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.

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 1.1 (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 1.2. One can replace "proper" with "projective" here without tears.

Example 1.3. 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 1.4 (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 1.5. 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 1.6. 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 1.7. 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 1.8 (abelian variety)**.** An *abelian variety* is a $\mathbb{C}$-variety A which is a complex torus satisfying one of the equivalent conditions of Theorem 1.6. 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 1.9. It turns out that there is a unique algebraic structure on the variety, so there is no worry about this being vague.

Theorem 1.6 involves Hermitian forms, so we will want to get a better handle on these.

Lemma 1.10. 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 1.11. 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 1.10 is that we are allowed to only pay attention to the imaginary part. It is worth having a name for this.

Definition 1.12 (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 $\psi_{\mathbb{R}}\colon V \times V \to \mathbb{R}$ produces a positive-definite Hermitian form via the construction of Lemma 1.10.

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 1.13. 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 $E^+ := E^c$; 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 1.14. 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 1.15 (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 1.13. We call the involution $c\colon E \to E$ the *complex conjugation* of E.

Remark 1.16. The field E need not be Galois.

Remark 1.17. 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 1.18. 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 1.19. 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 1.18, 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 1.14. 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 1.20 (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 1.21. 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 1.22. Fix a CM pair (E, Φ), and set $n \coloneqq \frac{1}{2}[E : \mathbb{Q}]$. Then set $\Lambda \coloneqq \mathcal{O}_E$, and use Φ to produce an embedding $\mathcal{O}_E \to \mathbb{C}^\Phi$ by $\alpha \mapsto (\sigma(\alpha))_{\sigma \in \Phi}$. Then $\mathbb{C}^\Phi / \mathcal{O}_E$ is a complex torus, and it will turn out to be an abelian variety.

Proof. Quickly, we show that $\mathcal{O}_E$ is a lattice of full rank in $\mathbb{C}^\Phi$. Fix an integral basis $\{\alpha_1, \dots, \alpha_{2n}\}$ of $\mathcal{O}_E$. 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 $\sigma_{n+i} \coloneqq \overline{\sigma_i}$ 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 1.10. We will choose $\xi \in \mathcal{O}_E$ judiciously and then set

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

For concreteness, we go ahead and embed E into $\mathbb{C}$ so that c is literally complex conjugation by Remark 1.14. As such, we will write $c(y)$ as $\overline{y}$. Now, to choose ξ, we note that a weak approximation argument grants $\xi_0 \in \mathcal{O}_E$ such that $\operatorname{Im}\sigma(\xi_0) > 0$ for each $\sigma \in \Phi$. 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

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

  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 1.23. 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 1.24 (group scheme)**.** Fix a base scheme S. Then a *group S-scheme* is a group object G in the category Sch_S of S-schemes. In other words, there exist S-morphisms $m\colon G \times_S G \to G$ (for multiplication) and $i\colon G \to G$ (for inversion) and $e\colon S \to G$ (for identity) making the following diagrams commute.

- Associativity:

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

- Identity:

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

- 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 1.25. 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 1.26 (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 1.27. 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 1.28 (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 1.29. One can even replace "k-variety" with "k-scheme" because being smooth over a scheme implies being regular, which implies reduced.

Remark 1.30. It turns out that being geometrically integral is equivalent to being connected, by some argument involving the connected component.

Remark 1.31. 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 1.32 (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 1.33. Here, smoothness can be verified by something like a Jacobian criterion, analogous to smoothness for embedded manifolds.

Remark 1.34. 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 1.8: 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 1.36. From there, being algebraic does imply one of the equivalent conditions of Theorem 1.6, and the converse is similar.

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

Proposition 1.35. 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 1.36. 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 1.37. 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 1.38. 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 1.39 (isogenies)**.** Fix abelian k-varieties A and B. A k-morphism $f\colon A \to B$ is a surjective homomorphism with finite kernel.

Example 1.40. 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 1.37. 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 1.41. 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 1.38, 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 1.35: 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 1.42. 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 1.43 (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 1.44. 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 1.41. 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 $\widetilde{\psi}'_0 := \operatorname{adj}\widetilde{\varphi}'_0$ 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 1.41 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 1.45. Being an equivalence relation, and in particular part (b) in Lemma 1.44, 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.

We can decompose abelian varieties based on their isogeny class.

Theorem 1.46 (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]. Read the proof for homework, and 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 1.47 (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 1.48. It is possible to have an abelian variety be simple over k but not over $\overline{k}$.

Corollary 1.49. 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 1.46, 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 1.46 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. ∎

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

Definition 1.50. 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

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

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 1.49 to compute it.

Corollary 1.51. 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 1.44. 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 1.52. 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 1.53. 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 1.44. 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 1.54. 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 1.52. In the event $A_i \sim B_j$, we can replace B_j by A_i by Corollary 1.53. ∎

Remark 1.55. Taking $A_i = B_j$ and $r_i = s_j$ in Corollary 1.54 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 1.56. 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 1.54 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 1.49 is unique up to permutation and isogeny.

1.3.2 Complex Multiplication

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

Definition 1.57 (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 1.58. It will turn out that this definition holds true for all abelian varieties over finite fields.

Remark 1.59. 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 1.41. 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 1.60. 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 1.61. 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 1.41 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 1.62. 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 1.63. 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.

Let's now specialize more directly to $\mathbb{C}$. We pick up the following definition.

Definition 1.64 (CM type)**.** Fix a CM field E, and let (A, i) be an abelian variety with complex multiplication by E. 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 $\Phi \subseteq \mathrm{Hom}(E, \mathbb{C})$. Then Φ is the CM type.

BIBLIOGRAPHY

[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