Explicit Construction of Abelian Extensions of Number Fields

Jared Asuncion

21 November 2019

Definition (algebraic number)

An algebraic number is a complex number which is a root of a polynomial with coefficients in $\mathbb{Z}$.

Definition (algebraic integer)

An algebraic integer is an algebraic number which is a root of a **monic** *polynomial with coefficients in $\mathbb{Z}$.*

Example

- $\sqrt{-5}$ *is a root of* $x^2 + 5$. *Hence, it is an algebraic integer.*
- 3.14 *is a root of* $50x - 157$. *Hence, it is an algebraic number.*
- π *is NOT an algebraic number.*

Definition

Let L/K be a field extension. The degree $[L : K]$ of a field extension L/K is defined to be the dimension of L as a K-vector space.

Definition (algebraic number field)

An algebraic number field is a field extension of $\mathbb{Q}$ of finite degree.

- Any element of a number field is algebraic.
- The set of algebraic integers $\mathcal{O}_K$ of K form a subring of K.
- $\mathbb{Q}(\sqrt{-5})$ is a number field of degree 2 since $\dim_{\mathbb{Q}}(K) = 2$.
- $\mathbb{Q}(\pi)$ and $\mathbb{C}$ are not number fields since they are not finite extensions of $\mathbb{Q}$.

Definition (Galois extension)

A field extension L/K is Galois if the group $\mathrm{Aut}(L/K)$ of automorphisms of L fixing K is equal to the degree of the extension.

Notation

If L/K is Galois, we will denote $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$.

- $K = \mathbb{Q}(i)$ is a Galois extension of $\mathbb{Q}$ since the automorphisms of K fixing $\mathbb{Q}$ are given by:

$$a + bi \mapsto a + bi$$
$$a + bi \mapsto a - bi$$

- $K = \mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$ since the only automorphism of K fixing $\mathbb{Q}$ is the identity automorphism.

Definition (abelian extension)

A Galois extension L/K is abelian if the group $\mathrm{Gal}(L/K)$ of automorphisms of L fixing K is abelian.

- $K = \mathbb{Q}(i)$ is an abelian extension since $|\mathrm{Gal}(L/K)| = 2$ and all groups of order 2 are abelian.
- $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$, is an abelian extension since its Galois group is $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Definition (abelian extension)

A Galois extension L/K is abelian if the group $\mathrm{Gal}(L/K)$ of automorphisms of L fixing K is abelian.

- $K = \mathbb{Q}(i)$ is an abelian extension since $|\mathrm{Gal}(L/K)| = 2$ and all groups of order 2 are abelian.
- $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$, is an abelian extension since its Galois group is $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Problem (Hilbert's 12th Problem)

Given a number field K, construct all abelian extensions of K by adjoining special values of particular analytic functions.

Problem (Hilbert's 12th Problem)

Given a number field K, construct all (finite) abelian extensions of K by adjoining special values of particular functions.

Theorem (Kronecker-Weber Theorem)

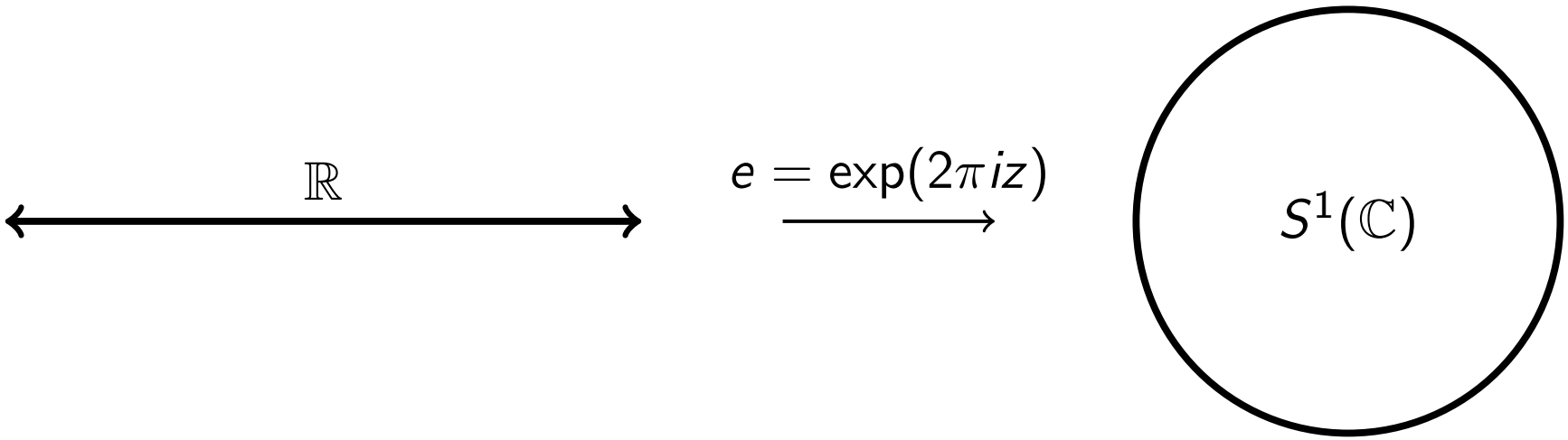
Every finite abelian extension of $\mathbb{Q}$ is contained in a field $\mathbb{Q}(\exp(2\pi iz))$ for some $z \in \mathbb{Q}$.

'particular function'

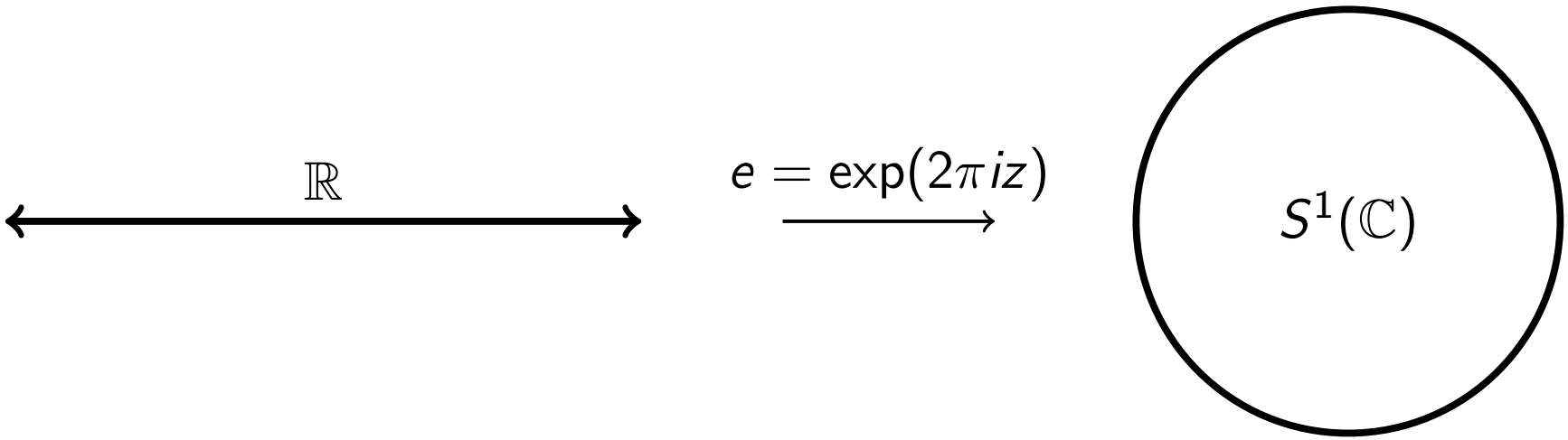
$$e : \mathbb{R} \to S^1(\mathbb{C})$$
$$z \to \exp(2\pi iz)$$

'special values'

Append $e(z)$ such that $z \in \mathbb{Q}$.

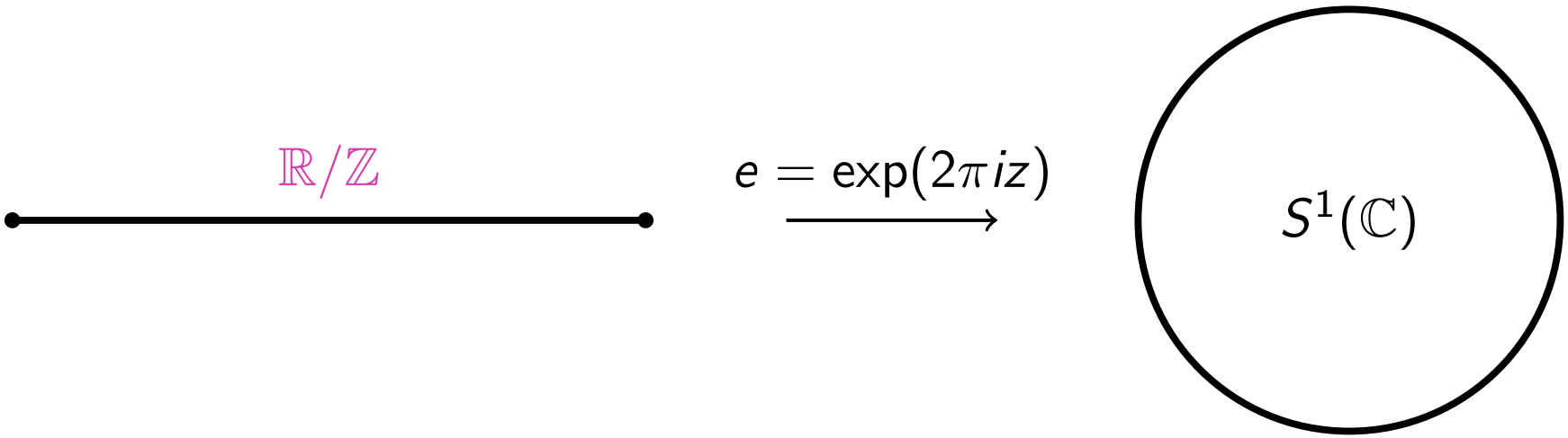


Observations



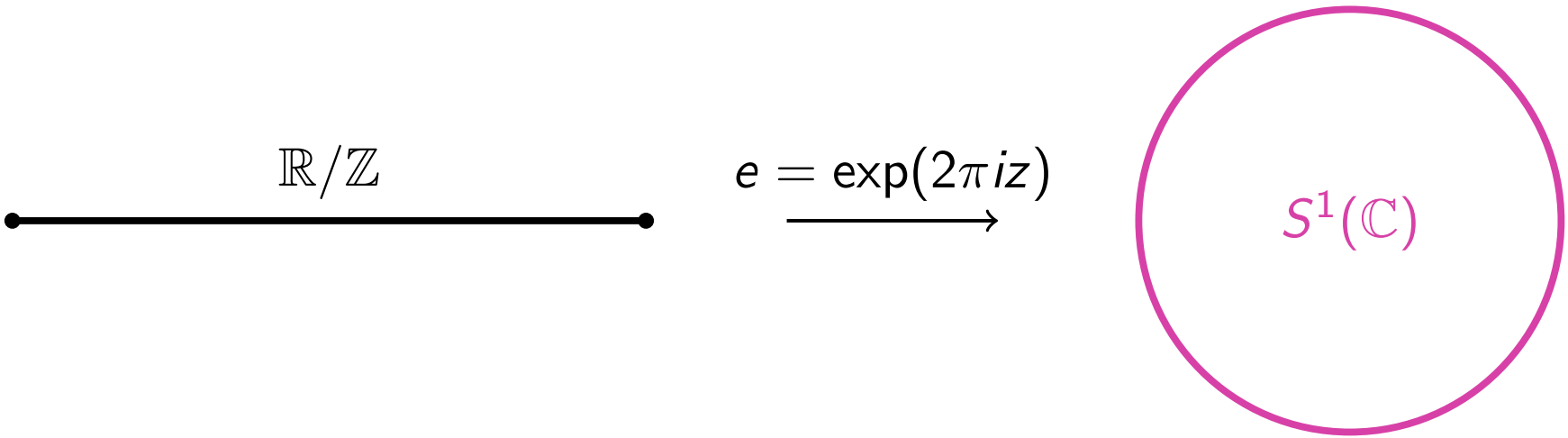
Observations

- The kernel of the map e is $\mathbb{Z}$.



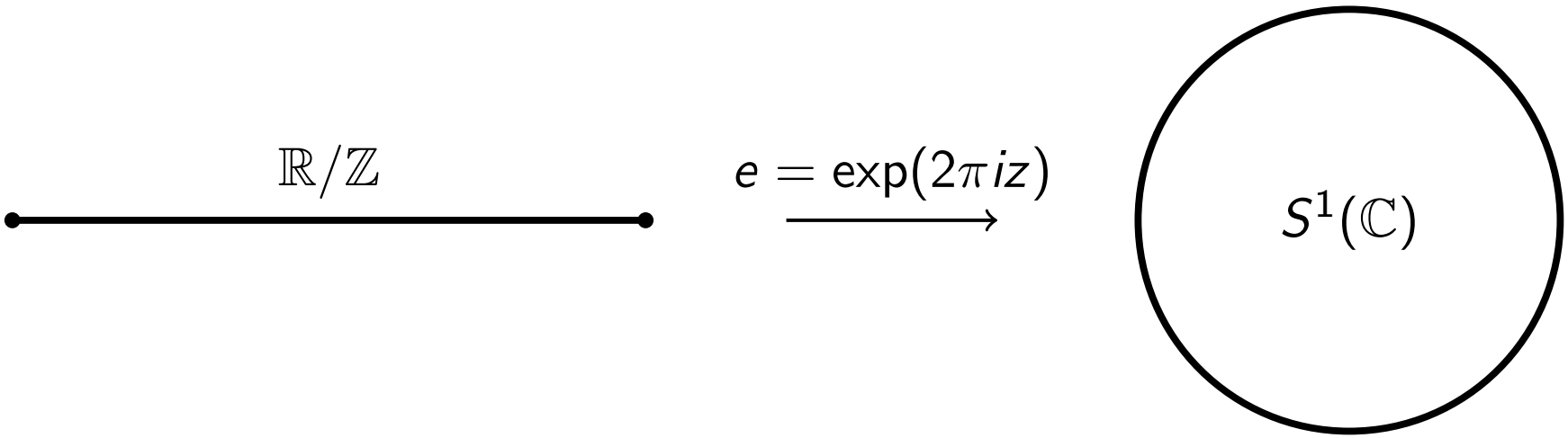
Observations

- The kernel of the map e is $\mathbb{Z}$.



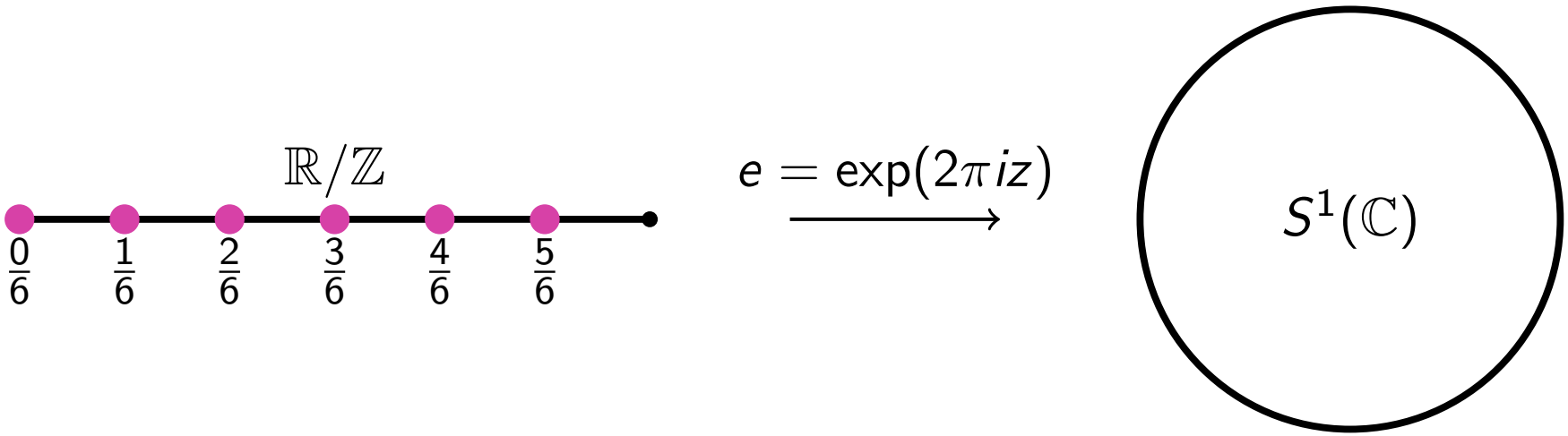
Observations

- The kernel of the map e is $\mathbb{Z}$.
- The image of the map is a geometric object, a circle.



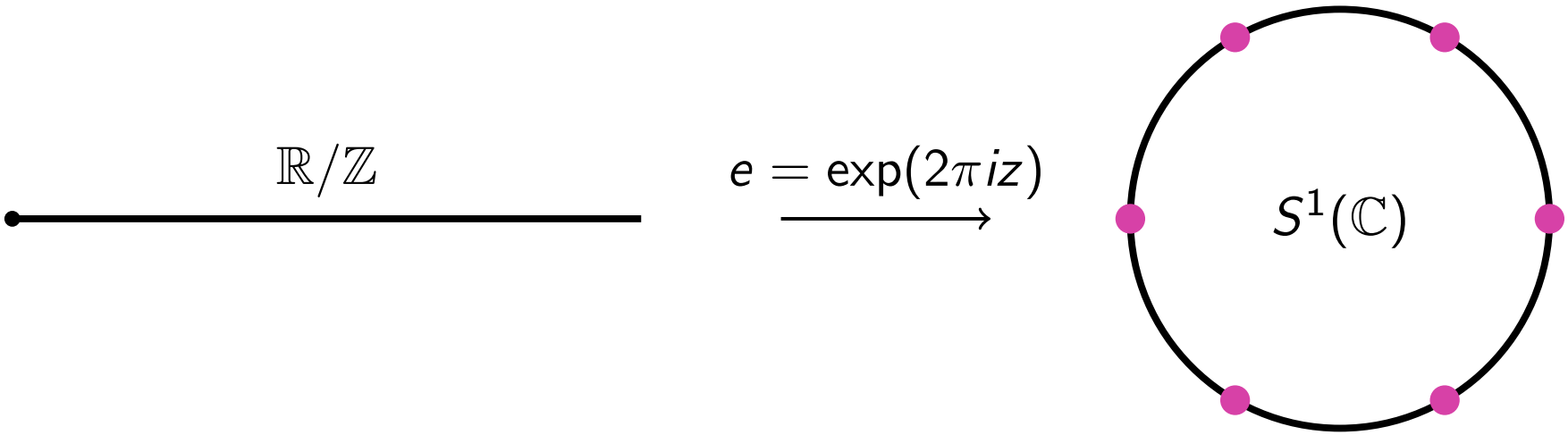
Observations

- The kernel of the map e is $\mathbb{Z}$.
- The image of the map is a geometric object, a circle.
- Both domain and codomain have a group structure.



Observations

- The kernel of the map e is $\mathbb{Z}$.
- The image of the map is a geometric object, a circle.
- Both domain and codomain have a group structure.
- The torsion points of the domain are easy to determine.



Observations

- The kernel of the map e is $\mathbb{Z}$.
- The image of the map is a geometric object, a circle.
- Both domain and codomain have a group structure.
- The torsion points of the domain are easy to determine.
- The torsion points of the codomain are what we append to $\mathbb{Q}$.

Class Field Theory

Class field theory tells us that every finite abelian extension of a number field K is contained in some ray class field extension $H_K(m)$ of K.

Class Field Theory

Class field theory tells us that every finite abelian extension of a number field K is contained in some ray class field extension $H_K(m)$ of K.

For the case when the base field is $\mathbb{Q}$, we have:

$$H_{\mathbb{Q}}(1) = \mathbb{Q}$$
$$H_{\mathbb{Q}}(m) = \mathbb{Q}(\exp(2\pi i \cdot 1/m)).$$

Class Field Theory

Class field theory tells us that every finite abelian extension of a number field K is contained in some ray class field extension $H_K(m)$ of K.

For the case when the base field is $\mathbb{Q}$, we have:

$$H_{\mathbb{Q}}(1) = \mathbb{Q}$$
$$H_{\mathbb{Q}}(m) = \mathbb{Q}(\exp(2\pi i \cdot 1/m)).$$

Hilbert's 12th Problem

What about other base fields?

Class Field Theory

Class field theory tells us that every finite abelian extension of a number field K is contained in some ray class field extension $H_K(m)$ of K.

For the case when the base field is $\mathbb{Q}$, we have:

$$H_{\mathbb{Q}}(1) = \mathbb{Q}$$
$$H_{\mathbb{Q}}(m) = \mathbb{Q}(\exp(2\pi i \cdot 1/m)).$$

Hilbert's 12th Problem

What about other base fields?

- The case $K = \mathbb{Q}(\sqrt{-D})$, totally imaginary quadratic number fields is explicitly solved using elliptic curves.
- No other case is completely solved.

Definition

An elliptic curve defined over k ($\operatorname{char} k \neq 2, 3$) is a smooth projective curve given by an equation of the form

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

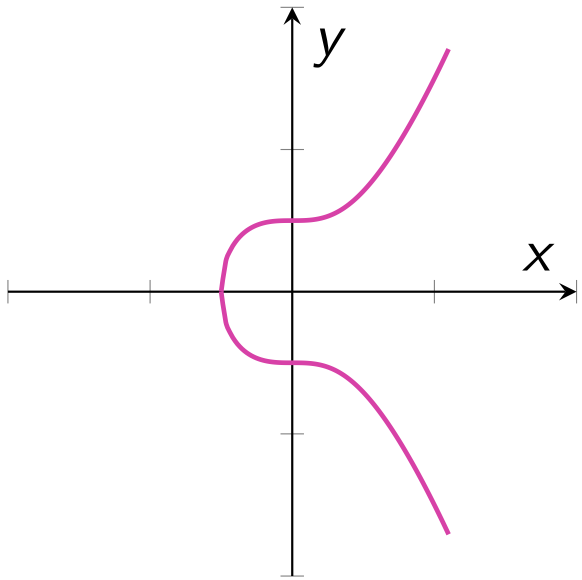
where $a, b \in k$ and $f(x)$ has no double roots in the algebraic closure of $\overline{k}$.

Definition

An elliptic curve defined over k ($\text{char}\, k \neq 2, 3$) is a smooth projective curve given by an equation of the form

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ and $f(x)$ has no double roots in the algebraic closure of $\overline{k}$.

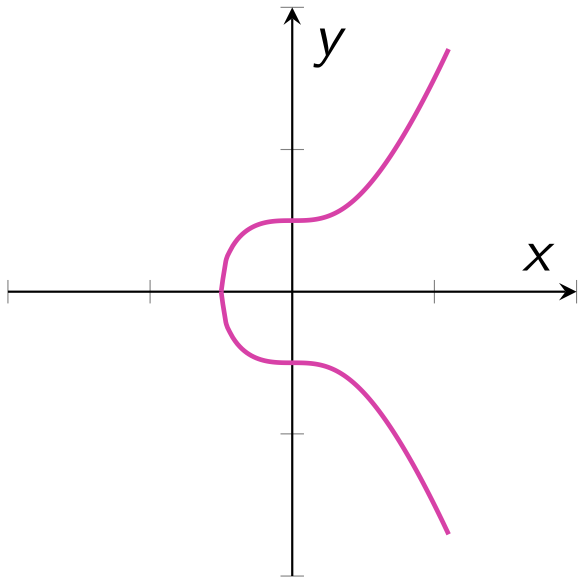


Definition

An elliptic curve defined over k ($\text{char}\, k \neq 2, 3$) is a smooth projective curve given by an equation of the form

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ and $f(x)$ has no double roots in the algebraic closure of $\overline{k}$.



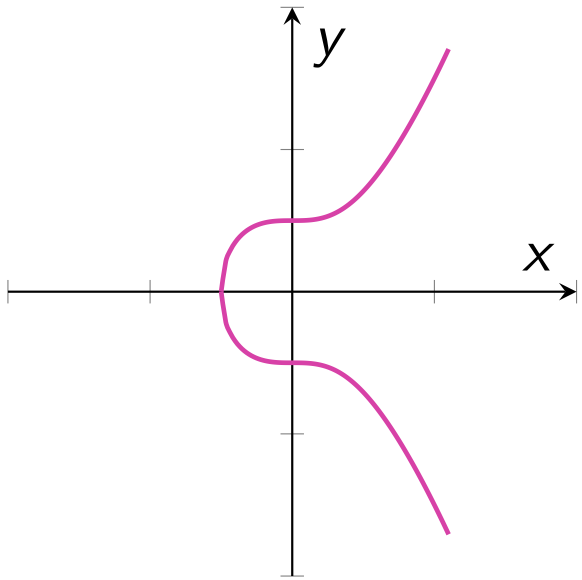
- It has exactly one point at infinity, which we denote by $\infty = (0 : 1 : 0)$.

Definition

An elliptic curve defined over k ($\text{char}\, k \neq 2, 3$) is a smooth projective curve given by an equation of the form

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ and $f(x)$ has no double roots in the algebraic closure of $\overline{k}$.



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

- It has exactly one point at infinity, which we denote by $\infty = (0 : 1 : 0)$.
- We will usually write the affine equation $y^2 = x^3 + ax + b$ to define elliptic curves and remember that there is an extra point at infinity.

Notation

Let $k \subseteq K$. The set of K-rational points of an elliptic curve E is given by

$$E(K) = \{\infty\} \cup \{(x, y) \in K \times K : y^2 = x^3 + ax + b\}.$$

Theorem

Let E be an elliptic curve over k. For each $k \subseteq K$, the set $E(K)$ has a group structure with ∞ as the identity element.

Notation

Let $k \subseteq K$. The set of K-rational points of an elliptic curve E is given by

$$E(K) = \{\infty\} \cup \{(x, y) \in K \times K : y^2 = x^3 + ax + b\}.$$

Theorem

Let E be an elliptic curve over k. For each $k \subseteq K$, the set $E(K)$ has a group structure with ∞ as the identity element.

For each integer $m \in \mathbb{Z}$, there is a corresponding group homomorphism (i.e. an endomorphism) from $E(K)$ to $E(K)$:

$$[-1] : E(K) \to E(K) \qquad [2] : E(K) \to E(K)$$

$$(x, y) \mapsto (x, -y) \qquad (x, y) \mapsto \left(\frac{f'(x)^2}{4f(x)} - a - 2x, \cdots \right)$$

Example

The elliptic curve $E : y^2 = x^3 + x$ *over* $\mathbb{Q}$ *has an endomorphism* $[i] : (x, y) \mapsto (-x, iy)$. *Hence* $\mathbb{Z} \subsetneq \operatorname{End} E$.

Example

The elliptic curve $E : y^2 = x^3 + x$ *over* $\mathbb{Q}$ *has an endomorphism* $[i] : (x, y) \mapsto (-x, iy)$. *Hence* $\mathbb{Z} \subsetneq \operatorname{End} E$.

Definition

Let K *be an imaginary quadratic number field and let* $\mathcal{O}_K$ *be its ring of integers. Let* $\operatorname{End} E$ *be the ring of endomorphisms of* E. *If* $\operatorname{End} E \cong \mathcal{O}_K$, *then* E *is said to have complex multiplication by* $\mathcal{O}_K$.

Example

The elliptic curve $E : y^2 = x^3 + x$ *over* $\mathbb{Q}$ *has an endomorphism* $[i] : (x, y) \mapsto (-x, iy)$. *Hence* $\mathbb{Z} \subsetneq \operatorname{End} E$.

Definition

Let K *be an imaginary quadratic number field and let* $\mathcal{O}_K$ *be its ring of integers. Let* $\operatorname{End} E$ *be the ring of endomorphisms of* E. *If* $\operatorname{End} E \cong \mathcal{O}_K$, *then* E *is said to have complex multiplication by* $\mathcal{O}_K$.

Theorem (Main Theorem of Complex Multiplication)

Let K *be an imaginary quadratic number field and let* E *be an elliptic curve over* $\mathbb{C}$ *with complex multiplication by* $\mathcal{O}_K$. *Then*

$$H_K(1) = k_0 K$$

where k_0 *is the field of moduli of* E.

Assume all lattices are of the form $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$ with $\mathrm{Im}(\tau_1/\tau_2) > 0$.

Assume all lattices are of the form $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$ with $\mathrm{Im}(\tau_1/\tau_2) > 0$.

Definition (Weierstrass $\wp$-function)

The Weierstrass $\wp$-function for a lattice Λ is defined to be

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n \in \Lambda \setminus (0,0)} \left(\frac{1}{(z+n)^2} - \frac{1}{n^2} \right).$$

Assume all lattices are of the form $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$ with $\mathrm{Im}(\tau_1/\tau_2) > 0$.

Definition (Weierstrass $\wp$-function)

The Weierstrass $\wp$-function for a lattice Λ is defined to be

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n \in \Lambda \setminus (0,0)} \left(\frac{1}{(z+n)^2} - \frac{1}{n^2} \right).$$

Theorem

The Weierstrass $\wp_\Lambda$-function is an elliptic function. This means that:

- $\wp_\Lambda$ *has countably many poles.* — *meromorphic*
- $\wp_\Lambda(z) = \wp_\Lambda(z + \tau_1) = \wp_\Lambda(z + \tau_2)$. — *doubly-periodic*

Definition (Eisenstein series)

The Eisenstein series of weight $2k$ where $k \geq 2$ is an integer is defined by the following series:

$$G_{2k}(\Lambda) = \sum_{n \in \Lambda \setminus (0,0)} \frac{1}{n^{2k}}.$$

Definition (Eisenstein series)

The Eisenstein series of weight $2k$ where $k \geq 2$ is an integer is defined by the following series:

$$G_{2k}(\Lambda) = \sum_{n \in \Lambda \setminus (0,0)} \frac{1}{n^{2k}}.$$

Theorem

The Weierstrass $\wp_\Lambda$-function satisfies the ordinary non-linear differential equation:

$$\wp'_\Lambda = 4\wp_\Lambda^3 - g_2(\Lambda)\wp_\Lambda - g_3(\Lambda)$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$.

Consider the map

$$f : \mathbb{C} \to \mathbb{P}^2(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1).$$

Consider the map

$$f : \mathbb{C} \to \mathbb{P}^2(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1).$$

Theorem

The map f is well-defined modulo Λ.

Proof idea: $\wp_\Lambda$ and $\wp'_\Lambda$ are periodic with respect to the lattice.

Consider the map

$$f : \mathbb{C} \to \mathbb{P}^2(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1).$$

Theorem

The map f is well-defined modulo Λ.

Proof idea: $\wp_\Lambda$ and $\wp'_\Lambda$ are periodic with respect to the lattice.

Theorem

The image of f is an elliptic curve over $\mathbb{C}$.

Proof idea: It satisfies the differential equation of the form $y^2 = 4x^3 - g_2x - g_3$. With an invertible change of variables, $(x, y) \mapsto (x, y/2)$, we find that the image satisfies the equation $y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{C}$.

Theorem

The map

$$f : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z)/2 : 1)$$

defines an isomorphism between the complex torus $\mathbb{C}/\Lambda$ *and the elliptic curve given by the equation*

$$E_\Lambda : y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$$

Theorem

The map

$$f : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z)/2 : 1)$$

defines an isomorphism between the complex torus $\mathbb{C}/\Lambda$ *and the elliptic curve given by the equation*

$$E_\Lambda : y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$$

- Observe that $z \in \Lambda$ is sent to ∞.

Theorem

The map

$$f : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$$
$$z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z)/2 : 1)$$

defines an isomorphism between the complex torus $\mathbb{C}/\Lambda$ *and the elliptic curve given by the equation*

$$E_\Lambda : y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$$

- Observe that $z \in \Lambda$ is sent to ∞.
- One can check verify that this is a group isomorphism.

Definition

Two complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are said to be isomorphic if their lattices Λ and Λ' are homothetic (i.e. $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$).

Definition

Two complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are said to be isomorphic if their lattices Λ and Λ' are homothetic (i.e. $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$).

Definition

The j-invariant of a lattice can be defined as a function on lattices:

$$j(\Lambda) = \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$$

Definition

Two complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are said to be isomorphic if their lattices Λ and Λ' are homothetic (i.e. $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$).

Definition

The j-invariant of a lattice can be defined as a function on lattices:

$$j(\Lambda) = \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$$

Theorem

Two elliptic curves are isomorphic if and only if they have the same j-invariant.

This means that $j(\Lambda) = j(\alpha\Lambda)$ for any $\alpha \in \mathbb{C}^\times$.

Definition

A field K is called a field of definition of an elliptic curve $E = \mathbb{C}/\Lambda$ if there exists an elliptic curve E' isomorphic to E defined over K.

Let Λ be a lattice. For any $\alpha \in \mathbb{C}^\times$,

$$\mathbb{Q}(g_2(\alpha\Lambda), g_3(\alpha\Lambda))$$

is a field of definition for the elliptic curve Λ.

Definition

A field K is called a field of definition of an elliptic curve $E = \mathbb{C}/\Lambda$ if there exists an elliptic curve E' isomorphic to E defined over K.

Let Λ be a lattice. For any $\alpha \in \mathbb{C}^\times$,

$$\mathbb{Q}(g_2(\alpha\Lambda), g_3(\alpha\Lambda))$$

is a field of definition for the elliptic curve Λ.

Definition

There exists a unique minimal field of definition k_0 for any elliptic curve E over $\mathbb{C}$. This field is called its field of moduli.

The field of moduli of an elliptic curve $E = \mathbb{C}/\Lambda$ is $\mathbb{Q}(j(\Lambda))$.
We write $j(E)$ to denote $j(\Lambda)$ for any Λ such that $E \cong \mathbb{C}/\Lambda$.

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

- Let E be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$.

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

- Let E be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$.
- The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}$.

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

- Let E be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$.
- The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}$.
- One can show that $E \cong \mathbb{C}/\mathcal{O}_K$.

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

- Let E be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$.
- The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}$.
- One can show that $E \cong \mathbb{C}/\mathcal{O}_K$.

$$j(\mathcal{O}_K) = 320\left(1975 + 884\sqrt{5}\right).$$

- Thus, the field of moduli of E is $\mathbb{Q}(\sqrt{5})$

Theorem (Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(1) = k_0 K = K(j(E))$$

where k_0 is the field of moduli of E.

- Let E be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$.
- The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}$.
- One can show that $E \cong \mathbb{C}/\mathcal{O}_K$.

$$j(\mathcal{O}_K) = 320\left(1975 + 884\sqrt{5}\right).$$

- Thus, the field of moduli of E is $\mathbb{Q}(\sqrt{5})$.
- Thus, $H_K(1) = K(\sqrt{5})$.

Let E be the same elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ from the previous slide. Recall that we took

$$\Lambda = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}.$$

Let E be the same elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ from the previous slide. Recall that we took

$$\Lambda = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}.$$

There exists α such that $E_{\alpha\Lambda}$ is defined over $\mathbb{Q}(\sqrt{5})$. One example for α is:

$$\alpha \approx 1.480525.$$

Let E be the same elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ from the previous slide. Recall that we took

$$\Lambda = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}.$$

There exists α such that $E_{\alpha\Lambda}$ is defined over $\mathbb{Q}(\sqrt{5})$. One example for α is:

$$\alpha \approx 1.480525.$$

We have

$$g_2(\alpha\Lambda) = g_3(\alpha\Lambda) = -4a \qquad a = \left(\frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}\right)$$

Let E be the same elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ from the previous slide. Recall that we took

$$\Lambda = \mathbb{Z} + \sqrt{-5}\,\mathbb{Z}.$$

There exists α such that $E_{\alpha\Lambda}$ is defined over $\mathbb{Q}(\sqrt{5})$. One example for α is:

$$\alpha \approx 1.480525.$$

We have

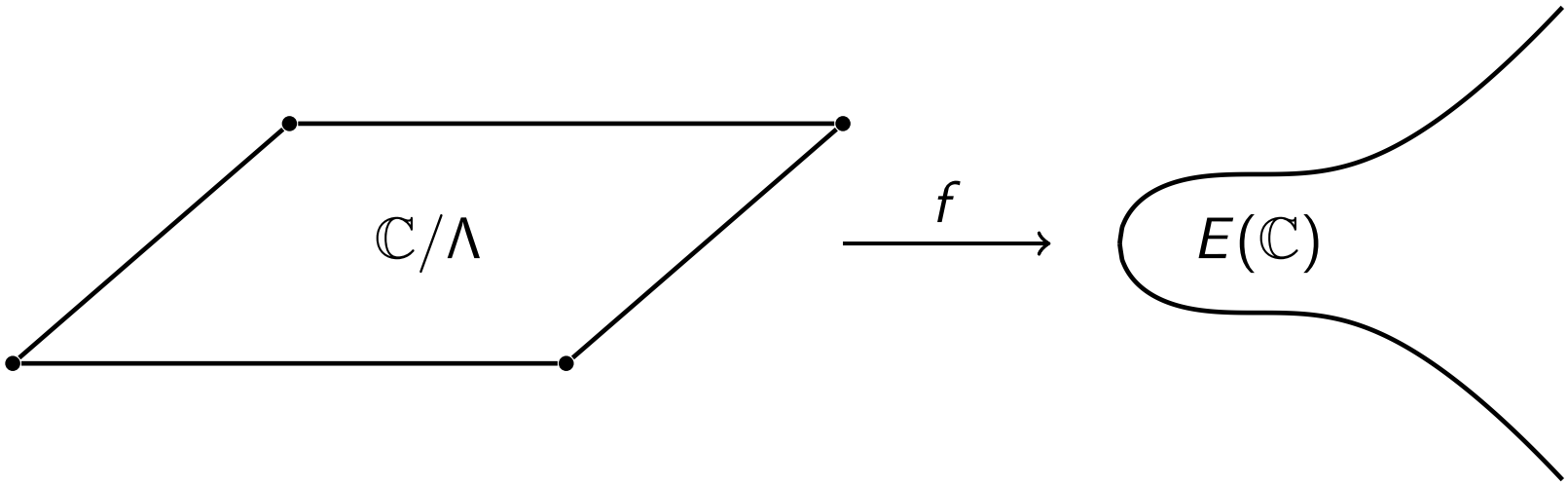
$$g_2(\alpha\Lambda) = g_3(\alpha\Lambda) = -4a \qquad a = \left(\frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}\right)$$

Then

$$E_{\alpha\Lambda} : x^3 - ax - a$$

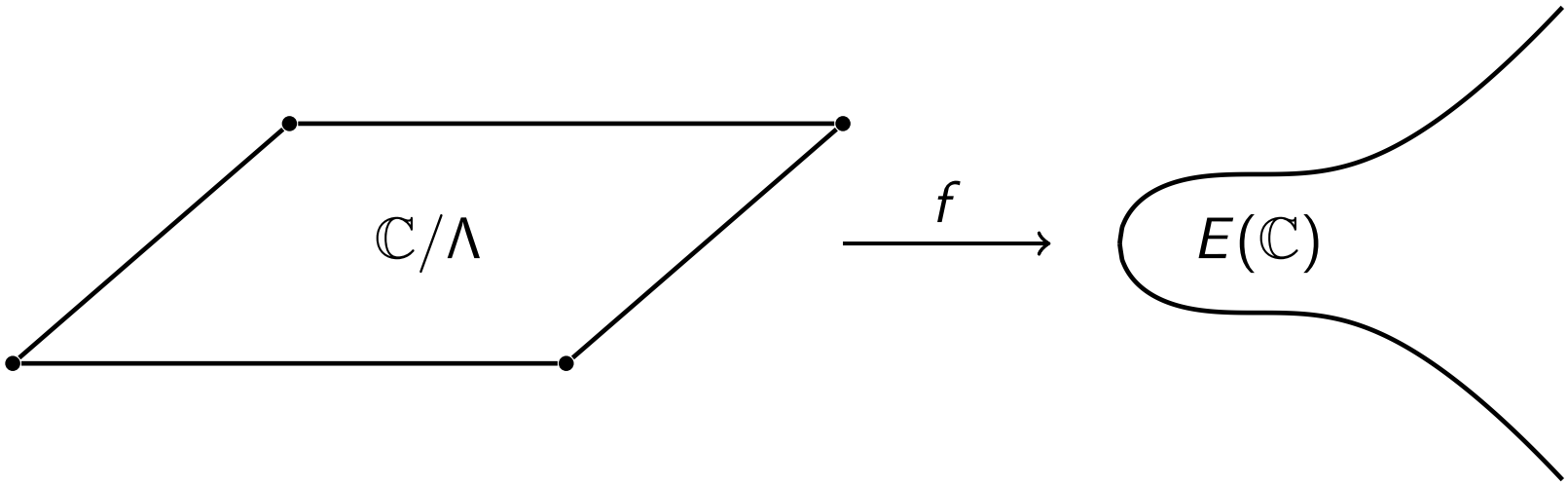
Notice that $a \in \mathbb{Q}(\sqrt{5})$.

Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

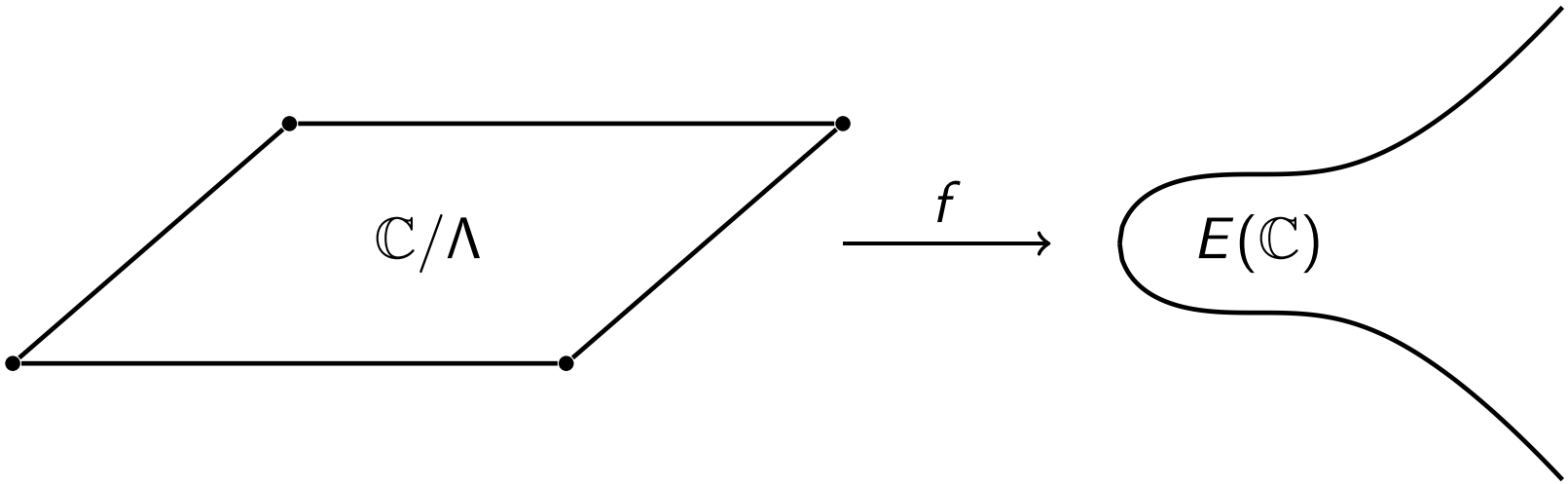
Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.

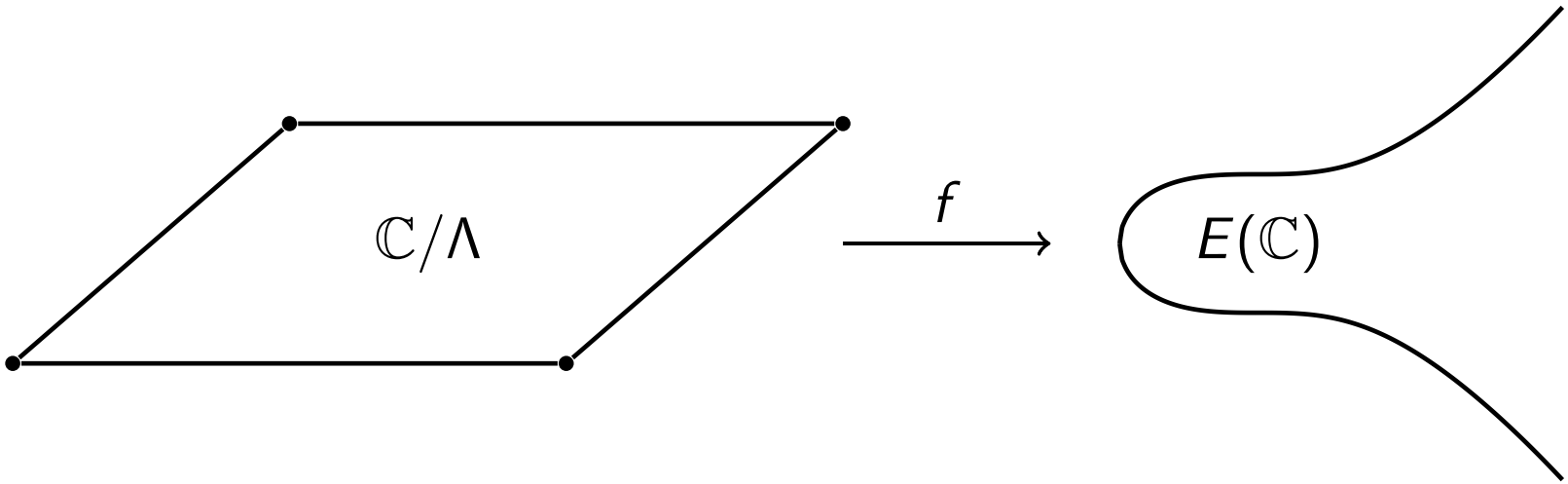
Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.
- The image of the map is a geometric object, an elliptic curve.

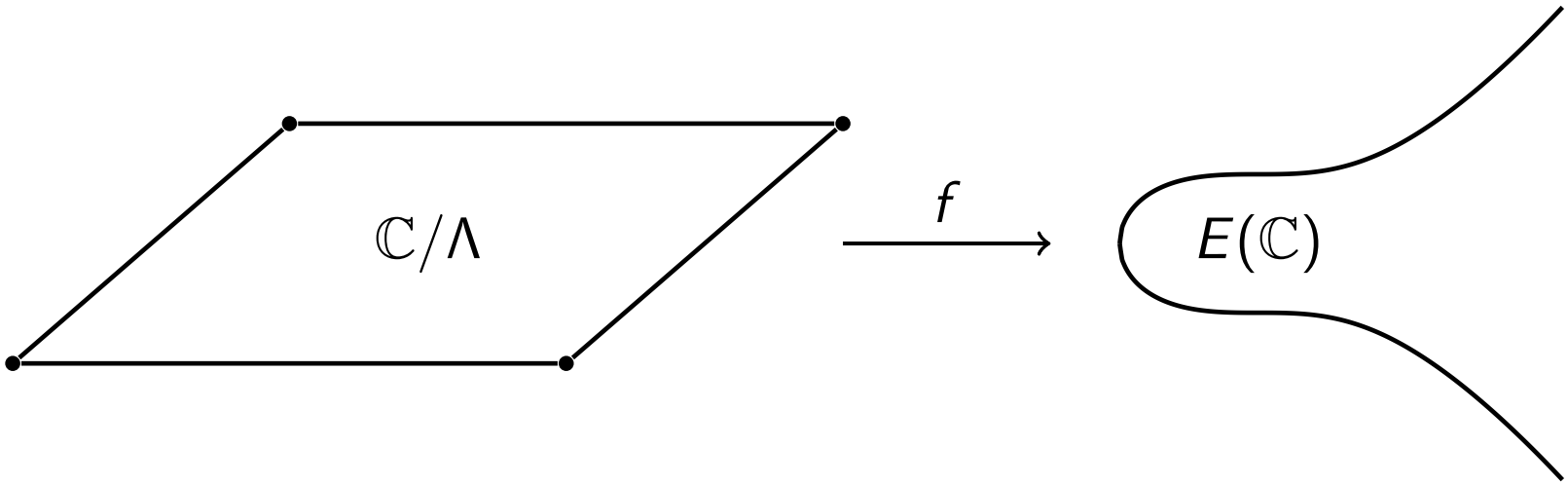
Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.
- The image of the map is a geometric object, an elliptic curve.
- Both domain and codomain have a group structure.

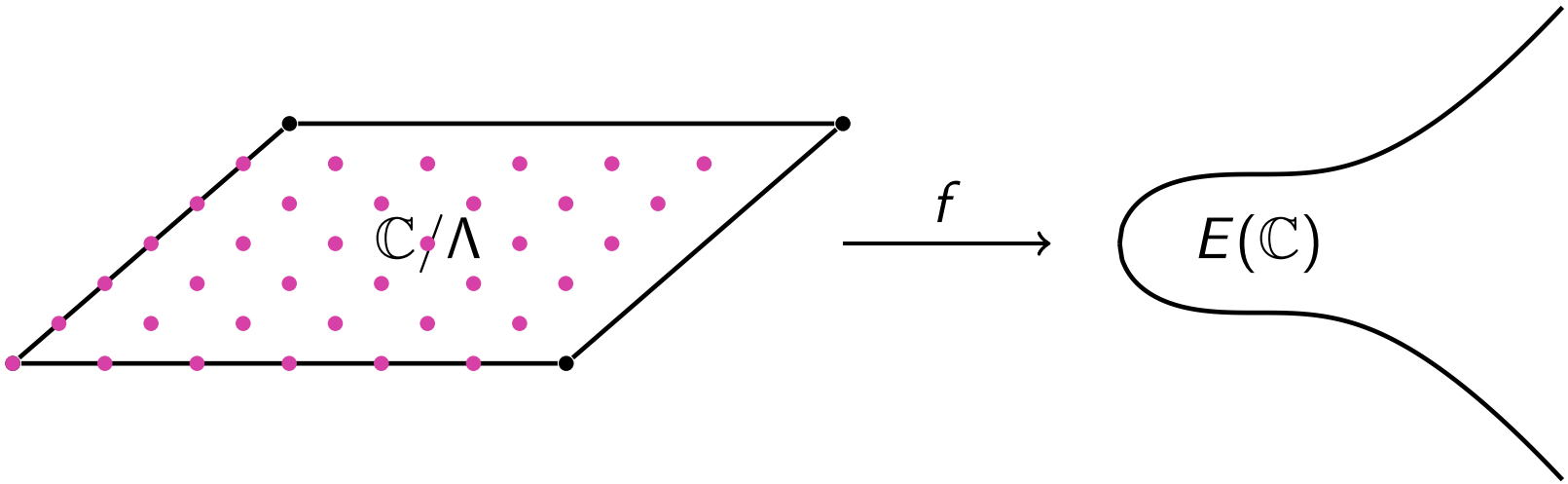
Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.
- The image of the map is a geometric object, an elliptic curve.
- Both domain and codomain have a group structure.
- The torsion points of the domain are easy to determine.

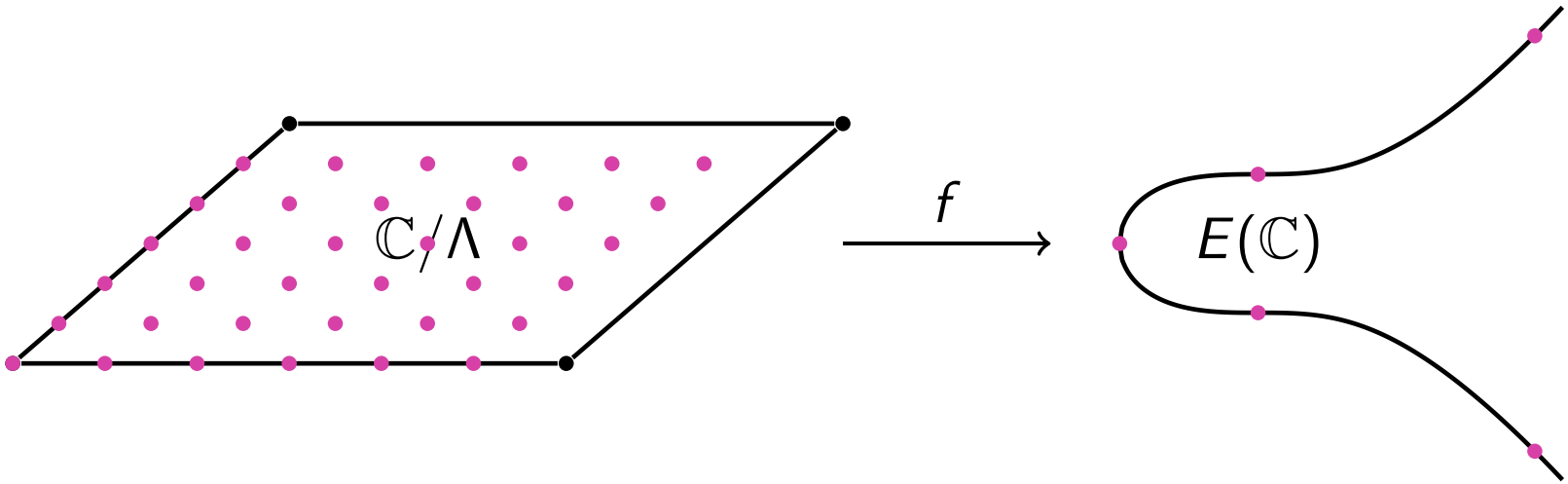
Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.
- The image of the map is a geometric object, an elliptic curve.
- Both domain and codomain have a group structure.
- The torsion points of the domain are easy to determine.

Recall that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $f : z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$:



Observations

- The kernel of the (original) map was $\Lambda \cong \mathbb{Z}^2$.
- The image of the map is a geometric object, an elliptic curve.
- Both domain and codomain have a group structure.
- The torsion points of the domain are easy to determine.
- The torsion points of the codomain have two coordinates!

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\mathrm{Aut}\, E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\mathrm{Aut}\, E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Recall $E_0 : x^3 - ax - a$ where $a = \frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}$.

- E_0 has complex multiplication by $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\operatorname{Aut} E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Recall $E_0 : x^3 - ax - a$ where $a = \frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}$.

- E_0 has complex multiplication by $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.
- The invertible elements of $\mathcal{O}_K$ are $\{\pm 1\}$. Thus, $\operatorname{Aut} E_0 = \{[\pm 1]\}$.

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\operatorname{Aut} E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Recall $E_0 : x^3 - ax - a$ where $a = \frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}$.

- E_0 has complex multiplication by $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.
- The invertible elements of $\mathcal{O}_K$ are $\{\pm 1\}$. Thus, $\operatorname{Aut} E_0 = \{[\pm 1]\}$.
- Since $x(P) = x(Q)$ if and only if $P = [\pm 1]Q$ then we can parametrize the points of $W := E_0/\operatorname{Aut} E_0$ by their x-coordinates.

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\operatorname{Aut} E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Recall $E_0 : x^3 - ax - a$ where $a = \frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}$.

- E_0 has complex multiplication by $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.
- The invertible elements of $\mathcal{O}_K$ are $\{\pm 1\}$. Thus, $\operatorname{Aut} E_0 = \{[\pm 1]\}$.
- Since $x(P) = x(Q)$ if and only if $P = [\pm 1]Q$ then we can parametrize the points of $W := E_0/\operatorname{Aut} E_0$ by their x-coordinates.
- Take $h : (x, y) \mapsto x$.

Definition (normalized Kummer variety)

Let E be an elliptic curve over $\mathbb{C}$ and let E_0 be an elliptic curve defined over its field of moduli k_0. The normalized Kummer variety of E is the pair (W, h) such that

- *W is the quotient of E_0 by its group $\operatorname{Aut} E_0$ of automorphisms.*
- *h is a morphism of varieties defined over k_0.*

Recall $E_0 : x^3 - ax - a$ where $a = \frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5}$.

- E_0 has complex multiplication by $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.
- The invertible elements of $\mathcal{O}_K$ are $\{\pm 1\}$. Thus, $\operatorname{Aut} E_0 = \{[\pm 1]\}$.
- Since $x(P) = x(Q)$ if and only if $P = [\pm 1]Q$ then we can parametrize the points of $W := E_0/\operatorname{Aut} E_0$ by their x-coordinates.
- Take $h : (x, y) \mapsto x$.
- (W, h) is a normalized Kummer variety of E.

Theorem (Second Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $H_K(1)$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = H_K(1)(h(t) : t \in \ker[m])$$

where (W, h) is a normalized Kummer variety for E.

Theorem (Second Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $H_K(1)$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = H_K(1)(h(t) : t \in \ker[m])$$

where (W, h) is a normalized Kummer variety for E.

We have solved for (W, h), a normalized Kummer variety for E.

- Recall W is a quotient of $E_0 = \mathbb{C}/\alpha\Lambda$ with $\alpha\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

Theorem (Second Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $H_K(1)$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = H_K(1)(h(t) : t \in \ker[m])$$

where (W, h) is a normalized Kummer variety for E.

We have solved for (W, h), a normalized Kummer variety for E.

- Recall W is a quotient of $E_0 = \mathbb{C}/\alpha\Lambda$ with $\alpha\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.
- Find the set T of 3-torsion points in $\mathbb{C}/\Lambda$. Easy! ex: $\omega_1/3 \in T$.

Theorem (Second Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $H_K(1)$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = H_K(1)(h(t) : t \in \ker[m])$$

where (W, h) is a normalized Kummer variety for E.

We have solved for (W, h), a normalized Kummer variety for E.

- Recall W is a quotient of $E_0 = \mathbb{C}/\alpha\Lambda$ with $\alpha\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.
- Find the set T of 3-torsion points in $\mathbb{C}/\Lambda$. Easy! ex: $\omega_1/3 \in T$.
- The x-coordinates of $E_0(\mathbb{C})$ are $\wp_{\alpha\Lambda}(z)$ for $z \in T$.

Theorem (Second Main Theorem of Complex Multiplication)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $H_K(1)$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = H_K(1)(h(t) : t \in \ker[m])$$

where (W, h) is a normalized Kummer variety for E.

We have solved for (W, h), a normalized Kummer variety for E.

- Recall W is a quotient of $E_0 = \mathbb{C}/\alpha\Lambda$ with $\alpha\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.
- Find the set T of 3-torsion points in $\mathbb{C}/\Lambda$. Easy! ex: $\omega_1/3 \in T$.
- The x-coordinates of $E_0(\mathbb{C})$ are $\wp_{\alpha\Lambda}(z)$ for $z \in T$.
- Hence, to get $H_K(3)$, we add to $H_K(1)$ the values of $\wp_{\alpha\Lambda}(z)$ for each $z \in T$.

We have:

$$\wp_{\alpha\Lambda}\left(\frac{\omega_1}{3}\right) = \frac{11}{486}\left(845 + 477\sqrt{15} + \sqrt{4120880 + 807270\sqrt{15}}\right)$$

$$\wp_{\alpha\Lambda}\left(\frac{\omega_2}{3}\right) = \frac{11}{486}\left(845 - 477\sqrt{15} - \sqrt{4120880 - 807270\sqrt{15}}\right)$$

$$\wp_{\alpha\Lambda}\left(\frac{\omega_1+\omega_2}{3}\right) = \frac{11}{486}\left(-845 - 379\sqrt{5} - \sqrt{-14070 - 6290\sqrt{5}}\right)$$

$$\wp_{\alpha\Lambda}\left(\frac{\omega_1+2\omega_2}{3}\right) = \frac{11}{486}\left(-845 - 379\sqrt{5} + \sqrt{-14070 - 6290\sqrt{5}}\right)$$

We find that $H_K(1)$ (those algebraic numbers above) $= H_K(1)(\sqrt{3})$.
Using the second main theorem of multiplication, we find that

$$H_K(3) = H_K(1)(\sqrt{3}) = K(\sqrt{5}, \sqrt{3}) \qquad K = \mathbb{Q}(\sqrt{-5})$$

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

Theorem (EC case)

Let K be an imaginary quadratic number field and let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_K(m) = K(j(E), h(t))$$

where $(E/\operatorname{Aut} E, h)$ is a normalized Kummer variety of E and t is a proper m-torsion point.

Theorem (PPAV case)

Let K be a CM field of degree $2g$ and let A be a simple g-dimensional principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then

$$H_{K^r}(m) \supseteq \underbrace{K^r(i(A), h(t))}_{\mathrm{CM}_{K^r}(m)}$$

where K^r is the reflex field of K and $(A/\operatorname{Aut} A, h)$ is a normalized Kummer variety of A and t is a proper m-torsion point.

What I (Try To) Do

- Take $g = 2$.
  i.e. K is a quartic CM field, A is a ppav of dimension 2
- Find $h(t)$ to compute $\mathrm{CM}_{K^r}(m)$.
- Figure out which are the proper m-torsion points.
- Determine which m satisfies $H_{K^r}(1) \subseteq \mathrm{CM}_{K^r}(m)$.
- Compute $H_{K^r}(1)$ as a subfield of $\mathrm{CM}_{K^r}(m)$.