Computing abelian extensions of quartic fields using complex multiplication

Jared Asuncion
Supervision: Andreas Enge and Marco Streng

JNCF 2020

degree $[L : K]$ of a field extension L of K is $\dim_K(L)$ (as a vector space).

$\mathbb{Q}(\sqrt{29}) = \mathbb{Q} + \mathbb{Q}\sqrt{29}$ $\qquad$ $[\mathbb{Q}(\sqrt{29}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{29})) = 2.$

degree $[L : K]$ of a field extension L of K is $\dim_K(L)$ (as a vector space).

$\mathbb{Q}(\sqrt{29}) = \mathbb{Q} + \mathbb{Q}\sqrt{29}$ $\qquad$ $[\mathbb{Q}(\sqrt{29}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{29})) = 2.$

number field: field extension $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] < \infty$

Examples: $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{29})$ $\qquad$ Non-examples: $\mathbb{F}_2, \mathbb{Q}[X], \mathbb{R}, \mathbb{C} = \mathbb{R}(i)$

degree $[L : K]$ of a field extension L of K is $\dim_K(L)$ (as a vector space).

$\mathbb{Q}(\sqrt{29}) = \mathbb{Q} + \mathbb{Q}\sqrt{29}$ $\qquad$ $[\mathbb{Q}(\sqrt{29}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{29})) = 2.$

number field: field extension $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] < \infty$

Examples: $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{29})$ $\qquad$ Non-examples: $\mathbb{F}_2, \mathbb{Q}[X], \mathbb{R}, \mathbb{C} = \mathbb{R}(i)$

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

$\mathrm{Aut}\left(\mathbb{Q}(\sqrt{29})/\mathbb{Q}\right)$ is generated by $a + b\sqrt{29} \mapsto a - b\sqrt{29}$.

degree $[L : K]$ of a field extension L of K is $\dim_K(L)$ (as a vector space).

$\mathbb{Q}(\sqrt{29}) = \mathbb{Q} + \mathbb{Q}\sqrt{29}$ $\qquad$ $[\mathbb{Q}(\sqrt{29}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{29})) = 2.$

number field: field extension $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] < \infty$

Examples: $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{29})$ $\qquad$ Non-examples: $\mathbb{F}_2, \mathbb{Q}[X], \mathbb{R}, \mathbb{C} = \mathbb{R}(i)$

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

$\mathrm{Aut}\left(\mathbb{Q}(\sqrt{29})/\mathbb{Q}\right)$ is generated by $a + b\sqrt{29} \mapsto a - b\sqrt{29}$.

abelian extension L of K: extension of number fields L/K such that

- $|\mathrm{Aut}(L/K)| = [L : K]$
- $\mathrm{Aut}(L/K)$ is abelian

$*$ means Galois extension

Let K be a number field.

Class Field Theory

There exists a set $\{H_K(m) : m \in \mathbb{Z}\}$ such that:
For any finite degree abelian extension L of K,

there exists $f \in \mathbb{Z}_{>0}$ such that $L \subseteq H_K(f)$.

$H_K(m)$ is called the ray class field of K for the modulus m.

Let K be a number field.

Class Field Theory

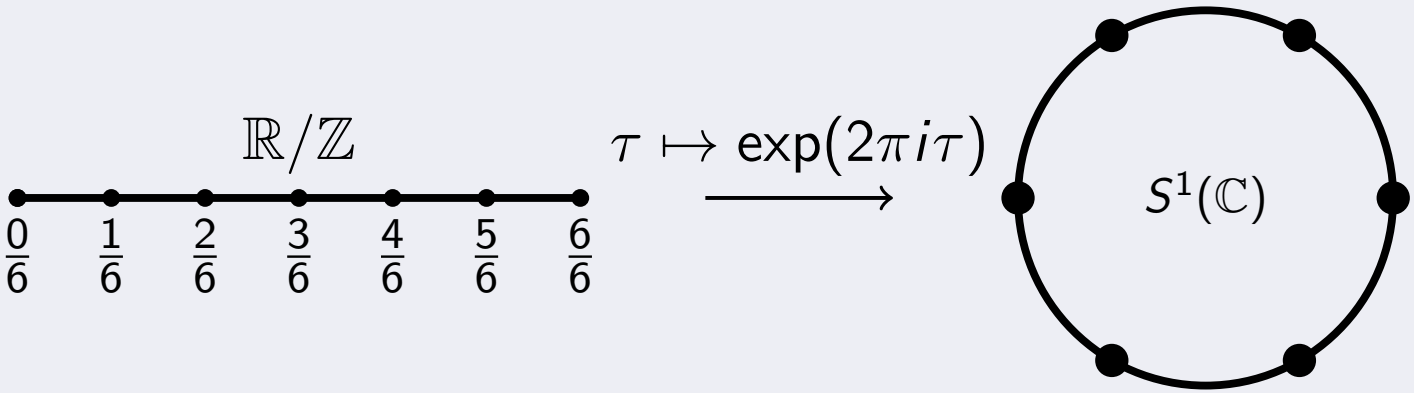
There exists a set $\{H_K(m) : m \in \mathbb{Z}\}$ such that:
For any finite degree abelian extension L of K,
there exists $f \in \mathbb{Z}_{>0}$ such that $L \subseteq H_K(f)$.
$H_K(m)$ is called the ray class field of K for the modulus m.

Kronecker-Weber Theorem (1896)

Let $m \in \mathbb{Z}_{>0}$.
Then $H_{\mathbb{Q}}(m) = \mathbb{Q}(\zeta_m) = \mathbb{Q}(\exp(2\pi i\tau) : \tau \in \frac{1}{m}\mathbb{Z})$.

Kronecker-Weber Theorem (1896)

Let $m \in \mathbb{Z}_{>0}$.
Then $H_{\mathbb{Q}}(m) = \mathbb{Q}(\zeta_m) = \mathbb{Q}(\exp(2\pi i\tau) : \tau \in \frac{1}{m}\mathbb{Z})$.



---

analytic function: map $\tau \mapsto \exp(2\pi i\tau)$ from $\mathbb{R}/\mathbb{Z}$ to the unit circle
special arguments: torsion points of the group $\mathbb{R}/\mathbb{Z}$

Kronecker-Weber Theorem (1896)

Let $m \in \mathbb{Z}_{>0}$.
Then $H_{\mathbb{Q}}(m) = \mathbb{Q}(\zeta_m) = \mathbb{Q}(\exp(2\pi i\tau) : \tau \in \frac{1}{m}\mathbb{Z})$.

---

analytic function: map $\tau \mapsto \exp(2\pi i\tau)$ from $\mathbb{R}/\mathbb{Z}$ to the unit circle
special arguments: torsion points of the group $\mathbb{R}/\mathbb{Z}$

Hilbert's 12th Problem (1900)

Let K be a number field.
Let $m \in \mathbb{Z}_{>0}$.
Then $H_K(m) =$???.

---

analytic function: ???
special arguments: ???

$K = \mathbb{Q}(\sqrt{-D})$ *with* $D \in \mathbb{Z}_{>0}$

Definition (CM field)

CM field K: number field which is
a totally imaginary quadratic extension (no embeddings of K into $\mathbb{R}$) of
a totally real number field K_0 (all embeddings of K_0 in $\mathbb{C}$ land in $\mathbb{R}$).

$K = \mathbb{Q}(\sqrt{-D})$ *with* $D \in \mathbb{Z}_{>0}$

Definition (CM field)

CM field K: number field which is
a totally imaginary quadratic extension (no embeddings of K into $\mathbb{R}$) of
a totally real number field K_0 (all embeddings of K_0 in $\mathbb{C}$ land in $\mathbb{R}$).

Example

$K = \mathbb{Q}(\sqrt{-D})$ with $D \in \mathbb{Z}_{>0}$ is a CM field of degree 2. $K_0 = \mathbb{Q}$

Definition (CM field)

CM field K: number field which is
a totally imaginary quadratic extension (no embeddings of K into $\mathbb{R}$) of
a totally real number field K_0 (all embeddings of K_0 in $\mathbb{C}$ land in $\mathbb{R}$).

Example

$K = \mathbb{Q}(\sqrt{-D})$ with $D \in \mathbb{Z}_{>0}$ is a CM field of degree 2. $K_0 = \mathbb{Q}$

An Oversimplification of CM Theory

Let K be a CM field of degree $2g$.
Let $m \in \mathbb{Z}_{>0}$.
CM theory gives an abelian extension $\mathrm{CM}_K(m) \subseteq H_K(m)$ of K.

An Oversimplification of CM Theory

Let K be a CM field of degree $2g$.
Let $m \in \mathbb{Z}_{>0}$.
CM theory gives an abelian extension $\mathrm{CM}_K(m) \subseteq H_K(m)$ of K.

Imaginary Quadratic Number Field

Let K be a CM field of degree 2.
Let $m \in \mathbb{Z}_{>0}$. Then

An Oversimplification of CM Theory

Let K be a CM field of degree $2g$.
Let $m \in \mathbb{Z}_{>0}$.
CM theory gives an abelian extension $\mathrm{CM}_K(m) \subseteq H_K(m)$ of K.

Imaginary Quadratic Number Field

Let K be a CM field of degree 2.
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(j(\tau))$$
$$\mathrm{CM}_K(m) = K(j(\tau), h(P) : P \in E_\tau[m])$$

where τ depends on K and $j(\tau)$ is an invariant of $\mathbb{C}^2/(\mathbb{Z} + \tau\mathbb{Z}) \cong E_\tau$.

Imaginary Quadratic Number Field

Let K be a CM field of degree 2.
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(j(\tau))$$
$$\mathrm{CM}_K(m) = K(j(\tau), h(P) : P \in E_\tau[m])$$

where τ depends on K and $j(\tau)$ is an invariant of $\mathbb{C}^2/(\mathbb{Z} + \tau\mathbb{Z}) \cong E_\tau$.

---

analytic function: map $P \mapsto h(P)$ from E_τ to $\mathbb{C}$
special arguments: torsion points of the group E_τ

Imaginary Quadratic Number Field

Let K be a CM field of degree 2.
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(j(\tau))$$
$$\mathrm{CM}_K(m) = K(j(\tau), h(P) : P \in E_\tau[m])$$

where τ depends on K and $j(\tau)$ is an invariant of $\mathbb{C}^2/(\mathbb{Z} + \tau\mathbb{Z}) \cong E_\tau$.

---

analytic function: map $P \mapsto h(P)$ from E_τ to $\mathbb{C}$
special arguments: torsion points of the group E_τ

A Miracle

Let K be a CM field of degree 2. Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(m) = H_K(m).$$

Primitive Quartic CM Field

Let K be a primitive CM field of degree 4. primitive: not bicyclic Galois
Let $m \in \mathbb{Z}_{>0}$. Then

Primitive Quartic CM Field

Let K be a primitive CM field of degree 4. primitive: not bicyclic Galois
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(i_1(\tau), i_2(\tau), i_3(\tau))$$
$$\mathrm{CM}_K(m) = K(i_1(\tau), i_2(\tau), i_3(\tau), h(P) : P \in A_\tau[m])$$

where τ depends on K and $i_k(\tau)$ are invariants of $\mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2) \cong A_\tau$.

Primitive Quartic CM Field

Let K be a primitive CM field of degree 4. primitive: not bicyclic Galois
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(i_1(\tau), i_2(\tau), i_3(\tau))$$
$$\mathrm{CM}_K(m) = K(i_1(\tau), i_2(\tau), i_3(\tau), h(P) : P \in A_\tau[m])$$

where τ depends on K and $i_k(\tau)$ are invariants of $\mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2) \cong A_\tau$.

---

analytic function: map $P \mapsto h(P)$ from A_τ to $\mathbb{C}$
special arguments: torsion points of the group A_τ

Primitive Quartic CM Field

Let K be a primitive CM field of degree 4. primitive: not bicyclic Galois
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(i_1(\tau), i_2(\tau), i_3(\tau))$$
$$\mathrm{CM}_K(m) = K(i_1(\tau), i_2(\tau), i_3(\tau), h(P) : P \in A_\tau[m])$$

where τ depends on K and $i_k(\tau)$ are invariants of $\mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2) \cong A_\tau$.

---

analytic function: map $P \mapsto h(P)$ from A_τ to $\mathbb{C}$
special arguments: torsion points of the group A_τ

No miracles here.

Let K be a primitive CM field of degree 4. Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(m) \subseteq H_K(m).$$

Primitive Quartic CM Field

Let K be a primitive CM field of degree 4. primitive: not bicyclic Galois
Let $m \in \mathbb{Z}_{>0}$. Then

$$\mathrm{CM}_K(1) = K(i_1(\tau), i_2(\tau), i_3(\tau))$$
$$\mathrm{CM}_K(m) = K(i_1(\tau), i_2(\tau), i_3(\tau), h(P) : P \in A_\tau[m])$$

where τ depends on K and $i_k(\tau)$ are invariants of $\mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2) \cong A_\tau$.

---

analytic function: map $P \mapsto h(P)$ from A_τ to $\mathbb{C}$
special arguments: torsion points of the group A_τ

Streng (2010)

Let K be a primitive CM field of degree 4. Let $m \in \mathbb{Z}_{>0}$. Then

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

is of exponent at most 2.

Streng (2010)

Let K be a primitive CM field of degree 4. Then

$$H_{K_0}(1)\,\mathrm{CM}_K(1) \subseteq H_K(1)$$

is of exponent at most 2.

Streng (2010)

Let K be a primitive CM field of degree 4. Then

$$H_{K_0}(1)\,\mathrm{CM}_K(1) \subseteq H_K(1)$$

is of exponent at most 2.

Optimist: Sometimes $H_{K_0}(1)\,\mathrm{CM}_K(1) = H_K(1)$! experimentally, 80%

Streng (2010)

Let K be a primitive CM field of degree 4. Then

$$H_{K_0}(1)\,\mathrm{CM}_K(1) \subseteq H_K(1)$$

is of exponent at most 2.

Optimist: Sometimes $H_{K_0}(1)\,\mathrm{CM}_K(1) = H_K(1)$! experimentally, 80%

Pessimist: Sometimes it's not. experimentally, 20%

Streng (2010)

Let K be a primitive CM field of degree 4. Then

$$H_{K_0}(1)\,\mathrm{CM}_K(1) \subseteq H_K(1)$$

is of exponent at most 2.

Optimist: Sometimes $H_{K_0}(1)\,\mathrm{CM}_K(1) = H_K(1)$! experimentally, 80%

Pessimist: Sometimes it's not. experimentally, 20%

Shimura (1968)

Let K be a primitive CM field of degree 4.
Then there is $m \in \mathbb{Z}_{>0}$ such that

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m). \qquad (\star)$$

Shimura (1968)

Let K be a primitive CM field of degree 4.
Then there is $m \in \mathbb{Z}_{>0}$ such that

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m). \qquad (\star)$$

Shimura (1968)

Let K be a primitive CM field of degree 4.
Then there is $m \in \mathbb{Z}_{>0}$ such that

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m). \qquad (\star)$$

Let $\mathcal{O}_K$ be the ring of integers of K.

$$\mathrm{Cl}_K(1) = \frac{\{ \text{ ideals of } \mathcal{O}_K \}}{\{ \text{ ideals of } \mathcal{O}_K \text{ generated by a single element } \}}$$

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S \rangle|$ is odd.
Let P be the set of primes of $\mathbb{Z}$ divisible by the elements of S.
Take $m = 4\prod_{p \in P} p$. Then, $(\star)$ is true.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.
Let $\mathrm{Cl}_K(1) = \langle[\mathfrak{p}_5]\rangle_8$ where $\mathfrak{p}_5 = 5\mathcal{O}_K + (y-2)\mathcal{O}_K$.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.
Let $\mathrm{Cl}_K(1) = \langle [\mathfrak{p}_5] \rangle_8$ where $\mathfrak{p}_5 = 5\mathcal{O}_K + (y-2)\mathcal{O}_K$.
Let $S = \{\, \mathfrak{p}_2 \,,\, \mathfrak{p}_5 \,\}$ where $\mathfrak{p}_2$ is the only prime ideal dividing $2\mathcal{O}_K$.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.
Let $\mathrm{Cl}_K(1) = \langle[\mathfrak{p}_5]\rangle_8$ where $\mathfrak{p}_5 = 5\mathcal{O}_K + (y-2)\mathcal{O}_K$.
Let $S = \{\mathfrak{p}_2, \mathfrak{p}_5\}$ where $\mathfrak{p}_2$ is the only prime ideal dividing $2\mathcal{O}_K$.
Then we take $P = \{2, 5\}$.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.
Let $\mathrm{Cl}_K(1) = \langle [\mathfrak{p}_5] \rangle_8$ where $\mathfrak{p}_5 = 5\mathcal{O}_K + (y-2)\mathcal{O}_K$.
Let $S = \{\mathfrak{p}_2, \mathfrak{p}_5\}$ where $\mathfrak{p}_2$ is the only prime ideal dividing $2\mathcal{O}_K$.
Then we take $P = \{2, 5\}$.
Take $m = 40$.

A. (2019)

Let K be a primitive CM field of degree 4.
Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that
S contains all prime ideals which divide $2\mathcal{O}_K$ and $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd.
Let P be the set of rational primes below the prime ideals in S.
Take $m = 4\prod_{p\in P} p$. Then, $H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)$ is true.

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.
Let $\mathrm{Cl}_K(1) = \langle [\mathfrak{p}_5] \rangle_8$ where $\mathfrak{p}_5 = 5\mathcal{O}_K + (y-2)\mathcal{O}_K$.
Let $S = \{\mathfrak{p}_2, \mathfrak{p}_5\}$ where $\mathfrak{p}_2$ is the only prime ideal dividing $2\mathcal{O}_K$.
Then we take $P = \{2, 5\}$.
Take $m = 40$.

$$H_K(1) \subseteq H_{K_0}(40)\,\mathrm{CM}_K(40).$$

$[H_{K_0}(40)\,\mathrm{CM}_K(40) : H_K(1)] = 49\,152.$

Given $m \in \mathbb{Z}_{>0}$.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)\ ?$$

Given $m \in \mathbb{Z}_{>0}$.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)\ ?$$

By Galois theory, this is equivalent to asking...

Given $m \in \mathbb{Z}_{>0}$.

$$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}\ ?$$

$\mathbf{A} := \mathrm{Aut}(H_K(m)/H_K(1))$

$\mathbf{B} := \mathrm{Aut}(H_K(m)/H_{K_0}(m))$

$\mathbf{C} := \mathrm{Aut}(H_K(m)/\mathrm{CM}_K(m))$

Given $m \in \mathbb{Z}_{>0}$.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m)\ ?$$

By Galois theory, this is equivalent to asking...

Given $m \in \mathbb{Z}_{>0}$.

$$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}\ ?$$

$$\mathbf{A} := \mathrm{Aut}(H_K(m)/H_K(1)) \cong \ker(\,\mathrm{Cl}_K(m) \to \mathrm{Cl}_K(1)\,)$$

$$\mathbf{B} := \mathrm{Aut}(H_K(m)/H_{K_0}(m)) \cong \ker(\,N_{K/K_0} : \mathrm{Cl}_K(m) \to \mathrm{Cl}_{K_0}(m)\,)$$

$$\mathbf{C} := \mathrm{Aut}(H_K(m)/\,\mathrm{CM}_K(m)) \cong \ker(\,\mathcal{N} : \mathrm{Cl}_K(m) \to \mathfrak{C}_K(m)\,)$$

$\mathbf{A} := \mathrm{Aut}(H_K(m)/H_K(1)) \cong \ker(\mathrm{Cl}_K(m) \to \mathrm{Cl}_K(1))$

$\mathbf{B} := \mathrm{Aut}(H_K(m)/H_{K_0}(m)) \cong \ker(N_{K/K_0} : \mathrm{Cl}_K(m) \to \mathrm{Cl}_{K_0}(m))$

$\mathbf{C} := \mathrm{Aut}(H_K(m)/\mathrm{CM}_K(m)) \cong \ker(\mathcal{N} : \mathrm{Cl}_K(m) \to \mathfrak{C}_K(m))$

Computing $\mathrm{Aut}(H_K(m)/\mathrm{CM}_K(m))$.

- $\mathrm{Cl}_K(m)$, $\mathrm{Cl}_K(1)$, $\mathrm{Cl}_{K_0}(m)$ ..... PARI/GP ✓
- N_{K/K_0} ..... PARI/GP ✓
- $\mathfrak{C}_K(m)$, $m = 1$ ..... RECIP (Streng) / CMH (Enge / Thomé) ✓
  $m \geq 1$ ..... (A. 2020) ✓

$\mathbf{A} := \mathrm{Aut}(H_K(m)/H_K(1)) \cong \ker(\mathrm{Cl}_K(m) \to \mathrm{Cl}_K(1))$

$\mathbf{B} := \mathrm{Aut}(H_K(m)/H_{K_0}(m)) \cong \ker(N_{K/K_0} : \mathrm{Cl}_K(m) \to \mathrm{Cl}_{K_0}(m))$

$\mathbf{C} := \mathrm{Aut}(H_K(m)/\mathrm{CM}_K(m)) \cong \ker(\mathcal{N} : \mathrm{Cl}_K(m) \to \mathfrak{C}_K(m))$

Computing $\mathrm{Aut}(H_K(m)/\mathrm{CM}_K(m))$.

- $\mathrm{Cl}_K(m)$, $\mathrm{Cl}_K(1)$, $\mathrm{Cl}_{K_0}(m)$ ..... PARI/GP ✓
- N_{K/K_0} ..... PARI/GP ✓
- $\mathfrak{C}_K(m)$, $m = 1$ ..... RECIP (Streng) / CMH (Enge / Thomé) ✓
  $m \geq 1$ ..... (A. 2020) ✓

$$0 \to \mathcal{O}_{K_0}^+/N_{K/K_0}(\mathcal{O}_{K,1}) \to \mathfrak{C}_K(m) \to \ker(\mathrm{Cl}_K(m) \to \mathrm{Cl}_{K_0}^+(1)) \to 0$$

- operations on group morphisms ..... `abgrp.gp` ✓

  kernels, images, quotients, group extensions

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$m = 1$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(1)/H_K(1)) &&\cong \langle [(1)] \rangle_1 \\
\mathbf{B} &= \mathrm{Aut}(H_K(1)/H_{K_0}(1)) &&\cong \langle [\mathfrak{p}_5] \rangle_8 \\
\mathbf{C} &= \mathrm{Aut}(H_K(1)/\mathrm{CM}_K(1)) &&\cong \langle [\mathfrak{p}_5^4] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$?

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$m = 1$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(1)/H_K(1)) \cong \langle [(1)] \rangle_1 \\
\mathbf{B} &= \mathrm{Aut}(H_K(1)/H_{K_0}(1)) \cong \langle [\mathfrak{p}_5] \rangle_8 \\
\mathbf{C} &= \mathrm{Aut}(H_K(1)/\mathrm{CM}_K(1)) \cong \langle [\mathfrak{p}_5^4] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$? **NO.** $\Rightarrow H_K(1) \not\subseteq H_{K_0}(1)\,\mathrm{CM}_K(1)$

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$m = 1$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(1)/H_K(1)) &&\cong \langle [(1)] \rangle_1 \\
\mathbf{B} &= \mathrm{Aut}(H_K(1)/H_{K_0}(1)) &&\cong \langle [\mathfrak{p}_5] \rangle_8 \\
\mathbf{C} &= \mathrm{Aut}(H_K(1)/\mathrm{CM}_K(1)) &&\cong \langle [\mathfrak{p}_5^4] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$? **NO.** $\Rightarrow H_K(1) \not\subseteq H_{K_0}(1)\,\mathrm{CM}_K(1)$

$m = 2$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(2)/H_K(1)) &&\cong && \langle [(\alpha_1)] \rangle_2 \times \langle [(\alpha_2)] \rangle_2 \\
\mathbf{B} &= \mathrm{Aut}(H_K(2)/H_{K_0}(2)) &&\cong \langle [\mathfrak{p}_5] \rangle_8 \times && \langle [(\alpha_1)] \rangle_2 \times \langle [(\alpha_2)] \rangle_2 \\
\mathbf{C} &= \mathrm{Aut}(H_K(2)/\mathrm{CM}_K(2)) &&\cong && \langle [(\alpha_1)] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$? **YES.** $\Rightarrow H_K(1) \subseteq H_{K_0}(2)\,\mathrm{CM}_K(2)$

Let $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$m = 1$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(1)/H_K(1)) &&\cong \langle [(1)] \rangle_1 \\
\mathbf{B} &= \mathrm{Aut}(H_K(1)/H_{K_0}(1)) &&\cong \langle [\mathfrak{p}_5] \rangle_8 \\
\mathbf{C} &= \mathrm{Aut}(H_K(1)/\mathrm{CM}_K(1)) &&\cong \langle [\mathfrak{p}_5^4] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$? **NO.** $\Rightarrow H_K(1) \not\subseteq H_{K_0}(1)\,\mathrm{CM}_K(1)$

$m = 2$

$$\begin{aligned}
\mathbf{A} &= \mathrm{Aut}(H_K(2)/H_K(1)) &&\cong && \langle [(\alpha_1)] \rangle_2 \times \langle [(\alpha_2)] \rangle_2 \\
\mathbf{B} &= \mathrm{Aut}(H_K(2)/H_{K_0}(2)) &&\cong \langle [\mathfrak{p}_5] \rangle_8 \times && \langle [(\alpha_1)] \rangle_2 \times \langle [(\alpha_2)] \rangle_2 \\
\mathbf{C} &= \mathrm{Aut}(H_K(2)/\mathrm{CM}_K(2)) &&\cong && \langle [(\alpha_1)] \rangle_2
\end{aligned}$$

$\mathbf{A} \supseteq \mathbf{B} \cap \mathbf{C}$? **YES.** $\Rightarrow H_K(1) \subseteq H_{K_0}(2)\,\mathrm{CM}_K(2)$

$\mathbf{A} \supseteq \mathbf{C}$! $\Rightarrow H_K(1) \subseteq \mathrm{CM}_K(2)$.

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$
- $m = 2$
- $m \neq 1, 2$

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$ ..... RECIP (Streng) / CMH (Enge, Thomé)) ✓
- $m = 2$
- $m \neq 1, 2$

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$ ..... RECIP (Streng) / CMH (Enge, Thomé)) ✓
- $m = 2$ ..... example after this slide ✓
- $m \neq 1, 2$

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$ ..... RECIP (Streng) / CMH (Enge, Thomé)) ✓
- $m = 2$ ..... example after this slide ✓

  Assume $\star$ for $m = 2$ and $[H_K(1) : K]$ is large:

  can find $H_K(1)$ faster than Kummer theory
- $m \neq 1, 2$

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$ ..... RECIP (Streng) / CMH (Enge, Thomé)) ✓
- $m = 2$ ..... example after this slide ✓

  Assume $\star$ for $m = 2$ and $[H_K(1) : K]$ is large:

  can find $H_K(1)$ faster than Kummer theory
- $m \neq 1, 2$ ..... map $P \mapsto h(P)$ from A_τ to $\mathbb{C}$ 🕒

Let K be a primitive quartic CM field.

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star)$$

So Far...

- Find m such that $\star$ is true. ..... ✓
- Given m, determine if $\star$ is true. ..... ✓

Computing $\mathrm{CM}_K(m)$.

- $m = 1$ ..... RECIP (Streng) / CMH (Enge, Thomé)) ✓ $\sim 80\%$
- $m = 2$ ..... example after this slide ✓ $\sim 10\%$

  Assume $\star$ for $m = 2$ and $[H_K(1) : K]$ is large:

  can find $H_K(1)$ faster than Kummer theory
- $m \neq 1, 2$ ..... map $P \mapsto h(P)$ from A_τ to $\mathbb{C}$ ⏲ $\sim 10\%$

$$H_K(1) \subseteq \mathrm{CM}_K(2) = K(\lambda_k(\tau) \,:\, k \in \{1,2,3\})$$

where $\lambda_k(\tau)$ are in terms of theta constants (analytic functions).

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$$H_K(1) \subseteq \mathrm{CM}_K(2) = K(\lambda_k(\tau) \,:\, k \in \{1,2,3\})$$

where $\lambda_k(\tau)$ are in terms of theta constants (analytic functions).

Some costly theta computations give:

$$\text{approximations } \tilde{\lambda}_k(\tau)^\sigma \qquad \text{for each } \sigma \in \mathrm{Aut}(\mathrm{CM}_K(2)/K).$$

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$$H_K(1) \subseteq \mathrm{CM}_K(2) = K(\lambda_k(\tau) \,:\, k \in \{1,2,3\})$$

where $\lambda_k(\tau)$ are in terms of theta constants (analytic functions).

Some costly theta computations give:

$$\text{approximations } \tilde{\lambda}_k(\tau)^\sigma \qquad \text{for each } \sigma \in \mathrm{Aut}(\mathrm{CM}_K(2)/K).$$

$$\begin{array}{rcccccc}
\mathbf{G} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/K) & = & \langle\sigma_1\rangle_8 & \times & \langle\sigma_2\rangle_2 \\
\mathbf{H} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/H_K(1)) & = & & & \langle\sigma_2\rangle_2 \\
\mathbf{G}/\mathbf{H} & = & \mathrm{Aut}(H_K(1)/K) & = & \langle\sigma_1\rangle_8 & &
\end{array}$$

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

Some costly theta computations give:

$$\text{approximations } \tilde{\lambda}_k(\tau)^\sigma \qquad \text{for each } \sigma \in \mathrm{Aut}(\mathrm{CM}_K(2)/K).$$

$$\begin{array}{rcccccc} \mathbf{G} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/K) & = & \langle\sigma_1\rangle_8 & \times & \langle\sigma_2\rangle_2 \\ \mathbf{H} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/H_K(1)) & = & & & \langle\sigma_2\rangle_2 \\ \mathbf{G}/\mathbf{H} & = & \mathrm{Aut}(H_K(1)/K) & = & \langle\sigma_1\rangle_8 & & \end{array}$$

$$H_K(1) = \mathrm{CM}_K(2)^{\mathbf{H}} = K(\lambda_k(\tau) + \lambda_k(\tau)^{\sigma_2} : k \in \{1,2,3\}).$$

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$$\begin{array}{rcccccc} \mathbf{G} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/K) & = & \langle\sigma_1\rangle_8 & \times & \langle\sigma_2\rangle_2 \\ \mathbf{H} & = & \mathrm{Aut}(\mathrm{CM}_K(2)/H_K(1)) & = & & & \langle\sigma_2\rangle_2 \\ \mathbf{G}/\mathbf{H} & = & \mathrm{Aut}(H_K(1)/K) & = & \langle\sigma_1\rangle_8 & & \end{array}$$

$$H_K(1) = \mathrm{CM}_K(2)^{\mathbf{H}} = K(\lambda_k(\tau) + \lambda_k(\tau)^{\sigma_2} : k \in \{1,2,3\}).$$

$$\tilde{p}_1(X) = \prod_{\sigma \in \mathbf{G}/\mathbf{H}} \left(X - \left(\tilde{\lambda}_1(\tau) + \tilde{\lambda}_1(\tau)^{\sigma_2}\right)^{\sigma}\right).$$

$$\approx X^8 - 36.591404X^7 + 530.70821X^6 - 3769.6792X^5 + \cdots$$

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$$H_K(1) = \mathrm{CM}_K(2)^{\mathbf{H}} = K(\lambda_k(\tau) + \lambda_k(\tau)^{\sigma_2} : k \in \{1, 2, 3\}).$$

$$\tilde{p}_1(X) = \prod_{\sigma \in \mathbf{G}/\mathbf{H}} \left(X - \left(\tilde{\lambda}_1(\tau) + \tilde{\lambda}_1(\tau)^{\sigma_2} \right)^{\sigma} \right).$$

$$\approx X^8 - 36.591404X^7 + 530.70821X^6 - 3769.6792X^5 + \cdots$$

Use an algorithm involving LLL to find

$$dp_1(X) = dX^8 + (9415170754271100000y^2 + 186957159620069475000)X^7 +$$
$$(3825208465541329538000y^2 + 8749908322905010620800000)X^6 + \ldots$$

where $d = 5^8\,7^4\,13^4\,23^4$.

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.

$$\tilde{p}_1(X) = \prod_{\sigma \in \mathbf{G}/\mathbf{H}} \left(X - \left(\tilde{\lambda}_1(\tau) + \tilde{\lambda}_1(\tau)^{\sigma_2} \right)^{\sigma} \right).$$

$$\approx X^8 - 36.591404X^7 + 530.70821X^6 - 3769.6792X^5 + \cdots$$

Use an algorithm involving LLL to find

$$dp_1(X) = dX^8 + (9415170754271100000y^2 + 186957159620069475000)X^7 + (3825208465541329538000y^2 + 8749908322905010620800000)X^6 + \ldots$$

where $d = 5^8\,7^4\,13^4\,23^4$.

$p_1(X)$ is a degree 8 irreducible polynomial in $K[X]$. So

$$H_K(1) = K(\alpha) \qquad \text{where } p_1(\alpha) = 0.$$

where $K = \mathbb{Q}(y)$ where $y^4 + 24y^2 + 28 = 0$.