Field of Definition of Abelian Surfaces with Maximal Picard Rank

Sophia Hou

MIT PRIMES

October 18 2025

Big Picture

- **Elliptic curves:** curves where we can add points!
- **Minimal field of definition of elliptic curve:** studied through their j-invariant, which tells us the smallest field where they can be defined.
- **Abelian surfaces:** a two-dimensional version of elliptic curves.
- Our question: *What is the smallest field of definition for these surfaces when they have the richest possible algebraic structure (maximal Picard rank)?*
- This connects classical ideas (elliptic curves, lattices, j-invariant) with modern research in algebraic geometry and number theory.

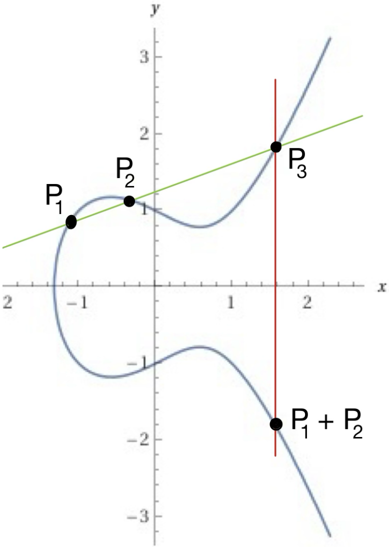
Roadmap

What is an elliptic curve?

- A (complex) **elliptic curve** is a special kind of curve,
- given with this kind of equation:

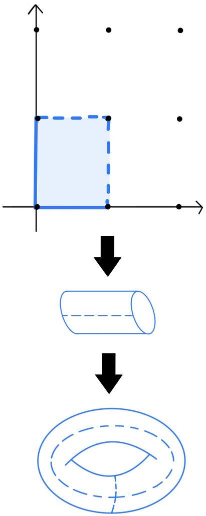
$$y^2 = x^3 + ax + b, \qquad \Delta = -16(4a^3 + 27b^2) \neq 0.$$

  where a, b are complex numbers
- We can add points!



Why do we call an elliptic curve a *complex torus*?

- A **lattice** is $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ with $\omega_2/\omega_1 \notin \mathbb{R}$.
- **Riemann's theorem (dim 1):** every complex torus $\mathbb{C}/\Lambda$ is an elliptic curve, and conversely every elliptic curve over $\mathbb{C}$ is isomorphic to some $\mathbb{C}/\Lambda$.



j-invariant of an elliptic curve

- Any elliptic curve E over $\mathbb{C}$ can be written as

$$E : y^2 = x^3 + ax + b, \quad \text{with } 4a^3 + 27b^2 \neq 0.$$

- The j-**invariant** uniquely determines its isomorphism class over $\mathbb{C}$:

$$j(E) = 1728\,\frac{4a^3}{4a^3 + 27b^2}.$$

Example

For

$$E : y^2 = x^3 - 2x + 1,$$

we have $a = -2$, $b = 1$, so

$$j(E) = 1728 \cdot \frac{4(-2)^3}{4(-2)^3 + 27(1)^2} = 1728 \cdot \frac{-32}{-5} = \frac{55296}{5}.$$

Minimal field of definition

- Any complex elliptic curve $E/\mathbb{C}$ is isomorphic to

$$E' : y^2 = x^3 + \frac{3j(E)}{1728 - j(E)}x + \frac{2j(E)}{1728 - j(E)}.$$

- The **minimal field of definition** of E is $\mathbb{Q}(j(E))$.

Example

For $E : y^2 = x^3 - 2x + 1$, we found $j(E) = \frac{55296}{5} \in \mathbb{Q}$. Therefore E can be defined over $\mathbb{Q}$ itself.
If $j(E)$ were an algebraic irrational (e.g. for CM curves like $j = 76771008 + 44330496\sqrt{3}$) the minimal field would be $\mathbb{Q}(j(E))$.

From curves to surfaces: what changes?

- In dimension 1, the j-invariant controls the minimal field of definition.
- In dimension 2, harder to describe the minimal field of definition for a general abelian surface
- However, **Picard-max** "very algebraic" abelian surfaces A become *products of CM elliptic curves*:

$$A \cong E_1 \times E_2, \qquad E_1 \sim E_2, \ \mathrm{End}(E_i) \text{ orders in an imaginary quadratic field.}$$

- Our Question: **what is the minimal field of definition of A (or its isomorphism class)**?
  $\Rightarrow$ This is the focus of the rest of the talk.

Roadmap

Elliptic Curves as Complex Lattices

- Every elliptic curve $E/\mathbb{C}$ can be viewed as a complex torus:

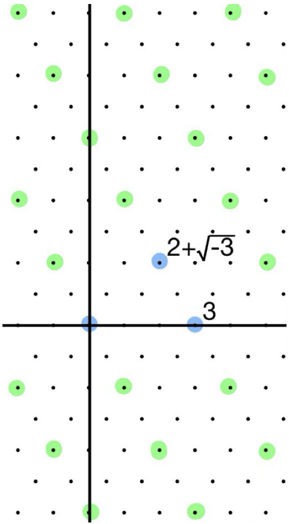
$$E = \mathbb{C}/\Lambda, \quad \Lambda = \langle \omega_1, \omega_2 \rangle.$$

- **Isogeny:**

$$E_1 = \mathbb{C}/\Lambda_1, E_2 = \mathbb{C}/\Lambda_2 \text{ are isogenous } \iff \text{ there exists } \alpha \in \mathbb{C} \text{ such that } \alpha\Lambda_1 \subseteq \Lambda_2.$$

Complex Multiplication and Example Lattice

- E has **complex multiplication (CM)** if $\mathrm{End}(E)$ is larger than $\mathbb{Z}$.
- Equivalently, $\mathrm{End}(E)$ is an order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{-n})$ in an imaginary quadratic field.
- Such orders have the form $\mathcal{O} = \mathbb{Z} + f\,\mathcal{O}_K$ with conductor f.



Example

For $\Lambda = \langle 3,\ 2+\sqrt{-3}\rangle$,

$$\mathrm{End}(\mathbb{C}/\Lambda) = \mathbb{Z}[3\sqrt{-3}].$$

- **First Main Theorem of Complex Multiplication:**

$$K(j(\mathcal{O})) = L_{\mathcal{O}}, \qquad \mathrm{Gal}(L_{\mathcal{O}}/K) \cong \mathrm{Cl}(\mathcal{O}).$$

- The field $L_{\mathcal{O}}$ is the *ring class field* of $\mathcal{O}$, i.e. the maximal abelian extension of K unramified outside primes dividing the conductor of $\mathcal{O}$.
- Real j: $j(E) \in \mathbb{R} \iff$ the class $[E] \in \mathrm{Cl}(\mathcal{O})$ has order ≤ 2.

$$\begin{tikzcd}
 & L_{\mathcal{O}} \arrow[dl, dash, dashed, "2"'] \arrow[ddr, dash, "|\mathrm{Cl}(\mathcal{O})|"] & \\
\mathbb{Q}(j(E)) \arrow[ddr, dash, "|\mathrm{Cl}(\mathcal{O})|"'] & & \\
 & & K \arrow[dl, dash, dashed, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Example: $\mathcal{O} = \mathbb{Z}[3\sqrt{-3}]$

- Here $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathbb{Z}[3\sqrt{-3}]$ has conductor 3.
- Its class group $\mathrm{Cl}(\mathcal{O})$ has order 3 with elements $\{1, [\Lambda], [\Lambda]^2\}$.
- Thus $[L_{\mathcal{O}} : K] = 3$ and $\mathrm{Gal}(L_{\mathcal{O}}/K) \cong \mathrm{Cl}(\mathcal{O})$.
- The class $[\Lambda]$ has order 3, so $j(\Lambda) \notin \mathbb{R}$.
- The three CM j-values form one real and one complex-conjugate pair, generating the same ring class field $L_{\mathcal{O}}$.

$$\begin{tikzcd}
 & L_{\mathcal{O}} \arrow[dl, dash, dashed, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(j(E)) \arrow[dr, dash, "3"'] & & K \arrow[dl, dash, dashed, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Roadmap

1. Elliptic Curves, Complex Tori, and Fields

2. CM theory

3. Our work on abelian surfaces

Picard-maximal Abelian Surfaces

Theorem (Schoen)

A complex abelian surface has maximal Picard rank $\iff$ it is isomorphic to

$$A \cong E_1 \times E_2, \quad \text{with } E_1, E_2 \text{ CM and isogenous.}$$

Theorem (Shioda-Mitani)

Up to isomorphism, such surfaces are classified by a pair (d, E):

$$\mathcal{A}_{d,E} := \mathbb{C}/\mathcal{O} \times E, \quad \mathcal{O} = \mathbb{Z}[d\alpha], \ \mathrm{End}(E) = \mathbb{Z}[\alpha].$$

Main Theorem

Setup. For a decomposition of the abelian surface $\mathcal{A}_{d,E} \simeq E_1 \times E_2$ the **field of definition** of the decomposition is $\mathbb{Q}(j(E), j(E_1), j(E_2))$.

Theorem (Devadas-Hou)

If $d = p^n$ is a prime power and E is an elliptic curve with CM by $\mathcal{O}$, the minimal field of definition of a decomposition of $\mathcal{A}_{p^n,E}$ is

$$\mathbb{Q}\big(j(E),\, j(E_1),\, j(E_2)\big) \;=\; \begin{cases} \text{the maximal real subfield of } L_{\mathcal{O}'}, & \text{if } j(E) \in \mathbb{R}, \\ L_{\mathcal{O}'}, & \text{if } j(E) \notin \mathbb{R}, \end{cases}$$

where $L_{\mathcal{O}'}$ is the ring class field of $\mathcal{O}' = \mathbb{Z} + p^n\mathcal{O}$.

Degrees. In the real-j case the degree $[L_{\mathcal{O}'} : \mathbb{Q}]$ is $|\mathrm{Cl}(\mathcal{O}')|$; otherwise it is $[L_{\mathcal{O}'} : \mathbb{Q}] = 2\,|\mathrm{Cl}(\mathcal{O}')|$.

How we proved it

1. **Decomposition lemma.** Show

$$\mathcal{A}_{p^n,E} \cong E_1 \times E_2 \iff \big(\mathrm{End}(E_1) = \mathcal{O},\ \mathrm{End}(E_2) = \mathcal{O}',\ [E_1] \cdot \phi([E_2]) = [E] \in \mathrm{Cl}(\mathcal{O})\big),$$

   where $\phi : \mathrm{Cl}(\mathcal{O}') \to \mathrm{Cl}(\mathcal{O})$ is the natural map.

2. **Degree lower bound.** $j(E_2)$ is a root of the Hilbert class polynomial of $\mathcal{O}'$ (which has degree $|\mathrm{Cl}(\mathcal{O}')|$) so

$$\big[\mathbb{Q}\big(j(E), j(E_1), j(E_2)\big) : \mathbb{Q}\big] \ \geq\ |\mathrm{Cl}(\mathcal{O}')|.$$

3. **Case split via CM/class field theory.**
   - If $j(E) \in \mathbb{R}$ (i.e. $[E]$ has order ≤ 2 in $\mathrm{Cl}(\mathcal{O})$), then $j(\mathbb{C}/\mathcal{O}')$ is real and the field generated is exactly the *real subfield* of $L_{\mathcal{O}'}$; the lower bound is sharp.
   - If $j(E) \notin \mathbb{R}$ (order > 2), then adjoining $j(E)$ and $j(E_1)$ gives all of $L_{\mathcal{O}}$, and together with $j(E_2)$ one obtains the *full* $L_{\mathcal{O}'}$.

Acknowledgments

I would like to thank my PRIMES mentor, Sheela Devadas, for her guidance and support throughout the PRIMES program. I would also like to thank the PRIMES organizers for the opportunity to conduct math research and present to the PRIMES community and the broader audience of young mathematicians.