D_n'/D_n lives in some finite set. We will basically show that there are not so many possibilities with $K_n \neq K_n'$, so for the moment, we drop the n from our notation. Set $L \coloneqq KK'$ and $M \coloneqq L(j) \cap L(j')$. Then we have the following tower of fields.



   Now, the degrees in the square are all bounded in degree by P, but the degree of $L(j)/L$ by some explicit class field theory is either h or $h/2$. All of this is able to imply that D and D' are all bounded, which proves our claim. Namely, h is proportional to $\sqrt{D}$ by the Brauer–Siegel theorem, but Gauss genus theory tells us that the 2-torsion of the class group is 2 to the power of the number of primes dividing D. As such, one can relate $h(\mathcal{O})$ to $h(\mathcal{O}_K)$ to achieve the bounding.

   From here, we are able to take $K = K'$ or the remainder of our argument. It remains to bound D'/D. Well, on one hand, $[K(j, j') : K(j')]$ is bounded above by $\deg P$, but on the other hand, it is bounded above by
$$\frac{\operatorname{lcm}(f, f')}{f} \prod_{p \mid \operatorname{lcm}(f,f')/f} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right)$$
   where f and f' are chosen so that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ and $\mathcal{O}' = \mathbb{Z} + f'\mathcal{O}_{K'}$. This tells us that f/f' is bounded, so we are done.

3. For the remainder of our proof, we will assume that all the $K_\bullet$s and $K'_\bullet$s are all the same. We go ahead and throw out j-invariants in the same Galois orbit. Now, we define the notation $E_n \coloneqq \mathbb{C}/\mathcal{O}_n$ with $\tau_n \coloneqq \frac{1}{2}(D_n + \sqrt{D_n})$. In particular, one can show that $\log|j_n| \approx \operatorname{Im}\tau_n \approx |D_n|^{1/2}$.

   Now, we claim that $j'_n \to \infty$ as $n \to \infty$. Well, we choose a fundamental domain $\mathcal{F}$, which is compact, so the τ_ns must converge somewhere if they are unbounded. But then one can show

$$|D_n|^{1/2} \sim \log|j_n| \sim -\log|j'_n - j'_\infty| \ll \mathcal{O}(\log|D'_n|),$$

   which is a problem.

4. To complete the proof, one passes to a subsequence to get inside $Y_0(N)$. ■

BIBLIOGRAPHY

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[Lan83] Serge Lang. *Complex multiplication*. Vol. 255. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1983, pp. viii+184. ISBN: 0-387-90786-6. DOI: 10.1007/978-1-4612-5485-0. URL: https://doi-org.libproxy.berkeley.edu/10.1007/978-1-4612-5485-0.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1990, pp. x+325. ISBN: 3-540-50587-3. DOI: 10.1007/978-3-642-51438-8. URL: https://doi-org.libproxy.berkeley.edu/10.1007/978-3-642-51438-8.

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

[Mum08] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, 2008, pp. xii+263. ISBN: 978-81-85931-86-9; 81-85931-86-0.

[CCO14] Ching-Li Chai, Brian Conrad, and Frans Oort. *Complex multiplication and lifting problems*. Vol. 195. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2014, pp. x+387. ISBN: 978-1-4704-1014-8. DOI: 10.1090/surv/195. URL: https://doi-org.libproxy.berkeley.edu/10.1090/surv/195.

[CP14] François Charles and Bjorn Poonen. "Bertini irreducibility theorems over finite fields". In: *Journal of the American Mathematical Society* 29.1 (Oct. 2014), pp. 81–94. ISSN: 1088-6834. DOI: 10.1090/s0894-0347-2014-00820-1. URL: http://dx.doi.org/10.1090/S0894-0347-2014-00820-1.

[Con15] Brian Conrad. *Abelian Varieties*. 2015. URL: https://virtualmath1.stanford.edu/~conrad/249CS15Page/handouts/abvarnotes.pdf.

[Kle16] Felix Klein. *Elementary Mathematics from a Higher Standpoint*. Trans. by Gert Schubring. Vol. II. Springer Berlin, Heidelberg, 2016.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

[Mil17] J. S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2017.

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

[Mil20a] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[Mil20b] James S. Milne. *Complex Multiplication (v0.10)*. Available at www.jmilne.org/math/. 2020.

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

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

List of Definitions