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
INTRODUCTION

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 $H\colon V \times V \to \mathbb{C}$ to its imaginary part $\psi := \operatorname{im} H$. Then we have a map $\psi\colon V \times V \to \mathbb{R}$, 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., $\psi(iv,v)\ge 0$ 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 $\sigma\ne\overline{\sigma}$, but $\sigma|_{E^+}=\overline{\sigma}|_{E^+}$ because E^+ is totally real, so we must then have $\sigma(\alpha)\ne\overline{\sigma(\alpha)}$. 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 $c \in \operatorname{Gal}(E^+/E)$ by $c(\alpha) := -\alpha$. 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 $E_1, \ldots, E_n \subseteq \overline{\mathbb{Q}}$. Then the composite field $E_1 \cdots E_n$ is CM.

Proof. By induction, we may take $n = 2$; define $E := E_1E_2$ 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
$$c(\alpha) := \sum_{i=1}^d c_1(a_{1i})c_2(a_{2i}).$$
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 $\sigma_1, \ldots, \sigma_n \colon E \to \mathbb{C}$ 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

$$c_\sigma(\sigma(\alpha)) := \sigma(c(\alpha)).$$

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 $\Phi \subseteq \operatorname{Hom}(E, \mathbb{C})$ such that

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

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 $n := \frac{1}{2}[E : \mathbb{Q}]$. Then set $\Lambda := \mathcal{O}_E$, 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 $\{\alpha_1, \ldots, \alpha_{2n}\}$ 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 $\Phi = \{\sigma_1, \ldots, \sigma_n\}$ and then $\sigma_{n+i} := \overline{\sigma_i}$ for $i \in \{1, \ldots, n\}$.) 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

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

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:

$$\begin{tikzcd} G\times_S G\times_S G \arrow[r, "m\times\mathrm{id}_G"] \arrow[d, "\mathrm{id}_G\times m"'] & G\times_S G \arrow[d, "m"] \\ G\times_S G \arrow[r, "m"] & G \end{tikzcd}$$

- Identity:

$$\begin{tikzcd} & G\times_S S \arrow[r, "\mathrm{id}_G\times e"] & G\times_S G \arrow[dr, "m"] & \\ G \arrow[ur] \arrow[rrr, equal] \arrow[dr] & & & G \\ & S\times_S G \arrow[r, "e\times\mathrm{id}_G"] & G\times_S G \arrow[ur, "m"'] & \end{tikzcd}$$

- Inversion:

$$\begin{tikzcd} & G\times_S G \arrow[dr, "m"] & \\ G \arrow[ur, "\mathrm{id}_G\times i"] \arrow[r] \arrow[dr, "i\times\mathrm{id}_G"'] & S \arrow[r, "e"] & G \\ & G\times_S G \arrow[ur, "m"'] & \end{tikzcd}$$

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 over $k = \mathbb{C}$. Consider the tangent space at the identity $e \in A$, which we will label T_eA. 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

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

but $A(\mathbb{C})$ is compact, and $\mathrm{GL}(T_eA)$ is an open submanifold, so the above map must be constant. Noting that $de_x = \mathrm{id}_{T_eA}$, we see that actually $dc_x = \mathrm{id}_{T_eA}$, which implies that c_x must be the identity, so the group law is commutative. ■

Remark 1.36. Continuing, there is 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. ∎

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, so $\pi_1(A(\mathbb{C})) \cong \Lambda$, from which the rest of the isomorphisms follow quickly. ∎

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.

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 $\Lambda \to \Lambda'$.

Sketch. The backward map is clear. For the forward map, note that a holomorphic map $V/\Lambda \to V'/\Lambda'$, lift to the universal cover to produce a holomorphic map $V \to V'$. To show that this map is linear, one shows that the derivative is constant, which follows from the compactness. ∎

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.

Bibliography

[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.

List of Definitions