Abelian extensions of number fields

Jared Asuncion

ALGANT Symposium

Definition

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

Definition

An abelian extension is a Galois extension in which the Galois group G is abelian.

Theorem (Kronecker-Weber Theorem (KWT))

The abelian extensions of $K = \mathbb{Q}$ are generated by values at rational arguments τ of the exponential function $\tau \mapsto \exp(2\pi i\tau)$.

Theorem (Kronecker-Weber Theorem (KWT))

The abelian extensions of $K = \mathbb{Q}$ are generated by values at rational arguments τ of the exponential function $\tau \mapsto \exp(2\pi i\tau)$.

Hilbert's twelfth problem

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

Theorem (Kronecker-Weber Theorem (KWT))

The abelian extensions of $K = \mathbb{Q}$ are generated by values at rational arguments τ of the exponential function $\tau \mapsto \exp(2\pi i\tau)$.

Hilbert's twelfth problem

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

Class field theory

Class field theory

- tells us that every finite abelian extension L of a number field K is contained in some *ray class field extension* $H_K(m)$ of K.
- gives us the structure of $\mathrm{Gal}(H_K(m)/K)$.

Theorem

For any integer $m \in \mathbb{Z}$:

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

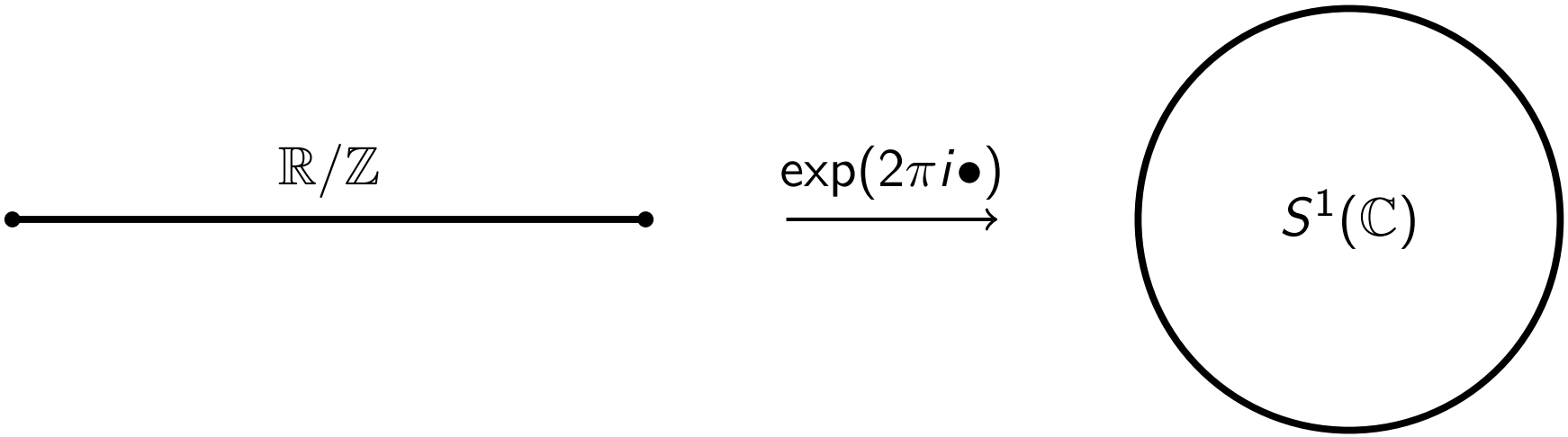
for any $n \in \mathbb{Z}$ coprime to m.

Theorem

For any integer $m \in \mathbb{Z}$:

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

for any $n \in \mathbb{Z}$ coprime to m.

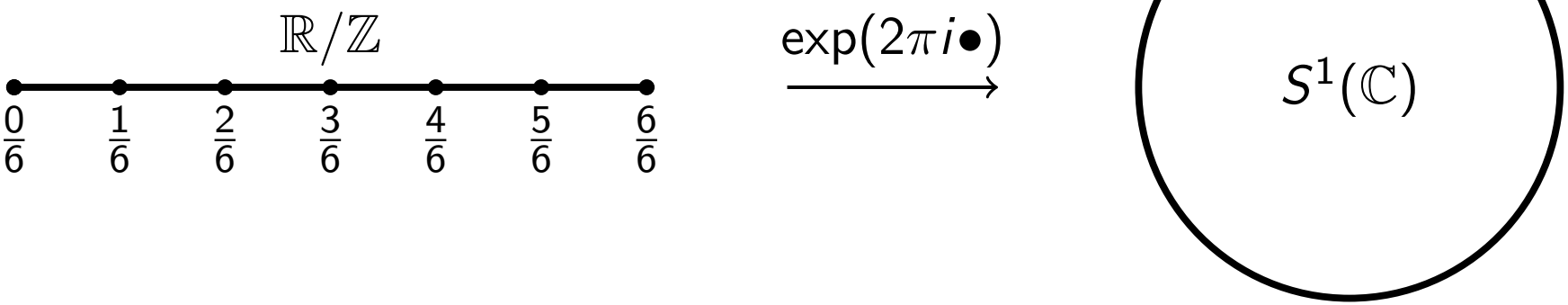


Theorem

For any integer $m \in \mathbb{Z}$:

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

for any $n \in \mathbb{Z}$ coprime to m.

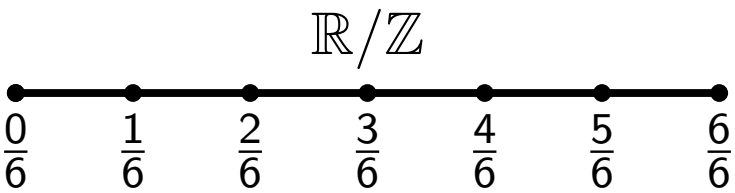


Theorem

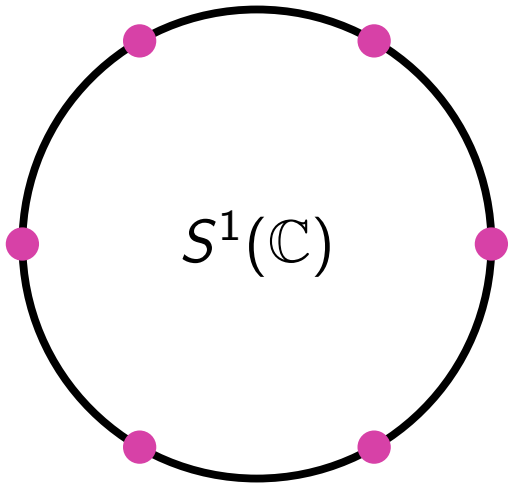
For any integer $m \in \mathbb{Z}$:

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

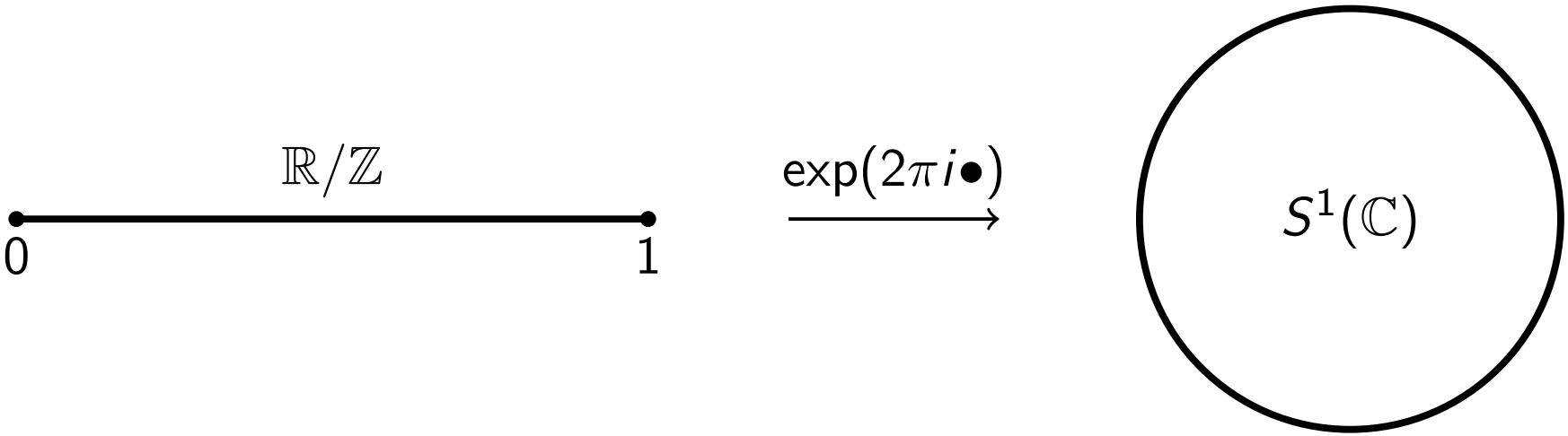
for any $n \in \mathbb{Z}$ coprime to m.



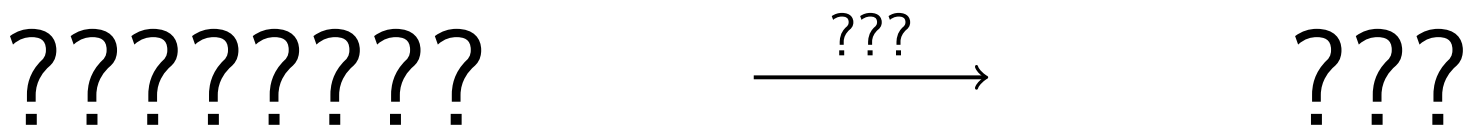
$\exp(2\pi i \bullet)$ $\longrightarrow$



For $K = \mathbb{Q}$, we have the following situation:



We have an analogue for when K is an imaginary quadratic number field.
i.e. $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$



Definition

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

$$y^2 = f(x) = x^3 + ax + b$$

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

An elliptic curve E over $\mathbb{C}$ is isomorphic to a complex torus.
That is, there exists an isomorphism

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

for some lattice Λ.

Definition

The j-invariant of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined to be

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

Consider an elliptic curve over $\mathbb{C}$, isomorphic to the complex torus $\mathbb{C}/\Lambda$. Then

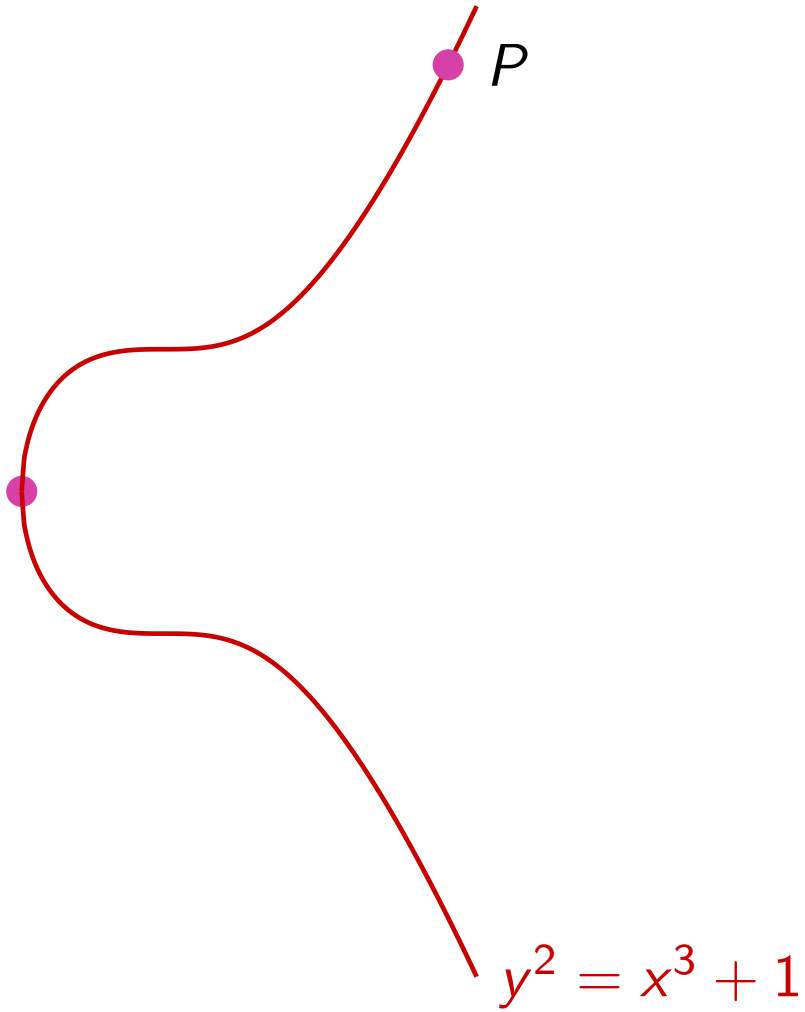
$$j(E) = \frac{60G_4(\Lambda)^3}{(60G_4(\Lambda))^3 - (140G_6(\Lambda))^2}$$

where $G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus 0} \omega^{-k}$, the kth Eisenstein series.

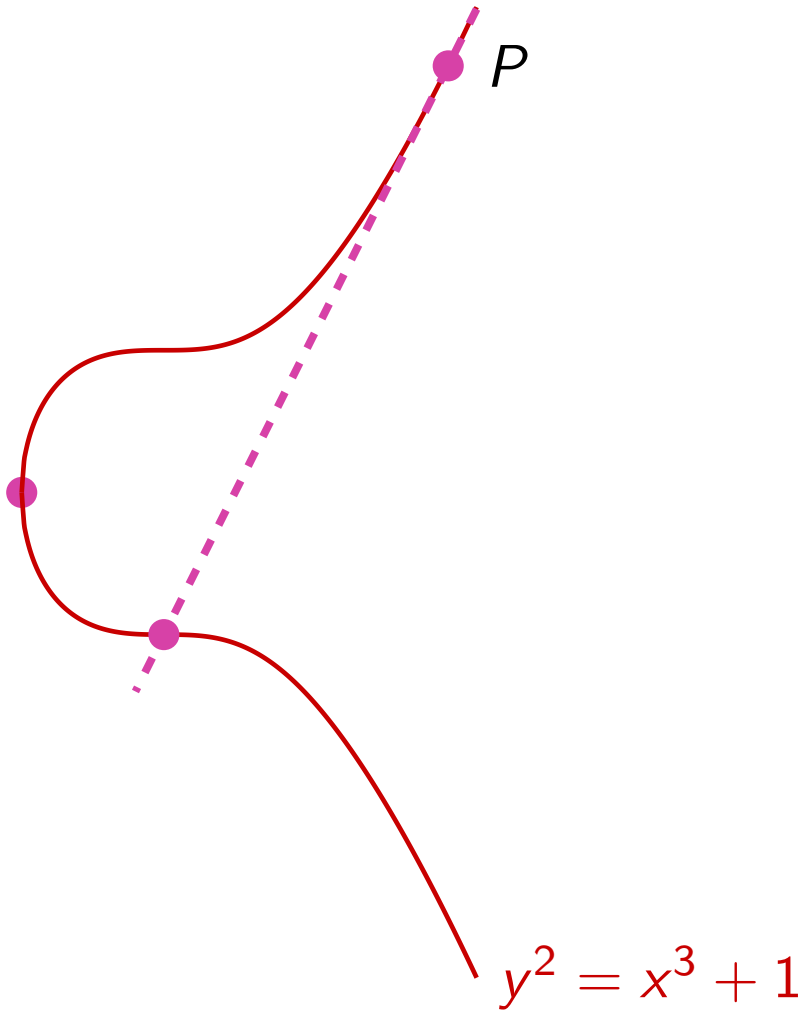
Remark

Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if they have the same j-invariant.

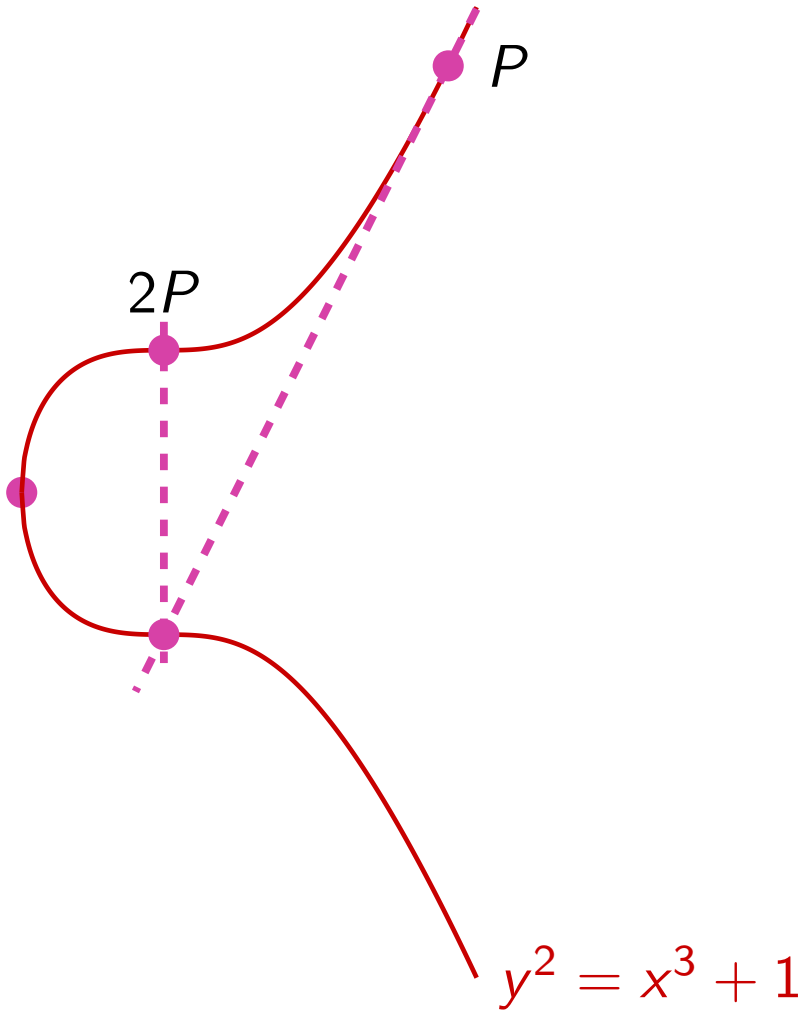
An elliptic curve has a group structure.



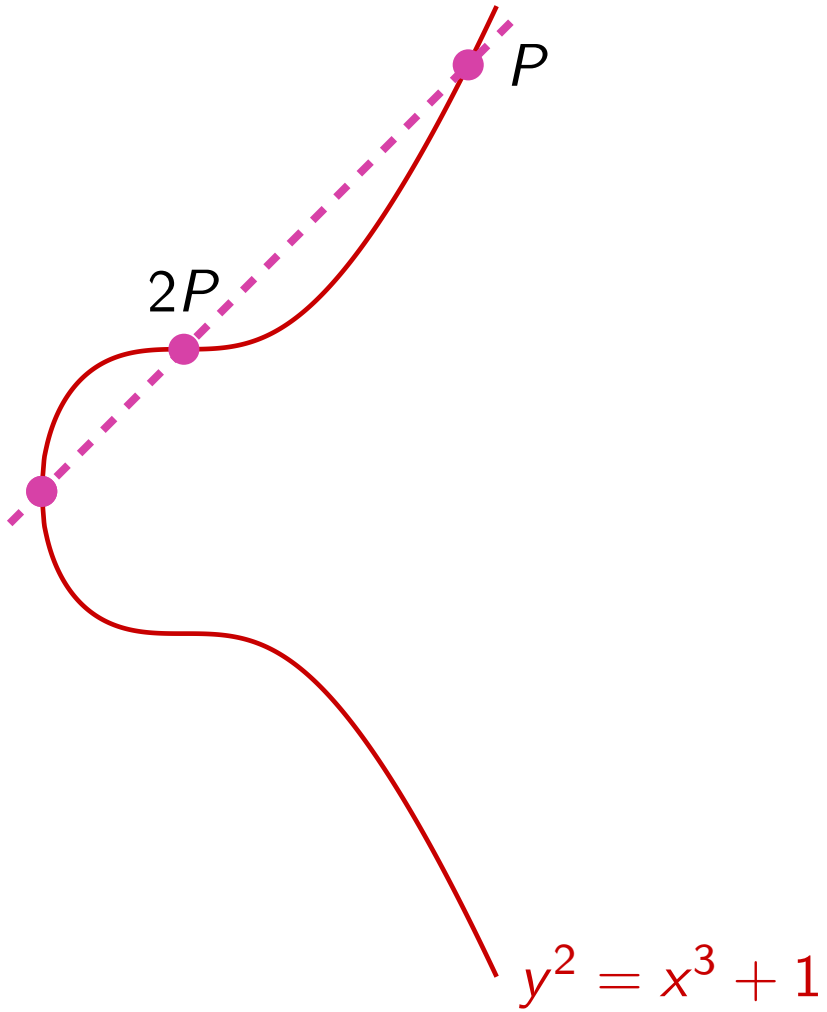
An elliptic curve has a group structure.



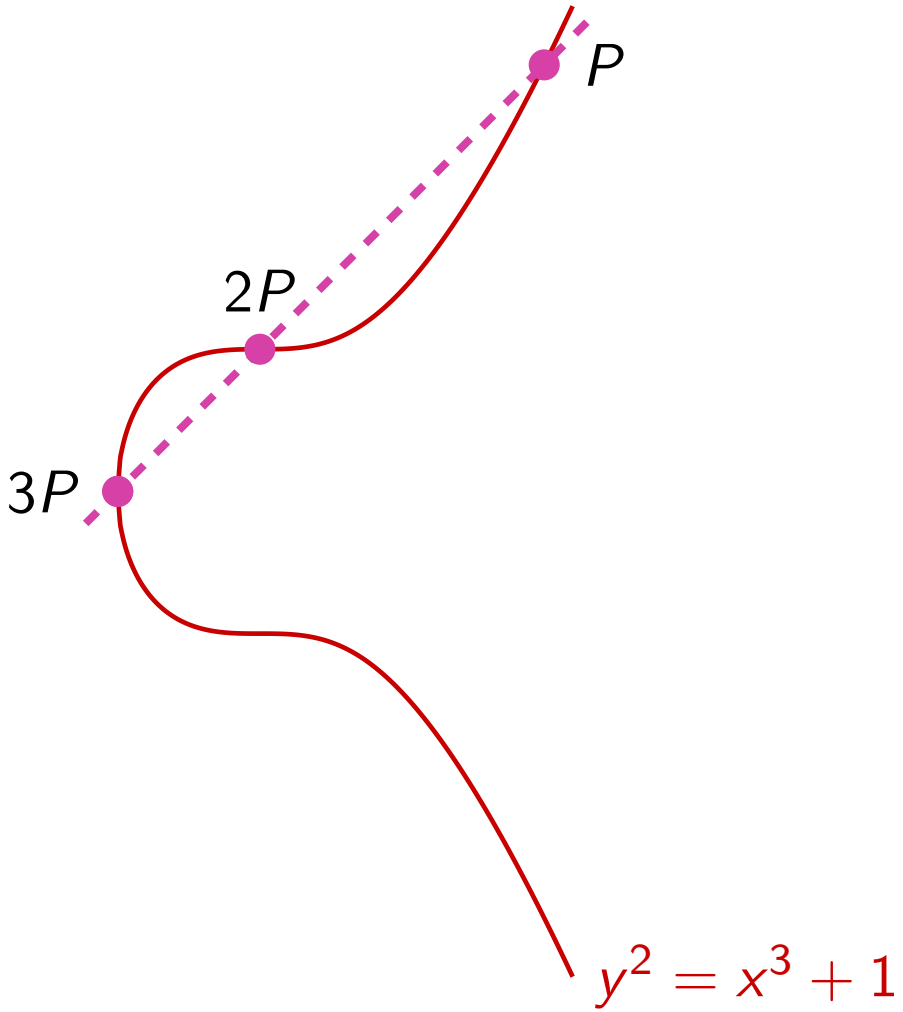
An elliptic curve has a group structure.



An elliptic curve has a group structure.



An elliptic curve has a group structure.



Definition

The multiplication-by-m map is a morphism which sends a point $P \in E$ to the point $mP \in E$.

The multiplication-by-m map is an endomorphism for any m. Hence

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

Definition

Let K be an imaginary quadratic number field. We say E has complex multiplication (CM) by $\mathcal{O}_K$ if there exists an inclusion $\mathcal{O}_K \hookrightarrow \operatorname{End} E$.

The elliptic curve

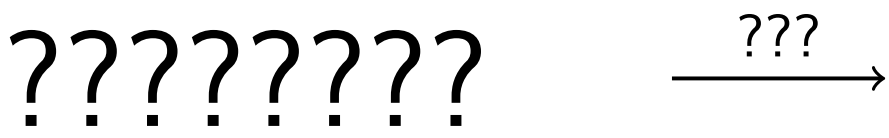
$$E : y^2 = x^3 + 1$$

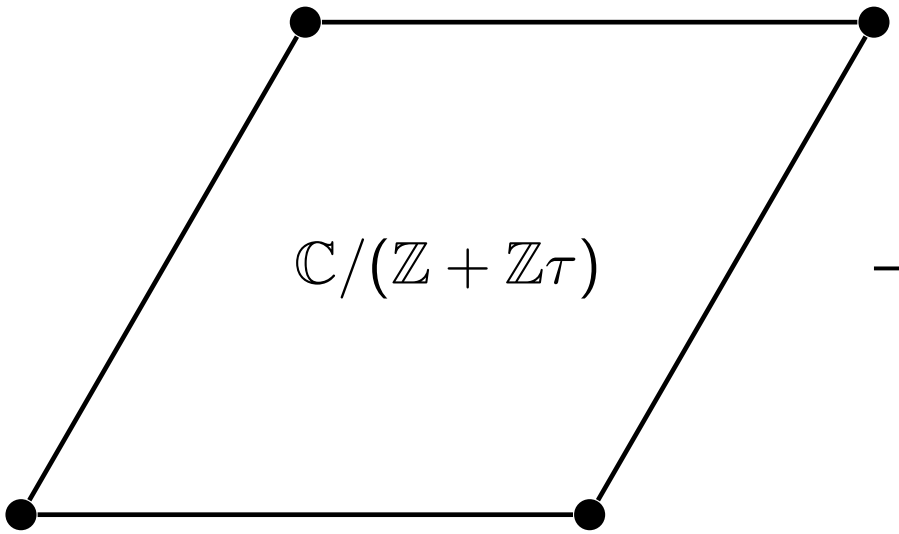
over $\mathbb{Q}$ has an endomorphism $w : (x, y) \mapsto (\zeta_3 x, y)$. In fact, $\mathbb{Z}[\zeta_3] \subset \operatorname{End} E$.

Theorem

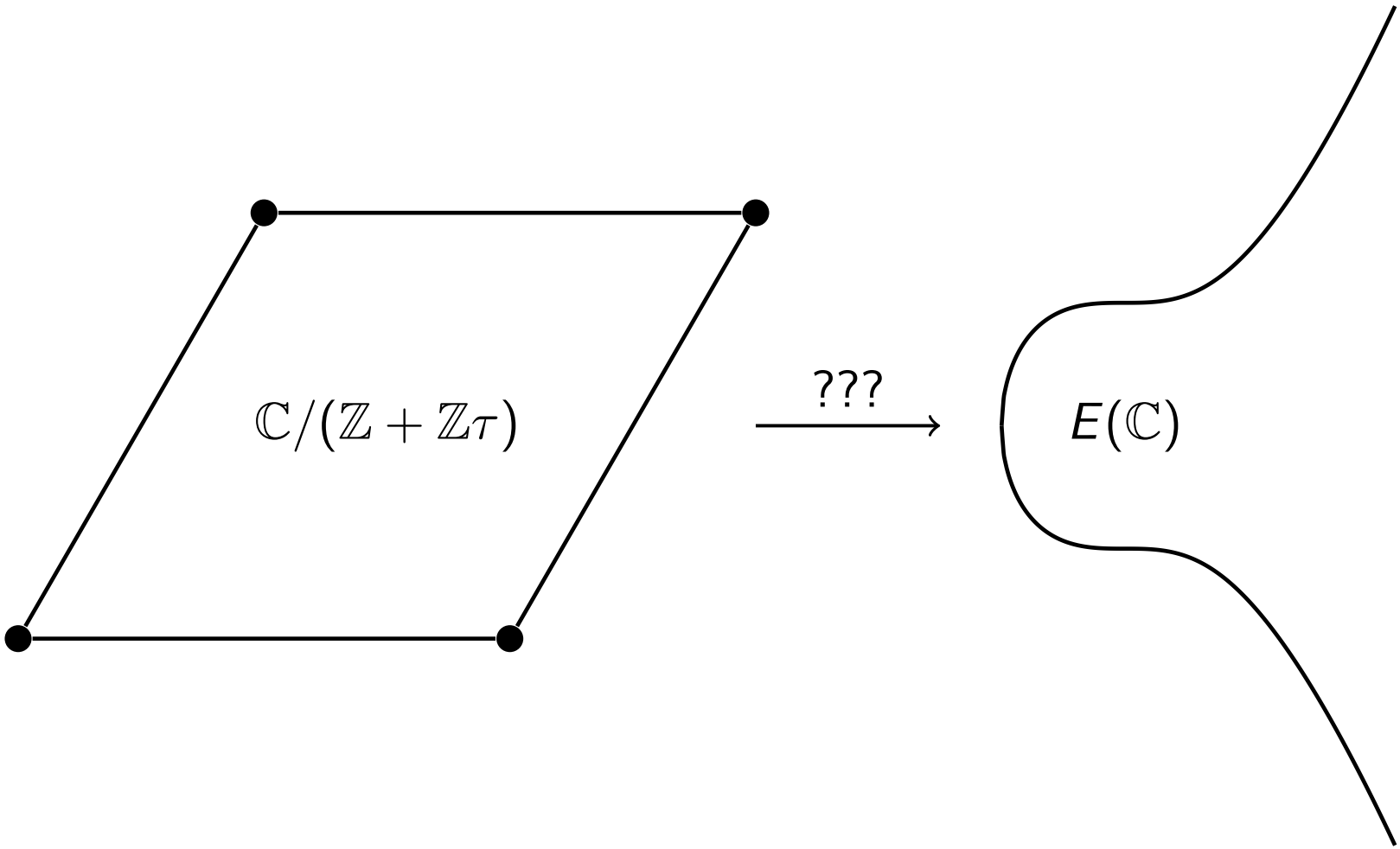
For an elliptic curve E over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ then

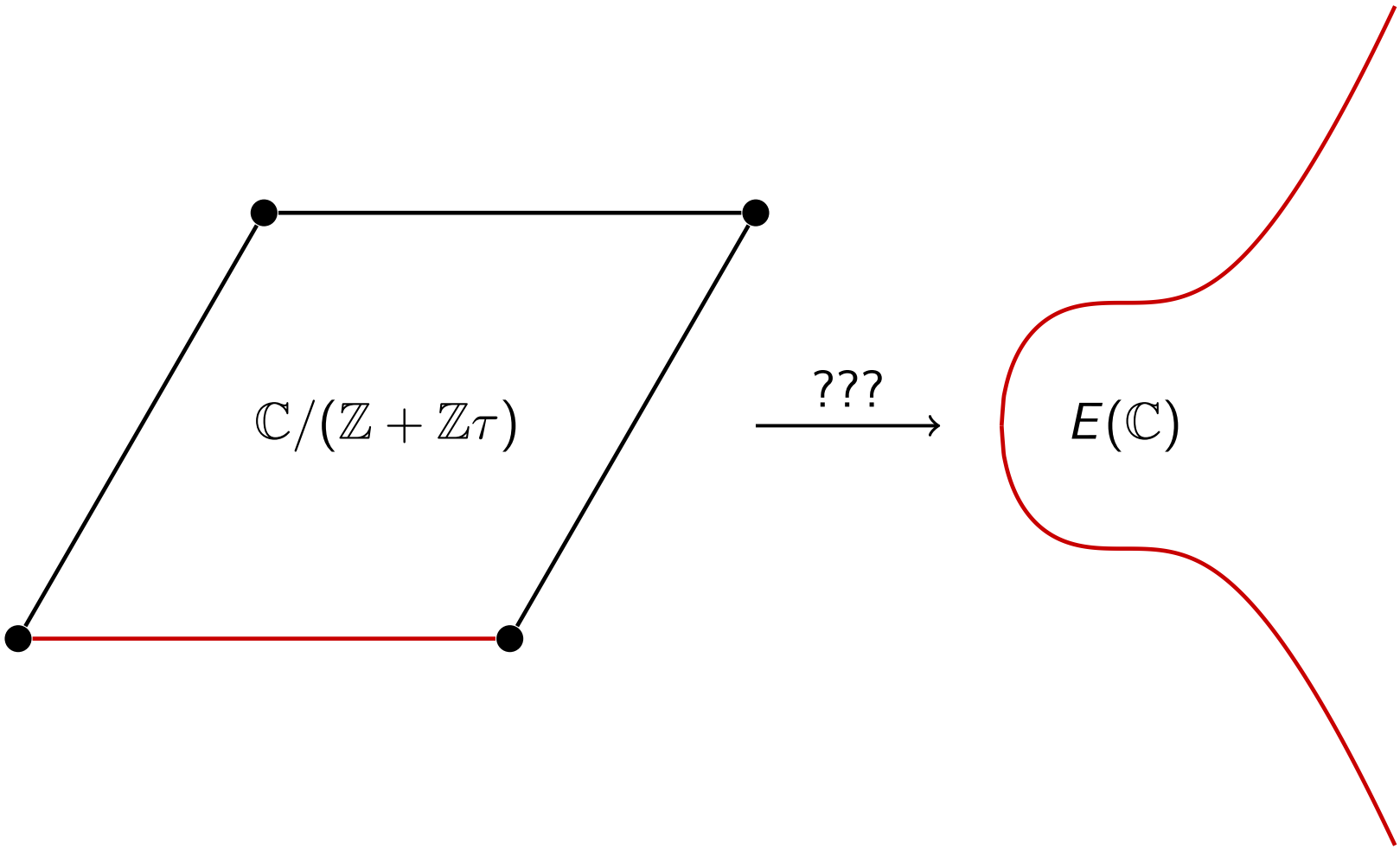
$$H_K(1) = K(j(E))$$
$$H_K(m) = K(j(E), ???)$$

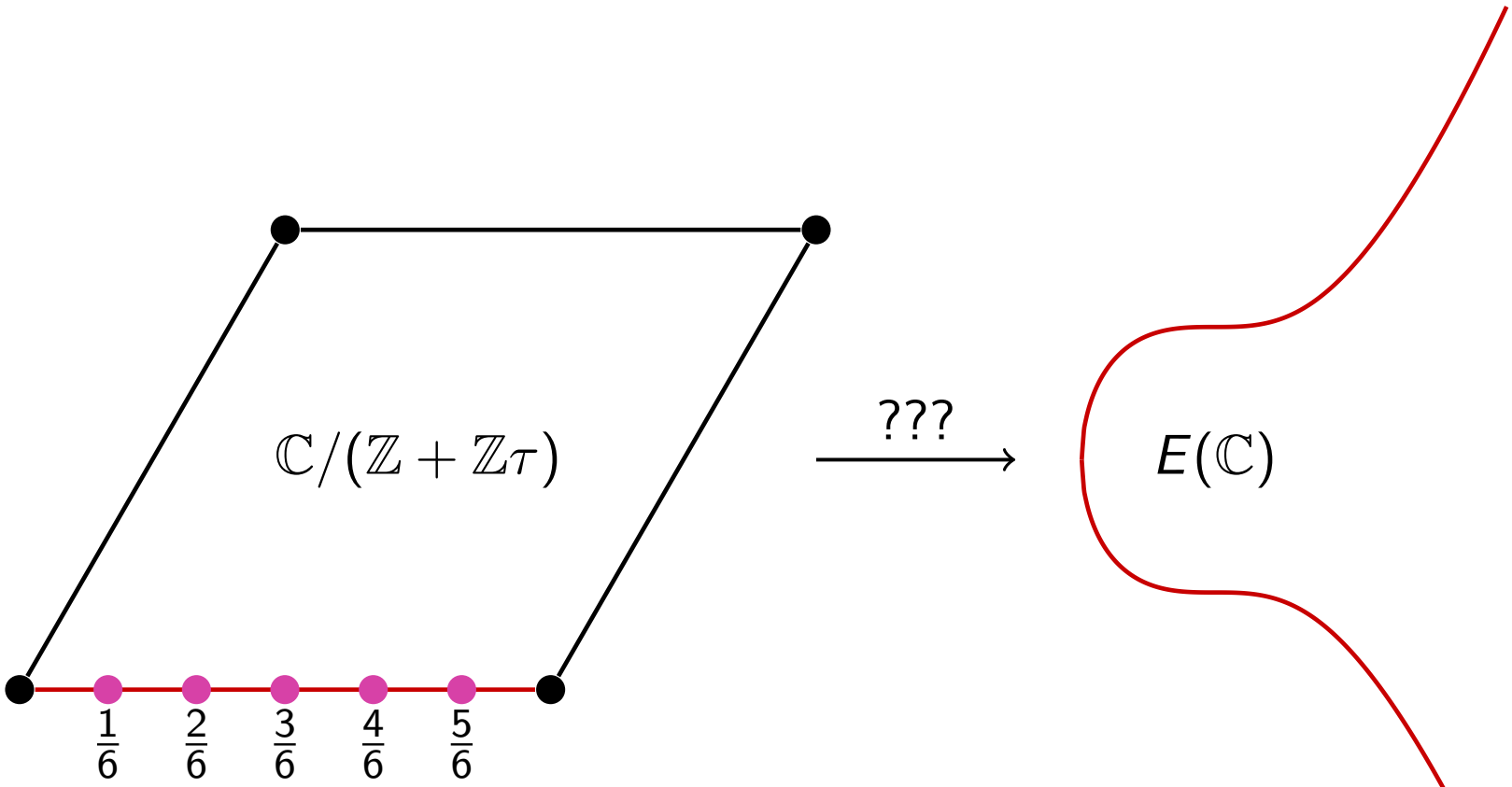


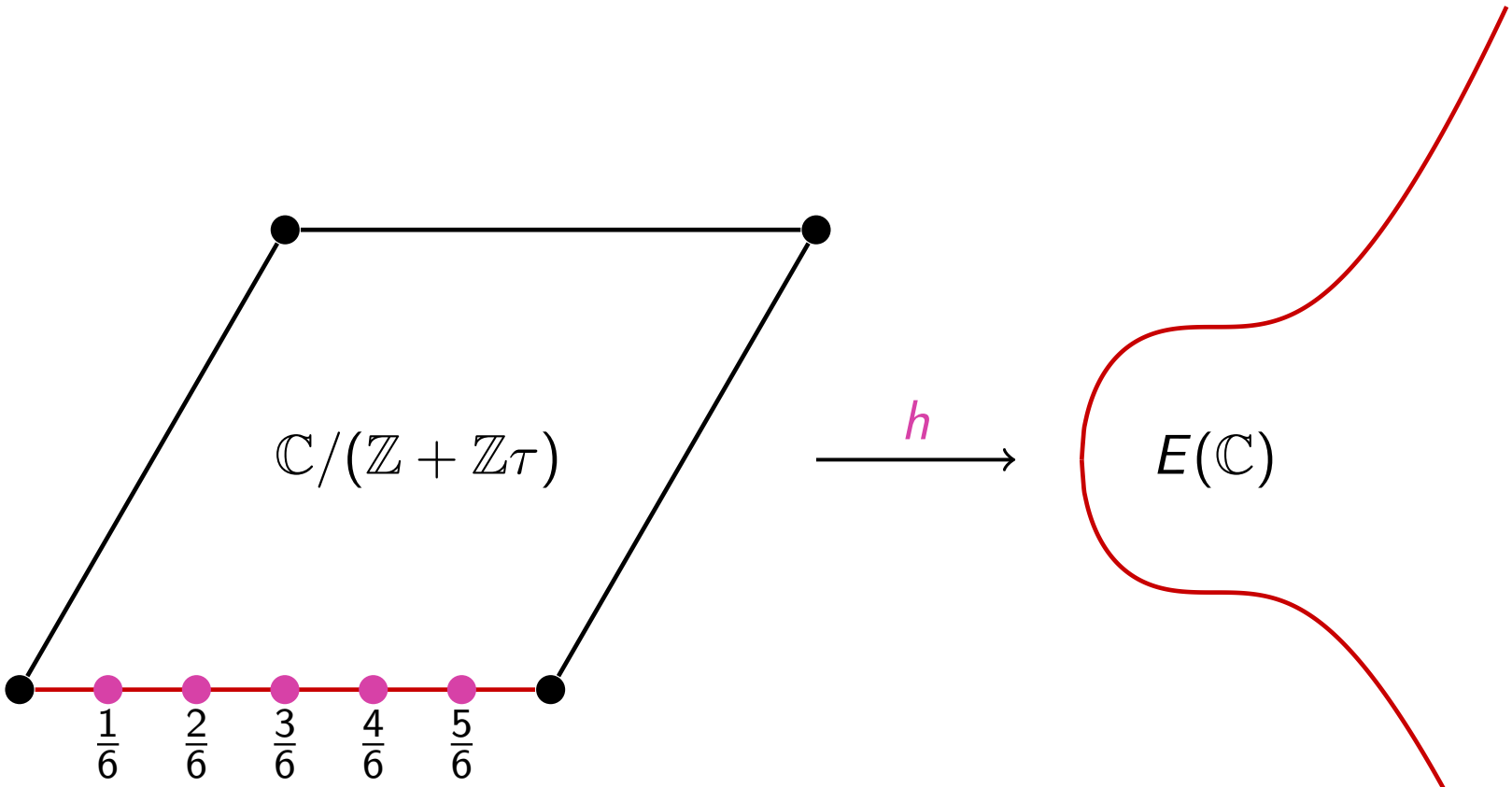


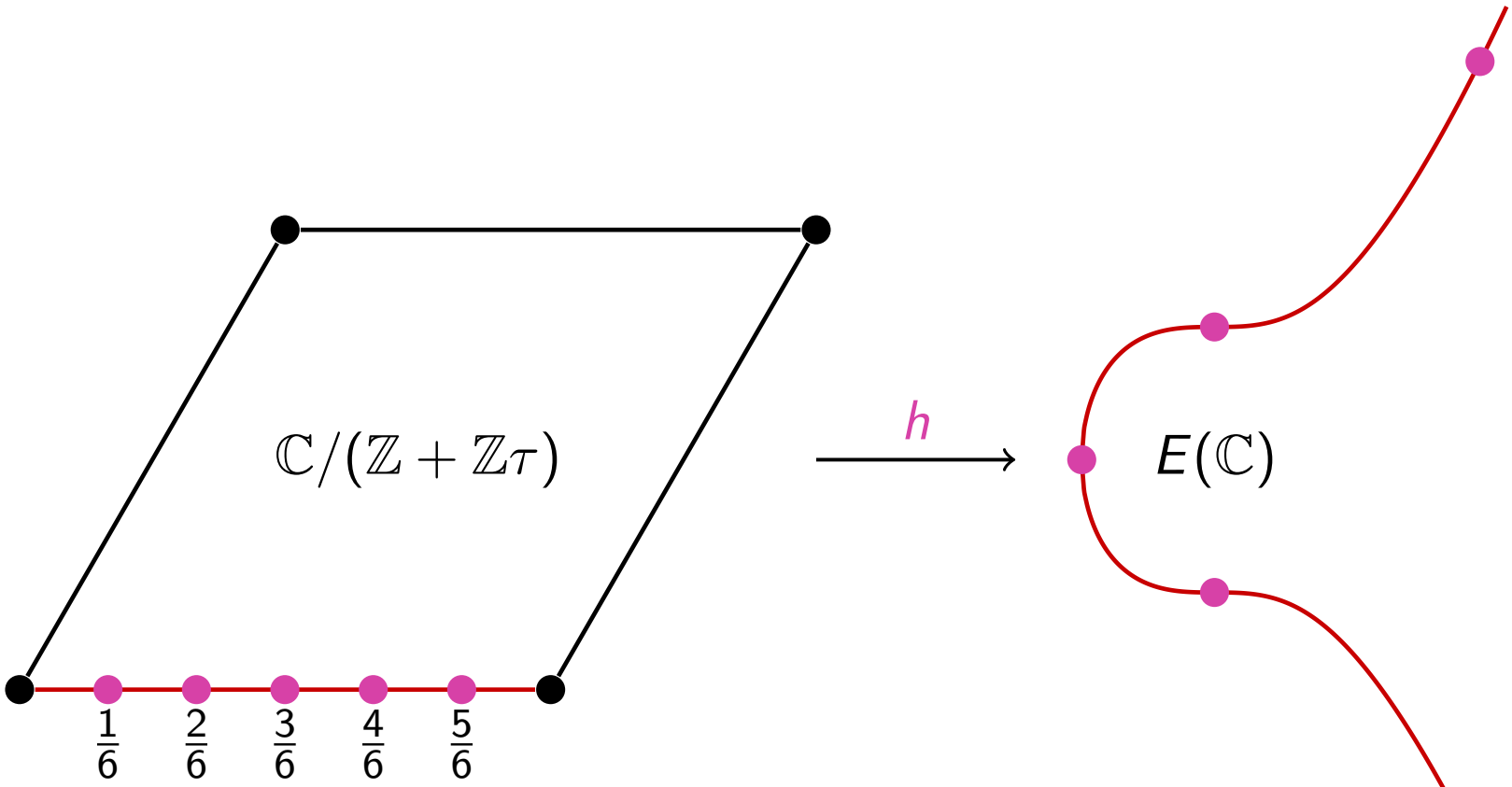
$\xrightarrow{???}$???


$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$
???
$E(\mathbb{C})$


$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$
???
$E(\mathbb{C})$


$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$
???
$E(\mathbb{C})$
$\frac{1}{6}$
$\frac{2}{6}$
$\frac{3}{6}$
$\frac{4}{6}$
$\frac{5}{6}$


$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$
h
$E(\mathbb{C})$
$\frac{1}{6}$
$\frac{2}{6}$
$\frac{3}{6}$
$\frac{4}{6}$
$\frac{5}{6}$


$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$
h
$E(\mathbb{C})$
$\frac{1}{6}$
$\frac{2}{6}$
$\frac{3}{6}$
$\frac{4}{6}$
$\frac{5}{6}$

An m-torsion point P on an elliptic curve E is said to be proper if

$$nP = 0 \qquad \text{if and only if} \qquad n \text{ is a multiple of } m.$$

An m-torsion point P on an elliptic curve E is said to be proper if

$$nP = 0 \qquad \text{if and only if} \qquad n \text{ is a multiple of } m.$$

Theorem (Main Theorem of Complex Multiplication for EC)

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

$$H_K(1) = K(j(E))$$
$$H_K(m) = K(j(E), h(t))$$

where $t \in E(\mathbb{C})$ is a proper m-torsion point.

Hilbert's twelfth problem

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

Hilbert's 12th is solved only for these fields:

- $K = \mathbb{Q}$
- K, imaginary quadratic number field
- ???

Then what?

The Main Theorem of Complex Multiplication has a version that deals with particular higher dimensional number fields.

Definition

A CM-field K is a totally imaginary number field which is a quadratic extension of a totally real number field K_0.

- An imaginary quadratic number field K is a degree 2 CM-field.

Definition

An abelian variety is a projective group variety.

- A complex elliptic curve E is an abelian variety of dimension 1.
- A complex abelian variety of dimension g is isomorphic to a g-dimensional complex torus $\mathbb{C}^g/\Lambda$.

j-invariant $j \rightsquigarrow$ Igusa invariant i

Weber function $h \rightsquigarrow F$

Theorem (Main Theorem of Complex Multiplication for AS)

j-invariant $j \rightsquigarrow$ Igusa invariant i

Weber function $h \rightsquigarrow F$

Theorem (Main Theorem of Complex Multiplication for AS)

Let A be an abelian surface over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$, where K is a quartic CM-field with cyclic Galois group. Then

$$H_K(1) \supseteq K(i(A))$$

and

$$H_K(m) \supseteq K(i(A), F(t))$$

where $t \in A(\mathbb{C})$ is a proper m-torsion point.

j-invariant $j \rightsquigarrow$ Igusa invariant i

Weber function $h \rightsquigarrow F$

Theorem (Main Theorem of Complex Multiplication for AS)

Let A be an abelian surface over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$, where K is a quartic CM-field with cyclic Galois group. Then

$$H_K(1) \supseteq K(i(A)) =: \mathrm{CM}_K(1)$$

and

$$H_K(m) \supseteq K(i(A), F(t)) =: \mathrm{CM}_K(m)$$

where $t \in A(\mathbb{C})$ is a proper m-torsion point.

j-invariant $j \rightsquigarrow$ Igusa invariant i

Weber function $h \rightsquigarrow F$

Theorem (Main Theorem of Complex Multiplication for AS)

Let A be an abelian surface over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$, where K is a quartic CM-field with cyclic Galois group. Then

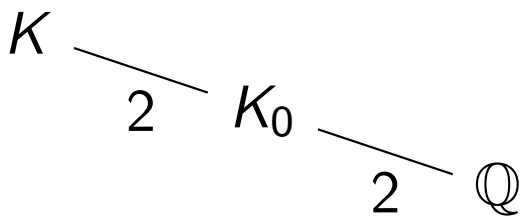
$$H_K(1) \supseteq K(i(A)) =: \mathrm{CM}_K(1)$$

and

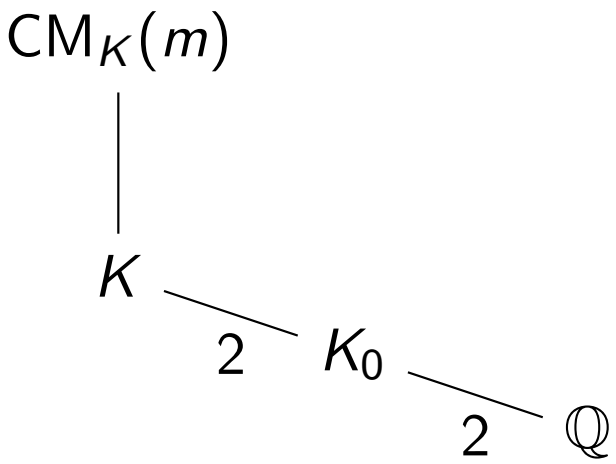
$$H_K(m) \supseteq K(i(A), F(t)) =: \mathrm{CM}_K(m)$$

where $t \in A(\mathbb{C})$ is a proper m-torsion point.

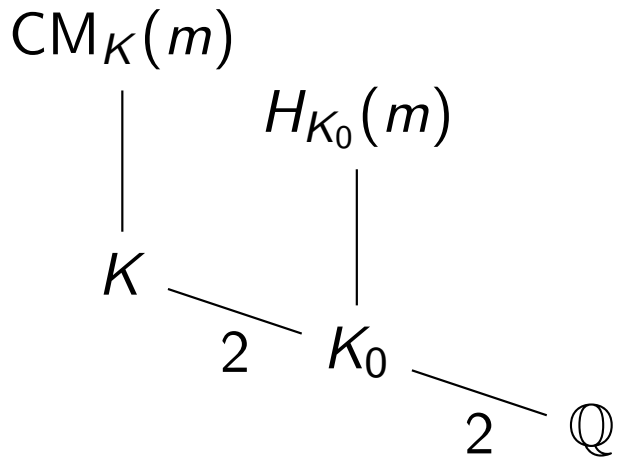
How to find $H_K(m)$?

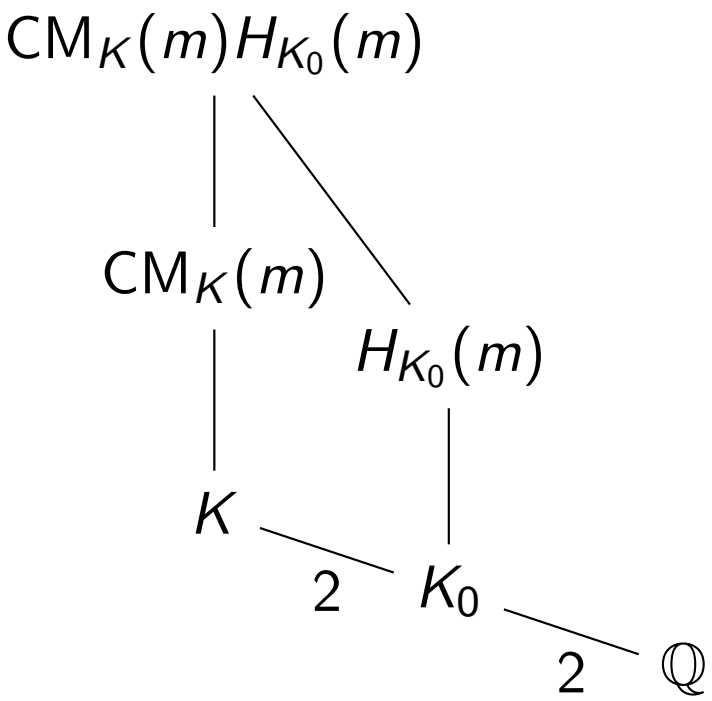

K
2
K0
2
Q

- We use the Main Theorem of CM and find $\mathrm{CM}_K(m)$.

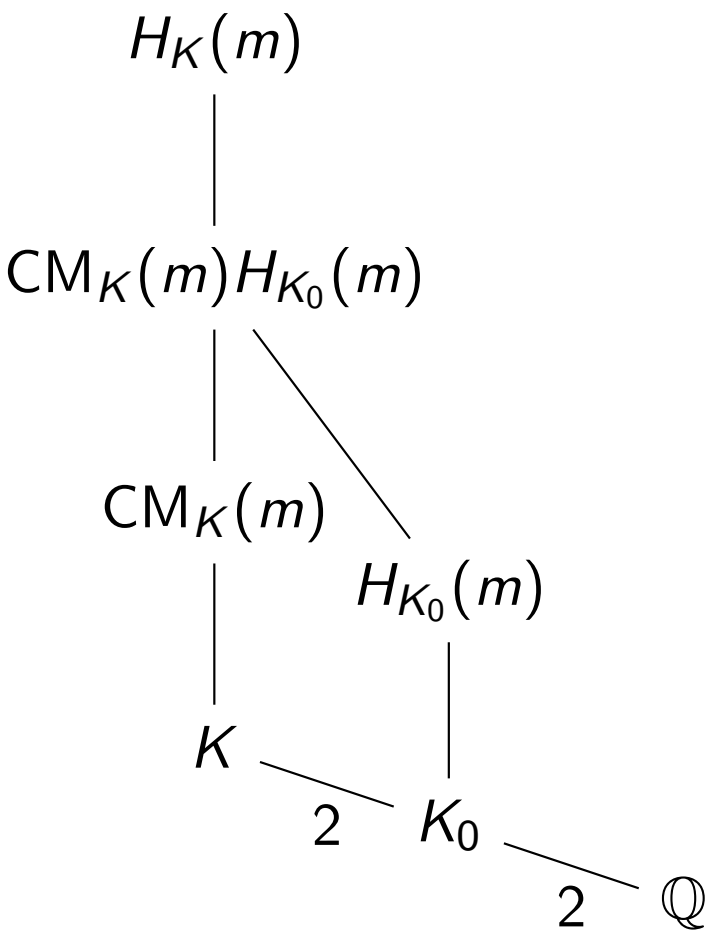


- We use the Main Theorem of CM and find $\mathrm{CM}_K(m)$.
- We use Stark's conjectures to find $H_{K_0}(m)$ for the totally real quadratic field.

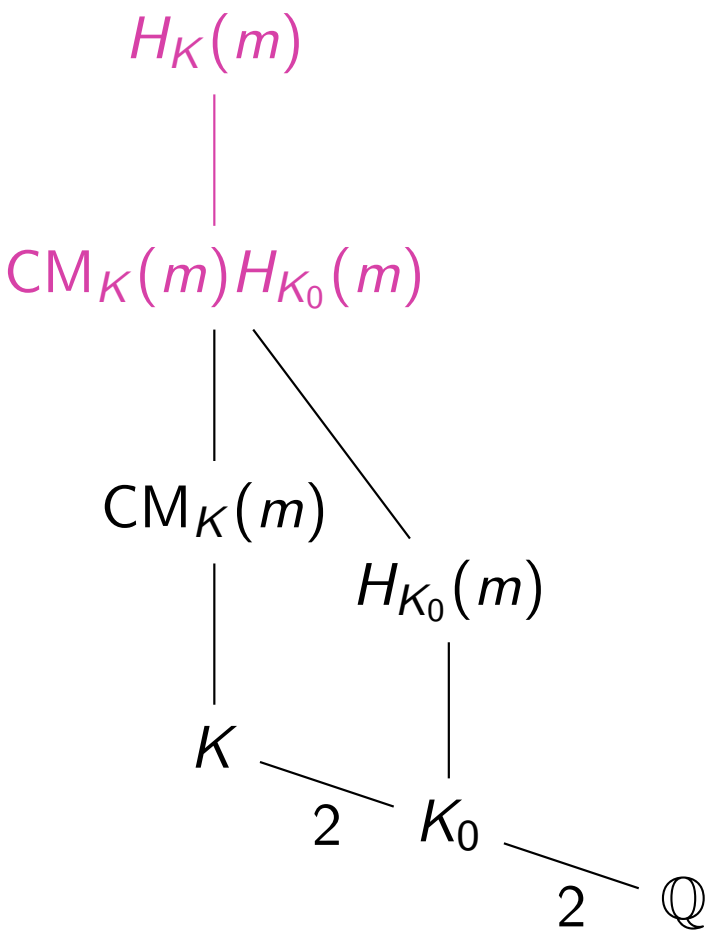




- We use the Main Theorem of CM and find $\mathrm{CM}_K(m)$.
- We use Stark's conjectures to find $H_{K_0}(m)$ for the totally real quadratic field.



- We use the Main Theorem of CM and find $\mathrm{CM}_K(m)$.
- We use Stark's conjectures to find $H_{K_0}(m)$ for the totally real quadratic field.



- We use the Main Theorem of CM and find $\mathrm{CM}_K(m)$.
- We use Stark's conjectures to find $H_{K_0}(m)$ for the totally real quadratic field.

Theorem (Streng, 2010)

Let K be a quartic CM-field with cyclic Galois group over $\mathbb{Q}$. The extension

$$H_K(m)/\,\mathrm{CM}_K(m)H_{K_0}(m)$$

is of at most exponent 2.

The extension having exponent 2 means that we need to take square roots of elements from the base field $\mathrm{CM}_K(1)H_{K_0}(1)$ to find $H_K(1)$.

- Are square roots from K sufficient? No.
- Use Kummer theory? Not feasible. Base field too big to compute class fields, etc.

Theorem (Shimura)

The Hilbert class field $H_K(1)$ is a subfield of $\mathrm{CM}_K(m)H_{K_0}(m)$ for some integer m.

- I have a theorem that gives an upper bound for such an m.
- For $m = 2$, one can use Shimura reciprocity to make the computations feasible.
- For $m > 2$, more work to be done.