

Abelian Extensions Arising from Elliptic Curves with Complex Multiplication

Asimina S. Hamakiotes

University of Connecticut

April 1, 2025
(This is NOT a joke.)

Motivation

Hilbert's 12th Problem

What are all of the abelian extensions of a number field K ?

Motivation

Hilbert's 12th Problem

What are all of the abelian extensions of a number field K ?

Let's begin with $K = \mathbb{Q}$.

Motivation

Hilbert's 12th Problem

What are all of the abelian extensions of a number field K ?

Let's begin with $K = \mathbb{Q}$.

Example: The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is abelian:

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sqrt{2} \mapsto \sqrt{2}, \sqrt{2} \mapsto -\sqrt{2}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Motivation

Hilbert's 12th Problem

What are all of the abelian extensions of a number field K ?

Let's begin with $K = \mathbb{Q}$.

Example: The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is abelian:

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sqrt{2} \mapsto \sqrt{2}, \sqrt{2} \mapsto -\sqrt{2}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Example: Consider $\mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - 3x - 1$. The 3 distinct roots are

$$\alpha, \quad -\alpha^2 + 2, \quad \alpha^2 - \alpha - 2.$$

The extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is abelian:

$$\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\alpha \mapsto \alpha, \alpha \mapsto -\alpha^2 + 2, \alpha \mapsto \alpha^2 - \alpha - 2\} \cong \mathbb{Z}/3\mathbb{Z}.$$

Cyclotomic fields

Definition

A *cyclotomic field* is an extension of \mathbb{Q} generated by a root of unity: it is $\mathbb{Q}(\zeta_n)$, where ζ_n is a root of $f(x) = x^n - 1$ with order n .

Cyclotomic fields

Definition

A *cyclotomic field* is an extension of \mathbb{Q} generated by a root of unity: it is $\mathbb{Q}(\zeta_n)$, where ζ_n is a root of $f(x) = x^n - 1$ with order n .

The two abelian extensions we saw are in cyclotomic fields:

- $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$,
- $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_9)$, where α is a root of $f(x) = x^3 - 3x - 1$.

Cyclotomic fields

Definition

A *cyclotomic field* is an extension of \mathbb{Q} generated by a root of unity: it is $\mathbb{Q}(\zeta_n)$, where ζ_n is a root of $f(x) = x^n - 1$ with order n .

The two abelian extensions we saw are in cyclotomic fields:

- $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$,
- $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_9)$, where α is a root of $f(x) = x^3 - 3x - 1$.

Cyclotomic extensions are abelian extensions of \mathbb{Q} :

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

by $\sigma \mapsto a \bmod n$, where $\sigma(\zeta_n) = \zeta_n^a$.

Cyclotomic fields

Definition

A *cyclotomic field* is an extension of \mathbb{Q} generated by a root of unity: it is $\mathbb{Q}(\zeta_n)$, where ζ_n is a root of $f(x) = x^n - 1$ with order n .

The two abelian extensions we saw are in cyclotomic fields:

- $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$,
- $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_9)$, where α is a root of $f(x) = x^3 - 3x - 1$.

Cyclotomic extensions are abelian extensions of \mathbb{Q} :

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

by $\sigma \mapsto a \bmod n$, where $\sigma(\zeta_n) = \zeta_n^a$.

All subfields of abelian extensions of \mathbb{Q} are abelian, because quotient groups of abelian groups are abelian.

Kronecker-Weber Theorem

Theorem (Kronecker-Weber Theorem)

The abelian extensions of \mathbb{Q} are precisely the subfields of cyclotomic fields.

Kronecker-Weber Theorem

Theorem (Kronecker-Weber Theorem)

The abelian extensions of \mathbb{Q} are precisely the subfields of cyclotomic fields.

Let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_n)$. Then F/\mathbb{Q} is Galois and $\text{Gal}(F/\mathbb{Q})$ is abelian.

Kronecker-Weber Theorem

Theorem (Kronecker-Weber Theorem)

The abelian extensions of \mathbb{Q} are precisely the subfields of cyclotomic fields.

Let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_n)$. Then F/\mathbb{Q} is Galois and $\text{Gal}(F/\mathbb{Q})$ is abelian.

Question: What are abelian extensions of number fields besides \mathbb{Q} ?

Kronecker-Weber Theorem

Theorem (Kronecker-Weber Theorem)

The abelian extensions of \mathbb{Q} are precisely the subfields of cyclotomic fields.

Let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_n)$. Then F/\mathbb{Q} is Galois and $\text{Gal}(F/\mathbb{Q})$ is abelian.

Question: What are abelian extensions of number fields besides \mathbb{Q} ?

A general answer given by class field theory is not explicit.

Kronecker-Weber Theorem

Theorem (Kronecker-Weber Theorem)

The abelian extensions of \mathbb{Q} are precisely the subfields of cyclotomic fields.

Let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_n)$. Then F/\mathbb{Q} is Galois and $\text{Gal}(F/\mathbb{Q})$ is abelian.

Question: What are abelian extensions of number fields besides \mathbb{Q} ?

A general answer given by class field theory is not explicit.

We can construct all the abelian extensions of $\mathbb{Q}(i)$ using an elliptic curve!

What is an elliptic curve?

Definition

An *elliptic curve* E defined over a field K is a smooth projective curve of genus 1, with at least one K -rational point.

What is an elliptic curve?

Definition

An *elliptic curve* E defined over a field K is a smooth projective curve of genus 1, with at least one K -rational point.

More concretely, an *elliptic curve* E defined over a field K is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

plus a “point at infinity” \mathcal{O} .

What is an elliptic curve?

Definition

An *elliptic curve* E defined over a field K is a smooth projective curve of genus 1, with at least one K -rational point.

More concretely, an *elliptic curve* E defined over a field K is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

plus a “point at infinity” \mathcal{O} .

When $\text{char}(K) \neq 2, 3$, it may be simplified to a short Weierstrass equation

$$y^2 = x^3 + Ax + B, \quad A, B \in K,$$

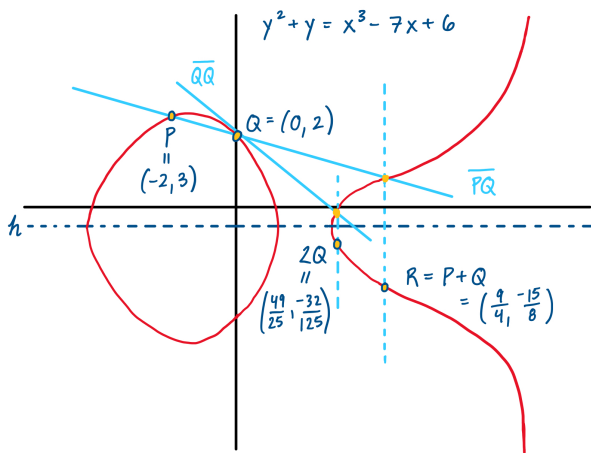
where $4A^3 + 27B^2 \neq 0$ (for smoothness).

Elliptic curve group law

There is a group law (abelian) on the L -rational points of E

$$E(L) = \{(x, y) \in E : x, y \in L\} \cup \mathcal{O},$$

with coordinates in any field $L \supset K$. We call $E(L)$ the *Mordell-Weil group* of E/L .



Torsion points on an elliptic curve

Theorem (Mordell-Weil Theorem)

Let F be a number field and let E/F be an elliptic curve. Then $E(F)$ is a finitely generated abelian group: $E(F) \cong E(F)_{\text{tors}} \oplus \mathbb{Z}^r$, where $r \in \mathbb{Z}_{\geq 0}$.

Torsion points on an elliptic curve

Theorem (Mordell-Weil Theorem)

Let F be a number field and let E/F be an elliptic curve. Then $E(F)$ is a finitely generated abelian group: $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^r$, where $r \in \mathbb{Z}_{\geq 0}$.

Let $N \geq 1$. The point $P \in E(F)$ is an N -torsion point if

$$\underbrace{P + P + \cdots + P}_{N \text{ times}} = [N]P = \mathcal{O},$$

where \mathcal{O} is the “point at infinity”.

Torsion points on an elliptic curve

Theorem (Mordell-Weil Theorem)

Let F be a number field and let E/F be an elliptic curve. Then $E(F)$ is a finitely generated abelian group: $E(F) \cong E(F)_{\text{tors}} \oplus \mathbb{Z}^r$, where $r \in \mathbb{Z}_{\geq 0}$.

Let $N \geq 1$. The point $P \in E(F)$ is an N -torsion point if

$$\underbrace{P + P + \cdots + P}_{N \text{ times}} = [N]P = \mathcal{O},$$

where \mathcal{O} is the “point at infinity”.

Definition

Let $N \geq 1$ be an integer and let

$$E[N] = \{P \in E(\overline{F}) : [N]P = \mathcal{O}\}.$$

This is called the N -torsion subgroup of $E(\overline{F})$.

Division field of an elliptic curve

Let F be a number field and let E/F be an elliptic curve.

Definition

The N^{th} -division field of E/F is

$$F(E[N]) = F(\{x(P), y(P) : P \in E[N]\}).$$

This is the field of definition of the coordinates of all points in $E[N]$.

Division field of an elliptic curve

Let F be a number field and let E/F be an elliptic curve.

Definition

The N^{th} -division field of E/F is

$$F(E[N]) = F(\{x(P), y(P) : P \in E[N]\}).$$

This is the field of definition of the coordinates of all points in $E[N]$.

Example

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. We have

$$\begin{aligned} E[2] &= \{\mathcal{O}, (0, 0), (i, 0), (-i, 0)\}, \\ \mathbb{Q}(E[2]) &= \mathbb{Q}(0, i, -i) = \mathbb{Q}(i). \end{aligned}$$

Division field of an elliptic curve

Let F be a number field and let E/F be an elliptic curve.

Definition

The N^{th} -division field of E/F is

$$F(E[N]) = F(\{x(P), y(P) : P \in E[N]\}).$$

This is the field of definition of the coordinates of all points in $E[N]$.

Example

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. We have

$$\begin{aligned} E[2] &= \{\mathcal{O}, (0, 0), (i, 0), (-i, 0)\}, \\ \mathbb{Q}(E[2]) &= \mathbb{Q}(0, i, -i) = \mathbb{Q}(i). \end{aligned}$$

Note that, similar to $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, the extension $F(E[N])/F$ is Galois.

Abelian extensions of $\mathbb{Q}(i)$

Theorem

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. For each integer $N \geq 1$, let

$$K_N = \mathbb{Q}(i)(E[N]).$$

Then K_N is a Galois extension of $\mathbb{Q}(i)$, and $\text{Gal}(K_N/\mathbb{Q}(i))$ is abelian.

Abelian extensions of $\mathbb{Q}(i)$

Theorem

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. For each integer $N \geq 1$, let

$$K_N = \mathbb{Q}(i)(E[N]).$$

Then K_N is a Galois extension of $\mathbb{Q}(i)$, and $\text{Gal}(K_N/\mathbb{Q}(i))$ is abelian.

For E above, $\mathbb{Q}(E[N])/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$ are Galois, so K_N/\mathbb{Q} is Galois. But K_N/\mathbb{Q} may not be abelian!

Abelian extensions of $\mathbb{Q}(i)$

Example

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. The 4-torsion points of E are

$$E[4] = \{\mathcal{O}, (0, 0), (1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}), (\pm i, 0), \text{ and 8 other points}\}$$

and $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{1 + \sqrt{2}})$.

It turns out that $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}(i)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is abelian, but $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \cong D_4$, which is not abelian.

Abelian extensions of $\mathbb{Q}(i)$

Example

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. The 4-torsion points of E are

$$E[4] = \{\mathcal{O}, (0, 0), (1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}), (\pm i, 0), \text{ and 8 other points}\}$$

and $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{1 + \sqrt{2}})$.

It turns out that $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}(i)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is abelian, but $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \cong D_4$, which is not abelian.

Theorem (Takagi)

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. The abelian extensions of $\mathbb{Q}(i)$ are precisely the subfields of $K_N = \mathbb{Q}(i)(E[N])$ for some $N \geq 1$.

Complex multiplication (CM)

Definition

Let E be an elliptic curve defined over a field F of characteristic 0. We say that E has *complex multiplication* (CM) if $\text{End}(E) \supsetneq \mathbb{Z}$.

Complex multiplication (CM)

Definition

Let E be an elliptic curve defined over a field F of characteristic 0. We say that E has *complex multiplication* (CM) if $\text{End}(E) \supsetneq \mathbb{Z}$.

If E/F has CM, then $\text{End}(E) \cong \mathcal{O}_{K,f}$, where $\mathcal{O}_{K,f}$ is the order in an imaginary quadratic field K with index $f \geq 1$ in \mathcal{O}_K .

Complex multiplication (CM)

Definition

Let E be an elliptic curve defined over a field F of characteristic 0. We say that E has *complex multiplication* (CM) if $\text{End}(E) \supsetneq \mathbb{Z}$.

If E/F has CM, then $\text{End}(E) \cong \mathcal{O}_{K,f}$, where $\mathcal{O}_{K,f}$ is the order in an imaginary quadratic field K with index $f \geq 1$ in \mathcal{O}_K .

Example

The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + x$ (64.a1) has the endomorphism

$$\phi(x, y) = (-x, iy),$$

where for $(x, y) \in E$, we have $(iy)^2 = (-x)^3 + (-x)$, so $(-x, iy) \in E$.

In this case, $\text{End}(E) \cong \mathbb{Z}[i] = \mathcal{O}_{K,1}$, the maximal order of $K = \mathbb{Q}(i)$.

Abelian extensions arising from elliptic curves with CM

Theorem

Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K . Let E be an elliptic curve with $\text{End}(E) \cong \mathcal{O}_K$ and j -invariant $j(E)$. Then

Abelian extensions arising from elliptic curves with CM

Theorem

Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K . Let E be an elliptic curve with $\text{End}(E) \cong \mathcal{O}_K$ and j -invariant $j(E)$. Then

- (1) $K(j(E))$ is the Hilbert class field of K ,*

Abelian extensions arising from elliptic curves with CM

Theorem

Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K . Let E be an elliptic curve with $\text{End}(E) \cong \mathcal{O}_K$ and j -invariant $j(E)$. Then

- (1) $K(j(E))$ is the Hilbert class field of K ,
- (2) $K(j(E), E_{\text{tors}})$ is an abelian extension of $K(j(E))$,

Abelian extensions arising from elliptic curves with CM

Theorem

Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K . Let E be an elliptic curve with $\text{End}(E) \cong \mathcal{O}_K$ and j -invariant $j(E)$. Then

- (1) $K(j(E))$ is the Hilbert class field of K ,
- (2) $K(j(E), E_{\text{tors}})$ is an abelian extension of $K(j(E))$,
- (3) $K(j(E), x(E_{\text{tors}}))$ is the maximal abelian extension of K when $j(E) \neq 0, 1728$ (there is an alternate expression when $j(E) = 0, 1728$).

Goal

Question: When can division fields be abelian over \mathbb{Q} or other fields?

Goal

Question: When can division fields be abelian over \mathbb{Q} or other fields?

Let F be a number field, E/F be an elliptic curve, and $N \geq 2$.

Question: When can division fields be abelian over \mathbb{Q} or other fields?

Let F be a number field, E/F be an elliptic curve, and $N \geq 2$.

- When is the N^{th} -division field $F(E[N])$ abelian over F ?

Question: When can division fields be abelian over \mathbb{Q} or other fields?

Let F be a number field, E/F be an elliptic curve, and $N \geq 2$.

- When is the N^{th} -division field $F(E[N])$ abelian over F ?
- If $F(E[N])/F$ is not abelian, then what is the maximal abelian extension of F contained in $F(E[N])$?

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let E/\mathbb{Q} be an elliptic curve. Let $N \geq 2$.

- *$\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2, 3, 4$, or 5 .*
- *More generally, if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3, 4, 5, 6$, or 8 .*

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let E/\mathbb{Q} be an elliptic curve. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2, 3, 4$, or 5 .
- More generally, if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3, 4, 5, 6$, or 8 .

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let E/\mathbb{Q} be an elliptic curve with complex multiplication. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2$ or 3 .
- More generally, if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3$, or 4 .

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let E/\mathbb{Q} be an elliptic curve. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2, 3, 4$, or 5 .
- More generally, if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3, 4, 5, 6$, or 8 .

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let E/\mathbb{Q} be an elliptic curve with complex multiplication. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2$ or 3 .
- More generally, if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3$, or 4 .

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Notation

The following notation will be used throughout the rest of the talk.

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,
- $\mathcal{O}_{K,f}$ is the order of conductor $f \geq 1$ in K , with discriminant $\Delta_K f^2$,

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,
- $\mathcal{O}_{K,f}$ is the order of conductor $f \geq 1$ in K , with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j -invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,
- $\mathcal{O}_{K,f}$ is the order of conductor $f \geq 1$ in K , with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j -invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,
- $\mathcal{O}_{K,f}$ is the order of conductor $f \geq 1$ in K , with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j -invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

$E/\mathbb{Q}(j_{K,f})$ is an elliptic curve with CM by $\mathcal{O}_{K,f}$, and a minimal field of definition for E is $\mathbb{Q}(j_{K,f})$.

Notation

The following notation will be used throughout the rest of the talk.

- K is an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers \mathcal{O}_K ,
- $\mathcal{O}_{K,f}$ is the order of conductor $f \geq 1$ in K , with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j -invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

$E/\mathbb{Q}(j_{K,f})$ is an elliptic curve with CM by $\mathcal{O}_{K,f}$, and a minimal field of definition for E is $\mathbb{Q}(j_{K,f})$.

Example

Let $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve given by (32.1-a1),

$$y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

with CM by $\mathcal{O}_{K,4} = \mathbb{Z}[4i]$, where $K = \mathbb{Q}(i)$.

Here, $j_{K,4} = -29071392966\sqrt{2} + 41113158120$, so $\mathbb{Q}(j_{K,4}) = \mathbb{Q}(\sqrt{2})$.

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, $f \geq 1$. Let $N \geq 2$ and let

$$G_{E,N} = \text{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$$

be the Galois group of the N^{th} -division field of $E/\mathbb{Q}(j_{K,f})$.

If $G_{E,N}$ is abelian, then N must equal 2, 3, or 4. Further, if $G_{E,N}$ is abelian, then it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $0 \leq k \leq 3$.

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) *If $j_{K,f} \neq 0, 1728$, then $G_{E,N}$ is abelian if and only if:*

- $N = 2$ and either
 - $\Delta_K f^2 \equiv 0 \pmod{4}$, or
 - $\Delta_K \equiv 1 \pmod{8}$ and $f \equiv 1 \pmod{2}$.

In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) If $j_{K,f} \neq 0, 1728$, then $G_{E,N}$ is abelian if and only if:

- $N = 2$ and either
 - $\Delta_K f^2 \equiv 0 \pmod{4}$, or
 - $\Delta_K \equiv 1 \pmod{8}$ and $f \equiv 1 \pmod{2}$.

In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) If $j_{K,f} = 1728$, then $G_{E,N}$ is abelian if and only if:

- $N = 2$. In this case, $G_{E,2} \cong \{0\}$ or $\mathbb{Z}/2\mathbb{Z}$ according to whether E is given by $y^2 = x^3 - dx$ with d a square or a non-square in \mathbb{Z} , respectively.
- $N = 4$ and E/\mathbb{Q} is given by $y^2 = x^3 + dx$ with $d \in \{\pm 1, \pm 4\}$ or $d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^3$, resp.

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) If $j_{K,f} \neq 0, 1728$, then $G_{E,N}$ is abelian if and only if:

- $N = 2$ and either
 - $\Delta_K f^2 \equiv 0 \pmod{4}$, or
 - $\Delta_K \equiv 1 \pmod{8}$ and $f \equiv 1 \pmod{2}$.

In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) If $j_{K,f} = 1728$, then $G_{E,N}$ is abelian if and only if:

- $N = 2$. In this case, $G_{E,2} \cong \{0\}$ or $\mathbb{Z}/2\mathbb{Z}$ according to whether E is given by $y^2 = x^3 - dx$ with d a square or a non-square in \mathbb{Z} , respectively.
- $N = 4$ and E/\mathbb{Q} is given by $y^2 = x^3 + dx$ with $d \in \{\pm 1, \pm 4\}$ or $d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^3$, resp.

(3) If $j_{K,f} = 0$, then $G_{E,N}$ is abelian if and only if:

- $N = 2$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ with d a cube in \mathbb{Z} . Then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} . If in addition d and $3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$, and if d or $3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example: Let $K = \mathbb{Q}(i)$ and $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example: Let $K = \mathbb{Q}(i)$ and $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

where $j(E) = -29071392966\sqrt{2} + 41113158120$.

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example: Let $K = \mathbb{Q}(i)$ and $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

where $j(E) = -29071392966\sqrt{2} + 41113158120$.

Note that E has CM by $\mathcal{O}_{K,4} = \mathbb{Z}[\sqrt{-16}]$.

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example: Let $K = \mathbb{Q}(i)$ and $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

where $j(E) = -29071392966\sqrt{2} + 41113158120$.

Note that E has CM by $\mathcal{O}_{K,4} = \mathbb{Z}[\sqrt{-16}]$.

Here $\Delta_K f^2 = -4 \cdot 16 = -64 \equiv 0 \pmod{4}$, so $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example

Theorem (H. and Lozano-Robledo, 2023)

If $j_{K,f} \neq 0, 1728$, then $G_{E,2}$ is abelian if and only if $\Delta_K f^2 \equiv 0 \pmod{4}$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example: Let $K = \mathbb{Q}(i)$ and $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + (15\sqrt{2} - 22)x + 46\sqrt{2} - 69,$$

where $j(E) = -29071392966\sqrt{2} + 41113158120$.

Note that E has CM by $\mathcal{O}_{K,4} = \mathbb{Z}[\sqrt{-16}]$.

Here $\Delta_K f^2 = -4 \cdot 16 = -64 \equiv 0 \pmod{4}$, so $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

One can check that $E(\mathbb{Q}(\sqrt{2}))[2] \cong \mathbb{Z}/2\mathbb{Z}$ is generated by a non-trivial 2-torsion point defined over $\mathbb{Q}(\sqrt{2})$, namely

$$P = \left(2\sqrt{2} - \frac{3}{2}, \frac{3}{4}\sqrt{2} - 2 \right).$$

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
Here $4d = 8$ is a cube in \mathbb{Z} , but d and $-3d$ are not squares in \mathbb{Z} .

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
Here $4d = 8$ is a cube in \mathbb{Z} , but d and $-3d$ are not squares in \mathbb{Z} .
Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
Here $4d = 8$ is a cube in \mathbb{Z} , but d and $-3d$ are not squares in \mathbb{Z} .
Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
Here $4d = 8$ is a cube in \mathbb{Z} , but d and $-3d$ are not squares in \mathbb{Z} .
Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.
Here $4d = 4^3$ is a cube in \mathbb{Z} , and d is a square in \mathbb{Z} .

Example

Theorem 1 (H. and Lozano-Robledo, 2023)

If $j_{K,f} = 0$, then $G_{E,3}$ is abelian if and only if $N = 3$ and E/\mathbb{Q} is given by $y^2 = x^3 + d$ such that $4d$ is a cube in \mathbb{Z} .

- If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
Here $4d = 8$ is a cube in \mathbb{Z} , but d and $-3d$ are not squares in \mathbb{Z} .
Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.
Here $4d = 4^3$ is a cube in \mathbb{Z} , and d is a square in \mathbb{Z} .
Therefore, $G_{E_2,3} \cong \mathbb{Z}/2\mathbb{Z}$.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E* :

$$\rho_{E,N}: \operatorname{Gal}(F(E[N])/F) \hookrightarrow \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \operatorname{Gal}(F(E[N])/F) = \operatorname{im}(\rho_{E,N}) \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E* :

$$\rho_{E,N}: \operatorname{Gal}(F(E[N])/F) \hookrightarrow \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \operatorname{Gal}(F(E[N])/F) = \operatorname{im}(\rho_{E,N}) \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

For an elliptic curve with CM, we know that $G_{E,N} \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is actually contained in something smaller, which is almost abelian.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E* :

$$\rho_{E,N}: \operatorname{Gal}(F(E[N])/F) \hookrightarrow \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \operatorname{Gal}(F(E[N])/F) = \operatorname{im}(\rho_{E,N}) \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

For an elliptic curve with CM, we know that $G_{E,N} \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is actually contained in something smaller, which is almost abelian.

$G_{E,N}$ is contained in the normalizer of Cartan subgroup of $\operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$ and that has an index 2 abelian subgroup.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

We define associated constants δ and ϕ as follows:

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

We define associated constants δ and ϕ as follows:

- If $\Delta_K f^2 \equiv 0 \pmod{4}$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

We define associated constants δ and ϕ as follows:

- If $\Delta_K f^2 \equiv 0 \pmod{4}$, or N is odd, let $\delta = \Delta_K f^2 / 4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \pmod{4}$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

We define associated constants δ and ϕ as follows:

- If $\Delta_K f^2 \equiv 0 \pmod{4}$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \pmod{4}$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z}, \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

We define associated constants δ and ϕ as follows:

- If $\Delta_K f^2 \equiv 0 \pmod{4}$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \pmod{4}$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z}, \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

The *normalizer of Cartan subgroup* $\mathcal{N}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle.$$

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}: \text{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \rightarrow \text{Aut}(E[N]) \cong \text{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}: \text{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \rightarrow \text{Aut}(E[N]) \cong \text{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

- 1 There is a $\mathbb{Z}/N\mathbb{Z}$ -basis of $E[N]$ such that $\text{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$,

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}: \text{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \rightarrow \text{Aut}(E[N]) \cong \text{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

- 1 There is a $\mathbb{Z}/N\mathbb{Z}$ -basis of $E[N]$ such that $\text{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$,
- 2 $\mathcal{C}_{\delta,\phi}(N) \cong (\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$ is a subgroup of **index 2** in $\mathcal{N}_{\delta,\phi}(N)$,

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}: \text{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \rightarrow \text{Aut}(E[N]) \cong \text{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

- 1 There is a $\mathbb{Z}/N\mathbb{Z}$ -basis of $E[N]$ such that $\text{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$,
- 2 $\mathcal{C}_{\delta,\phi}(N) \cong (\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$ is a subgroup of **index 2** in $\mathcal{N}_{\delta,\phi}(N)$,
- 3 The index of $\text{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$ is a divisor of 2, 4, or 6.

Sketch of proof

Theorem (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2, 3$, or 4 .

Sketch of proof:

Sketch of proof

Theorem (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2, 3$, or 4 .

Sketch of proof:

- (1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞} , up to conjugation.

Sketch of proof

Theorem (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2, 3$, or 4 .

Sketch of proof:

- (1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞} , up to conjugation.
- (2) We understand what subgroups of $\mathcal{N}_{\delta,\phi}(N)$ are images of $\rho_{E,N}$ and we give conditions that will help characterize when a subgroup of $\mathcal{N}_{\delta,\phi}(N)$ is abelian (e.g. the Cartan subgroup is abelian).

Sketch of proof

Theorem (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2, 3$, or 4 .

Sketch of proof:

- (1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞} , up to conjugation.
- (2) We understand what subgroups of $\mathcal{N}_{\delta,\phi}(N)$ are images of $\rho_{E,N}$ and we give conditions that will help characterize when a subgroup of $\mathcal{N}_{\delta,\phi}(N)$ is abelian (e.g. the Cartan subgroup is abelian).
- (3) We apply the above results to all possible images $G_{E,N} = \mathrm{im} \rho_{E,N}$ from (1) and analyze under what circumstances $G_{E,N}$ is abelian.



Conditions for determining if $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \quad c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \quad \text{and} \quad c_{\delta,\phi}(a,b) = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Lemma (H. and Lozano-Robledo, 2023)

Let $N \geq 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1, c_{\delta,\phi}(a,b) \in G$, for some $a, b \in \mathbb{Z}/N\mathbb{Z}$, such that the two matrices commute, then

$$b\phi \equiv 0 \pmod{N} \quad \text{and} \quad 2b \equiv 0 \pmod{N}. \tag{1}$$

Moreover, if $\phi = 0$, and if $c_\varepsilon, c_{\delta,0}(a,b) \in G$ for some $\varepsilon \in \{\pm 1\}$, such that the two matrices commute, then the same conditions as (1) hold.

Conditions for determining in $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \quad c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \quad \text{and} \quad c_{\delta,\phi}(a,b) = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Corollary (H. and Lozano-Robledo, 2023)

Let $N \geq 3$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a,b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Conditions for determining in $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \quad c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \quad \text{and} \quad c_{\delta,\phi}(a,b) = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Corollary (H. and Lozano-Robledo, 2023)

Let $N \geq 3$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a,b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Proof: Assume that $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ is abelian. Then c_1 (or c_ε if $\phi = 0$) and $c_{\delta,\phi}(a,b)$ commute, so by the previous lemma, we have

$$b\phi \equiv 0 \pmod{N} \quad \text{and} \quad 2b \equiv 0 \pmod{N}.$$

If $N \geq 3$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $2b \equiv 0 \pmod{N} \implies 2 \equiv 0 \pmod{N}$. Therefore, G cannot be abelian.



Example of proving that $G_{E,N}$ is not abelian

Corollary (H. and Lozano-Robledo, 2023)

Let $N \geq 3$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a, b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Example

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$. Let p be an odd prime dividing $\Delta_K f^2$, and $j_{K,f} \neq 0, 1728$. For $\varepsilon \in \{\pm 1\}$, consider the image

$$G_{E,p} = \left\langle \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \left\{ \begin{pmatrix} a & b \\ \delta b & a \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}, b \in \mathbb{Z}/p\mathbb{Z} \right\} \right\rangle.$$

Observe that $c_{\delta,0}(1, 1) = \begin{pmatrix} 1 & 1 \\ \delta & 1 \end{pmatrix} \in G_{E,p}$ and $b = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Therefore, $G_{E,p}$ is not abelian, and hence, G_{E,p^n} is not abelian.

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ need not be abelian.

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ need not be abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ need not be abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ need not be abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

- $\mathbb{Q}(E[4])/\mathbb{Q}$ is not abelian, $G_{E,4} \cong D_4$:

$$G_{E,4} = \left\langle \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}).$$

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ need not be abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

- $\mathbb{Q}(E[4])/\mathbb{Q}$ is not abelian, $G_{E,4} \cong D_4$:

$$G_{E,4} = \left\langle \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}).$$

Question

What is the maximal abelian extension contained in $F(E[N])/F$?

Abelian extensions contained in $F(E[N])/F$

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where $F = \mathbb{Q}(j_{K,f})$.

Abelian extensions contained in $F(E[N])/F$

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where $F = \mathbb{Q}(j_{K,f})$.

(1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.

Abelian extensions contained in $F(E[N])/F$

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where $F = \mathbb{Q}(j_{K,f})$.

- (1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.
- (2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.

Abelian extensions contained in $F(E[N])/F$

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where $F = \mathbb{Q}(j_{K,f})$.

- (1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.
- (2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.
- (3) Let $N \geq 3$, $d \in F$ such that $\sqrt{d} \notin K$, and E^d be the twist of E by d . Then there is an explicitly computable integer $\alpha = \alpha(E^d)$ such that $F(\sqrt{\alpha}) \subseteq F(E[N])$, with α unique up to squares when $j_{K,f} \neq 0, 1728$, 4th-powers when $j_{K,f} = 1728$, and 6th-powers when $j_{K,f} = 0$.

Abelian extensions contained in $F(E[N])/F$

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where $F = \mathbb{Q}(j_{K,f})$.

- (1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.
- (2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.
- (3) Let $N \geq 3$, $d \in F$ such that $\sqrt{d} \notin K$, and E^d be the twist of E by d . Then there is an explicitly computable integer $\alpha = \alpha(E^d)$ such that $F(\sqrt{\alpha}) \subseteq F(E[N])$, with α unique up to squares when $j_{K,f} \neq 0, 1728$, 4th-powers when $j_{K,f} = 1728$, and 6th-powers when $j_{K,f} = 0$.

Therefore, we have that $K(j_{K,f}, \zeta_N, \sqrt{\alpha})$ is an abelian extension contained in $F(E[N])/F$, which is sometimes just $K(j_{K,f}, \zeta_N)$ if $\sqrt{\alpha} \in K(j_{K,f}, \zeta_N)$.

Field diagram

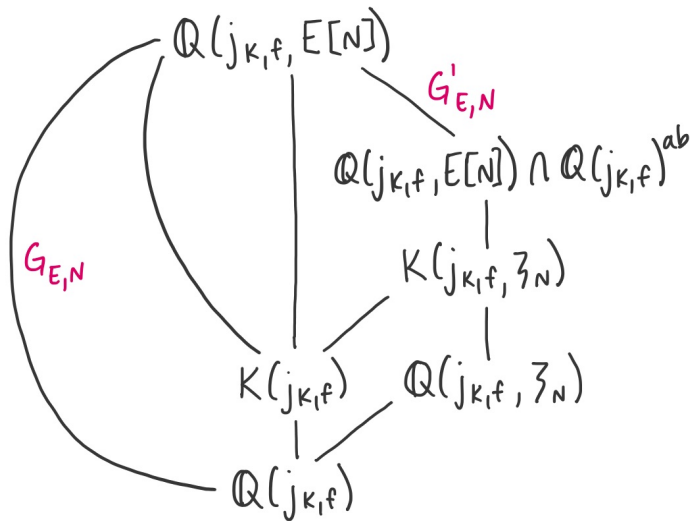
Let $N \geq 3$. Let $G_{E,N} = \text{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$.

Let $G'_{E,N}$ denote the commutator subgroup of $G_{E,N}$.

Field diagram

Let $N \geq 3$. Let $G_{E,N} = \text{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$.

Let $G'_{E,N}$ denote the commutator subgroup of $G_{E,N}$.



How to find the max abelian subextension of $F(E[N])/F$

Sketch of proof:

How to find the max abelian subextension of $F(E[N])/F$

Sketch of proof:

- (1) We have explicit matrix group descriptions for G_{E,p^n} , so we can compute their commutator subgroups G'_{E,p^n} explicitly.

How to find the max abelian subextension of $F(E[N])/F$

Sketch of proof:

- (1) We have explicit matrix group descriptions for G_{E,p^n} , so we can compute their commutator subgroups G'_{E,p^n} explicitly.
- (2) We know $K(j_{K,f}, \zeta_{p^n})$ or $K(j_{K,f}, \zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension of K and can use that to find an upper bound for the size of G'_{E,p^n} .

How to find the max abelian subextension of $F(E[N])/F$

Sketch of proof:

- (1) We have explicit matrix group descriptions for G_{E,p^n} , so we can compute their commutator subgroups G'_{E,p^n} explicitly.
- (2) We know $K(j_{K,f}, \zeta_{p^n})$ or $K(j_{K,f}, \zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension of K and can use that to find an upper bound for the size of G'_{E,p^n} .
- (3) We can use the surjective reduction map $\pi : G'_{E,p^{n+1}} \rightarrow G'_{E,p^n}$ to get a lower bound for the size of G'_{E,p^n} .

How to find the max abelian subextension of $F(E[N])/F$

Sketch of proof:

- (1) We have explicit matrix group descriptions for G_{E,p^n} , so we can compute their commutator subgroups G'_{E,p^n} explicitly.
- (2) We know $K(j_{K,f}, \zeta_{p^n})$ or $K(j_{K,f}, \zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension of K and can use that to find an upper bound for the size of G'_{E,p^n} .
- (3) We can use the surjective reduction map $\pi : G'_{E,p^{n+1}} \rightarrow G'_{E,p^n}$ to get a lower bound for the size of G'_{E,p^n} .
- (4) It turns out that the upper and lower bounds agree, so it must be that

$$K(j_{K,f}, \zeta_{p^n}) \quad \text{or} \quad K(j_{K,f}, \zeta_{p^n}, \sqrt{\alpha})$$

is the maximal abelian subextension of $\mathbb{Q}(j_{K,f}, E[p^n])/\mathbb{Q}(j_{K,f})$.



Maximal abelian subextensions

Theorem (H., 2024)

Let E/\mathbb{Q} be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K , $f \geq 1$.

Maximal abelian subextensions

Theorem (H., 2024)

Let E/\mathbb{Q} be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K , $f \geq 1$.

(1) If p is any prime such that $p \nmid \Delta_K f^2$, then

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

Maximal abelian subextensions

Theorem (H., 2024)

Let E/\mathbb{Q} be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K , $f \geq 1$.

(1) If p is any prime such that $p \nmid \Delta_K f^2$, then

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

(2) If $p > 2$ is prime such that $p \mid \Delta_K f^2$, then

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{p^n}) & \text{if } E \text{ is a "simplest model",} \\ \mathbb{Q}(\zeta_{p^n}, \sqrt{\alpha}) & \text{if } E \text{ is a twist of previous case.} \end{cases}$$

Maximal abelian subextensions

Theorem (H., 2024)

Let E/\mathbb{Q} be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K , $f \geq 1$.

(1) If p is any prime such that $p \nmid \Delta_K f^2$, then

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

(2) If $p > 2$ is prime such that $p \mid \Delta_K f^2$, then

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{p^n}) & \text{if } E \text{ is a "simplest model",} \\ \mathbb{Q}(\zeta_{p^n}, \sqrt{\alpha}) & \text{if } E \text{ is a twist of previous case.} \end{cases}$$

(3) Let $p = 2$ and $2 \mid \Delta_K f^2$.

- If $\Delta_K f^2 = -12$ or -28 , then $\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{2^{n+1}})$.
- If $\Delta_K f^2 = -4, -8$, or -16 , then

$$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{2^{n+1}}) & \text{if } E \text{ is a "simplest model",} \\ \mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha}) & \text{if } E \text{ is a twist of previous case.} \end{cases}$$

“Simplest model”

Definition

A *simplest model* at a prime p is an elliptic curve $E/\mathbb{Q}(j_{K,f})$ such that $[\mathcal{N}_{\delta,\phi}(p^n) : G_{E,p^n}] = 2, 4$ or 6 (depending on $j_{K,f}$).

| j -invariant | Δ_K | f | Elliptic curve $E_{\Delta_K,f}$ |
|-----------------------------|------------|-----|---------------------------------------|
| 0 | -3 | 1 | $y^2 = x^3 + 16$ |
| $2^4 3^3 5^3$ | | 2 | $y^2 = x^3 - 15x + 22$ |
| $-2^{15} 3 \cdot 5^3$ | | 3 | $y^2 = x^3 - 480x + 4048$ |
| $2^6 3^3$ | -4 | 1 | $y^2 = x^3 + x$ |
| $2^3 3^3 11^3$ | | 2 | $y^2 = x^3 - 11x + 14$ |
| $-3^3 5^3$ | -7 | 1 | $y^2 = x^3 - 1715x + 33614$ |
| $3^3 5^3 17^3$ | | 2 | $y^2 = x^3 - 29155x + 1915998$ |
| $2^6 5^3$ | -8 | 1 | $y^2 = x^3 - 4320x + 96768$ |
| -2^{15} | -11 | 1 | $y^2 = x^3 - 9504x + 365904$ |
| $-2^{15} 3^3$ | -19 | 1 | $y^2 = x^3 - 608x + 5776$ |
| $-2^{18} 3^3 5^3$ | -43 | 1 | $y^2 = x^3 - 13760x + 621264$ |
| $-2^{15} 3^3 5^3 11^3$ | -67 | 1 | $y^2 = x^3 - 117920x + 15585808$ |
| $-2^{18} 3^3 5^3 23^3 29^3$ | -163 | 1 | $y^2 = x^3 - 34790720x + 78984748304$ |

TABLE 1. CM elliptic curves over \mathbb{Q}

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14 .

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14 .

Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n}, \sqrt{-14})$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14 .

Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n}, \sqrt{-14})$.

The simplest CM curve E' has image

$$G_{E',7^n} = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \left\{ \begin{pmatrix} a & b \\ \delta b & a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^{\times 2}, b \in \mathbb{Z}/7\mathbb{Z} \right\} \right\rangle,$$

which is an index 2 subgroup of $\mathcal{N}_{\delta,0}(7^n)$. Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n})$.

Questions?

Abelian extensions of $\mathbb{Q}(i)$

Theorem

Let E/\mathbb{Q} be the elliptic curve $y^2 = x^3 + x$. For each integer $N \geq 1$, let $K_N = \mathbb{Q}(i)(E[N])$. Then $G := \text{Gal}(K_N/\mathbb{Q}(i))$ is abelian.

Proof: Let $P = (x, y) \in E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.

Let A be the action by i on E , so $A \cdot (x, y) = (-x, iy)$.

For $\sigma \in G$, let M_σ be the action by σ on E , so $M_\sigma \cdot (x, y) = (\sigma(x), \sigma(y))$.

The action by σ and i on E commute:

$$\begin{aligned} M_\sigma(A(x, y)) &= M_\sigma(-x, iy) = (\sigma(-x), \sigma(iy)) = (-\sigma(x), i\sigma(y)) \quad \text{and} \\ A(M_\sigma(x, y)) &= A(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)). \end{aligned}$$

Since $\text{End}(E[N]) \cong M_2(\mathbb{Z}/N\mathbb{Z})$, we can view A and G in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

It turns out that any two matrices in $M_2(\mathbb{Z}/N\mathbb{Z})$ that commute with A will commute with each other. Therefore, $G := \text{Gal}(K_N/\mathbb{Q}(i))$ is abelian.



Existence of Weil pairing consequence

Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K . Let E be an elliptic curve with CM by \mathcal{O}_K . Let ζ_N be a primitive N^{th} root of unity.

We know that $K(\zeta_N)/K$ is an abelian extension. Therefore, it must be contained in the maximal abelian extension $K(j(E), h(E_{\text{tors}}))$.

Corollary

There exist points $S, T \in E[m]$ such that the Weil pairing $e_m(S, T)$ is a primitive m^{th} root of unity.

Therefore, the existence of the Weil pairing implies that $K(\zeta_N) \subset K(E[N])$.

Example of $K(\zeta_N) \subset K(E[N])$

Example

Let $K = \mathbb{Q}(\sqrt{-3})$, so $\mathcal{O}_K = \mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$. The elliptic curve

$E/\mathbb{Q} : y^2 = x^3 + 2$ (36.a4) has CM by \mathcal{O}_K , with $j(E) = 0$.

Since K has class number 1, the maximal abelian extension of K is $K(E_{\text{tors}})$, so all abelian extensions of K are contained in $K(E_{\text{tors}})$.

The 3-torsion points of E are

$$E[3] = \{\mathcal{O}, (0, 0), (-2, 0), (1 \pm \sqrt{-3})\},$$

so $K(E[3]) = K(\sqrt{-3}) = \mathbb{Q}(\sqrt{-3})$.

Let ζ_3 be a primitive 3rd root of unity. Observe that $\zeta_3 \in K(\sqrt{-3})$.

Therefore, $K(\zeta_3) \subset K(E[3]) = K(\sqrt{-3}) = \mathbb{Q}(\sqrt{-3})$.

Abelian extension of the Hilbert class field

Sketch of proof: Let $L_m = K(j(E), E[m])$. Since L is the compositum of all the L_m 's, it suffices to show that L_m is an abelian extension of $K(j(E))$.

- $\rho : \text{Gal}(\bar{K}/K(j(E))) \rightarrow \text{Aut}(E[m])$ determined by the condition

$$\rho(\sigma)(T) = T^\sigma \text{ for all } \sigma \in \text{Gal}(\bar{K}/K(j(E))) \text{ and } T \in E[m].$$

- The elements $\sigma \in \text{Gal}(L_m/K(j(E)))$ commute with elements of \mathcal{O}_K in their action on $E[m]$:

$$([\alpha]T)^\sigma = [\alpha](T^\sigma) \text{ for all } T \in E[m] \text{ and } \alpha \in \mathcal{O}_K.$$

- ρ is a homomorphism from $\text{Gal}(\bar{K}/K(j(E)))$ to the group of $\mathcal{O}_K/m\mathcal{O}_K$ -module automorphisms of $E[m]$, and hence ρ induces

$$\phi : \text{Gal}(L_m/K(j(E))) \hookrightarrow \text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]).$$

- $E[m]$ is a free $\mathcal{O}_K/m\mathcal{O}_K$ -module of rank 1, so

$$\text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) \cong (\mathcal{O}_K/m\mathcal{O}_K)^*.$$



Non-abelian extension for non-CM elliptic curve

Example (Non-example)

$E/\mathbb{Q} : y^2 + y = x^3 - x^2$ (11.a3) is a non-CM elliptic curve with $j(E) = -4096/11$.

One can compute (or check on LMFDB) that

$$G_{E,4} = \text{im } \rho_{E,4} = \text{GL}(2, \mathbb{Z}/4\mathbb{Z}),$$

where

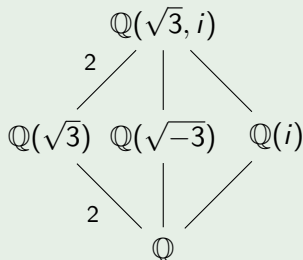
$$\rho_{E,4} : \text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \rightarrow \text{GL}(2, \mathbb{Z}/4\mathbb{Z}).$$

Therefore, $\mathbb{Q}(E[4])/\mathbb{Q}$ is non-abelian.

Hilbert class field example

Example (Hilbert class field of $K = \mathbb{Q}(\sqrt{3})$)

Similarly, $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(\sqrt{3})$ is unramified at all primes in $\mathbb{Z}[\sqrt{3}]$.

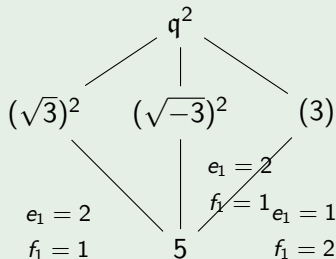
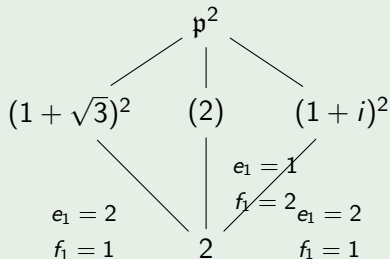


- $\text{disc}_{\mathbb{Z}}(\mathbb{Z}[\sqrt{3}]) = 12 = 2^2 \cdot 3$, so only 2 and 3 ramify in $\mathbb{Q}(\sqrt{3})$
- $\text{disc}_{\mathbb{Z}}\left(\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right) = -3$, so only 3 ramifies in $\mathbb{Q}(\sqrt{-3})$
- $\text{disc}_{\mathbb{Z}}(\mathbb{Z}[i]) = -4 = -2^2$, so only 2 ramifies in $\mathbb{Q}(i)$

Hilbert class field example

Example (cont'd)

Since $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$, we have that $4 = efg$.



$2 \mid e, 2 \mid f \Rightarrow e = 2, f = 2, g = 1. \quad 2 \mid e, 2 \mid f \Rightarrow e = 2, f = 2, g = 1.$

Therefore, we conclude that the primes 2 and 3 are unramified in $\mathbb{Q}(\sqrt{3}, i)$; however, $\mathbb{Q}(\sqrt{3}, i)$ is not the Hilbert class field of $\mathbb{Q}(\sqrt{3})$.

Observe that $K = \mathbb{Q}(\sqrt{3})$ has class number 1, so the Hilbert class field H of K must be a degree 1 extension of K . In fact, $H = \mathbb{Q}(\sqrt{3})$.