Computing Hilbert class fields of quartic fields using complex multiplication

Jared Asuncion
supervisors: Andreas Enge, Marco Streng

28 November 2019

Definition (degree of a field extension)

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 (degree of a field extension)

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.

For example, consider the field extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$.
$\mathbb{Q}(\sqrt{-5})$ is a $\mathbb{Q}$-vector space with basis $\{1, \sqrt{-5}\}$.
Hence $[\mathbb{Q}[\sqrt{-5}] : \mathbb{Q}] = 2$.

Definition (degree of a field extension)

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.

Definition (degree of a field extension)

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.

$[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$. Hence it is a number field.

Definition (degree of a field extension)

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.

Definition (group of automorphisms of L fixing K)

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}\, L : \sigma(x) = x \text{ for each } x \in K\}$$

$\sigma \in \mathrm{Aut}\, L$ is an invertible ring homomorphism from L to L.

Definition (degree of a field extension)

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.

Definition (group of automorphisms of L fixing K)

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}\, L : \sigma(x) = x \text{ for each } x \in K\}$$

$\sigma \in \mathrm{Aut}\, L$ is an invertible ring homomorphism from L to L.

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) = \{\, a+b\sqrt{-5} \mapsto a + b\sqrt{-5},\ \ a+b\sqrt{-5} \mapsto a - b\sqrt{-5} \,\}.$$

It is a group of order 2.

Definition (degree of a field extension)

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.

Definition (group of automorphisms of L fixing K)

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}\, L : \sigma(x) = x \text{ for each } x \in K\}$$

Definition (abelian extension)

A number field extension L/K is said to be an abelian extension if:

- $|\mathrm{Aut}(L/K)| = [L : K]$ *i.e. a Galois extension*
- $\mathrm{Aut}(L/K)$ *is commutative.*

Theorem (Kronecker-Weber Theorem)

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

Theorem (Kronecker-Weber Theorem)

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

Example

$$\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\zeta_{20})$$

where $\zeta_{20} = \exp(2\pi i \cdot 1/20)$.

$$\sqrt{-5} = 2\zeta_{20}^7 - \zeta_{20}^5 + 2\zeta_{20}^3.$$

Theorem (Kronecker-Weber Theorem)

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

Theorem (Kronecker-Weber Theorem)

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

Class Field Theory

Assume $K = \mathbb{Q}$ or K is a number field such that there does NOT exist an injective ring homomorphism $\sigma : K \hookrightarrow \mathbb{R}$. i.e. K has no real embeddings

Theorem (Kronecker-Weber Theorem)

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

Class Field Theory

Assume $K = \mathbb{Q}$ or K is a number field such that there does NOT exist an injective ring homomorphism $\sigma : K \hookrightarrow \mathbb{R}$. i.e. K has no real embeddings

Class field theory tells us:

- The existence of a ray class field $H_K(m)$.
- Every finite degree abelian extension of K is contained in a ray class field $H_K(m)$.
- Information on the structure of $\mathrm{Aut}(H_K(m)/K)$.

Theorem (Kronecker-Weber Theorem)

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

Class Field Theory

Assume $K = \mathbb{Q}$ or K is a number field such that there does NOT exist an injective ring homomorphism $\sigma : K \hookrightarrow \mathbb{R}$. i.e. K has no real embeddings

Class field theory tells us:

- The existence of a ray class field $H_K(m)$.
- Every finite degree abelian extension of K is contained in a ray class field $H_K(m)$.
- Information on the structure of $\mathrm{Aut}(H_K(m)/K)$.

$$H_{\mathbb{Q}}(m) = \mathbb{Q}(\zeta_m) \qquad \mathrm{Aut}(H_{\mathbb{Q}}(m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

$$\zeta_m := \exp(2\pi i \cdot 1/m) \qquad \zeta_m \mapsto \zeta_m^n \leftrightarrow n \in (\mathbb{Z}/m\mathbb{Z})^\times$$

Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

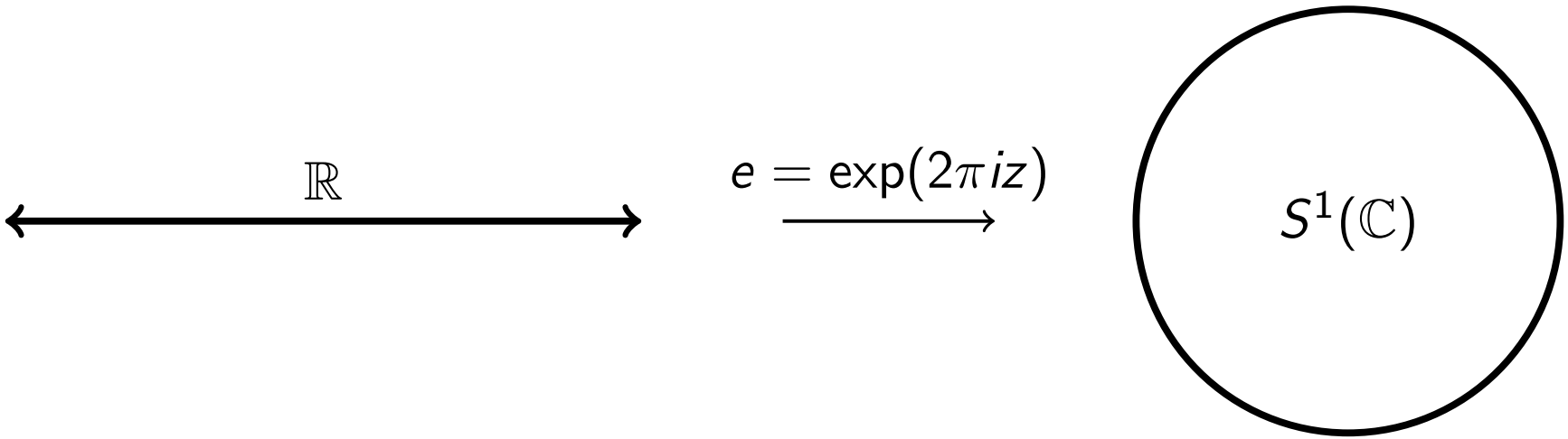
Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

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



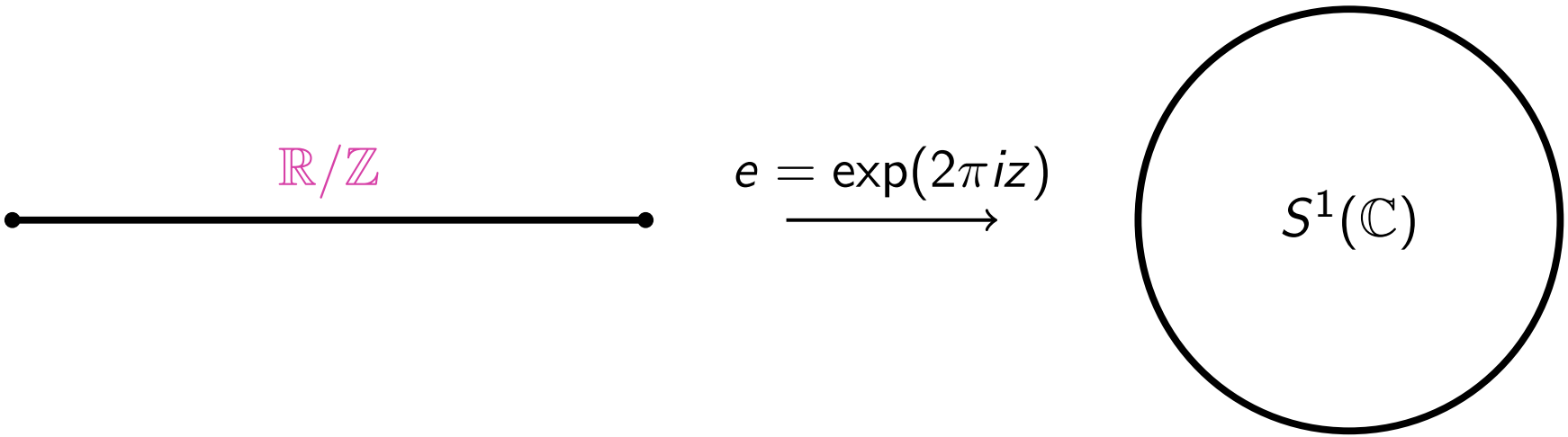
Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

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



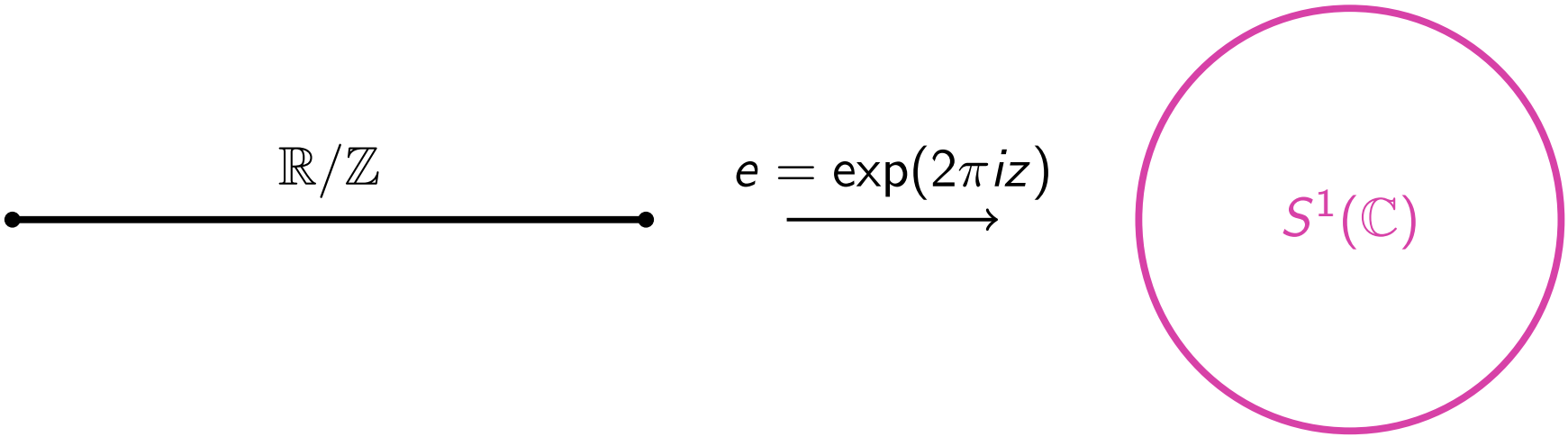
Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

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



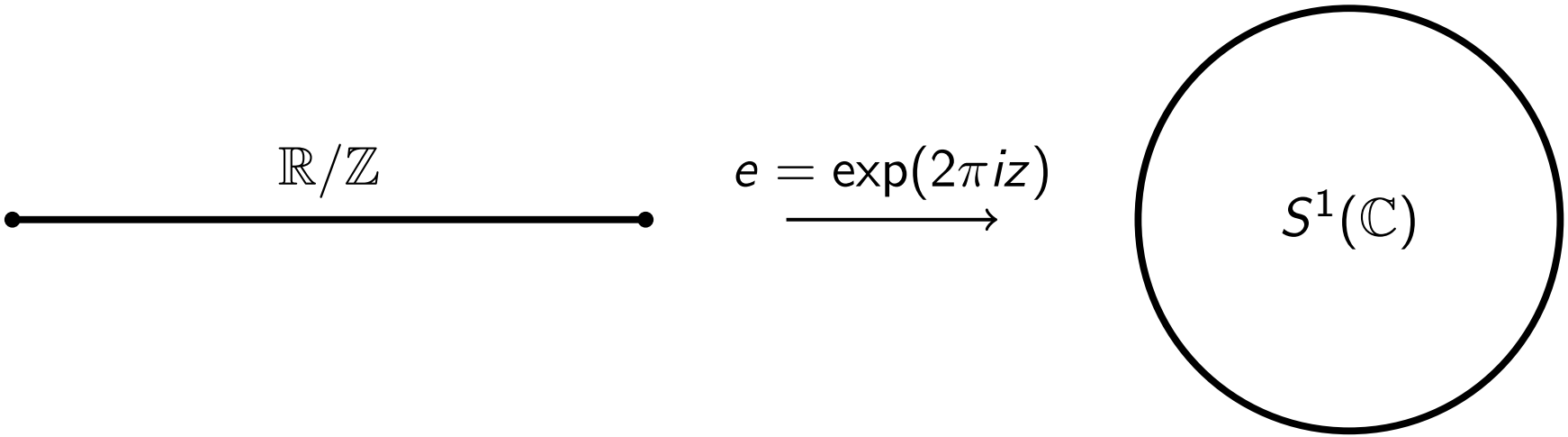
Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

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



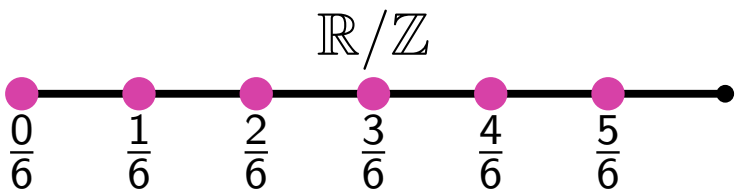
Theorem (Kronecker-Weber Theorem)

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

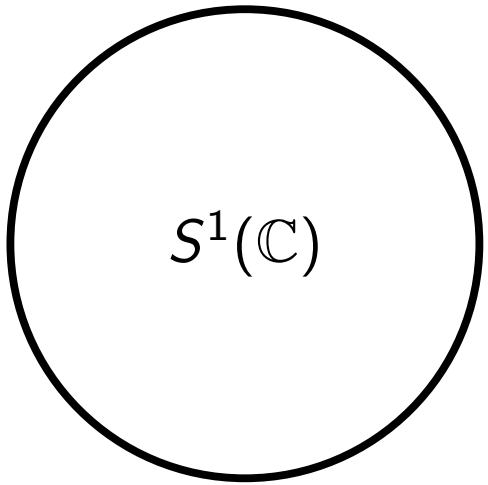
Problem (Hilbert's 12th Problem)

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

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



$$e = \exp(2\pi iz) \longrightarrow$$



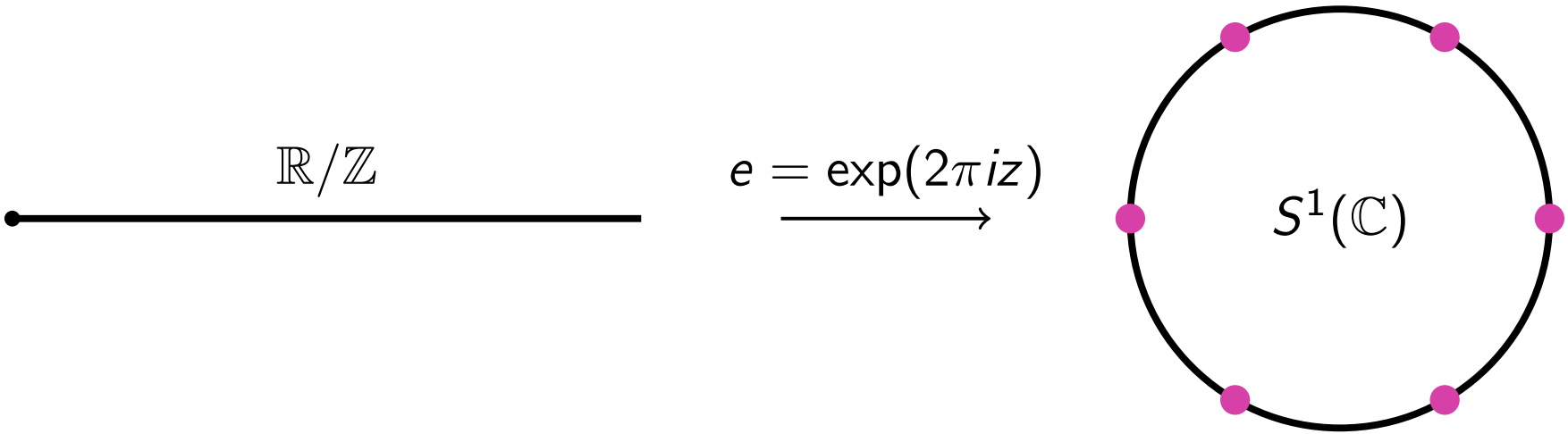
Theorem (Kronecker-Weber Theorem)

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

Problem (Hilbert's 12th Problem)

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

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



Only other explicitly solved case: imaginary quadratic number fields:

$$K = \mathbb{Q}(\sqrt{-D}) \qquad\qquad D > 0.$$

Instead of a circle, the geometric object is an elliptic curve.

Only other explicitly solved case: imaginary quadratic number fields:

$$K = \mathbb{Q}(\sqrt{-D}) \qquad\qquad D > 0.$$

Instead of a circle, the geometric object is an elliptic curve.

Definition (eliptic curve)

An elliptic curve defined over $\mathbb{C}$ is a smooth projective curve given by an equation of the form

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

where $a, b \in \mathbb{C}$ and $x^3 + ax + b$ has no double roots.

Only other explicitly solved case: imaginary quadratic number fields:

$$K = \mathbb{Q}(\sqrt{-D}) \qquad\qquad D > 0.$$

Instead of a circle, the geometric object is an elliptic curve.

Definition (eliptic curve)

An elliptic curve defined over $\mathbb{C}$ is a smooth projective curve given by an equation of the form

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

where $a, b \in \mathbb{C}$ and $x^3 + ax + b$ has no double roots.

- There is a unique point $\infty = (0 : 1 : 0)$ when we set $Z = 0$.

Only other explicitly solved case: imaginary quadratic number fields:

$$K = \mathbb{Q}(\sqrt{-D}) \qquad\qquad D > 0.$$

Instead of a circle, the geometric object is an elliptic curve.

Definition (eliptic curve)

An elliptic curve defined over $\mathbb{C}$ is a smooth projective curve given by an equation of the form

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

where $a, b \in \mathbb{C}$ and $x^3 + ax + b$ has no double roots.

- There is a unique point $\infty = (0 : 1 : 0)$ when we set $Z = 0$.
- We usually write $y^2 = x^3 + ax + b$ instead. $Z \neq 0$.

Only other explicitly solved case: imaginary quadratic number fields:

$$K = \mathbb{Q}(\sqrt{-D}) \qquad D > 0.$$

Instead of a circle, the geometric object is an elliptic curve.

Definition (eliptic curve)

An elliptic curve defined over $\mathbb{C}$ is a smooth projective curve given by an equation of the form

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

where $a, b \in \mathbb{C}$ and $x^3 + ax + b$ has no double roots.

- There is a unique point $\infty = (0 : 1 : 0)$ when we set $Z = 0$.
- We usually write $y^2 = x^3 + ax + b$ instead. $Z \neq 0$.
- $E(\mathbb{C}) = \{\infty\} \cup \{(x, y) \in \mathbb{C} \times \mathbb{C} : y^2 = x^3 + ax + b\}$ has a group structure. The identity element is ∞.

Observation 1

Since $E(\mathbb{C})$ is a group, for any $m \in \mathbb{Z}_{>0}$, the multiplication-by-m is a group homomorphism from E to E (i.e. an endomorphism).

$$\mathbb{Z} \subseteq \operatorname{End} E.$$

$$\begin{aligned}[-1] : E(\mathbb{C}) &\to E(\mathbb{C}) \\ (x, y) &\mapsto (x, -y)\end{aligned}$$

Observation 1

Since $E(\mathbb{C})$ is a group, for any $m \in \mathbb{Z}_{>0}$, the multiplication-by-m is a group homomorphism from E to E (i.e. an endomorphism).

$$\mathbb{Z} \subseteq \operatorname{End} E.$$

Observation 2

Some elliptic curves, such as $\tilde{E} : y^2 = x^3 + x$, have more endomorphisms.

$$[-1] : \tilde{E}(\mathbb{C}) \to \tilde{E}(\mathbb{C}) \qquad (x, y) \mapsto (x, -y)$$

$$[i] : \tilde{E}(\mathbb{C}) \to \tilde{E}(\mathbb{C}) \qquad (x, y) \mapsto (-x, iy)$$

Observation 1

Since $E(\mathbb{C})$ is a group, for any $m \in \mathbb{Z}_{>0}$, the multiplication-by-m is a group homomorphism from E to E (i.e. an endomorphism).

$$\mathbb{Z} \subseteq \operatorname{End} E.$$

Observation 2

Some elliptic curves, such as $\tilde{E} : y^2 = x^3 + x$, have more endomorphisms.

$$[-1] : \tilde{E}(\mathbb{C}) \to \tilde{E}(\mathbb{C}) \qquad (x, y) \mapsto (x, -y)$$

$$[i] : \tilde{E}(\mathbb{C}) \to \tilde{E}(\mathbb{C}) \qquad (x, y) \mapsto (-x, iy)$$

$$\operatorname{End} \tilde{E} \cong \mathbb{Z} + \mathbb{Z}i = \mathcal{O}_K \qquad K = \mathbb{Q}(i)$$

Fact

Let E be an elliptic curve over $\mathbb{C}$. Then

$$\mathbb{C}/\Lambda \cong E(\mathbb{C})$$

for some lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ with

$$\tau \in \mathbb{H}_1 = \{x + yi \in \mathbb{C} : x, y \in \mathbb{R},\ y > 0\}.$$

Fact

Let E be an elliptic curve over $\mathbb{C}$. Then

$$\mathbb{C}/\Lambda \cong E(\mathbb{C})$$

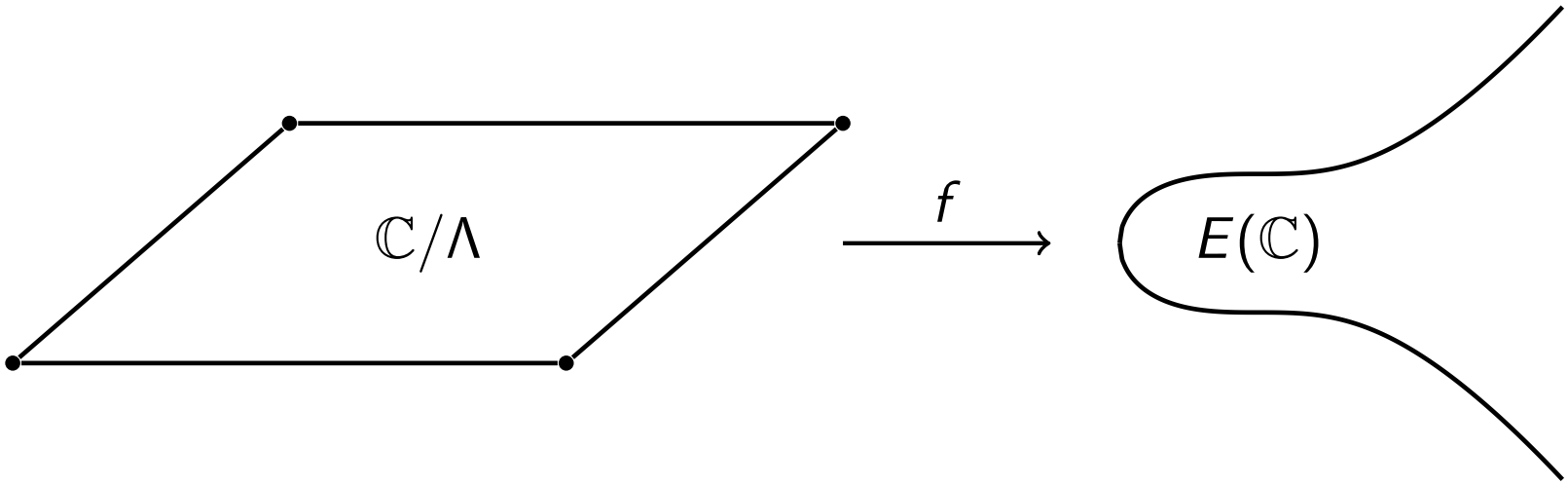
for some lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ with

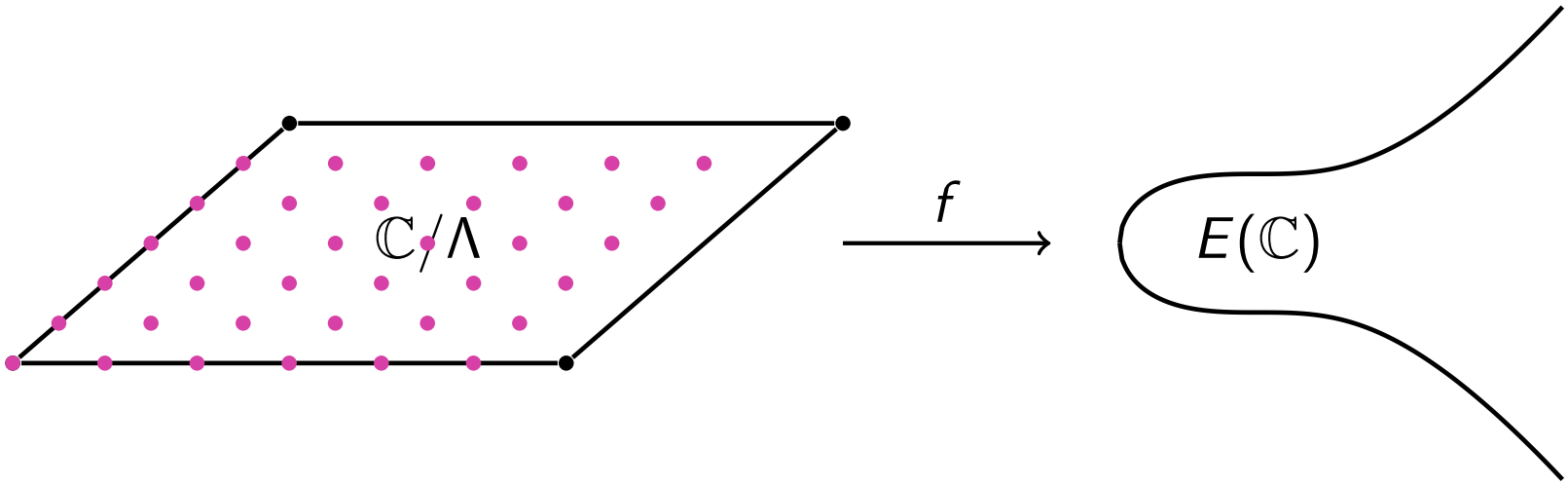
$$\tau \in \mathbb{H}_1 = \{x + yi \in \mathbb{C} : x, y \in \mathbb{R},\ y > 0\}.$$

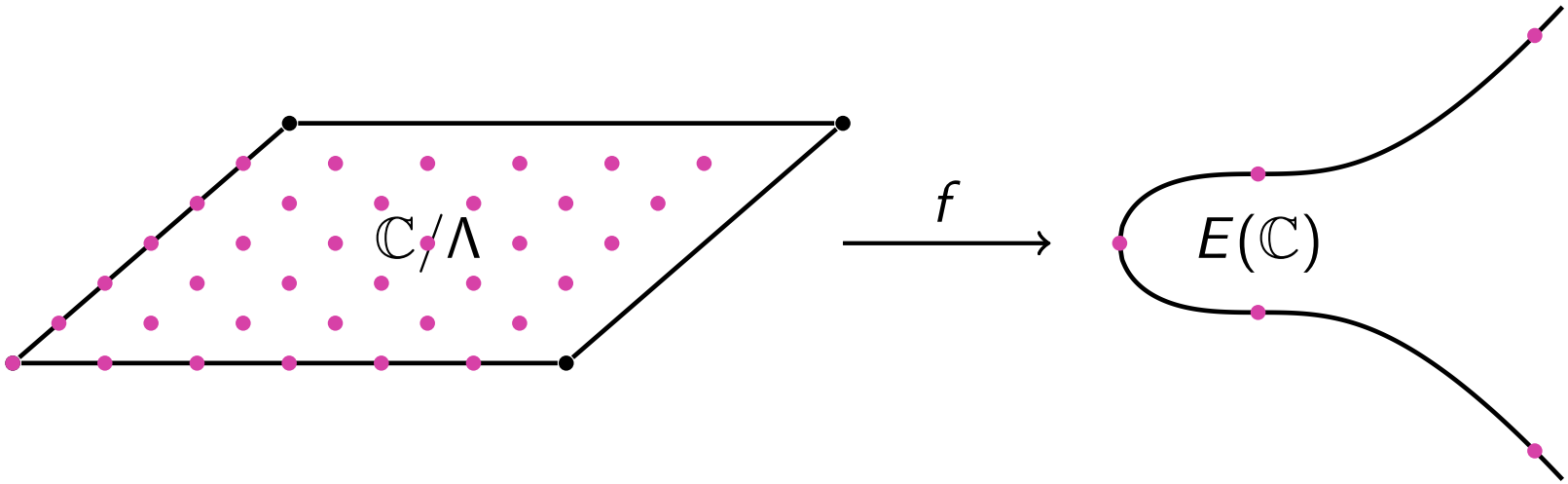
There exists a map $j : \mathbb{H}_1 \to \mathbb{C}$ such that

$$j(\tau) = j(\tau') \qquad \Leftrightarrow \qquad \mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$$

This map is called the j-invariant.
We will write $j(E) := j(\tau)$ for the j-invariant of $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$.


$\mathbb{C}/\Lambda$
f
$E(\mathbb{C})$


$\mathbb{C}/\Lambda$
f
$E(\mathbb{C})$

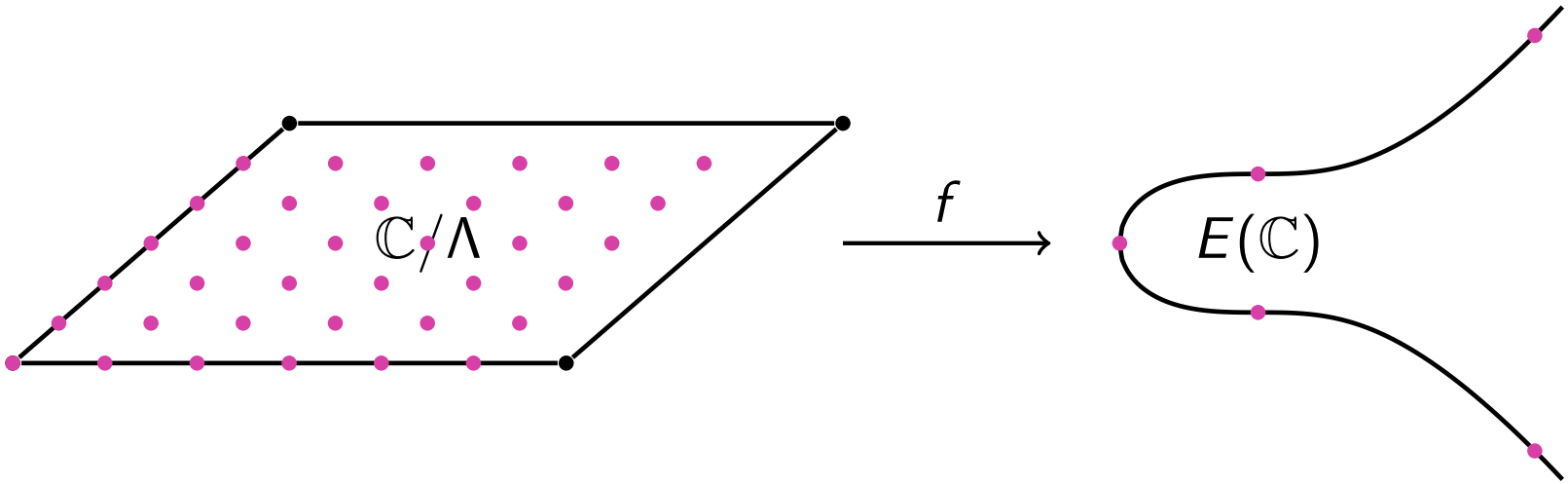

$\mathbb{C}/\Lambda$
f
$E(\mathbb{C})$

Theorem

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be a complex elliptic curve such that $\operatorname{End} E \cong \mathcal{O}_K$. *Then:*

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C})\,,\ [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).



Definition (CM field)

A CM-field K is a totally imaginary number field (no embeddings $\sigma : K \hookrightarrow \mathbb{R}$ exist) which is a degree 2 extension of a totally real number field K_0 (image of all embeddings $\sigma : K_0 \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$).

Definition (CM field)

A CM-field K is a totally imaginary number field (no embeddings $\sigma : K \hookrightarrow \mathbb{R}$ exist) which is a degree 2 extension of a totally real number field K_0 (image of all embeddings $\sigma : K_0 \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$).

For degree 4 (quartic) CM-fields K:

cyclic

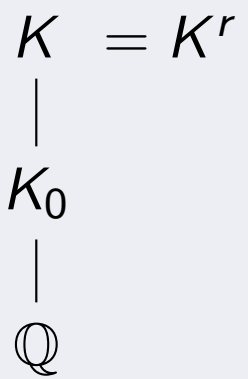
$$\begin{array}{ll} K & = K^r \\ | & \\ K_0 & \\ | & \\ \mathbb{Q} & \end{array}$$

Definition (CM field)

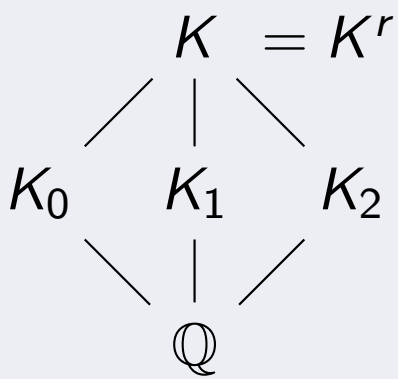
A CM-field K is a totally imaginary number field (no embeddings $\sigma : K \hookrightarrow \mathbb{R}$ exist) which is a degree 2 extension of a totally real number field K_0 (image of all embeddings $\sigma : K_0 \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$).

For degree 4 (quartic) CM-fields K:

cyclic



bicyclic

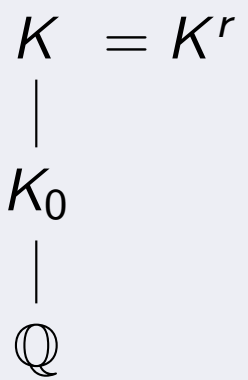


Definition (CM field)

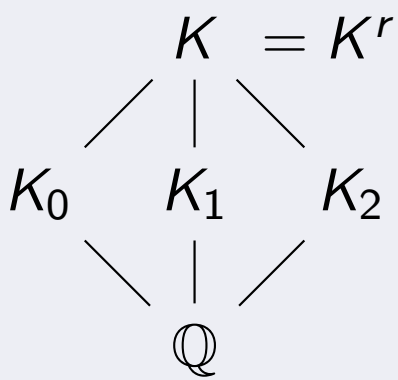
A CM-field K is a totally imaginary number field (no embeddings $\sigma : K \hookrightarrow \mathbb{R}$ exist) which is a degree 2 extension of a totally real number field K_0 (image of all embeddings $\sigma : K_0 \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$).

For degree 4 (quartic) CM-fields K:

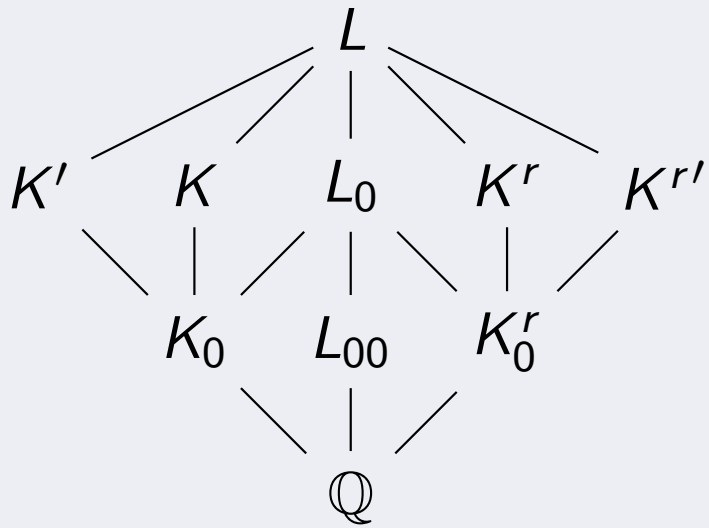
cyclic



bicyclic



not Galois

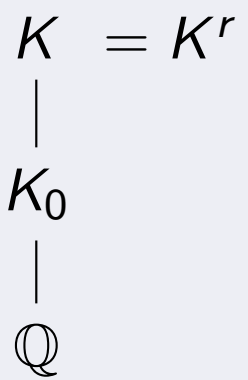


Definition (CM field)

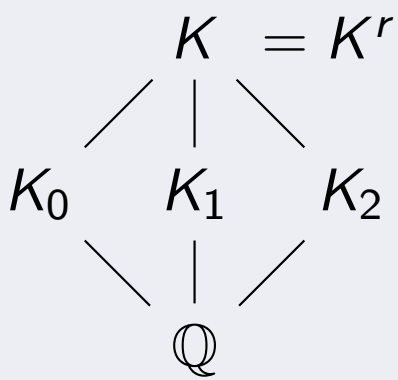
A CM-field K is a totally imaginary number field (no embeddings $\sigma : K \hookrightarrow \mathbb{R}$ exist) which is a degree 2 extension of a totally real number field K_0 (image of all embeddings $\sigma : K_0 \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$).

For degree 4 (quartic) CM-fields K:

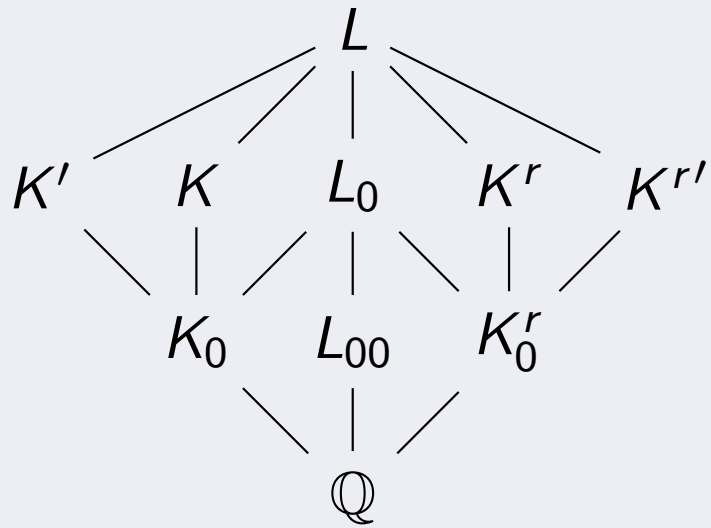
cyclic



bicyclic



not Galois



primitive $\Leftrightarrow$ cyclic or non-Galois

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C}),\ [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C})\,, [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,, [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C}),\ [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C}),\ [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C}),\ [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C})\,, [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,, [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C})\,, [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,, [m](P) = \infty)$$

where h is an analogue of the Weber function.

Theorem (Main Theorem of CM (ec))

Let K be an imaginary quadratic number field. Let $m \in \mathbb{Z}_{>0}$.
Let E be an elliptic curve over $\mathbb{C}$ such that $\operatorname{End} E \cong \mathcal{O}_K$. Then:

$$H_K(m) = K(j(E),\ h(P) : P \in E(\mathbb{C})\,, [m](P) = \infty)$$

where h is a Weber function (a 'normalized' x-coordinate function).

Theorem (Main Theorem of CM (ppas), Shimura-Taniyama, 1950s)

Let K be a primitive quartic CM field. Let $m \in \mathbb{Z}_{>0}$.
Let A be a principally polarized abelian surface over $\mathbb{C}$ such that $\operatorname{End} A \cong \mathcal{O}_K$. Then:

$$H_{K^r}(m) \supseteq K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,, [m](P) = \infty)$$

where h is an analogue of the Weber function.

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,,\ [m](P) = \infty)$$

Theorem (Shimura, 1962)

Let K^r be the reflex field of a primitive quartic CM field K. There exists $m \in \mathbb{Z}_{>0}$ such that

$$H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m) \qquad (\star)$$

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

Theorem (Shimura, 1962)

Let K^r be the reflex field of a primitive quartic CM field K. There exists $m \in \mathbb{Z}_{>0}$ such that

$$H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m) \qquad (\star)$$

- (Crespo 1989) Embedding problems with ramification conditions
- (Cohen 1999) Advanced topics in computational number theory

Theorem (A.)

Let S be a finite set of prime ideals of $\mathcal{O}_{K^r}$ such that:
S contains all prime ideals above 2 and $|\mathrm{Cl}_{K^r}(1)/\langle S\rangle|$ is odd.
Let $P = \{p : p$ is a rational prime below $\mathfrak{p}$ for some $\mathfrak{p} \in S\}$.
Let $m = 4\prod_{p\in P} p$. Then $\star$ is satisfied.

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C})\,,\ [m](P) = \infty)$$

What We Know

For a primitive quartic CM field K:

- how to find an m such that $H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m)$.
- how to decide if $H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m)$ for any $m \in \mathbb{Z}_{>0}$.
- how to compute $H_{K_0^r}(m)$ (using Stark's conjectures)
- how to compute a defining polynomial for $\mathrm{CM}_{K^r}(m)$ for $m = 1, 2$.
- how to compute a defining polynomial for $H_{K^r}(1)$ by viewing it as a subfield of $\mathrm{CM}_{K^r}(2)$

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

What We Know

For a primitive quartic CM field K:

- how to find an m such that $H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m)$.
- how to decide if $H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m)$ for any $m \in \mathbb{Z}_{>0}$.
- how to compute $H_{K_0^r}(m)$ (using Stark's conjectures)
- how to compute a defining polynomial for $\mathrm{CM}_{K^r}(m)$ for $m = 1, 2$.
- how to compute a defining polynomial for $H_{K^r}(1)$ by viewing it as a subfield of $\mathrm{CM}_{K^r}(2)$

What We Have

- working implementation of the above computations
- example for which our implementation is faster than Kummer theory implementations in Magma and PARI

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

Things to Work On

- how to find $\mathrm{CM}_{K^r,\Phi^r}(m)$ for any other m.
- statistics on how often an integer $m \in \mathbb{Z}_{>0}$ is the minimal m such that

$$H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m).$$

$$\mathrm{CM}_{K^r} = K^r(i(A),\ h(P) : P \in A(\mathbb{C}),\ [m](P) = \infty)$$

Things to Work On

- how to find $\mathrm{CM}_{K^r,\Phi^r}(m)$ for any other m.
- statistics on how often an integer $m \in \mathbb{Z}_{>0}$ is the minimal m such that

$$H_{K^r}(1) \subseteq H_{K_0^r}(m) \cdot \mathrm{CM}_{K^r}(m).$$

Dank u voor uw aandacht.