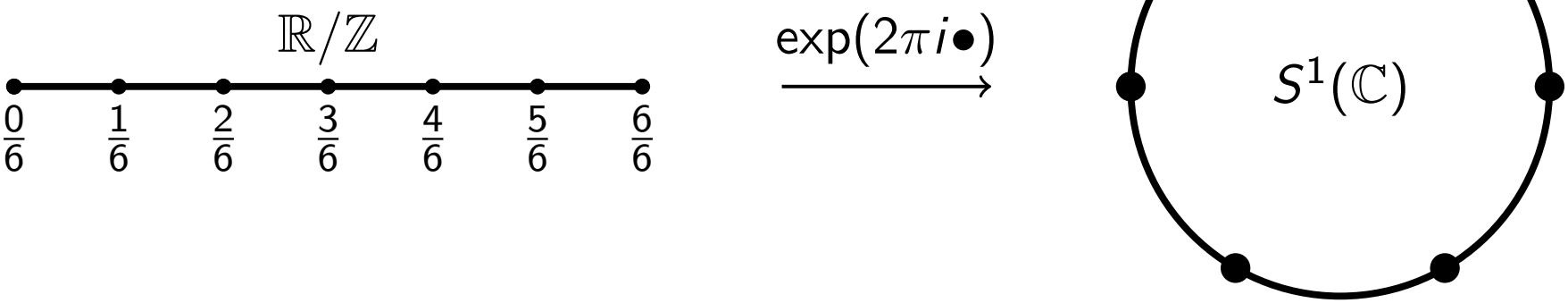
Computing Hilbert Class Fields of Quartic Fields Using Complex Multiplication

Jared Asuncion
Supervisors: Andreas Enge and Marco Streng

Journee Arithmetique

Theorem (Kronecker-Weber Theorem (KWT))

The abelian extensions of $K = \mathbb{Q}$ are contained in the cyclotomic fields 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.

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 twelfth problem is only solved in the following cases:

- $K = \mathbb{Q}$
- $K = \mathbb{Q}(\sqrt{-D})$, $D < 0$

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 twelfth problem is only solved in the following cases:

- $K = \mathbb{Q}$
- $K = \mathbb{Q}(\sqrt{-D})$, $D < 0$

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 (Kronecker-Weber Theorem (KWT))

For the case where $K = \mathbb{Q}$,

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

Theorem (Kronecker-Weber Theorem (KWT))

For the case where $K = \mathbb{Q}$,

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

Theorem (Main Theorem of Complex Multiplication for Elliptic Curves)

Let K *be an imaginary quadratic number field. Let* E *be an elliptic curve such that there exists* $\iota : K \hookrightarrow \operatorname{End} E \otimes \mathbb{Q}$ *with* $\iota^{-1}(\operatorname{End} E) = \mathcal{O}_K$. *Then*

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

where $j(E)$ *is the* j*-invariant of* E, $t \in E$ *is a torsion point of order* m, h *is the Weber function.*

A higher-dimensional version of the main theorem of CM was discovered around half a century later.

A higher-dimensional version of the main theorem of CM was discovered around half a century later.

Definition

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

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

A higher-dimensional version of the main theorem of CM was discovered around half a century later.

Definition

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

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

Definition

A principally polarized abelian variety is a projective group variety with an associated isomorhism $\phi : A \to A^\vee$.

An elliptic curve is a principally polarized abelian variety of dimension 1.

imaginary quadratic number field $\rightsquigarrow$ quartic CM field

elliptic curve E $\rightsquigarrow$ principally polarized abelian surface A

abelian extensions of K $\rightsquigarrow$

j-invariant j $\rightsquigarrow$

Weber function h $\rightsquigarrow$

imaginary quadratic number field $\rightsquigarrow$ quartic CM field

elliptic curve E $\rightsquigarrow$ principally polarized abelian surface A

abelian extensions of K $\rightsquigarrow$ abelian extensions of K^r

j-invariant j $\rightsquigarrow$

Weber function h $\rightsquigarrow$

$$\begin{aligned}
\text{imaginary quadratic number field} &\rightsquigarrow \text{quartic CM field} \\
\text{elliptic curve } E &\rightsquigarrow \text{principally polarized abelian surface } A \\
\text{abelian extensions of } K &\rightsquigarrow \text{abelian extensions of } K^r \\
\text{j-invariant } j &\rightsquigarrow \text{Igusa invariants } i = (i_1, i_2, i_3) \\
\text{Weber function } h &\rightsquigarrow
\end{aligned}$$

imaginary quadratic number field $\rightsquigarrow$ quartic CM field

elliptic curve $E \rightsquigarrow$ principally polarized abelian surface A

abelian extensions of $K \rightsquigarrow$ abelian extensions of K^r

j-invariant $j \rightsquigarrow$ Igusa invariants $i = (i_1, i_2, i_3)$

Weber function $h \rightsquigarrow F$, associated to a Kummer variety

imaginary quadratic number field $\rightsquigarrow$ quartic CM field

elliptic curve $E \rightsquigarrow$ principally polarized abelian surface A

abelian extensions of $K \rightsquigarrow$ abelian extensions of K^r

j-invariant $j \rightsquigarrow$ Igusa invariants $i = (i_1, i_2, i_3)$

Weber function $h \rightsquigarrow F$, associated to a Kummer variety

Theorem (Main Theorem of Complex Multiplication for PPAbSurfs)

Let K be a quartic CM field. Let K^r be its reflex. Let A be a principally polarized abelian surface such that there exists $\iota : K \hookrightarrow \operatorname{End} A \otimes \mathbb{Q}$ with $\iota^{-1}(\operatorname{End} A) = \mathcal{O}_K$. Then

$$H_{K^r}(1) \supset K^r(i(A))$$
$$H_{K^r}(m) \supset K^r(i(A), F(t))$$

where t is an point of A of order m.

Theorem (Main Theorem of Complex Multiplication for PPAbSurfs)

Let K be a quartic CM field. Let K^r be its reflex. Let A be a principally polarized abelian surface such that there exists $\iota : K \hookrightarrow \operatorname{End} A \otimes \mathbb{Q}$ with $\iota^{-1}(\operatorname{End} A) = \mathcal{O}_K$. Then

$$H_{K^r}(1) \supset K^r(i(A))$$
$$H_{K^r}(m) \supset K^r(i(A), F(t))$$

where t is an point of A of order m.

$K^r(i(A))$ does not always give us the entire Hilbert class field $H_{K^r}(1)$.

Goal

Find a way to compute $H_{K^r}(1)$.

Define

$$\mathrm{CM}_{K^r}(m) = \begin{cases} K^r(i(A)) & m = 1 \\ K^r(i(A), F(t)) & m \neq 1, \text{ as in the theorem.} \end{cases}$$

Denote by $H_{K_0^r}(m)$ the Hilbert class field of K_0 for the modulus m.

Define

$$\mathrm{CM}_{K^r}(m) = \begin{cases} K^r(i(A)) & m = 1 \\ K^r(i(A), F(t)) & m \neq 1, \text{ as in the theorem.} \end{cases}$$

Denote by $H_{K_0^r}(m)$ the Hilbert class field of K_0 for the modulus m.

Theorem (Streng 2010)

Let K^r be a primitive quartic CM-field. Then the extension

$$\Xi_{K^r}(m) := \mathrm{CM}_{K^r}(m) H_{K_0^r}(m) \subseteq H_K(m)$$

is an extension of at most exponent 2.

Define

$$\mathrm{CM}_{K^r}(m) = \begin{cases} K^r(i(A)) & m = 1 \\ K^r(i(A), F(t)) & m \neq 1, \text{ as in the theorem.} \end{cases}$$

Denote by $H_{K_0^r}(m)$ the Hilbert class field of K_0 for the modulus m.

Theorem (Streng 2010)

Let K^r be a primitive quartic CM-field. Then the extension

$$\Xi_{K^r}(m) := \mathrm{CM}_{K^r}(m) H_{K_0^r}(m) \subseteq H_K(m)$$

is an extension of at most exponent 2.

Theorem (Shimura 1962)

There exists an integer m such that

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

Theorem (Shimura 1962)

There exists an integer m such that $H_{K^r}(1) \subseteq \Xi_{K^r}(m)$.

Theorem (Shimura 1962)

There exists an integer m such that $H_{K^r}(1) \subseteq \Xi_{K^r}(m)$.

We have an effective version of this.

Theorem (A. 2019)

Let S be a finite set of prime ideals of K^r such that

- *S contains all prime ideals of K^r above 2*
- *$\mathrm{Cl}_{K^r}(1)/\langle S \rangle$ has odd order.*

Theorem (Shimura 1962)

There exists an integer m such that $H_{K^r}(1) \subseteq \Xi_{K^r}(m)$.

We have an effective version of this.

Theorem (A. 2019)

Let S be a finite set of prime ideals of K^r such that

- *S contains all prime ideals of K^r above 2*
- *$\mathrm{Cl}_{K^r}(1)/\langle S \rangle$ has odd order.*

Let P be the set of rational primes that are below the primes in S. Let

$$m = 4 \cdot \prod_{p \in P} p.$$

Theorem (Shimura 1962)

There exists an integer m such that $H_{K^r}(1) \subseteq \Xi_{K^r}(m)$.

We have an effective version of this.

Theorem (A. 2019)

Let S be a finite set of prime ideals of K^r such that

- *S contains all prime ideals of K^r above 2*
- *$\mathrm{Cl}_{K^r}(1)/\langle S \rangle$ has odd order.*

Let P be the set of rational primes that are below the primes in S. Let

$$m = 4 \cdot \prod_{p \in P} p.$$

Then

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

Theorem (A.)

Let $m = 4\prod_{p\in P} p$. *Then*

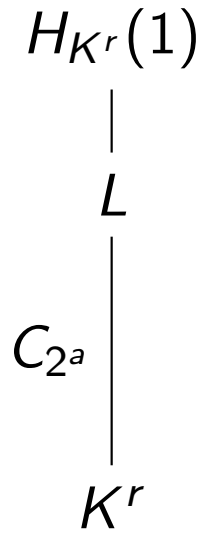
$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

Theorem (A.)

Let $m = 4\prod_{p \in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- Take L/K^r to be the largest unramified abelian extension of K^r whose degree is a power of 2.

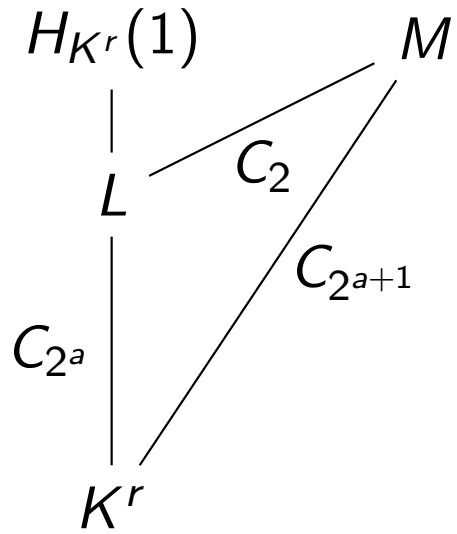


Theorem (A.)

Let $m = 4\prod_{p \in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- Take L/K^r to be the largest unramified abelian extension of K^r whose degree is a power of 2.
- $\exists M$ cyclic extension such that $\mathrm{Gal}(M/K^r) = C_{2^{a+1}}$

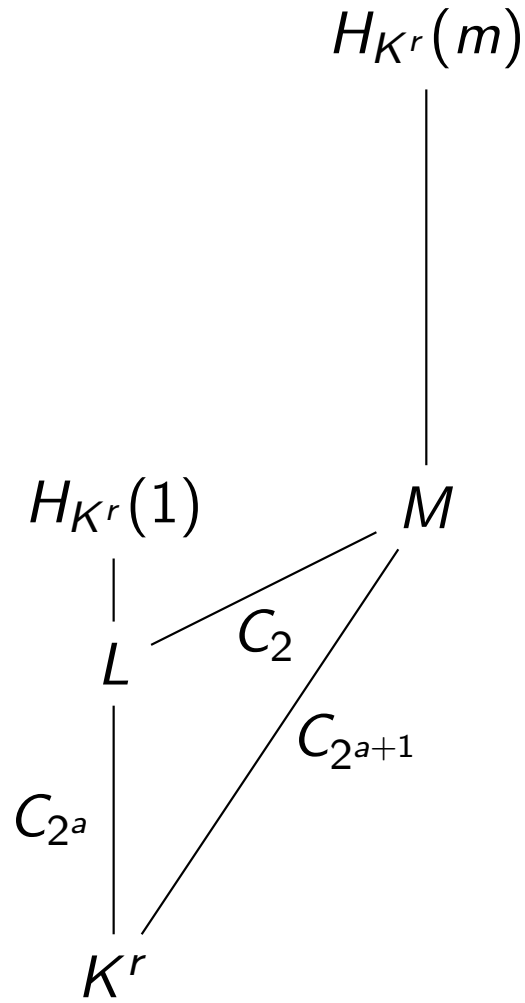


Theorem (A.)

Let $m = 4\prod_{p \in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- Take L/K^r to be the largest unramified abelian extension of K^r whose degree is a power of 2.
- $\exists M$ cyclic extension such that $\mathrm{Gal}(M/K^r) = C_{2^{a+1}}$
- $\exists m$ such that $M \subseteq H_{K^r}(m)$

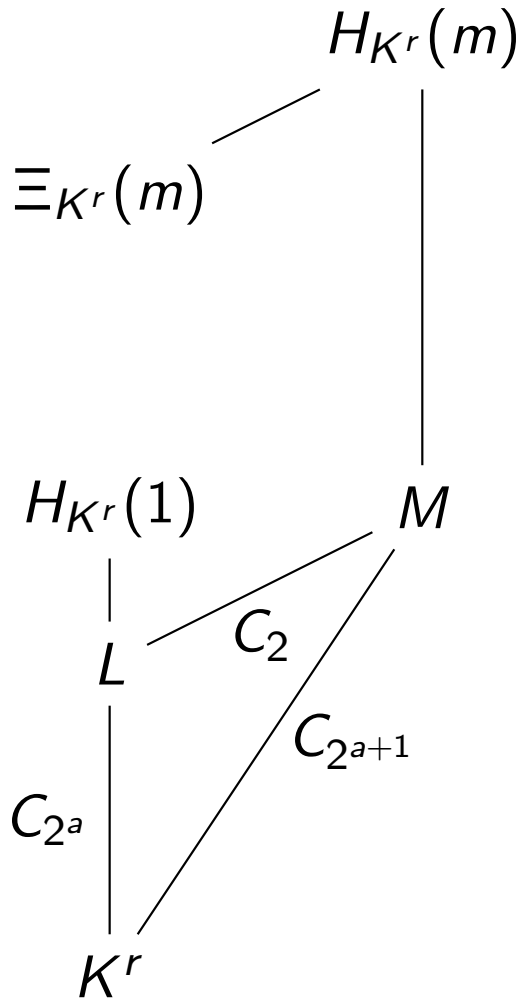


Theorem (A.)

Let $m = 4\prod_{p \in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- Take L/K^r to be the largest unramified abelian extension of K^r whose degree is a power of 2.
- $\exists M$ cyclic extension such that $\mathrm{Gal}(M/K^r) = C_{2^{a+1}}$
- $\exists m$ such that $M \subseteq H_{K^r}(m)$
- $\Xi_{K^r}(m) \subseteq H_{K^r}(m)$

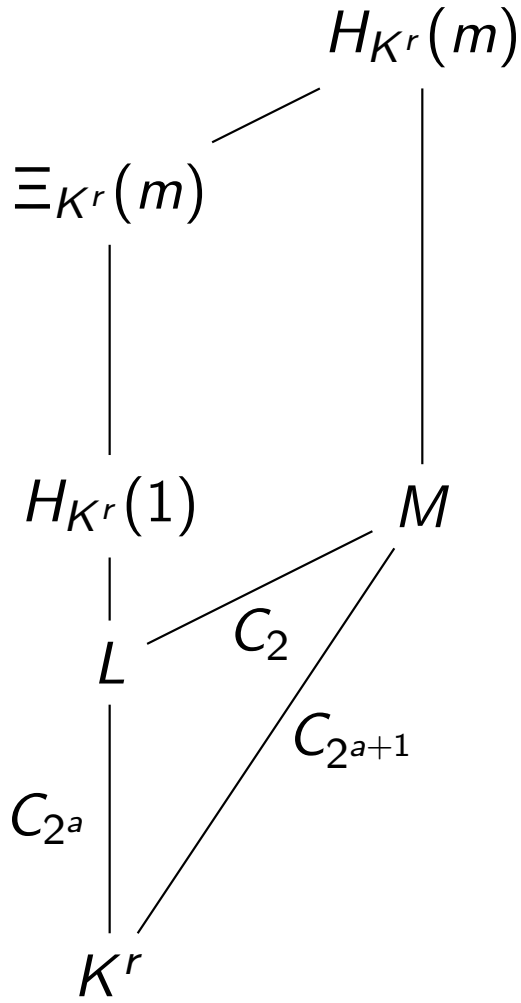


Theorem (A.)

Let $m = 4\prod_{p\in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- $H_{K^r}(1) \subseteq \Xi_m$
  using class field theory, and definition of M and m

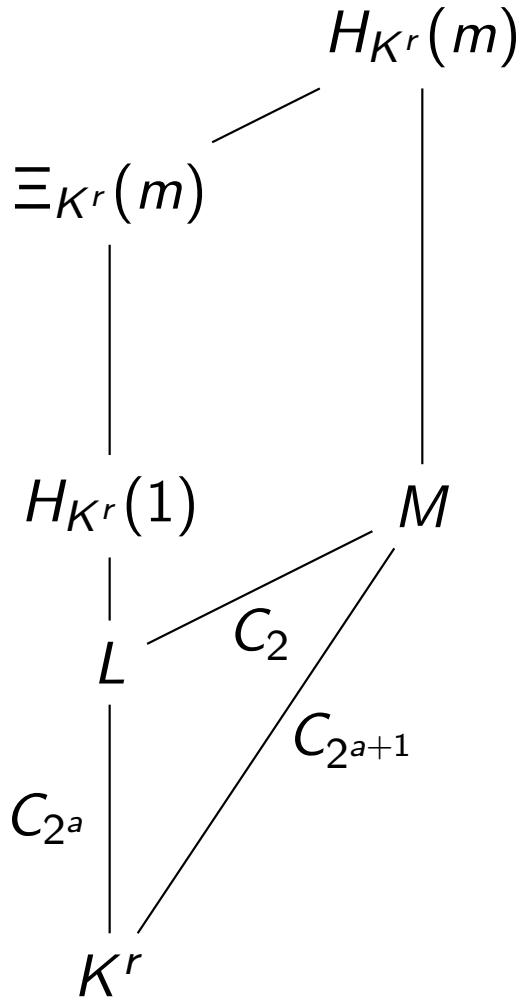


Theorem (A.)

Let $m = 4\prod_{p\in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- $H_{K^r}(1) \subseteq \Xi_m$
  using class field theory, and definition of M and m
- (Crespo 1989) Can choose M such that M does not ramify outside S.

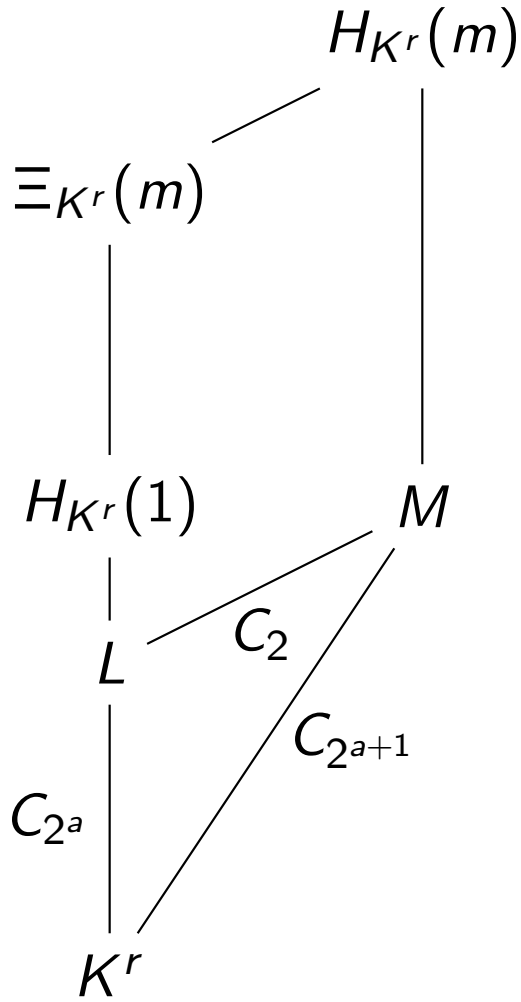


Theorem (A.)

Let $m = 4\prod_{p\in P} p$. *Then*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(m).$$

- $H_{K^r}(1) \subseteq \Xi_m$
  using class field theory, and definition of M and m
- (Crespo 1989) Can choose M such that M does not ramify outside S.
- (Cohen 1999) Bound the valuations at the primes.



Example

Take

$$K^r = \mathbb{Q}(y) \cong \frac{\mathbb{Q}[Y]}{(Y^4 + 26Y^2 + 89)}.$$

We know that

$$\mathrm{Cl}_{K^r}(1) = C_4 \cong \langle \mathfrak{k} \rangle \qquad \textit{where} \quad \mathfrak{k} = (11, y)$$

Take

$$S = \{\mathfrak{p}_2, \mathfrak{k}\} \qquad \Rightarrow \qquad P = \{2, 11\}$$

and so

$$m = 4 \cdot (2 \cdot 11) = 88$$

then

$$H_{K^r}(1) \subseteq \Xi_{K^r}(88).$$

From the previous slide:

$$H_{K^r}(1) \subseteq \Xi_{K^r}(88).$$

Example

Note that

$$H_{K^r}(1) \subseteq \Xi_{K^r}(88)$$

is an extension of huge degree. We know that for each $d \mid m$

$$\Xi_{K^r}(d) \subseteq \Xi_{K^r}(m).$$

Trying all divisors of 88*, we find that*

$$H_{K^r}(1) \subseteq \Xi_{K^r}(2)$$

It suffices to compute $H_{K^r}(1)$ as a subfield of $\Xi_{K^r}(2)$.

Computing $H_{K^r}(1)$

Let m be such that $H_{K^r}(1) \subseteq \Xi_{K^r}(m)$.

- Compute $H_{K_0^r}(m)$ using Stark's conjectures.
- Compute $\mathrm{CM}_{K^r}(m)$ using complex multiplication.
- Take the composite to obtain $\Xi_{K^r}(m)$.
- Use Galois theory to view $H_{K^r}(1)$ as a subfield of $\Xi_{K^r}(m)$.

State of the Art

- There exist implementations to compute $H_{K_0^r}(m)$.
- There exist implementations for computing $\mathrm{CM}_{K^r}(m)$ for $m = 1, 2$.
- Currently studying how to compute $\mathrm{CM}_{K^r}(m)$ for larger m.