Tower decomposition of Hilbert class fields

Jared Guissmo E. Asuncion

July 20, 2017

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Certify primality of p using the Atkin-Morain ECPP algorithm.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Construct an elliptic curve E over $\mathbb{F}_p$ with N points where N is in terms of p and D.

$$\Downarrow$$

Certify primality of p using the Atkin-Morain ECPP algorithm.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Find a root $j \in \mathbb{F}_p$ of the
Hilbert class polynomial of $\mathbb{Q}(\sqrt{-D})$.

$\Downarrow$

Construct an elliptic curve E over $\mathbb{F}_p$ with N points
where N is in terms of p and D.

$\Downarrow$

Certify primality of p using the Atkin-Morain ECPP algorithm.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Find a root x of the Weber polynomial $\mathscr{W}_D$.

$\Downarrow$

Find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial of $\mathbb{Q}(\sqrt{-D})$.

$\Downarrow$

Construct an elliptic curve E over $\mathbb{F}_p$ with N points where N is in terms of p and D.

$\Downarrow$

Certify primality of p using the Atkin-Morain ECPP algorithm.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Find a root x of the Weber polynomial $\mathscr{W}_D$.

$\Downarrow$

Find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial of $\mathbb{Q}(\sqrt{-D})$.

$\Downarrow$

Construct an elliptic curve E over $\mathbb{F}_p$ with N points where N is in terms of p and D.

$\Downarrow$

Certify primality of p using the Atkin-Morain ECPP algorithm.

We discuss the solution given in Enge (2003) more thoroughly.

Let $K = \mathbb{Q}(\sqrt{-D})$. Let $\mathcal{O}_K$ be its ring of integers. Let

$$\mathrm{Cl}(\mathcal{O}_K) = \frac{\text{fractional ideals of } \mathcal{O}_K}{\text{principal fractional ideals of } \mathcal{O}_K}.$$

Let $K = \mathbb{Q}(\sqrt{-D})$. Let $\mathcal{O}_K$ be its ring of integers. Let

$$\mathrm{Cl}(\mathcal{O}_K) = \frac{\text{fractional ideals of } \mathcal{O}_K}{\text{principal fractional ideals of } \mathcal{O}_K}.$$

Definition

The Weber polynomial is a defining polynomial for the Hilbert class field H_K given by

$$\mathscr{W}_D(X) = \prod_{\mathfrak{k} \in \mathrm{Cl}(\mathcal{O}_K)} (X - x_{\mathfrak{k}})$$

where $x_{\mathfrak{k}}$ is a complex number dependent on $\mathfrak{k}$.

Example

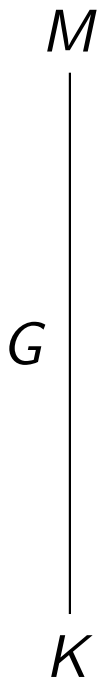
Let $K = \mathbb{Q}(\sqrt{-D})$ *where* $D = 335$. *Let* $\mathfrak{z}$ *be the trivial class group of* $\mathrm{Cl}(\mathcal{O}_K)$. *We have*

$$H_K = K(x_{\mathfrak{z}})$$

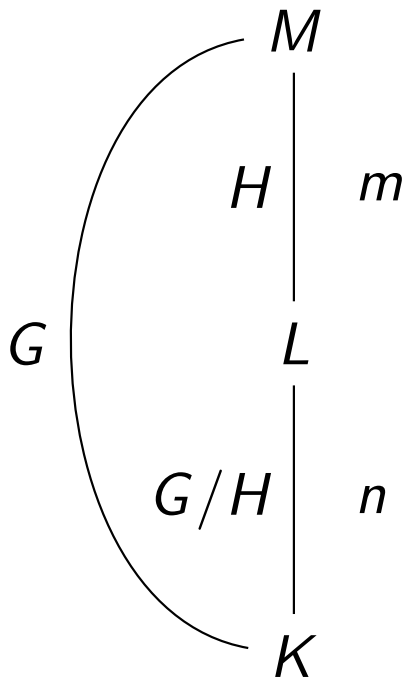
with defining polynomial

$$\begin{aligned}\mathscr{W}_D(X) = {} & X^{18} - 4X^{17} - 20X^{16} - 55X^{15} - 106X^{14} - 144X^{13} \\ & - 163X^{12} - 174X^{11} - 179X^{10} - 171X^9 - 144X^8 - 102X^7 \\ & - 64X^6 - 42X^5 - 33X^4 - 25X^3 - 14X^2 - 5X - 1.\end{aligned}$$

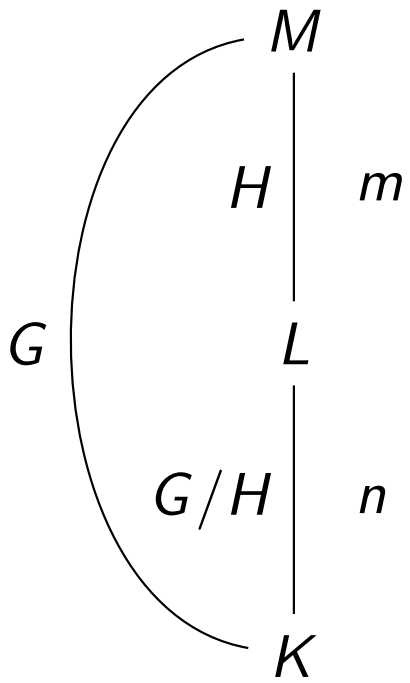
Let M be a Galois extension of a field K with $G = \mathrm{Gal}(M/K)$.
Let x be a root of f such that $M = K(x)$.



Let M be a Galois extension of a field K with $G = \mathrm{Gal}(M/K)$.
Let x be a root of f such that $M = K(x)$.

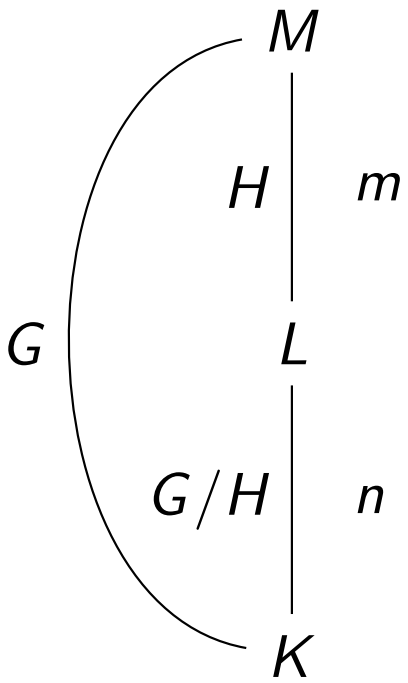


Let M be a Galois extension of a field K with $G = \mathrm{Gal}(M/K)$.
Let x be a root of f such that $M = K(x)$.



$$W = \prod_{h \in H}(X - x^h) \in L[X]$$

Let M be a Galois extension of a field K with $G = \mathrm{Gal}(M/K)$.
Let x be a root of f such that $M = K(x)$.



$W = \prod_{h \in H}(X - x^h) \in L[X]$

$V = ???$

$$W = \prod_{h \in H} (X - x^h)$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

U_g

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

$$U_g = \prod_{h \in H} (X - x^{gh})$$

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

$$U_g = \prod_{h \in H} (X - x^{gh}) = X^m + \vartheta_{m-1}^g X^{m-1} + \vartheta_{m-2}^g X^{m-2} + \ldots + \vartheta_1^g X + \vartheta_0^g$$

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

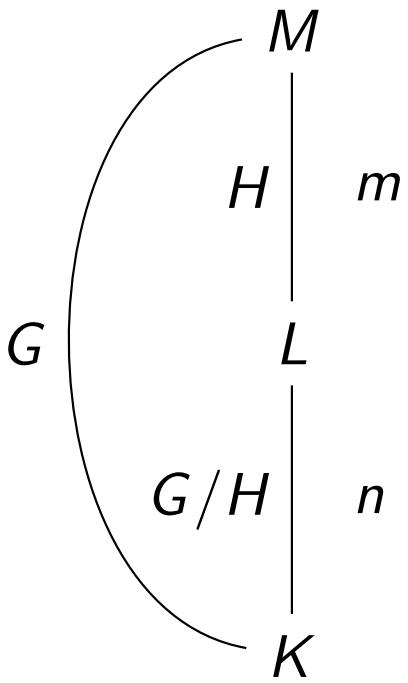
$$W = \prod_{h \in H} (X - x^h) = X^m + \vartheta_{m-1} X^{m-1} + \vartheta_{m-2} X^{m-2} + \ldots + \vartheta_1 X + \vartheta_0$$

$$U_g = \prod_{h \in H} (X - x^{gh}) = X^m + \vartheta_{m-1}^g X^{m-1} + \vartheta_{m-2}^g X^{m-2} + \ldots + \vartheta_1^g X + \vartheta_0^g$$

Definition

$$V_k = \prod_{g \in G/H} (Y - \vartheta_k^g)$$

Let M be a Galois extension of a field K with $G = \mathrm{Gal}(M/K)$.
Let x be a root of f such that $M = K(x)$.

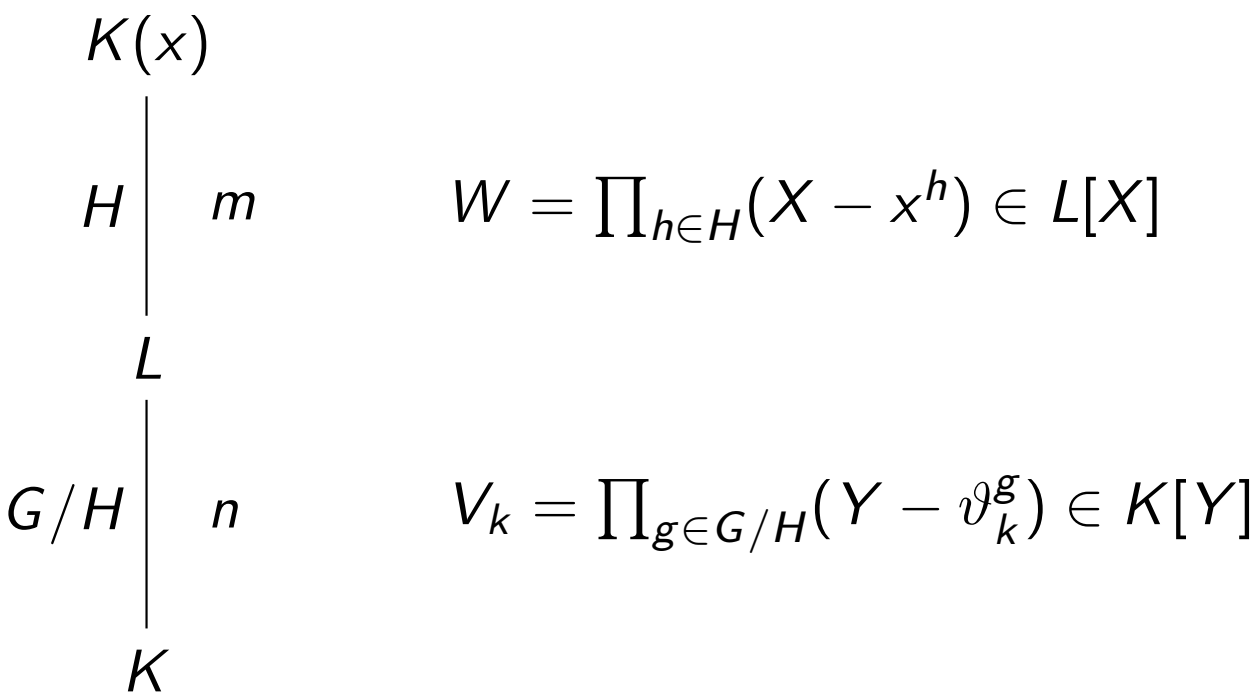


$$W = \prod_{h \in H}(X - x^h) \in L[X]$$

$$V_k = \prod_{g \in G/H}(Y - \vartheta_k^g) \in K[Y]$$

In the case where $x := x_{\mathfrak{k}}$ and

$$K = \mathbb{Q}(\sqrt{-D}), \qquad M = H_K = K(x), \qquad f = \mathscr{W}_D, \qquad x \in \mathbb{R}, \text{ root of } f.$$



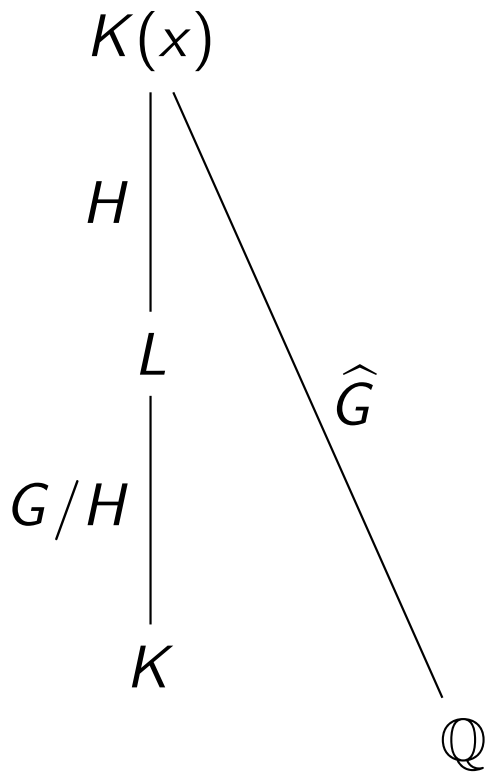
$$W = \prod_{h \in H}(X - x^h) \in L[X]$$

$$V_k = \prod_{g \in G/H}(Y - \vartheta_k^g) \in K[Y]$$

In the case where $x := x_{\mathfrak{k}}$ and

$$K = \mathbb{Q}(\sqrt{-D}), \qquad M = H_K = K(x), \qquad f = \mathscr{W}_D, \qquad x \in \mathbb{R}, \text{ root of } f.$$

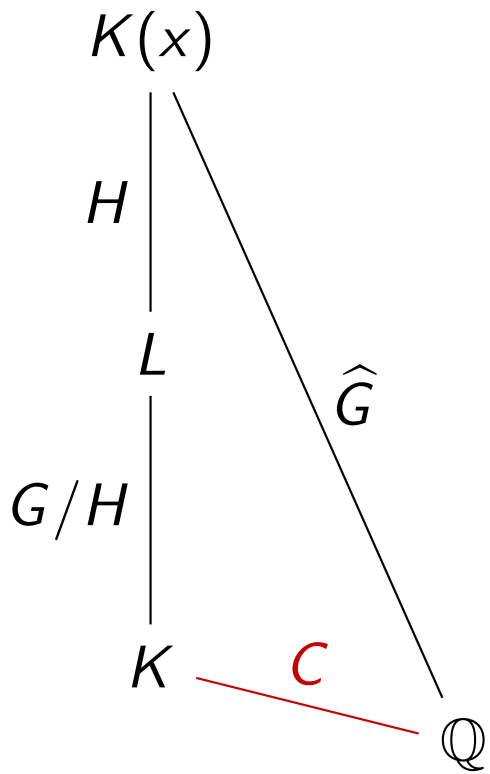
$$K' = \mathbb{Q}$$



In the case where $x := x_{\mathfrak{k}}$ and

$$K = \mathbb{Q}(\sqrt{-D}), \qquad M = H_K = K(x), \qquad f = \mathscr{W}_D, \qquad x \in \mathbb{R}, \text{ root of } f.$$

$$K' = \mathbb{Q}$$

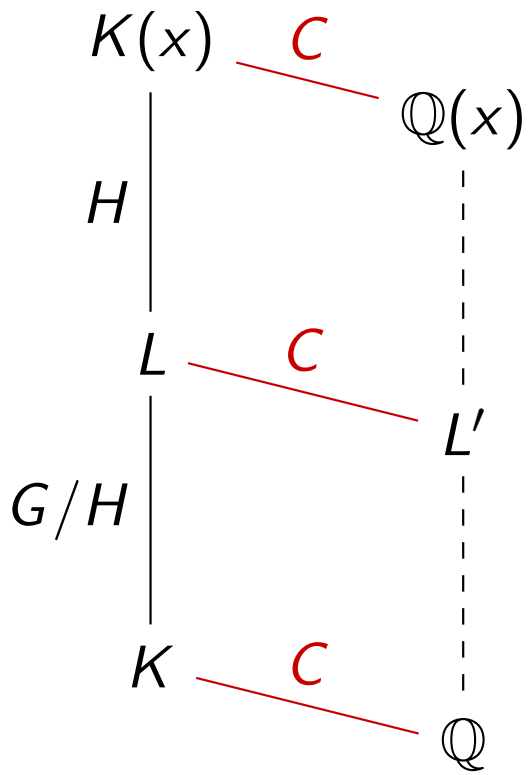


In the case where $x := x_{\mathfrak{k}}$ and

$$K = \mathbb{Q}(\sqrt{-D}), \qquad M = H_K = K(x), \qquad f = \mathscr{W}_D, \qquad x \in \mathbb{R}, \text{ root of } f.$$

We have corresponding smaller fields

$$K' = \mathbb{Q} \qquad M' = \mathbb{Q}(x)$$



$$W = \prod_{h \in H}(X - x^h) \in L[X]$$

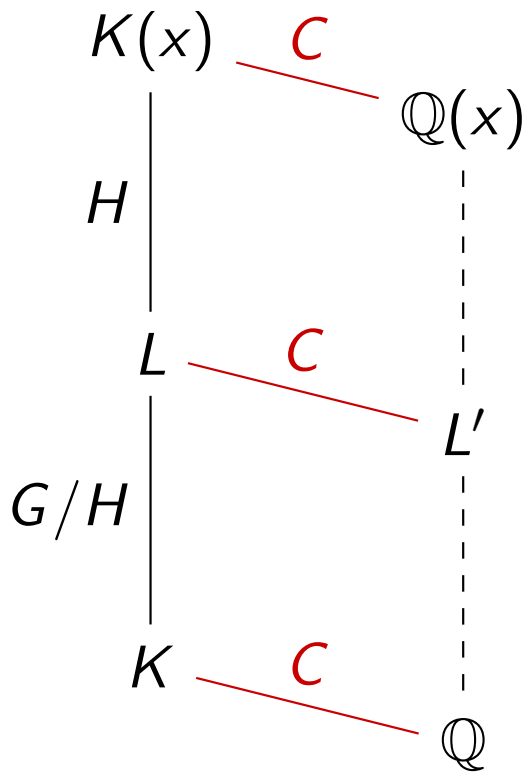
$$V_k = \prod_{g \in G/H}(Y - \vartheta_k^g) \in K[Y]$$

In the case where $x := x_{\mathfrak{k}}$ and

$$K = \mathbb{Q}(\sqrt{-D}), \qquad M = H_K = K(x), \qquad f = \mathscr{W}_D, \qquad x \in \mathbb{R}, \text{ root of } f.$$

We have corresponding smaller fields

$$K' = \mathbb{Q} \qquad M' = \mathbb{Q}(x)$$



$$W = \prod_{h \in H}(X - x^h) \in L'[X]$$

$$V_k = \prod_{g \in G/H}(Y - \vartheta_k^g) \in K'[Y]$$

Example

Let $D = 335$

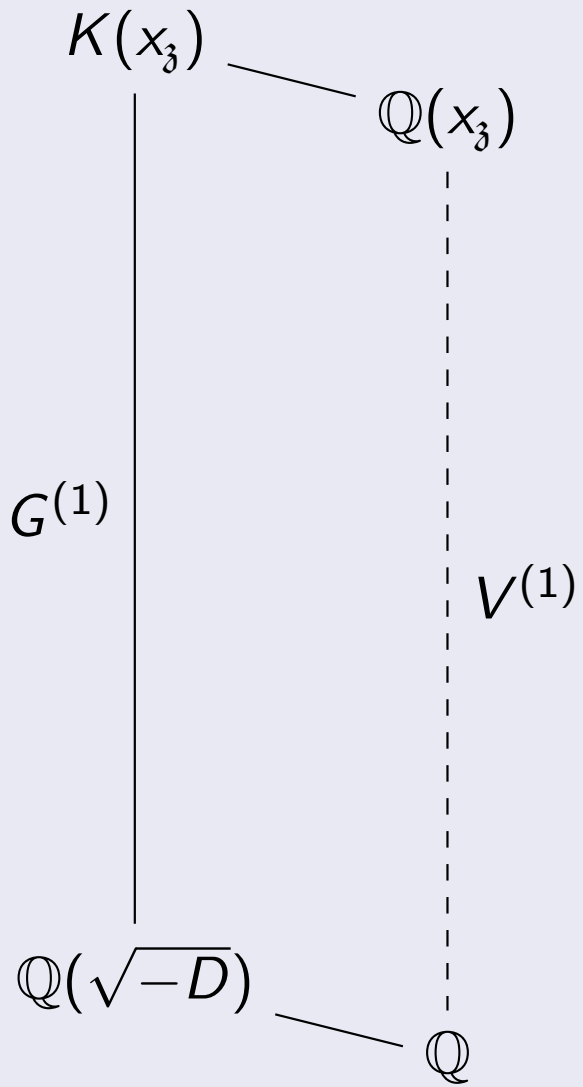
$$K = \mathbb{Q}(\sqrt{-335})$$
$$M = H_K = K(x_{\mathfrak{z}})$$

where $\mathfrak{z} \in \mathrm{Cl}(\mathcal{O}_K)$ *is the trivial ideal class.*

Note that

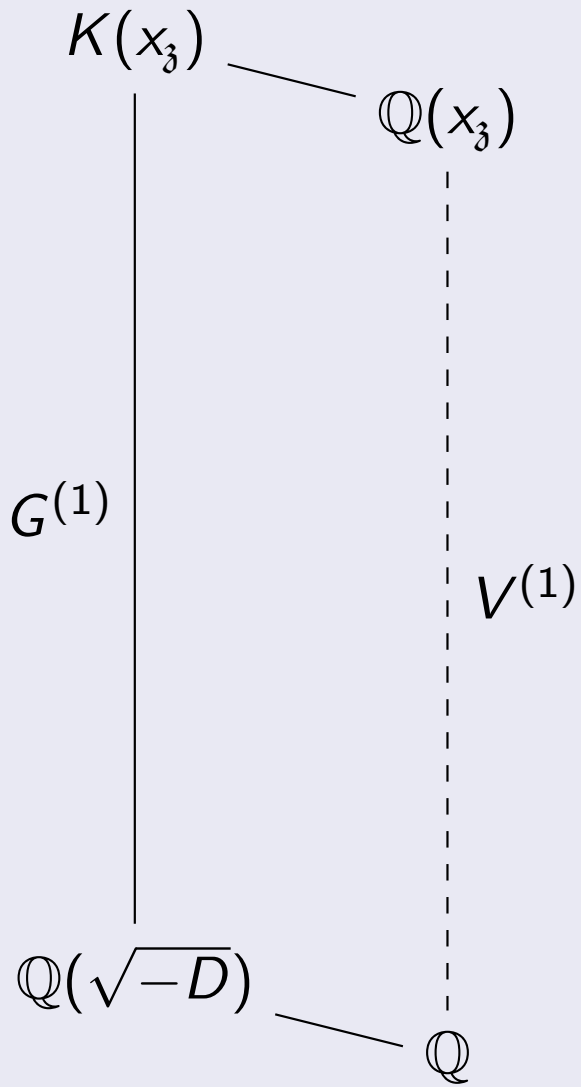
$$G^{(1)} = G \cong \mathrm{Cl}(\mathcal{O}_K) = \langle \mathfrak{k} \rangle$$

is cyclic with order 18.



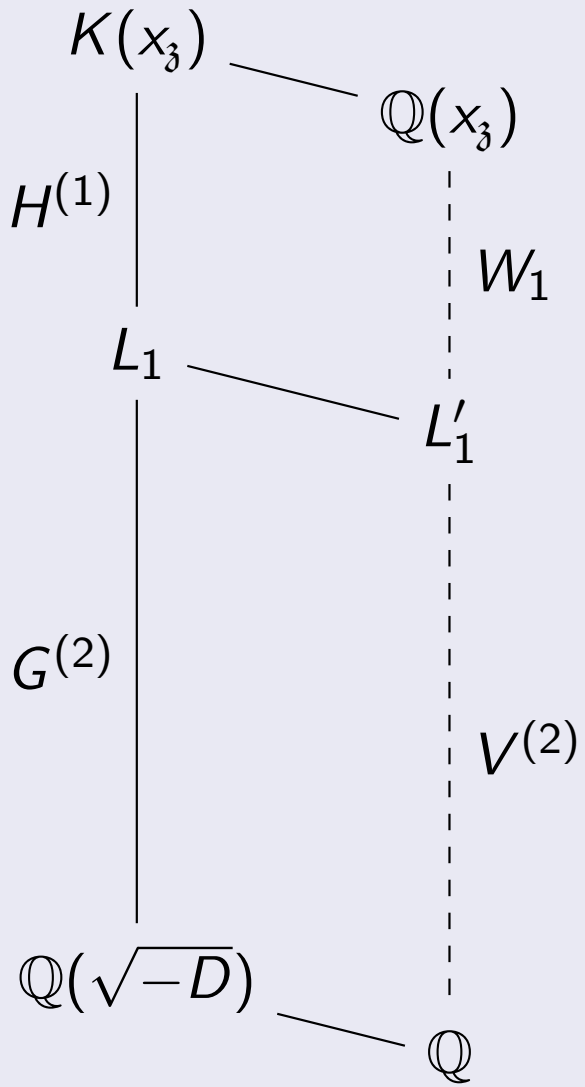
Example

$$G^{(1)} := \langle \mathfrak{k} \rangle$$
$$H^{(1)} := \langle \mathfrak{k}^6 \rangle$$
$$V^{(1)} := \mathscr{W}_{335}$$



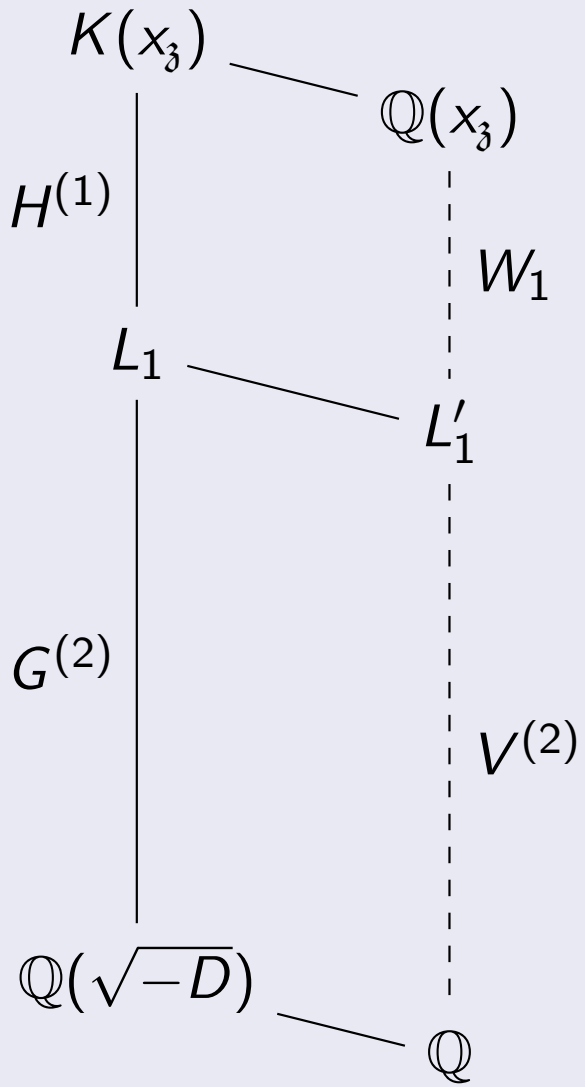
Example

$$G^{(2)} := \langle \mathfrak{t} \rangle / \langle \mathfrak{t}^6 \rangle$$
$$H^{(1)} := \langle \mathfrak{t}^6 \rangle$$
$$W_1 :\approx X^3 - 6.9X^2 - 5.7X - 5.1$$
$$V^{(2)} := Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1$$



Example

$$G^{(2)} := \langle \mathfrak{t} \rangle / \langle \mathfrak{t}^6 \rangle$$
$$H^{(1)} := \langle \mathfrak{t}^6 \rangle$$
$$W_1 :\approx X^3 - 6.9X^2 - 5.7X - 5.1$$
$$V^{(2)} := Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1$$



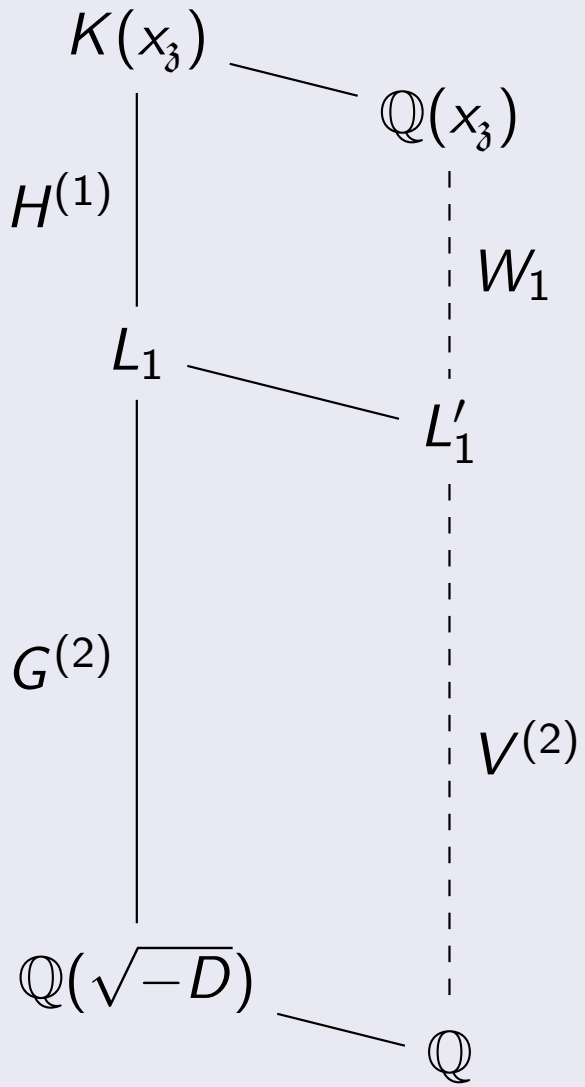
Example

$$G^{(2)} := \langle \mathfrak{t} \rangle / \langle \mathfrak{t}^6 \rangle$$

$$H^{(1)} := \langle \mathfrak{t}^6 \rangle$$

$$W_1 :\approx X^3 - 6.9X^2 - 5.7X - 5.1$$

$$V^{(2)} := Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1$$



Problem

Coefficients of W are floating point numbers. We want to express them symbolically.

Lemma (Hecke representation)

Let $L = K(\alpha)$ and $V \in K[Y]$ a minimal polynomial for α. We can write any $\vartheta \in L$ as

$$\vartheta = \frac{g_\vartheta(\alpha)}{V'(\alpha)}$$

with

$$g_\vartheta(Y) = \sum_{i=0}^{n-1} \vartheta_i \frac{V(Y)}{Y - \alpha_i} \in K[Y].$$

We can solve the following Hecke representations for the coefficients of

$$W_1 \approx X^3 - 6.938X^2 - 5.742X - 5.124.$$

We have

$$\begin{aligned} V^{(2)'}(Y) &= 6Y^5 + 20Y^4 - 76Y^3 + 24Y^2 - 22Y - 1 \\ g_{1,2}(Y) &= -4Y^5 + 38Y^4 - 24Y^3 + 44Y^2 + 5Y + 6 \\ g_{1,1}(Y) &= -Y^5 + 43Y^4 - 52Y^3 + 26Y^2 - 21Y - 7 \\ g_{1,0}(Y) &= -4Y^5 + 23Y^4 - 9Y^3 - 11Y^2 + 10Y - 4 \end{aligned}$$

Hence

$$-6.938 \leftrightarrow \frac{g_{1,2}(Y)}{V^{(2)'}(Y)} \qquad -5.742 \leftrightarrow \frac{g_{1,1}(Y)}{V^{(2)'}(Y)} \qquad -5.124 \leftrightarrow \frac{g_{1,0}(Y)}{V^{(2)'}(Y)}$$

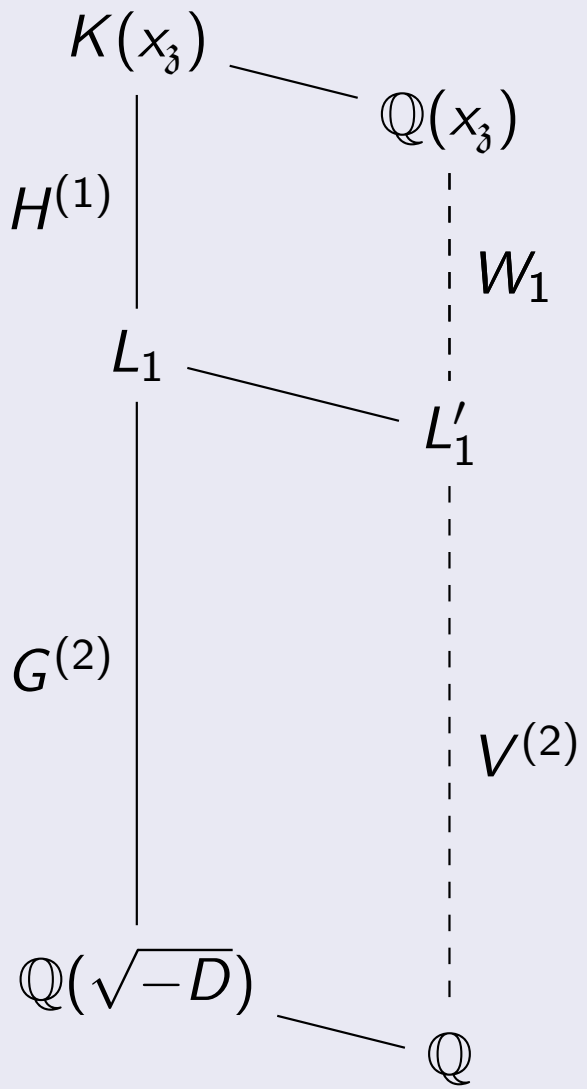
Example

$$W_1 := X^3 + \frac{1}{V^{(2)\prime}(Y)} \sum_{j=0}^{2} g_{1,j}(Y) X^j$$

$$G^{(2)} := \langle \mathfrak{k} \rangle / \langle \mathfrak{k}^6 \rangle$$

$$H^{(2)} := \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

$$V^{(2)} := Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1$$



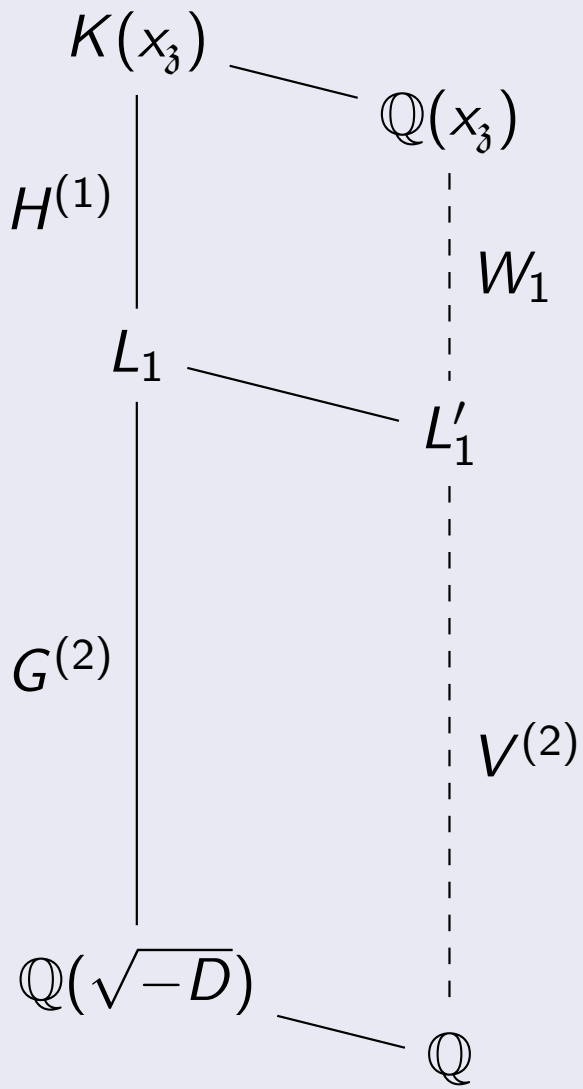
Example

$$W_1 := X^3 + \frac{1}{V^{(2)\prime}(Y)} \sum_{j=0}^{2} g_{1,j}(Y) X^j$$

$G^{(2)} := \langle \mathfrak{k} \rangle / \langle \mathfrak{k}^6 \rangle$

$H^{(2)} := \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$

$V^{(2)} := Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1$

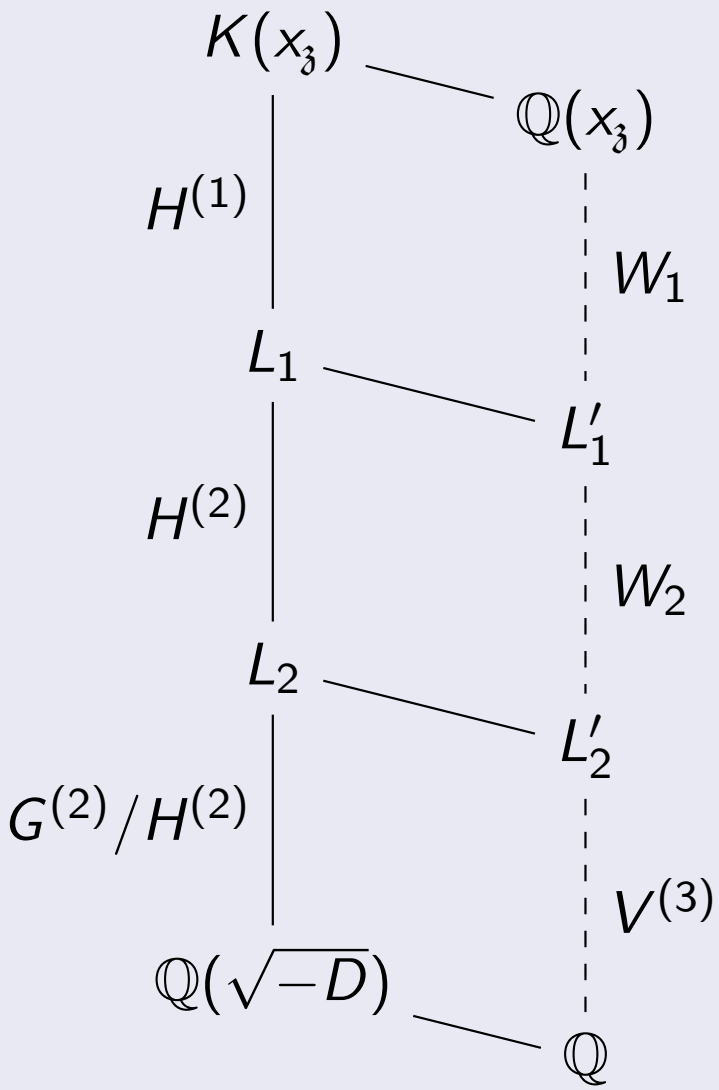


Example

$$W_1 := X^3 + \frac{1}{V^{(2)\prime}(Y)} \sum_{j=0}^{2} g_{1,j}(Y) X^j$$

$$W_2 := Y^3 + \frac{1}{V^{(3)\prime}(Z)} \sum_{j=0}^{2} g_{2,j}(Z) Y^j$$

$$V^{(3)} := Z^2 - 4Z - 16$$

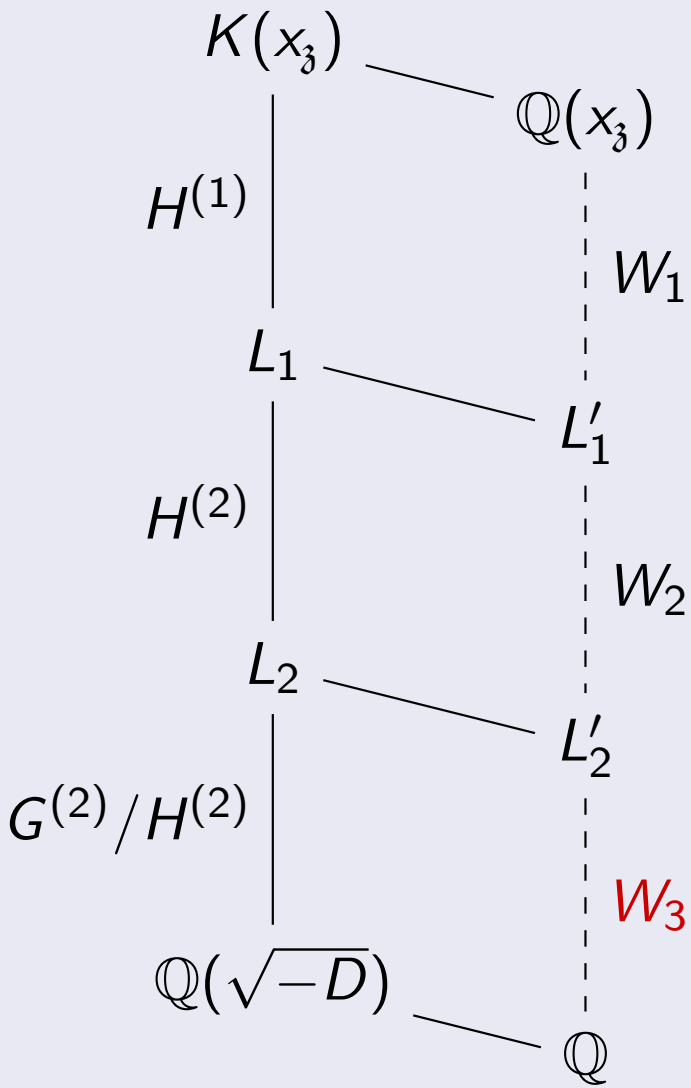


Example

$$W_1 := X^3 + \frac{1}{V^{(2)\prime}(Y)} \sum_{j=0}^{2} g_{1,j}(Y) X^j$$

$$W_2 := Y^3 + \frac{1}{V^{(3)\prime}(Z)} \sum_{j=0}^{2} g_{2,j}(Z) Y^j$$

$$W_3 := Z^2 - 4Z - 16$$



Problem

How do we know which roots correspond to the same coset?

Problem

How do we know which roots correspond to the same coset?

We want an ordering of the roots

$$x_0, \ldots, x_{mn-1}$$

such that

- Each block of m roots will correspond to the elements of one of the cosets gH of G/H.
- The first block of m (i.e. $x_0, \ldots, x_{m-1}$) correspond to the elements of H.

Problem

How do we know which roots correspond to the same coset?

We want an ordering of the roots

$$x_0, \ldots, x_{mn-1}$$

such that

- Each block of m roots will correspond to the elements of one of the cosets gH of G/H.
- The first block of m (i.e. $x_0, \ldots, x_{m-1}$) correspond to the elements of H.

This way, we can set

$$U_i(X) := \prod_{j=0}^{m-1} (X - x_{im+j}).$$

For the next iteration, we have a new set of roots

$$\vartheta_0, \ldots, \vartheta_{m-1}.$$

We want the first $m^{(2)} = |H^{(2)}|$ elements of this to be from $H^{(2)}$. And so on until the last iteration.

For the next iteration, we have a new set of roots

$$\vartheta_0, \ldots, \vartheta_{m-1}.$$

We want the first $m^{(2)} = |H^{(2)}|$ elements of this to be from $H^{(2)}$. And so on until the last iteration.

Definition

A normal series of a group G is a sequence of normal subgroups of G such that

$$H_0 := 1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_t := G.$$

Moreover, each H_i/H_{i-1} is called a factor group.

For the next iteration, we have a new set of roots

$$\vartheta_0, \ldots, \vartheta_{m-1}.$$

We want the first $m^{(2)} = |H^{(2)}|$ elements of this to be from $H^{(2)}$. And so on until the last iteration.

Definition

A normal series of a group G is a sequence of normal subgroups of G such that

$$H_0 := 1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_t := G.$$

Moreover, each H_i/H_{i-1} is called a factor group.

Set

$$H^{(\iota)} = \frac{H_\iota}{H_{\iota-1}}$$

For the next iteration, we have a new set of roots

$$\vartheta_0, \ldots, \vartheta_{m-1}.$$

We want the first $m^{(2)} = |H^{(2)}|$ elements of this to be from $H^{(2)}$. And so on until the last iteration.

Definition

A normal series of a group G is a sequence of normal subgroups of G such that

$$H_0 := 1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_t := G.$$

Moreover, each H_i/H_{i-1} is called a factor group.

Set

$$H^{(\iota)} = \frac{H_\iota}{H_{\iota-1}} \lhd \frac{G}{H_{\iota-1}} \cong G^{(\iota)}.$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \lhd \langle \mathfrak{k}^6 \rangle \lhd \langle \mathfrak{k}^2 \rangle \lhd G.$$

Start with the element of H_0.

$$\mathfrak{k}^0.$$

List the coset representatives of $H^{(1)} = H_1/H_0$.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}.$$

Multiply them to the current list in that order.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}.$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \triangleleft \langle \mathfrak{k}^6 \rangle \triangleleft \langle \mathfrak{k}^2 \rangle \triangleleft G.$$

We continue from the previous list

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}.$$

List the coset representatives of $H^{(2)} = H_2/H_1$.

$$\mathfrak{k}^0, \mathfrak{k}^2, \mathfrak{k}^4.$$

Multiply them to the current list in that order.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}.$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \triangleleft \langle \mathfrak{k}^6 \rangle \triangleleft \langle \mathfrak{k}^2 \rangle \triangleleft G.$$

We continue from the previous list

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}$$

List the coset representatives of $H^{(3)} = H_3/H_2$.

$$\mathfrak{k}^0, \mathfrak{k}^1$$

Multiply them to the current list in that order.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}, \mathfrak{k}^1, \mathfrak{k}^7, \mathfrak{k}^{13}, \mathfrak{k}^3, \mathfrak{k}^9, \mathfrak{k}^{15}, \mathfrak{k}^5, \mathfrak{k}^{11}, \mathfrak{k}^{17}$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \lhd \langle \mathfrak{k}^6 \rangle \lhd \langle \mathfrak{k}^2 \rangle \lhd G.$$

Finally, we have the final list.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}, \mathfrak{k}^1, \mathfrak{k}^7, \mathfrak{k}^{13}, \mathfrak{k}^3, \mathfrak{k}^9, \mathfrak{k}^{15}, \mathfrak{k}^5, \mathfrak{k}^{11}, \mathfrak{k}^{17}$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \triangleleft \langle \mathfrak{k}^6 \rangle \triangleleft \langle \mathfrak{k}^2 \rangle \triangleleft G.$$

Finally, we have the final list.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}, \mathfrak{k}^1, \mathfrak{k}^7, \mathfrak{k}^{13}, \mathfrak{k}^3, \mathfrak{k}^9, \mathfrak{k}^{15}, \mathfrak{k}^5, \mathfrak{k}^{11}, \mathfrak{k}^{17}$$

Take the corresponding $x_{\mathfrak{k}}$. (Write $x_i = x_{\mathfrak{k}^i}$.)

$$x_0, x_6, x_{12}, x_2, x_8, x_{14}, x_4, x_{10}, x_{16}, x_1, x_7, x_{13}, x_3, x_9, x_{15}, x_5, x_{11}, x_{17}$$

In our example, we had

$$H^{(1)} = \langle \mathfrak{k}^6 \rangle \quad \text{and} \quad H^{(2)} = \langle \mathfrak{k}^2 \rangle / \langle \mathfrak{k}^6 \rangle$$

In our example, we (implicitly) had

$$1 \triangleleft \langle \mathfrak{k}^6 \rangle \triangleleft \langle \mathfrak{k}^2 \rangle \triangleleft G.$$

Finally, we have the final list.

$$\mathfrak{k}^0, \mathfrak{k}^6, \mathfrak{k}^{12}, \mathfrak{k}^2, \mathfrak{k}^8, \mathfrak{k}^{14}, \mathfrak{k}^4, \mathfrak{k}^{10}, \mathfrak{k}^{16}, \mathfrak{k}^1, \mathfrak{k}^7, \mathfrak{k}^{13}, \mathfrak{k}^3, \mathfrak{k}^9, \mathfrak{k}^{15}, \mathfrak{k}^5, \mathfrak{k}^{11}, \mathfrak{k}^{17}$$

Take the corresponding $x_{\mathfrak{k}}$. (Write $x_i = x_{\mathfrak{k}^i}$.)

$$\underbrace{x_0, x_6, x_{12}, x_2, x_8, x_{14}, x_4, x_{10}, x_{16}, x_1, x_7, x_{13}, x_3, x_9, x_{15}, x_5, x_{11}, x_{17}}_{\mathcal{R}_V}$$

Using PARI, we have this list of roots $\mathcal{R}_V$.

x_0	7.8	x_1	$-0.27 + 1.5i$
x_6	$-0.41 + 0.70i$	x_7	$-0.26 - 0.48i$
x_{12}	$-0.41 - 0.70i$	x_{13}	$0.62 - 0.78i$
x_2	$-0.052 + 0.92i$	x_3	$-0.75 - 0.41i$
x_8	$-0.78 + 0.27i$	x_9	-1.1
x_{14}	$0.60 - 0.44i$	x_{15}	$-0.75 + 0.41i$
x_4	$0.60 + 0.44i$	x_5	$0.62 + 0.78i$
x_{10}	$-0.78 - 0.27i$	x_{11}	$-0.26 + 0.48i$
x_{16}	$-0.052 - 0.92i$	x_{17}	$-0.27 - 1.5i$

Each partition represents the roots of one of the U^g.

Using PARI, we have this list of roots $\mathcal{R}_V$.

x_0	7.8	x_1	$-0.27 + 1.5i$
x_6	$-0.41 + 0.70i$	x_7	$-0.26 - 0.48i$
x_{12}	$-0.41 - 0.70i$	x_{13}	$0.62 - 0.78i$
x_2	$-0.052 + 0.92i$	x_3	$-0.75 - 0.41i$
x_8	$-0.78 + 0.27i$	x_9	-1.1
x_{14}	$0.60 - 0.44i$	x_{15}	$-0.75 + 0.41i$
x_4	$0.60 + 0.44i$	x_5	$0.62 + 0.78i$
x_{10}	$-0.78 - 0.27i$	x_{11}	$-0.26 + 0.48i$
x_{16}	$-0.052 - 0.92i$	x_{17}	$-0.27 - 1.5i$

Each partition represents the roots of one of the U^g.
In particular,

$$U_0 = (x - x_0)(X - x_1)(X - x_2) = X^3 - 6.9X^2 - 5.7X - 5.1$$

Algorithm

INPUT:

- *An ordered list $\mathcal{L}$ of the elements of the group $G = \mathrm{Gal}(M/K)$, using the normal series*

$$\langle e \rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_{t-1} \lhd H_t = G.$$

of G. Note that $|G| = d$.

- *An ordered list $\mathcal{R}_V = (x_0, \ldots, x_{d-1})$ of the roots of V obtained from taking the corresponding roots of $\mathcal{L}$.*

Algorithm

OUTPUT:

- *A list of intermediate fields L'_{i-1}/L'_i for $i = 1, \ldots, t$ (where $M_0 = L'_0$ and $K_0 = L'_t$) and their respective irreducible polynomials $W_i \in L'_i[X]$.*

Algorithm

ALGORITHM

For each $\iota = 1, 2, \ldots, t-1$, do the following:

1. *Compute the U_i's for this iteration.*
2. *Find $V^{(\iota+1)}$ by taking different V_k's and see if they're irreducible.*
3. *Express the coefficients of $W = U_0$ as their Hecke representations.*

Problem

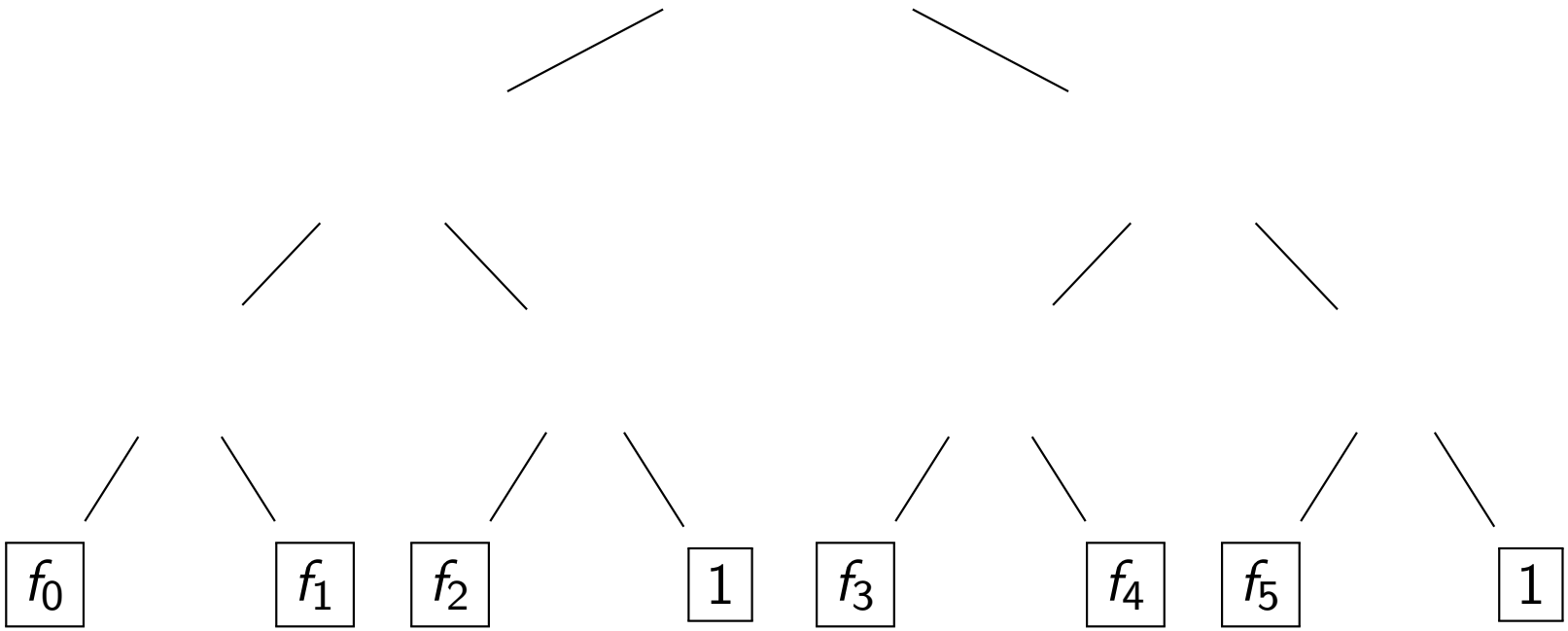
How to multiply polynomials quickly?

Problem

How to multiply polynomials quickly?

$$f_0 = Y - (-0.23 - 0.75i) \qquad f_3 = Y - (-0.23 - 0.75i)$$
$$f_1 = Y - (-0.23 + 0.75i) \qquad f_4 = Y - (-0.23 + 0.75i)$$
$$f_2 = Y - 6.9 \qquad f_5 = Y - 2.6$$

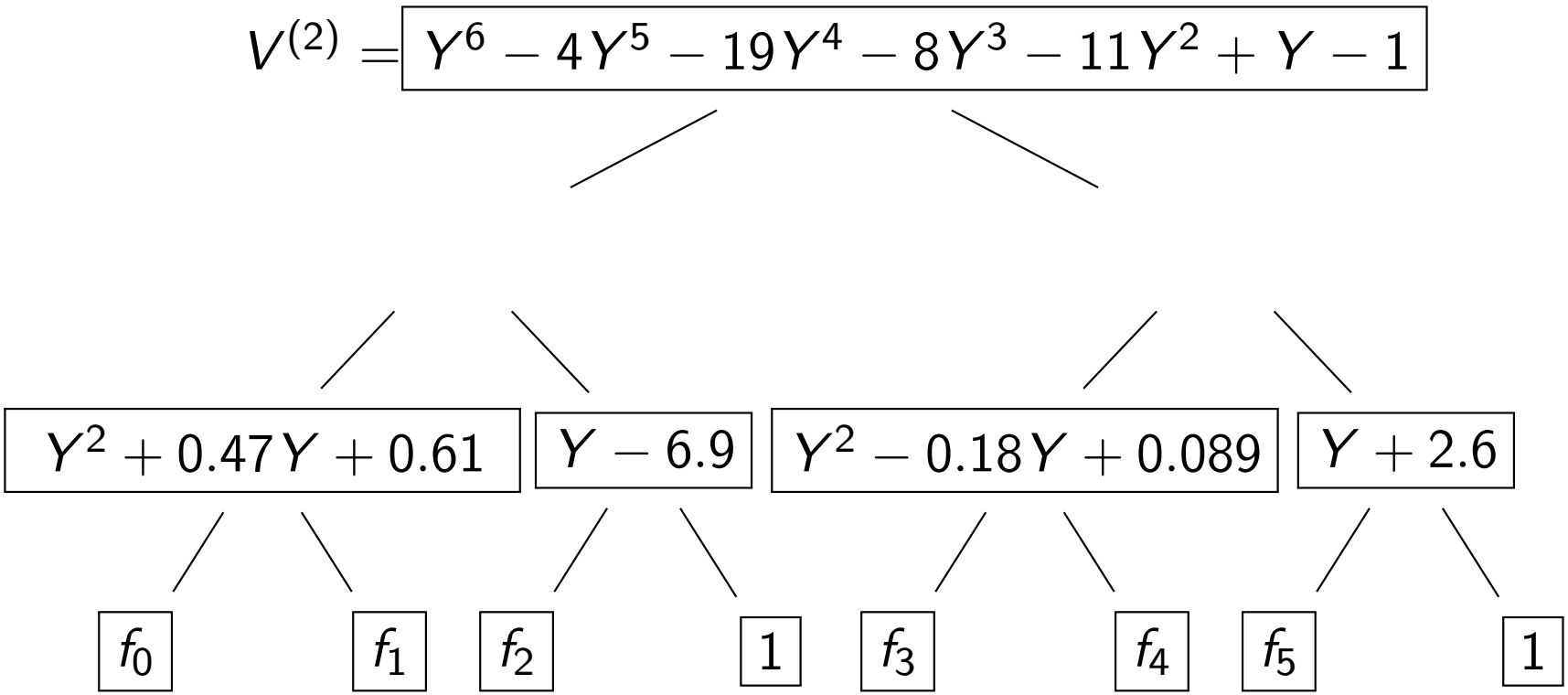
$$V^{(2)} = \boxed{Y^6 - 4Y^5 - 19Y^4 - 8Y^3 - 11Y^2 + Y - 1}$$



Problem

How to multiply polynomials quickly?

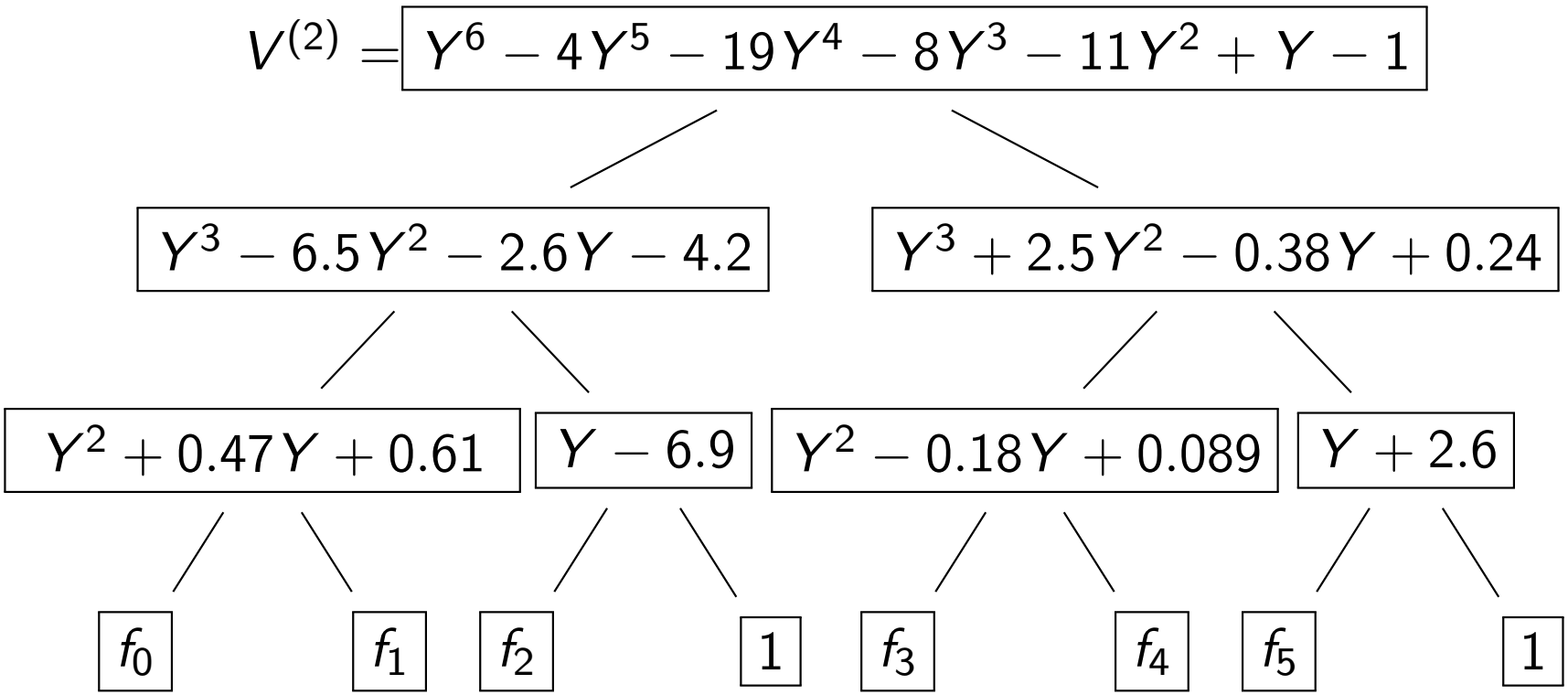
$$f_0 = Y - (-0.23 - 0.75i) \qquad f_3 = Y - (-0.23 - 0.75i)$$
$$f_1 = Y - (-0.23 + 0.75i) \qquad f_4 = Y - (-0.23 + 0.75i)$$
$$f_2 = Y - 6.9 \qquad f_5 = Y - 2.6$$



Problem

How to multiply polynomials quickly?

$$f_0 = Y - (-0.23 - 0.75i) \qquad f_3 = Y - (-0.23 - 0.75i)$$
$$f_1 = Y - (-0.23 + 0.75i) \qquad f_4 = Y - (-0.23 + 0.75i)$$
$$f_2 = Y - 6.9 \qquad f_5 = Y - 2.6$$



Let $M_X(n)$ be the number of multiplications in $\mathbb{C}$ required to multiply two polynomials with at most n coefficients in $\mathbb{C}[X]$. We assume that

$$M_X(n) + M_X(m) \leq M_X(n+m).$$

Let $M_X(n)$ be the number of multiplications in $\mathbb{C}$ required to multiply two polynomials with at most n coefficients in $\mathbb{C}[X]$. We assume that

$$M_X(n) + M_X(m) \leq M_X(n+m).$$

Theorem

Computing a subproduct tree which has s leaves takes at most

$$O(M_X(s) \log s)$$

multiplications in $\mathbb{C}$.

Let $M_X(n)$ be the number of multiplications in $\mathbb{C}$ required to multiply two polynomials with at most n coefficients in $\mathbb{C}[X]$. We assume that

$$M_X(n) + M_X(m) \leq M_X(n+m).$$

Theorem

Computing a subproduct tree which has s leaves takes at most

$$O(M_X(s)\log s)$$

multiplications in $\mathbb{C}$.

Let $f(s)$ be the time it takes to compute a subproduct tree with s leaves. Then

$$f(s) = 2f(s/2) + M_X(s/2).$$

Moreover, $f(1) = 0$. We have

$$f(s) = \sum_{i=1}^{k} 2^i M_X(s/2) \leq \sum_{i=1}^{k} M_X(s) = kM_X(s) = O(M_X(s)\log s).$$

Algorithm

ALGORITHM

For each $\iota = 1, 2, \ldots, t-1$, *do the following:*

1. *Compute the* U_i*'s for this iteration.*
2. *Find* $V^{(\iota+1)}$ *by taking different* V_k*'s and see if they're irreducible.*
3. *Express the coefficients of* $W = U_0$ *as their Hecke representations.*

Corollary

Computing all of the U_i for one iteration takes at most

$$O(nM_X(m)\log m)$$

operations in $\mathbb{C}$.

We create a subproduct tree for each U_i.

Corollary

Computing V for one iteration takes at most

$$O(mM_X(n)\log n)$$

operations in $\mathbb{C}$.

We create a subproduct tree for each V_k and check if it is irreducible.

Algorithm

ALGORITHM

For each $\iota = 1, 2, \ldots, t-1$, do the following:

1. *Compute the U_i's for this iteration.*
2. *Find $V^{(\iota+1)}$ by taking different V_k's and see if they're irreducible.*
3. *Express the coefficients of $W = U_0$ as their Hecke representations.*

Theorem

Computing the Hecke representation of the coefficients of U_0 takes

$$O(mM_X(n)\log n)$$

operations in $\mathbb{C}$.

Theorem

One iteration of the main algorithm takes at most

$$O(mM_X(n)\log n + nM_X(m)\log m)$$

operations in $\mathbb{C}$.

Theorem

One iteration of the main algorithm takes at most

$$O(mM_X(n)\log n + nM_X(m)\log m)$$

operations in $\mathbb{C}$.

Since we are working in $\mathbb{C}$, we can use the Fast Fourier transform where $M_X(n) = n\log n$. Under this model, we find that the main algorithm takes at most

$$O\left(mn(\log^2 m + \log^2 n)\right)$$

operations in $\mathbb{C}$.

Corollary

Let $K = \mathbb{Q}(\sqrt{-D})$ *and* $M = H_K$. *Note that the*

$$|G| = |\mathrm{Gal}(M/K)| = |\mathrm{Cl}(\mathcal{O}_K)| = h$$

where h *is the class number. Then the main algorithm requires at most*

$$O(h \log^3 h)$$

operations in $\mathbb{C}$.

Corollary

Let $K = \mathbb{Q}(\sqrt{-D})$ *and* $M = H_K$. *Note that the*

$$|G| = |\mathrm{Gal}(M/K)| = |\mathrm{Cl}(\mathcal{O}_K)| = h$$

where h *is the class number. Then the main algorithm requires at most*

$$O(h \log^3 h)$$

operations in $\mathbb{C}$.

Assuming h is not prime, the larger integer between m and n is at most $h/2$. Hence $\log m = O(\log h)$ and $\log n = O(\log h)$. Thus,

$$O\left(mn(\log^2 m + \log^2 n)\right) = O(h \log^2 h).$$

Finally, we approximate t, the number of factors of h, to be $O(\log h)$. Note that $t - 1$ is the number of iterations we need. From there, we get the result.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Find a root x of the Weber polynomial $\mathscr{W}_D$.

$\Downarrow$

Find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial of $\mathbb{Q}(\sqrt{-D})$.

$\Downarrow$

Construct an elliptic curve E over $\mathbb{F}_p$ with N points where N is in terms of p and D.

$\Downarrow$

Certify primality of p using the Atkin-Morain ECPP algorithm.

We discuss the solution given in Enge (2003) more thoroughly.

Algorithm (CM algorithm)

1. *Compute the Hilbert class polynomial* $h_K \in \mathbb{Z}[X]$ *for the field* $K = \mathbb{Q}(\sqrt{-D})$ *where* $-4D = (p+1-N)^2 - 4p$.
2. *Compute a root* $j \in \mathbb{F}_p$ *of* h_K, *viewed as a polynomial over* $\mathbb{F}_p$.
3. *Let*

$$E = \begin{cases} Y^2 = X^3 + aX - a & \text{for } j \neq 0, 1728 \\ Y^2 = X^3 + 1 & \text{for } j = 0 \\ Y^2 = X^3 + X & \text{for } j = 1728 \end{cases}$$

   where $a = \frac{27j}{4(1728-j))}$.
4. *If* $|E(\mathbb{F}_p)| = N$, *return* E. *Otherwise, return its quadratic twist.*

Suppose we want to find an elliptic curve over the finite field $\mathbb{F}_p$ with N points where $p = 479$ and $N = 456$. Note that

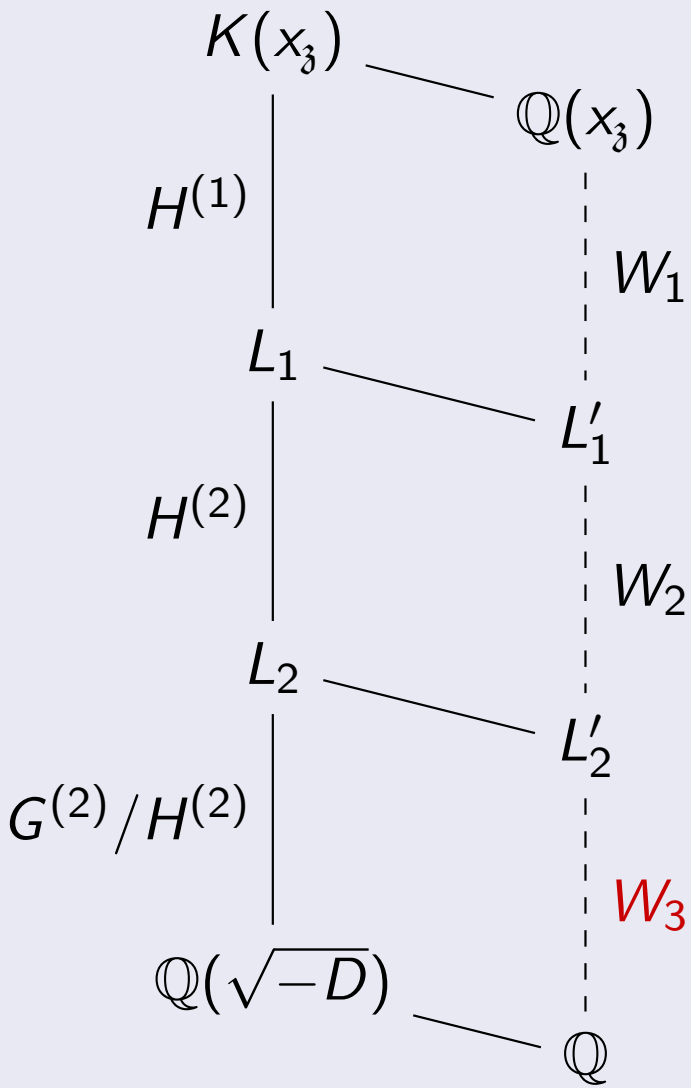
$$(p+1-N)^2 - 4p = (479+1-456)^2 - 4(479) = -1340 = -4 \cdot 335.$$

Example

$$W_1 := X^3 + \frac{1}{V^{(2)\prime}(Y)} \sum_{j=0}^{2} g_{1,j}(Y) X^j$$

$$W_2 := Y^3 + \frac{1}{V^{(3)\prime}(Z)} \sum_{j=0}^{2} g_{2,j}(Z) Y^j$$

$$W_3 := Z^2 - 4Z - 16$$



We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_2(Y) = Y^3 + \frac{4Z + 32}{2Z - 4}Y^2 - \frac{3Z + 4}{2Z - 4}Y + \frac{4Z + 12}{2Z - 4}$$

$$W_1(X) = X^3 + \frac{g_{1,2}(Y)}{V^{(2)\prime}(Y)}X^2 + \frac{g_{1,1}(Y)}{V^{(2)\prime}(Y)}X + \frac{g_{1,0}(Y)}{V^{(2)\prime}(Y)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4Z+32}{2Z-4}Y^2 - \frac{3Z+4}{2Z-4}Y + \frac{4Z+12}{2Z-4}$$

$$W_1(X) = X^3 + \frac{g_{1,2}(Y)}{V^{(2)\prime}(Y)}X^2 + \frac{g_{1,1}(Y)}{V^{(2)\prime}(Y)}X + \frac{g_{1,0}(Y)}{V^{(2)\prime}(Y)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_1(X) = X^3 + \frac{g_{1,2}(Y)}{V^{(2)\prime}(Y)}X^2 + \frac{g_{1,1}(Y)}{V^{(2)\prime}(Y)}X + \frac{g_{1,0}(Y)}{V^{(2)\prime}(Y)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$

$$W_1(X) = X^3 + \frac{g_{1,2}(Y)}{V^{(2)\prime}(Y)}X^2 + \frac{g_{1,1}(Y)}{V^{(2)\prime}(Y)}X + \frac{g_{1,0}(Y)}{V^{(2)\prime}(Y)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$

$$W_2(332) = (332)^3 + 46(332)^2 + 227(332) + 24 = 0$$

$$W_1(X) = X^3 + \frac{g_{1,2}(Y)}{V^{(2)\prime}(Y)}X^2 + \frac{g_{1,1}(Y)}{V^{(2)\prime}(Y)}X + \frac{g_{1,0}(Y)}{V^{(2)\prime}(Y)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$

$$W_2(332) = (332)^3 + 46(332)^2 + 227(332) + 24 = 0$$

$$W_1(X) = X^3 + \frac{g_{1,2}(332)}{V^{(2)\prime}(332)}X^2 + \frac{g_{1,1}(332)}{V^{(2)\prime}(332)}X + \frac{g_{1,0}(332)}{V^{(2)\prime}(332)}$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$

$$W_2(332) = (332)^3 + 46(332)^2 + 227(332) + 24 = 0$$

$$W_1(X) = X^3 + \frac{g_{1,2}(332)}{V^{(2)\prime}(332)}X^2 + \frac{g_{1,1}(332)}{V^{(2)\prime}(332)}X + \frac{g_{1,0}(332)}{V^{(2)\prime}(332)}$$

$$W_1(X) = X^3 + 332X^2 + 184X + 434$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$

$$W_3(46) = 46^2 - 4(46) - 16 = 0$$

$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$

$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$

$$W_2(332) = (332)^3 + 46(332)^2 + 227(332) + 24 = 0$$

$$W_1(X) = X^3 + \frac{g_{1,2}(332)}{V^{(2)\prime}(332)}X^2 + \frac{g_{1,1}(332)}{V^{(2)\prime}(332)}X + \frac{g_{1,0}(332)}{V^{(2)\prime}(332)}$$

$$W_1(X) = X^3 + 332X^2 + 184X + 434$$

$$W_1(81) = (81)^3 + 332(81)^2 + 184(81) + 434 = 0$$

We compute in $\mathbb{F}_p$ with $p = 479$.

$$W_3(Z) = Z^2 - 4Z - 16$$
$$W_3(46) = 46^2 - 4(46) - 16 = 0$$
$$W_2(Y) = Y^3 + \frac{4(46)+32}{2(46)-4}Y^2 - \frac{3(46)+4}{2(46)-4}Y + \frac{4(46)+12}{2(46)-4}$$
$$W_2(Y) = Y^3 + 46Y^2 + 227Y + 24$$
$$W_2(332) = (332)^3 + 46(332)^2 + 227(332) + 24 = 0$$
$$W_1(X) = X^3 + \frac{g_{1,2}(332)}{V^{(2)\prime}(332)}X^2 + \frac{g_{1,1}(332)}{V^{(2)\prime}(332)}X + \frac{g_{1,0}(332)}{V^{(2)\prime}(332)}$$
$$W_1(X) = X^3 + 332X^2 + 184X + 434$$
$$W_1(81) = (81)^3 + 332(81)^2 + 184(81) + 434 = 0$$

Note that for $x = 81$, we have $\mathscr{W}_{335}(x) = 0$ as a polymomial in $\mathbb{F}_p$, with $p = 479$.

We convert this into a root of the Hilbert class polynomial h_K by the formula [Konstantinou]:

$$j = \frac{(x^{-24} - 16)^3}{x^{-24}} = 117.$$

Finally, we take

$$a = \frac{27(j)}{4(1728 - j)} = 417.$$

And so we take the elliptic curve

$$Y^2 = X^3 + 417X + 62$$

and this curve has $N = 456$ points.

Problem

Given a finite abelian extension M/K generated by the polynomial h, find an intermediate field L and the respective polynomials W and V, for M/L and L/K.

Motivation

Find a root x of the Weber polynomial $\mathscr{W}_D$.

$\Downarrow$

Find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial of $\mathbb{Q}(\sqrt{-D})$.

$\Downarrow$

Construct an elliptic curve E over $\mathbb{F}_p$ with N points where N is in terms of p and D.

$\Downarrow$

Certify primality of p using the Atkin-Morain ECPP algorithm.

Numerical experiments.

Made an implementation to decompose towers for $D \equiv 7 \pmod 8$, $D \not\equiv 0 \pmod 3$ and $D < 1000000$.

Numerical experiments.

Made an implementation to decompose towers for $D \equiv 7 \pmod 8$, $D \not\equiv 0 \pmod 3$ and $D < 1000000$.

- 1 of them has class number 1.
- 5256 of them have prime class number.
- 70745 of them have class number with at least two prime factors.

Numerical experiments.

Made an implementation to decompose towers for $D \equiv 7 \pmod 8$, $D \not\equiv 0 \pmod 3$ and $D < 1000000$.

- 1 of them has class number 1.
- 5256 of them have prime class number.
- 70745 of them have class number with at least two prime factors.

Took the precision $\eta = \frac{1}{9} h_D \log D$.

- Slowest was $D = 947231$ with $h_D = 883 \times 2$, which took 5.382 seconds.
- Slowest "smooth" class number was $D = 905339$ with $h_D = 1536 = 2^9 \times 3$, which took 2.087 seconds.

Numerical experiments.

Made an implementation to decompose towers for $D \equiv 7 \pmod 8$, $D \not\equiv 0 \pmod 3$ and $D < 1000000$.

- 1 of them has class number 1.
- 5256 of them have prime class number.
- 70745 of them have class number with at least two prime factors.

Took the precision $\eta = \frac{1}{9} h_D \log D$.

- Slowest was $D = 947231$ with $h_D = 883 \times 2$, which took 5.382 seconds.
- Slowest "smooth" class number was $D = 905339$ with $h_D = 1536 = 2^9 \times 3$, which took 2.087 seconds.

Only 5 instances where taking the trace does not result in an irreducible V.

Additional observations

- We should choose the normal series such that we get rid of the bigger factors first.

Additional observations

- We should choose the normal series such that we get rid of the bigger factors first.
- We do not actually need to compute the Weber polynomial.

Additional observations

- We should choose the normal series such that we get rid of the bigger factors first.
- We do not actually need to compute the Weber polynomial.
- We can lower the precision after each iteration since the coefficients will in general be of lower magnitude.

Tower decomposition of Hilbert class fields

Jared Guissmo E. Asuncion

July 20, 2017