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 $J \colon V \to V$ 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 $J \colon V \to V$ 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:

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

- Identity:

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

- 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 [Mil20, 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 $\exp\colon W \to B$. (Namely, the kernel of $\exp\colon W \to A$ 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 [Mil20, 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

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

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 $i\colon E \to \mathrm{End}^0(A)$. 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

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

and in fact E acts on $\mathrm{Lie}\, A(\mathbb{C})$. Decomposing $\mathrm{Lie}\, A(\mathbb{C})$ as an E-representation as $\bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$ where $\Phi \subseteq \mathrm{Hom}(E, \mathbb{C})$. (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 $\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \overline{\Phi}$ 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 $\mathrm{Lie}\, A(\mathbb{C})$ and parts coming from $\overline{\mathrm{Lie}(A(\mathbb{C}))}$. Irreducible components in $\mathrm{Lie}\, A(\mathbb{C})$ are $\bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$, and irreducible components in $\overline{\mathrm{Lie}(A(\mathbb{C}))}$ are then $\bigoplus_{\varphi \in \Phi} \mathbb{C}_{c\varphi}$, and in total everything must sum up to a faithful module over $E \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{\varphi \in \mathrm{Hom}(E,\mathbb{C})} \mathbb{C}_\varphi$ of rank 1, so we see $\Phi \sqcup c\Phi = \mathrm{Hom}(E, \mathbb{C})$, 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 [Mil20, 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 [Mil20, 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

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

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 ([Mil20, 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.

(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 $\alpha = \mathrm{id}_E$. ∎

Coherence of Lie?

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. Fix geometrically integral k-varieties X, Y, and Z. Further, assume X and Y are proper. 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 will prove Theorem 2.7 next lecture. For now, let's see how this is used.

Corollary 2.8. 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 2.9. Of course, an induction can extend past three projections.

In particular, we will use Corollary 2.8 in order to compute $[n]^*\mathcal{L}$.

Corollary 2.10. 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 2.8 for the inductive step. Namely, $n = 0$ and $n = -1$ have no content, and then one can induct upwards and downwards from there. ■

Remark 2.11. The quadratic relation here is what is used in the construction of the Néron–Tate height.

BIBLIOGRAPHY

[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.

[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. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, pp. xii+263. ISBN: 978-81-85931-86-9; 81-85931-86-0.

[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.

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

[Mil20] James S. Milne. *Complex Multiplication (v0.10)*. Available at www.jmilne.org/math/. 2020.

List of Definitions