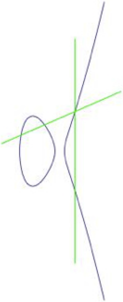
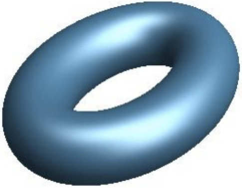
Elliptic curves with complex multiplication

Valerio Talamanca (Università Roma Tre & RNTA)





CIMPA research school on
Isogenies of elliptic curves and their applications to cryptography
Universidad del Cauca
July 24th - August 4th, 2023

Lattices in $\mathbb{C}$ and complex tori

Let $\Lambda \subset \mathbb{C}$ be a lattice and consider the associated complex tori defined as $\mathbb{C}/\Lambda$. Recall that the Weierstrass $\wp$-function defined as

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

gives rise, together with its derivative, to a map to the projective plane:

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\longrightarrow \mathbb{P}_2(\mathbb{C}) \\ z &\longmapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \end{aligned}$$

whose image is an elliptic curve, that we will denote by E_Λ, which has Weierstrass equation

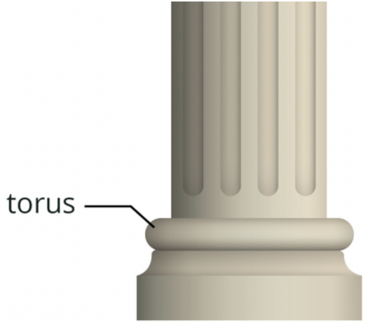
$$y^2 = 4x^3 + g_2(\Lambda)x + g_3(\Lambda)$$

The uniformization theorem tells us that every elliptic curve over $\mathbb{C}$ arises in this way.

Why $\mathbb{C}/\Lambda$ is called a torus?

Why $\mathbb{C}/\Lambda$ is called a torus?

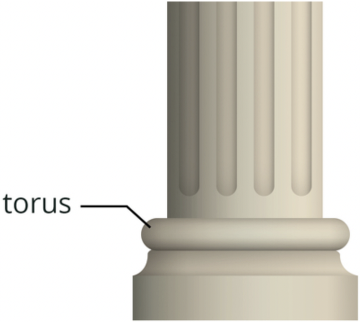
The name comes from architecture



in architecture a torus is a particular roman moulding at the base of doric style column.

Why $\mathbb{C}/\Lambda$ is called a torus?

The name comes from architecture



in architecture a torus is a particular roman moulding at the base of doric style column.
The latin word torus had several other meanings including rope, swelling, pillow, bed, coffin and lover.

Holomorphic maps of complex tori

Question

What about maps?

Holomorphic maps of complex tori

Question

What about maps?

If α is such that $\alpha\Lambda_1 \subseteq \Lambda_2$, then we can define a surjective map $\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, by setting

$$\phi_\alpha([z]_{\Lambda_1}) = [\alpha z]_{\Lambda_2}.$$

It can be shown that this is a holomorphic map.

Holomorphic maps of complex tori

Question

What about maps?

If α is such that $\alpha\Lambda_1 \subseteq \Lambda_2$, then we can define a surjective map $\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, by setting

$$\phi_\alpha([z]_{\Lambda_1}) = [\alpha z]_{\Lambda_2}.$$

Consider

$$\{\alpha \in \mathbb{C} \,:\, \alpha\Lambda_1 \subseteq \Lambda_2\} \to \left\{ \frac{\mathbb{C}}{\Lambda_1} \xrightarrow{\phi} \frac{\mathbb{C}}{\Lambda_2} : \phi(0) = 0 \textit{ and } \phi \textit{ holomorphic} \right\}$$

$$\alpha \mapsto \phi_\alpha$$

Theorem

Let Λ_1 and Λ_2 be two lattices. Then the above association is a bijection. Moreover $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if Λ_1 and Λ_2 are homothetic.

Endomorphisms of elliptic curves over $\mathbb{C}$

In particular we get that given a lattice Λ and its associated elliptic curve E_Λ, the endomorphism ring of E_Λ is isomorphic to

$$\{\alpha \in \mathbb{C} \,:\, \alpha\Lambda \subset \Lambda\} = R_\Lambda$$

Note that we immediately recover the fact that $\mathrm{End}(E_\Lambda)$ contains $\mathbb{Z}$.

Endomorphisms of elliptic curves over $\mathbb{C}$

In particular we get that given a lattice Λ and its associated elliptic curve E_Λ, the endomorphism ring of E_Λ is isomorphic to the following

$$\{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} = R_\Lambda$$

Note that we immediately recover the fact that $\mathrm{End}(E_\Lambda)$ contains $\mathbb{Z}$.
Moreover given $\alpha \in R_\Lambda$ we fix $[\alpha] : E_\Lambda \to E_\Lambda$, by requiring that the following diagram is commutative

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[r, "\phi_\alpha"] \arrow[d, "\Phi"] & \mathbb{C}/\Lambda \arrow[d, "\Phi"] \\
E_\Lambda \arrow[r, "{[\alpha]}"] & E_\Lambda
\end{tikzcd}$$

Complex multiplication

Definition

Let $E/\mathbb{C}$ be an elliptic curve. We say that E as complex multiplication (CM for short) if $\mathrm{End}(E)$ *is strictly bigger than* $\mathbb{Z}$.

Complex multiplication

Definition

Let $E/\mathbb{C}$ be an elliptic curve. We say that E as complex multiplication (CM for short) if $\mathrm{End}(E)$ *is strictly bigger than* $\mathbb{Z}$.

Example

Let E be the elliptic curve $y^2 = x^3 + x$, then the map $(x, y) \mapsto (-x, iy)$ induces an endomorphism ϕ of E. Clearly ϕ has order 4, *and so* $\mathrm{End}(E)$ *is bigger than* $\mathbb{Z}$ *and hence E has complex multiplication.*

Complex multiplication

Definition

Let $E/\mathbb{C}$ be an elliptic curve. We say that E as complex multiplication (CM for short) if $\mathrm{End}(E)$ *is strictly bigger than $\mathbb{Z}$.*

Example

Let E be the elliptic curve having Weierstrass equation $y^2 = x^3 + x$, then the map $(x, y) \mapsto (-x, iy)$ induces an endomorphism ϕ of E. Clearly ϕ has order 4, *and so* $\mathrm{End}(E)$ *is bigger than $\mathbb{Z}$ and hence E has complex multiplication.*

Example

Let E be the elliptic curve having Weierstrass equation $y^2 = x^3 + 1$, and let ρ be a primitive cubic root of unity. Then the map $(x, y) \mapsto (\rho x, y)$ induces an endomorphism ϕ of E. Clearly ϕ has order 3, *and so E has complex multiplication.*

Complex multiplication

Definition

Let $E/\mathbb{C}$ be an elliptic curve. We say that E as complex multiplication (CM for short) if $\mathrm{End}(E)$ *is strictly bigger than $\mathbb{Z}$.*

So if E is a complex CM elliptic curve, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quadratic imaginary field, and $\mathrm{End}(E)$ is an order in that field.
As a matter of notation if $\mathrm{End}(E) \cong \mathcal{O} \subset \mathbb{C}$ and $K = \mathcal{O} \otimes \mathbb{Q}$ we will say that E has complex multiplication by $\mathcal{O}$, or that E has complex multiplication by K.

Complex multiplication

It is easier to treat the case of elliptic curves having complex multiplication by the full ring of integers of K, (i.e. the maximal order), and so we will restrict ourselves to that case.

Complex multiplication

It is easier to treat the case of elliptic curves having complex multiplication by the full ring of integers of K, (i.e. the maximal order), and so we will restrict ourselves to that case.
But we do not miss much doing so as the next theorem shows:

Theorem

Suppose that E has complex multiplication by an order $\mathcal{O} \subset K$. Then there exists an elliptic curve E' isogenous to E and having complex multiplication by $\mathcal{O}_K$.

Construction of elliptic curves with complex multiplication

Question

Suppose we are given an imaginary quadratic field K, how do we construct elliptic curves with complex multiplication by $\mathcal{O}_K$?

Construction of elliptic curves with complex multiplication

Question

Suppose we are given an imaginary quadratic field K, how do we construct elliptic curves with complex multiplication by $\mathcal{O}_K$?

Suppose $\mathfrak{a} \subset \mathcal{O}_K$ is a fractional ideal. Then $\mathfrak{a} \subset K \subset \mathbb{C}$ is a lattice in $\mathbb{C}$. Consider $E_\mathfrak{a}$, then its endomorphism ring is given by

$$\begin{aligned} \operatorname{End}(E_\mathfrak{a}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K, : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ {}^1 &= \mathcal{O}_K \end{aligned}$$

[1] Exercise: prove this equality

Construction of elliptic curves with complex multiplication

Question

Suppose we are given an imaginary quadratic field K, how do we construct elliptic curves with complex multiplication by $\mathcal{O}_K$?

Suppose $\mathfrak{a} \subset \mathcal{O}_K$ is a fractional ideal. Then $\mathfrak{a} \subset K \subset \mathbb{C}$ is a lattice in $\mathbb{C}$. Consider $E_{\mathfrak{a}}$, then its endomorphism ring is given by

$$\begin{aligned} \mathrm{End}(E_{\mathfrak{a}}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K, : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \mathcal{O}_K \end{aligned}$$

Hence every fractional ideal $\mathfrak{a}$ of K, gives rise to an elliptic curve $E_{\mathfrak{a}}$ having complex multiplication by K.

Construction of elliptic curves with complex multiplication

Hence every fractional ideal $\mathfrak{a}$ of K, gives rise to an elliptic curve $E_{\mathfrak{a}}$ having complex multiplication by K.
Recall that given two lattices Λ_1 and Λ_2, then E_{Λ_1} and E_{Λ_2} are isomorphic if and only if Λ_1 and Λ_2 are homothetic.

Construction of elliptic curves with complex multiplication

Hence every fractional ideal $\mathfrak{a}$ of K, gives rise to an elliptic curve $E_{\mathfrak{a}}$ having complex multiplication by K.

Recall that given two lattices Λ_1 and Λ_2, then E_{Λ_1} and E_{Λ_2} are isomorphic if and only if Λ_1 and Λ_2 are homothetic.

Let $\overline{\mathfrak{a}}$ denote the class of $\mathfrak{a}$ in $Cl(\mathcal{O}_K)$, the class group of $\mathcal{O}_K$. Thus if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ (i.e. there exists $c \in K$ such that $c\mathfrak{a} = \mathfrak{b}$) then $E_{\mathfrak{a}}$ and $E_{\mathfrak{b}}$ are isomorphic. It follows that we have a map

$$Cl(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$
$$\mathfrak{a} \mapsto E_{\mathfrak{a}}$$

Construction of elliptic curves with complex multiplication

Hence every fractional ideal $\mathfrak{a}$ of K, gives rise to an elliptic curve $E_{\mathfrak{a}}$ having complex multiplication by K.
Recall that given two lattices Λ_1 and Λ_2, then E_{Λ_1} and E_{Λ_2} are isomorphic if and only if Λ_1 and Λ_2 are homothetic.
Thus if $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic (i.e. $c\mathfrak{a} = \mathfrak{b}$) then $E_{\mathfrak{a}}$ and $E_{\mathfrak{b}}$ are isomorphic. It follows that we have a map

$$Cl(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$
$$\mathfrak{a} \mapsto E_{\mathfrak{a}}$$

Moreover it is injective: $E_{\mathfrak{a}} \cong E_{\mathfrak{b}} \iff$ there exists $c \in \mathbb{C}$ such that $\mathfrak{a} = c\mathfrak{b}$. But then $c \in K$ and so $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Let Λ be a lattice such that E_Λ has complex multiplication by $\mathcal{O}_K$. For any $\mathfrak{a}$, we set:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \ : \ \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

Let Λ be a lattice such that E_Λ has complex multiplication by $\mathcal{O}_K$. For any $\mathfrak{a}$, we set:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \,:\, \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

Proposition

Let $\Lambda \subset \mathbb{C}$ be a lattice. Assume that E_Λ has complex multiplication by $\mathcal{O}_K$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non zero fractional ideal of K. Then

Let Λ be a lattice such that E_Λ has complex multiplication by $\mathcal{O}_K$. For any $\mathfrak{a}$, we set:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \,:\, \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

Proposition

Let $\Lambda \subset \mathbb{C}$ be a lattice. Assume that E_Λ has complex multiplication by $\mathcal{O}_K$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non zero fractional ideal of K. Then

- $\mathfrak{a}\Lambda$ *is a lattice in* $\mathbb{C}$

Let Λ be a lattice such that E_Λ has complex multiplication by $\mathcal{O}_K$. For any $\mathfrak{a}$, we set:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \ : \ \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

Proposition

Let $\Lambda \subset \mathbb{C}$ be a lattice. Assume that E_Λ has complex multiplication by $\mathcal{O}_K$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non zero fractional ideal of K. Then

- $\mathfrak{a}\Lambda$ *is a lattice in* $\mathbb{C}$
- $E_{\mathfrak{a}\Lambda}$ *has complex multiplication by* $\mathcal{O}_K$

Let Λ be a lattice such that E_Λ has complex multiplication by $\mathcal{O}_K$. For any $\mathfrak{a}$, we set:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \ : \ \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

Proposition

Let $\Lambda \subset \mathbb{C}$ be a lattice. Assume that E_Λ has complex multiplication by $\mathcal{O}_K$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non zero fractional ideal of K. Then

- $\mathfrak{a}\Lambda$ *is a lattice in* $\mathbb{C}$
- $E_{\mathfrak{a}\Lambda}$ *has complex multiplication by* $\mathcal{O}_K$
- $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ *if and only if* $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ *in* $Cl(\mathcal{O}_K)$.

Proposition

Let K be an imaginary quadratic number field, and $\mathcal{O}_K$ its ring of integers. The map

$$Cl(\mathcal{O}_K) \times \mathrm{Ell}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$
$$(\bar{\mathfrak{a}}, E_\Lambda) \mapsto \bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

is a simply transitive action of $Cl(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$. In particular

$$\# Cl(\mathcal{O}_K) = \# \mathrm{Ell}(\mathcal{O}_K)$$

$\mathfrak{a}$-torsion points

Let E be an elliptic curve with complex multiplication by K. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we set

$$E[\mathfrak{a}] = \{P \in E \,:\, [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

and we call it the group of $\mathfrak{a}$-torsion of E.

$\mathfrak{a}$-torsion points

Let E be an elliptic curve with complex multiplication by K. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we set

$$E[\mathfrak{a}] = \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

and we call it the group of $\mathfrak{a}$-torsion of E.

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$, and fix an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Since $\Lambda \subset \mathfrak{a}^{-1}\Lambda$ we have a natural isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$ and hence a natural isogeny $E \to \overline{\mathfrak{a}} * E = E_{\mathfrak{a}^{-1}\Lambda}$.

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$\mathbb{C}/\Lambda[\mathfrak{a}] = \{z \in \mathbb{C} : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$(\mathbb{C}/\Lambda)[\mathfrak{a}] = \{z \in \mathbb{C} \,:\, \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$\begin{aligned}(\mathbb{C}/\Lambda)[\mathfrak{a}] &= \{z \in \mathbb{C}/\Lambda : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in \Lambda\}/\Lambda\end{aligned}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$\begin{aligned}(\mathbb{C}/\Lambda)[\mathfrak{a}] &= \{z \in \mathbb{C}/\Lambda : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda \\ &= \{z \in \mathbb{C} : z\mathfrak{a} \in \Lambda\}/\Lambda\end{aligned}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$\begin{aligned}(\mathbb{C}/\Lambda)[\mathfrak{a}] &= \{z \in \mathbb{C}/\Lambda : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda \\ &= \{z \in \mathbb{C} : z\mathfrak{a} \in \Lambda\}/\Lambda \\ &= \mathfrak{a}^{-1}\Lambda/\Lambda\end{aligned}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

Let's first look on the complex tori side. Suppose that $E = E_\Lambda$, as usual Λ a lattice in $\mathbb{C}$. Then

$$\begin{aligned}
(\mathbb{C}/\Lambda)[\mathfrak{a}] &= \{z \in \mathbb{C}/\Lambda \,:\, \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\
&= \{z \in \mathbb{C} \,:\, \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\,\}/\Lambda \\
&= \{z \in \mathbb{C} \,:\, z\mathfrak{a} \in \Lambda\}/\Lambda \\
&= \mathfrak{a}^{-1}\Lambda/\Lambda \\
&= \ker\left(\mathbb{C}/\Lambda \xrightarrow{z \mapsto z} \mathbb{C}/\mathfrak{a}^{-1}\Lambda\right)
\end{aligned}$$

$\mathfrak{a}$-torsion points

Question

Can we determine the isogeny of which $E[\mathfrak{a}]$ is the kernel?

So we have $(\mathbb{C}/\Lambda)[\mathfrak{a}] = \ker\left(\mathbb{C}/\Lambda \xrightarrow{z \mapsto z} \mathbb{C}/\mathfrak{a}^{-1}\Lambda\right)$. Fix an analytic isomorphism from $(\mathbb{C}/\Lambda)$ to $E(\mathbb{C})$. Then $(\mathbb{C}/\Lambda)[\mathfrak{a}]$ corresponds to $E[\mathfrak{a}]$ and $\ker\left(\mathbb{C}/\Lambda \xrightarrow{z \mapsto z} \mathbb{C}/\mathfrak{a}^{-1}\Lambda\right)$ corresponds to the kernel of the natural isogeny from E to $\overline{\mathfrak{a}} * E$.

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

- *$E[\mathfrak{a}]$ is the kernel of the natural isogeny $E \to \overline{\mathfrak{a}} * E$*

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

- *$E[\mathfrak{a}]$ is the kernel of the natural isogeny $E \to \overline{\mathfrak{a}} * E$*
- *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

- *$E[\mathfrak{a}]$ is the kernel of the natural isogeny $E \to \overline{\mathfrak{a}} * E$*
- *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*

Corollary

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$.

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

- *$E[\mathfrak{a}]$ is the kernel of the natural isogeny $E \to \overline{\mathfrak{a}} * E$*
- *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*

Corollary

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$.

- *Let $\mathfrak{a}$ be an integral ideal, then the natural isogeny $E \to \overline{\mathfrak{a}} * E$ has degree $\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{a})$.*

$\mathfrak{a}$-torsion points

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$.

- *$E[\mathfrak{a}]$ is the kernel of the natural isogeny $E \to \overline{\mathfrak{a}} * E$*
- *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*

Corollary

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$.

- *Let $\mathfrak{a}$ be an integral ideal, then the natural isogeny $E \to \overline{\mathfrak{a}} * E$ has degree $\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{a})$.*
- *Let $\alpha \in \mathcal{O}_K$, then the endomorphism $[\alpha] \in \mathrm{End}(E)$ has degree $|\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)|$.*

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

The proof is left as an exercise which means is in the exercise sheet.

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

The proof is left as an exercise which means is in the exercise sheet.
Hints:

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

The proof is left as an exercise which means is in the exercise sheet.
Hints:

- Prove that if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

The proof is left as an exercise which means is in the exercise sheet.
Hints:

- Prove that if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.
- Prove that if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then $j(E^\sigma) = j(E)$

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number.

The proof is left as an exercise which means is in the exercise sheet.
Hints:

- Prove that if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.
- Prove that if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then $j(E^\sigma) = j(E)$

You can freely use the following fact:

Fact

Let $\alpha \in \mathbb{C}$ be such that the set $\{\sigma(\alpha) : \sigma \in \mathrm{Aut}(\mathbb{C})\}$ is finite, the α is an algebraic number.

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

If F is any field set

$$\mathrm{Ell}_F(\mathcal{O}_K) = \frac{\{\text{Elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } F}$$

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

If F is any field set

$$\mathrm{Ell}_F(\mathcal{O}_K) = \frac{\{\text{Elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } F}$$

Then if we fix an embedding of $\overline{Q}$ in to $\mathbb{C}$ we get a map

$$\iota : \mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

If F is any field set

$$\mathrm{Ell}_F(\mathcal{O}_K) = \frac{\{\text{Elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } F}$$

Then if we fix an embedding of $\overline{Q}$ in to $\mathbb{C}$ we get a map

$$\iota : \mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$

then one has that ι is a bijection.

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

If F is any field set

$$\mathrm{Ell}_F(\mathcal{O}_K) = \frac{\{\text{Elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } F}$$

Then if we fix an embedding of $\overline{Q}$ in to $\mathbb{C}$ we get a map

$$\iota : \mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$

From $\mathbb{C}$ to $\overline{\mathbb{Q}}$

If F is any field set

$$\mathrm{Ell}_F(\mathcal{O}_K) = \frac{\{\text{Elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } F}$$

Then if we fix an embedding of $\overline{Q}$ in to $\mathbb{C}$ we get a map

$$\iota : \mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$$

then one has that ι is a bijection. To prove it we need to recall the following result about elliptic curves:

Theorem

Two elliptic curves E and E' over an algebraically closed field $\overline{L}$ are isomorphic if and only they have the same j-invariant. Moreover if $j_0 \in \overline{L}$, then there exists an elliptic curve E_0 defined over $L(j_0)$ such that $j(E_0) = j_0$.

Consider $\mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$. On it we have an action of $\mathrm{Gal}(\overline{K}/K)$, sending E to E^σ. Recall that we have a transitive action of $Cl(\mathcal{O}_K)$ so it must exists $\overline{\mathfrak{a}} \in Cl(\mathcal{O}_K)$ such that

$$\overline{\mathfrak{a}} * E = E^\sigma$$

Consider $\mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$. On it we have an action of $\mathrm{Gal}(\overline{K}/K)$, sending E to E^σ. Recall that we have a transitive action of $Cl(\mathcal{O}_K)$ so it must exists $\overline{\mathfrak{a}_E}\in Cl(\mathcal{O}_K)$ such that

$$\overline{\mathfrak{a}_E} * E = E^\sigma$$

Now the amazing fact is that actually $\mathfrak{a}_E$ does not depends on E.

Consider $\mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$. On it we have an action of $\mathrm{Gal}(\overline{K}/K)$, sending E to E^σ. Recall that we have a transitive action of $Cl(\mathcal{O}_K)$ so it must exists $\overline{\mathfrak{a}_\sigma} \in Cl(\mathcal{O}_K)$ such that

$$\overline{\mathfrak{a}_\sigma} * E = E^\sigma$$

Theorem

Let $K/\mathbb{Q}$ be an imaginary quadratic field. Then there exists a homomorphism $\Psi : \mathrm{Gal}(\overline{K}/K) \to Cl(\mathcal{O}_K)$, uniquely determined by requiring that $E^\sigma = \Psi(\sigma) * E$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and all $E \in \mathrm{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$.

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then

- $H = K(j(E))$ *is the Hilbert class field of K.*

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then

- $H = K(j(E))$ *is the Hilbert class field of* K.
- $[K(j(E)) : K] = \# Cl(\mathcal{O}_K) = \# \mathrm{Gal}(H/K) = \# \mathrm{Ell}(\mathcal{O}_K)$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then

- $H = K(j(E))$ *is the Hilbert class field of* K.
- $[K(j(E)) : K] = \# Cl(\mathcal{O}_K) = \# \operatorname{Gal}(H/K) = \# \operatorname{Ell}(\mathcal{O}_K)$
- *Set* $\# Cl(\mathcal{O}_K) = h_k$ *and suppose that* $E_1, \ldots E_{h_k}$ *be a complete set of representatives for* $\operatorname{Ell}(\mathcal{O}_K)$. *Then* $j(E_1), \ldots j(E_{h_k})$, *is a complete set of* $\operatorname{Gal}(\overline{K}/K)$ *conjugates for* $j(E)$

Theorem

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then

- *$H = K(j(E))$ is the Hilbert class field of K.*
- $[K(j(E)) : K] = \# Cl(\mathcal{O}_K) = \# \mathrm{Gal}(H/K) = \# \mathrm{Ell}(\mathcal{O}_K)$
- *Set $\# Cl(\mathcal{O}_K) = h_k$ and suppose that $E_1, \ldots E_{h_k}$ be a complete set of representatives for $\mathrm{Ell}(\mathcal{O}_K)$. Then $j(E_1), \ldots j(E_{h_k})$, is a complete set of $\mathrm{Gal}(\overline{K}/K)$ conjugates for $j(E)$*
- *For every non zero fractional ideal $\mathfrak{a}$ of K we have:*

$$j(E)^{[\mathfrak{a}, H/K]} = j(\overline{\mathfrak{a}} * E)$$

where $[\mathfrak{a}, H/K] \in \mathrm{Gal}(H/K)$ is the Artin symbol of $\mathfrak{a}$.