Class Group Computations in Number Fields and Applications to Cryptography

Alexandre Gélin

Laboratoire d'Informatique de Paris 6
UPMC – Sorbonne Universités

25/04/2017

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q} \Rightarrow \exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} \simeq \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q} \Rightarrow \exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} \simeq \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals
- Group of units

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q} \Rightarrow \exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} \simeq \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals

  Quotient by principal ideals $\Rightarrow$ class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$

- Group of units

  Finitely generated $\Rightarrow$ fundamental units

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q} \Rightarrow \exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} \simeq \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals
  Quotient by principal ideals $\Rightarrow$ class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$
- Group of units
  Finitely generated $\Rightarrow$ fundamental units

Aim: Compute the structure of the class group.

Outline

Subexponential L-notation : $L_N(0,c) \approx (\log N)^c \quad L_N(1,c) \approx N^c$

$$L_N(\alpha, c) = \exp\left((c+o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right).$$

1969 Shanks: quadratic number fields in $O(|\Delta_{\mathbb{K}}|^{\frac{1}{5}})$.

1989 Hafner and McCurley: imaginary quadratic number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, \sqrt{2})$.

1990 Buchmann: all number fields with fixed degree in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, 1.7)$.

2014 Biasse and Fieker: all number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{2}{3}+\varepsilon)$ in general and $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2})$ if $n \leq \log(|\Delta_{\mathbb{K}}|)^{3/4-\varepsilon}$.

2014 Biasse and Fieker: number fields defined by a *good* polynomial in $L_{|\Delta_{\mathbb{K}}|}(a)$, $\frac{1}{3} \leq a < \frac{1}{2}$.

Index calculus

1. **Factor base**
   Fix a factor base composed of small elements.

2. **Relation collection**
   Collect some relations between those small elements, corresponding to linear equations.

3. **Linear algebra**
   Deduce the sought result performing linear algebra on the system built.

The factor base

$$\mathcal{B} = \{\text{prime ideals in } \mathcal{O}_{\mathbb{K}} \text{ of norm below } B\}$$

B determined so that $\mathcal{B}$ **generates the whole class group**.

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbb{K}} = \sqrt{|\Delta_{\mathbb{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

Bach's bound: assuming GRH, classes of ideals of norm less than $12(\log|\Delta_{\mathbb{K}}|)^2$ generate the class group.

The factor base

$$\mathcal{B} = \{\text{prime ideals in } \mathcal{O}_{\mathbb{K}} \text{ of norm below } B\}$$

B determined so that $\mathcal{B}$ **generates the whole class group**.

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbb{K}} = \sqrt{|\Delta_{\mathbb{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

Bach's bound: assuming GRH, classes of ideals of norm less than $12(\log|\Delta_{\mathbb{K}}|)^2$ generate the class group.

Practically

$$B = L_{|\Delta_{\mathbb{K}}|}(\beta, c_b).$$

Relation collection

$$\mathcal{B} = (\mathfrak{p}_1, \cdots, \mathfrak{p}_N)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\phi} & \mathcal{I} & \xrightarrow{\pi} & \mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \\ (e_1, \cdots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

$$\mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \simeq \mathbb{Z}^N / \left\{ (e_1, \cdots, e_N) \in \mathbb{Z}^N \mid \prod_i \mathfrak{p}_i^{e_i} = (\alpha)\mathcal{O}_{\mathbb{K}} \right\}$$

Relation collection

$$\mathcal{B} = (\mathfrak{p}_1, \cdots, \mathfrak{p}_N)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\phi} & \mathcal{I} & \xrightarrow{\pi} & \mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \\ (e_1, \cdots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

$$\mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \simeq \mathbb{Z}^N / \left\{ (e_1, \cdots, e_N) \in \mathbb{Z}^N \mid \prod_i \mathfrak{p}_i^{e_i} = (\alpha)\mathcal{O}_{\mathbb{K}} \right\}$$

Idea:

1. Pick at random $A = \prod_i \mathfrak{p}_i^{v_i}$.
2. Find a *reduced* ideal A' in the same class.
3. If A' splits on $\mathcal{B}$ ($\Leftrightarrow A' = \prod_i \mathfrak{p}_i^{v'_i}$) then

$$A(A')^{-1} = \prod_i \mathfrak{p}_i^{v_i - v'_i} \quad \text{is principal.}$$

Linear algebra

- Relations stored in a matrix of size about $N \times N$.
- Structure of the class group given by the *Smith Normal Form* of the matrix.
- First compute *Hermite Normal Form* with a premultiplier because we need kernel vectors.
- Storjohann and Labahn algorithm, runtime in $N^{\omega+1}$ ($2 \leq \omega \leq 3$ exponent of matrix multiplication)

Verification

We find a tentative class group H, but the class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.
$\Rightarrow$ Need an approximation of the class number $h_K = |\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Verification

We find a tentative class group H, but the class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.
$\Rightarrow$ Need an approximation of the class number $h_K = |\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Class number formula + Euler Product:

$$h_{\mathbb{K}}\mathrm{Reg}_{\mathbb{K}} = \mathrm{EP} \cdot \frac{w_{\mathbb{K}} \cdot \sqrt{|\Delta_{\mathbb{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}.$$

Verification

We find a tentative class group H, but the class group $\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.
$\Rightarrow$ Need an approximation of the class number $h_K = |\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Class number formula + Euler Product:

$$h_{\mathbb{K}}\mathsf{Reg}_{\mathbb{K}} = \mathsf{EP} \cdot \frac{w_{\mathbb{K}} \cdot \sqrt{|\Delta_{\mathbb{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}.$$

From the relations, we can also deduce a candidate for an approximation of Reg_K and perform the verification step.

Subexponential L-notation : $L_N(0,c) \approx (\log N)^c \quad L_N(1,c) \approx N^c$

$$L_N(\alpha, c) = \exp\left((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right).$$

1969 Shanks: quadratic number fields in $O(|\Delta_{\mathbb{K}}|^{\frac{1}{5}})$.

1989 Hafner and McCurley: imaginary quadratic number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, \sqrt{2})$.

1990 Buchmann: all number fields with fixed degree in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, 1.7)$.

2014 Biasse and Fieker: all number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{2}{3} + \varepsilon)$ in general and $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2})$ if $n \leq \log(|\Delta_{\mathbb{K}}|)^{3/4-\varepsilon}$.

2014 Biasse and Fieker: number fields defined by a *good* polynomial in $L_{|\Delta_{\mathbb{K}}|}(a)$, $\frac{1}{3} \leq a < \frac{1}{2}$.

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

Definition

Let $T = \sum a_k X^k \in \mathbb{Z}[X]$. The height of T is defined as the maximal norm of its coefficients, namely

$$H(T) = \max_k |a_k|.$$

Classes from Biasse and Fieker work

Definition

Let $n_0, d_0 > 0$ and $0 < \alpha < \frac{1}{2}$.

$$\mathcal{C}_{n_0,d_0,\alpha} = \left\{ \mathbb{K} = \mathbb{Q}[X]/(T) \middle| \begin{array}{l} \deg(T) = n_0(\log|\Delta_{\mathbb{K}}|)^{\alpha}(1+o(1)) \\ \log H(T) = d_0(\log|\Delta_{\mathbb{K}}|)^{1-\alpha}(1+o(1)) \end{array} \right\}$$

Theorem

If we know such a good polynomial, there exists an algorithm with runtime $L_{|\Delta_{\mathbb{K}}|}(a)$ for class group computation with

$$a = \max\left(\alpha, \frac{1-\alpha}{2}\right).$$

Our results [GJ16]

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathcal{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbb{K} = \frac{\mathbb{Q}[X]}{(T)} \middle| \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log |\Delta_{\mathbb{K}}|}{\log \log |\Delta_{\mathbb{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log |\Delta_{\mathbb{K}}|)^{\gamma} (\log \log |\Delta_{\mathbb{K}}|)^{1-\gamma} \end{array} \right\}$$

Our results [GJ16]

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathcal{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbb{K} = \frac{\mathbb{Q}[X]}{(T)} \middle| \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log |\Delta_{\mathbb{K}}|}{\log \log |\Delta_{\mathbb{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log |\Delta_{\mathbb{K}}|)^{\gamma} (\log \log |\Delta_{\mathbb{K}}|)^{1-\gamma} \end{array} \right\}$$

Proposition

If there exists a polynomial T such that $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal one in time $L_{|\Delta_{\mathbb{K}}|}(\alpha)$.

Our results [GJ16]

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathcal{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbb{K} = \frac{\mathbb{Q}[X]}{(T)} \middle| \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log |\Delta_{\mathbb{K}}|}{\log \log |\Delta_{\mathbb{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log |\Delta_{\mathbb{K}}|)^{\gamma} (\log \log |\Delta_{\mathbb{K}}|)^{1-\gamma} \end{array} \right\}$$

Proposition

If there exists a polynomial T such that $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal one in time $L_{|\Delta_{\mathbb{K}}|}(\alpha)$.

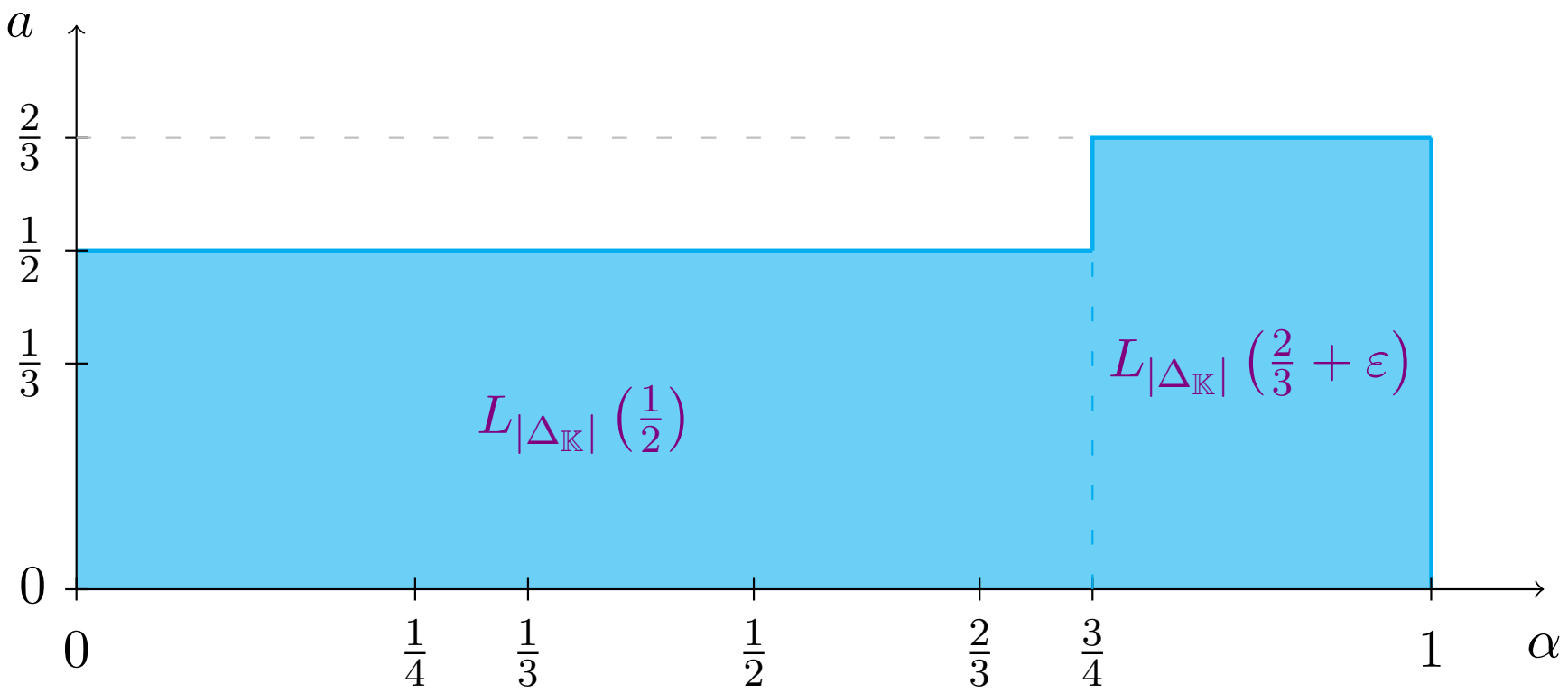
Theorem

Under GRH and smoothness heuristics, for every $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, $\alpha < \frac{1}{2}$, there exists an $L_{\Delta_{\mathbb{K}}}(a)$ algorithm for class group computation with

$$a = \max\left(\alpha, \frac{\gamma}{2}\right).$$

State of the art [BF14]

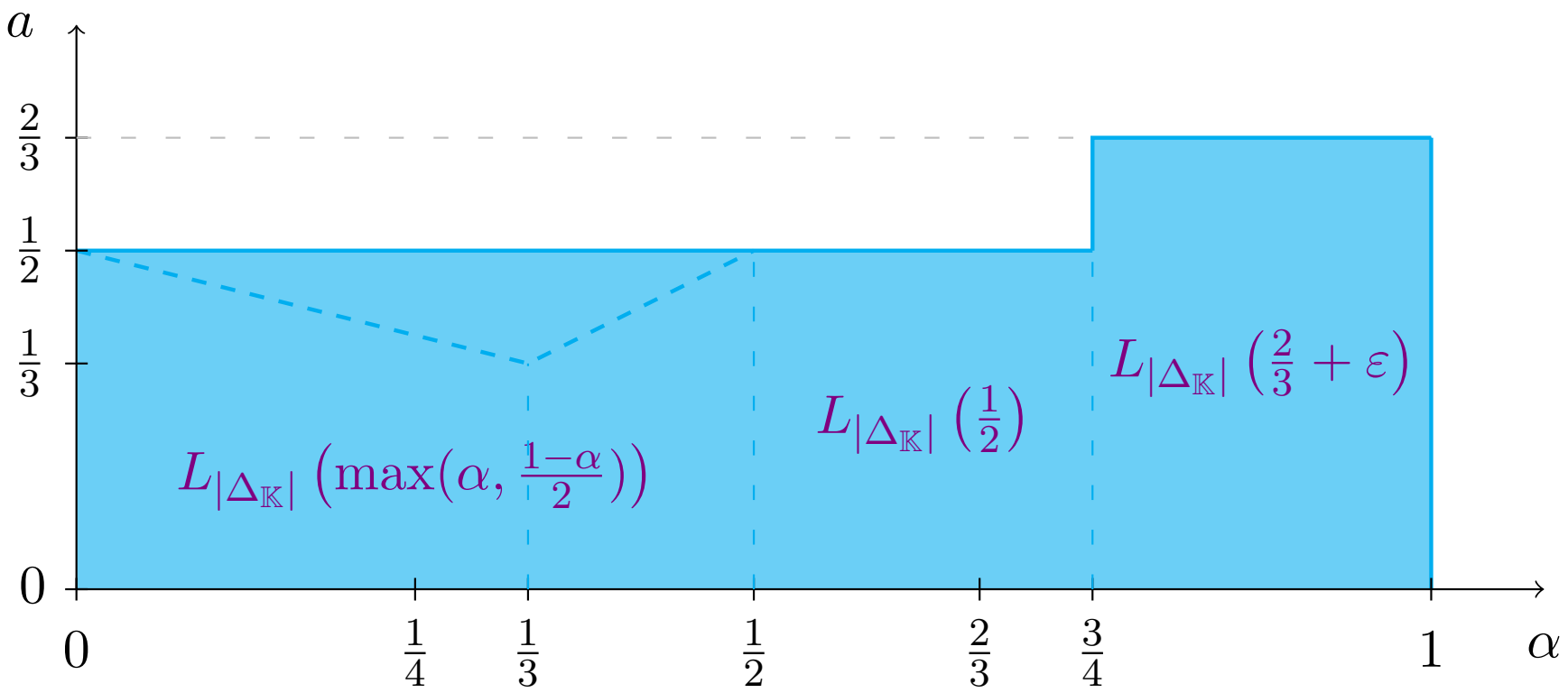
General case:



First general subexponential algorithm.

State of the art [BF14]

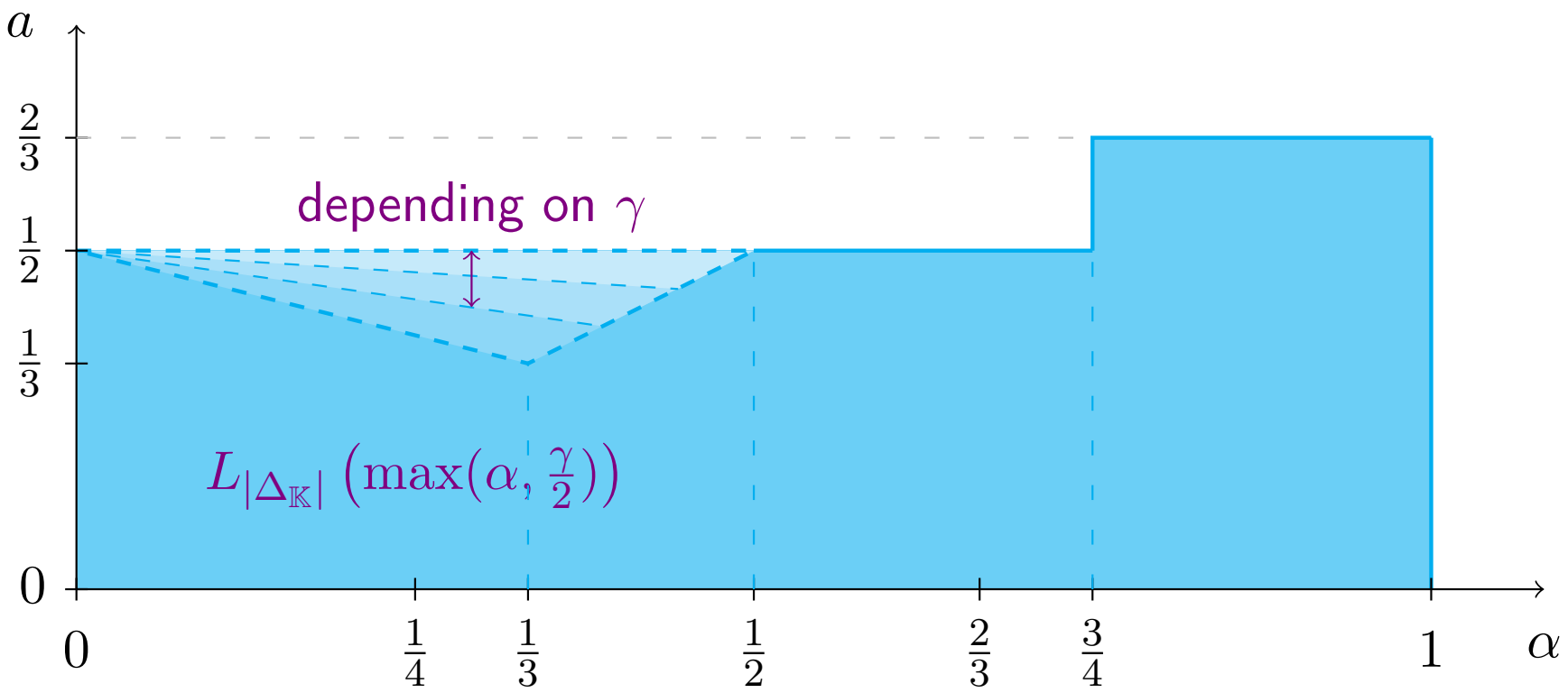
Special case:



Only if $\mathbb{K}$ is defined by T such that $H(T) = L_{|\Delta_{\mathbb{K}}|}(1-\alpha)$.

Our work [GJ16]

General case:



Without any condition.

Outline

The Principal Ideal Problem

Definition

The *Principal Ideal Problem* (PIP) consists in finding a generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbb{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g'} = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$.
  2. From $\boldsymbol{g'}$, find a short generator of the ideal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbb{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g'} = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$.
  2. From $\boldsymbol{g'}$, find a short generator of the ideal.

Campbell, Groves, and Sheperd (2014) found a solution the second point for power-of-two cyclotomic fields. Cramer, Ducas, Peikert, and Regev (2016) provided a proof and an extension to prime-power cyclotomic fields.

FHE scheme – Smart and Vercauteren PKC 2010

Key Generation:

1. Fix the security parameter $N = 2^n$.
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_{2N})$.
3. Set $G(X) = 1 + 2 \cdot S(X)$,
   for $S(X)$ of degree $N - 1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$,
   such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime.
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbb{K}}$.
5. Return the secret key $\mathsf{sk} = \boldsymbol{g}$ and the public key $\mathsf{pk} = \mathsf{HNF}(\langle \boldsymbol{g} \rangle)$.

FHE scheme – Smart and Vercauteren PKC 2010

Key Generation:

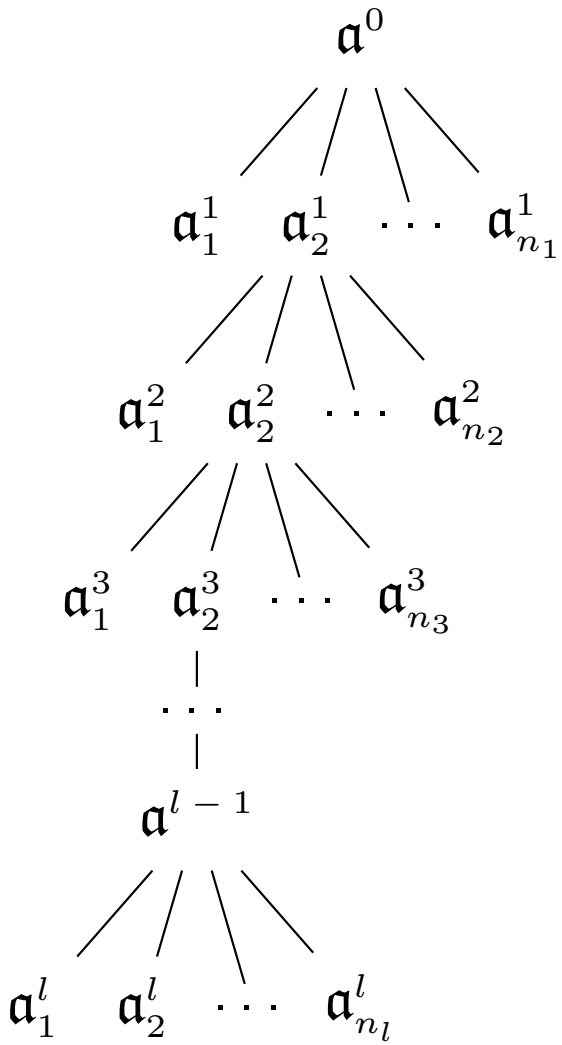
1. Fix the security parameter $N = 2^n$.
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_{2N})$.
3. Set $G(X) = 1 + 2 \cdot S(X)$,
   for $S(X)$ of degree $N - 1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$,
   such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime.
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbb{K}}$.
5. Return the secret key $\mathsf{sk} = \boldsymbol{g}$ and the public key $\mathsf{pk} = \mathsf{HNF}(\langle \boldsymbol{g} \rangle)$.

Our goal: Recover the secret key from the public key.

Outline of the algorithm [BEFGK17]

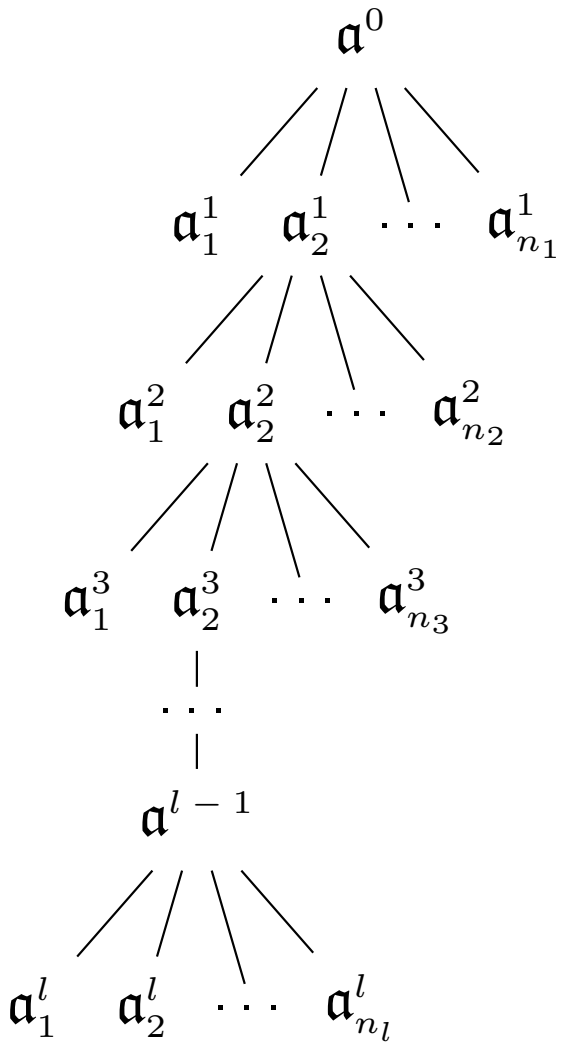
1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension.
2. Then a descent makes the size of involved ideals decrease.
3. Collect relations and run linear algebra to construct small ideals and a generator.
4. Eventually run the derivation of the small generator from a bigger one.

The descent strategy



Input ideal – Norm arbitrary large

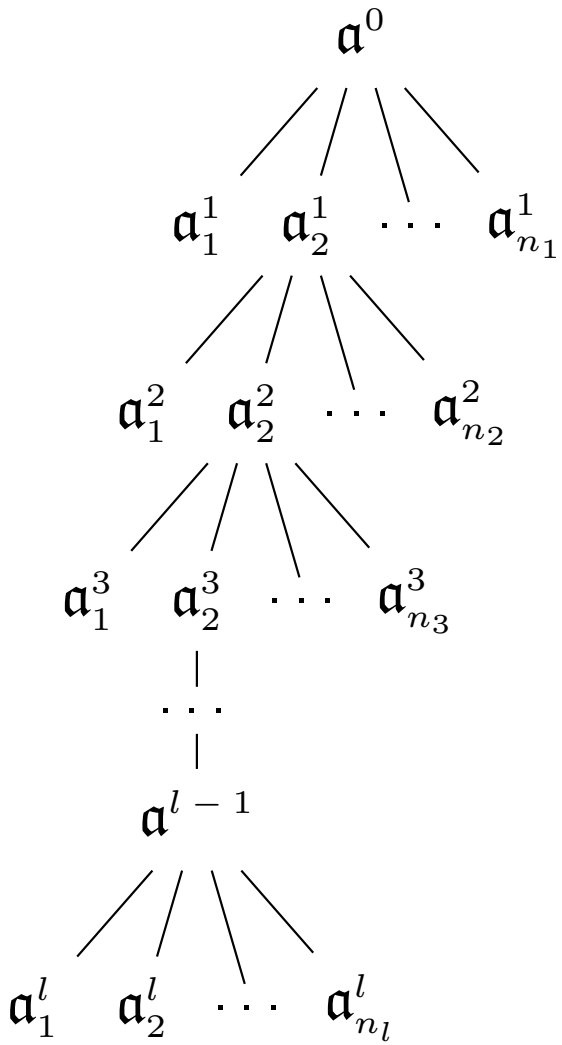
The descent strategy



Input ideal – Norm arbitrary large

Initial reduction – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{2}\right)$

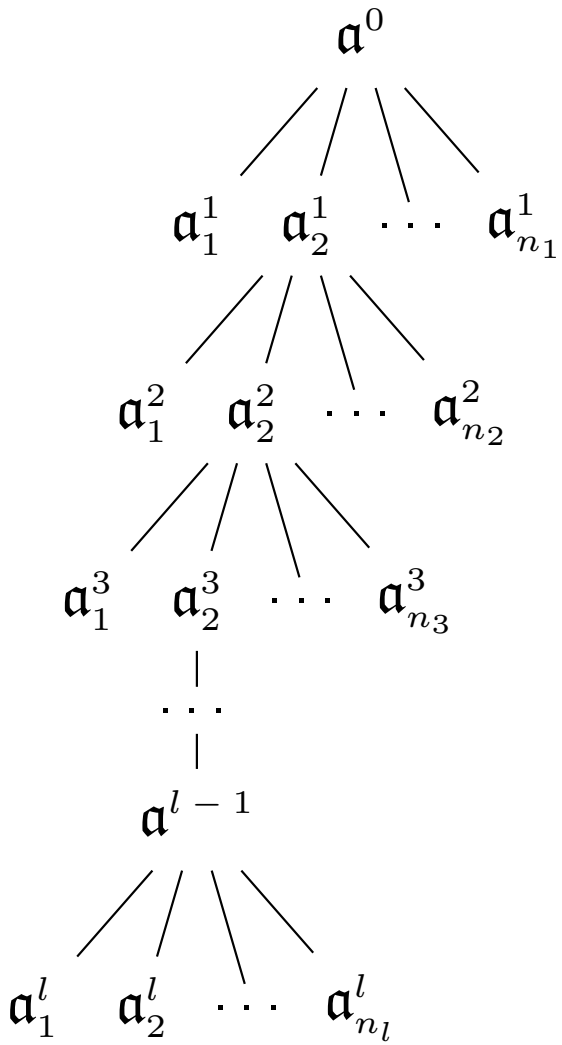
The descent strategy



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

The descent strategy

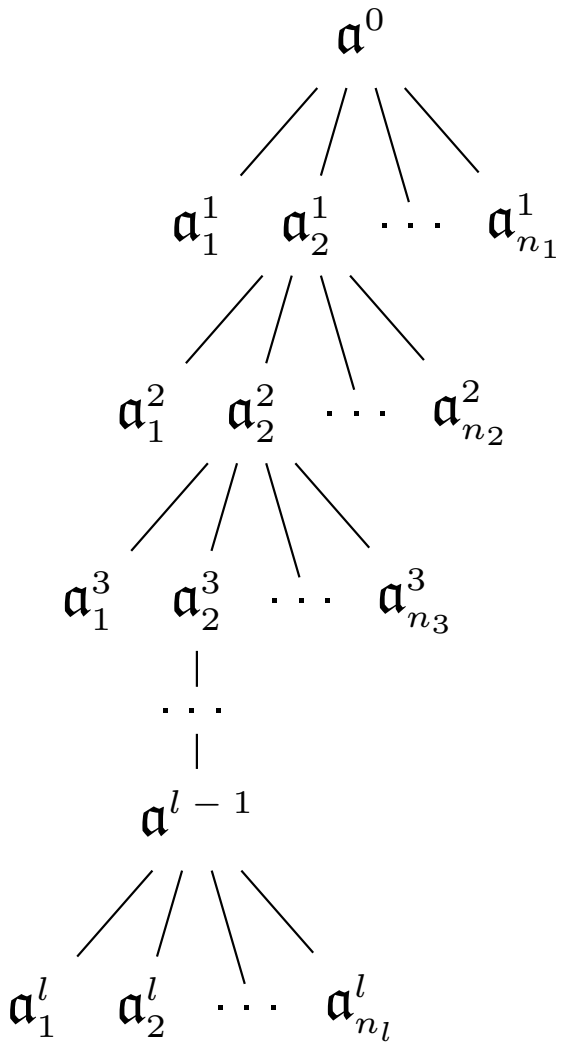


Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{4}\right)$

The descent strategy

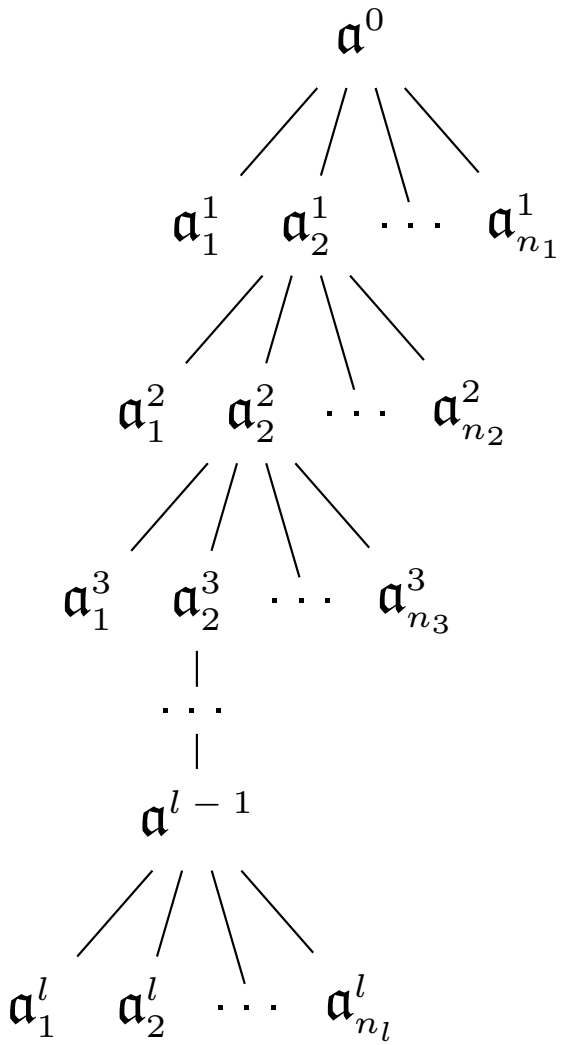


Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

The descent strategy



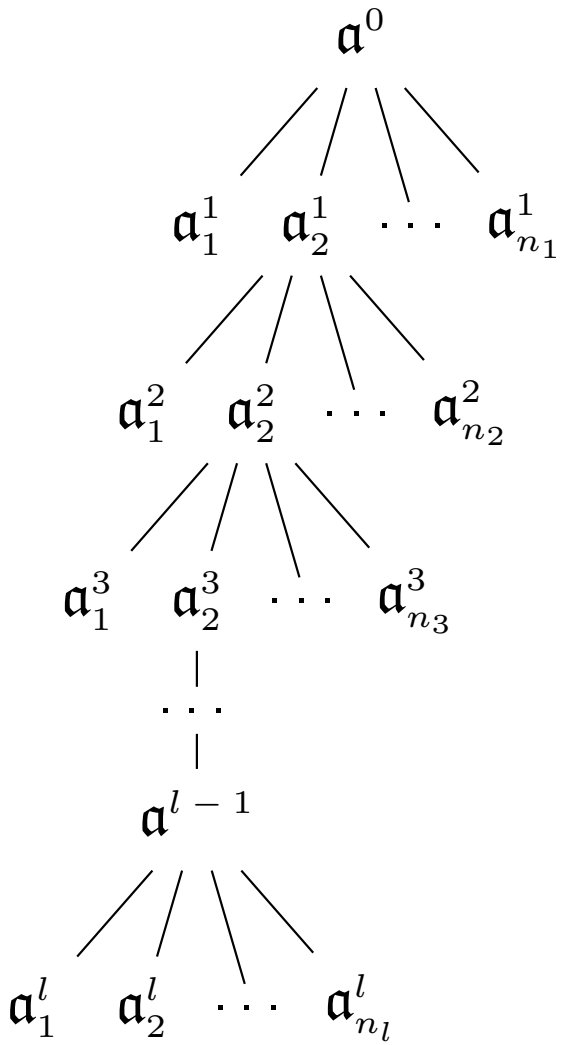
Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{9}{8}\right)$

The descent strategy



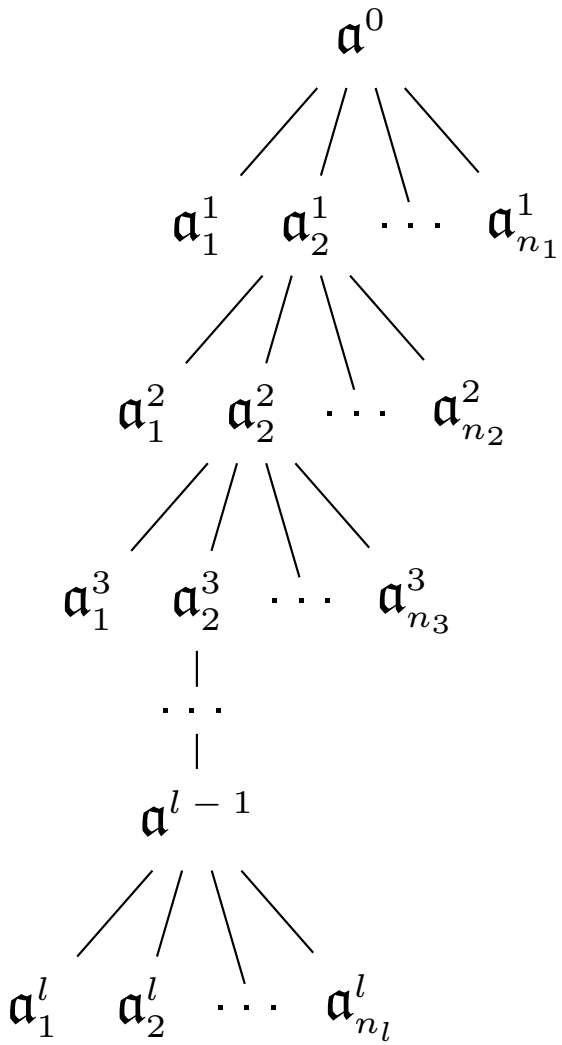
Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

The descent strategy



Input ideal – Norm arbitrary large

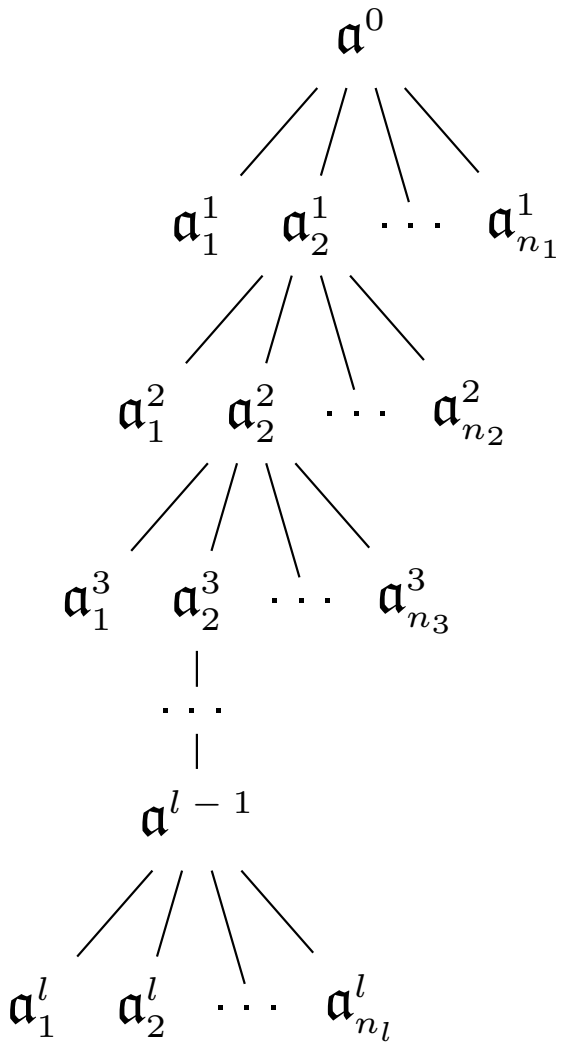
Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – Norm: $\approx L_{|\Delta_{\mathbb{K}}|}(1)$

The descent strategy



Input ideal – Norm arbitrary large

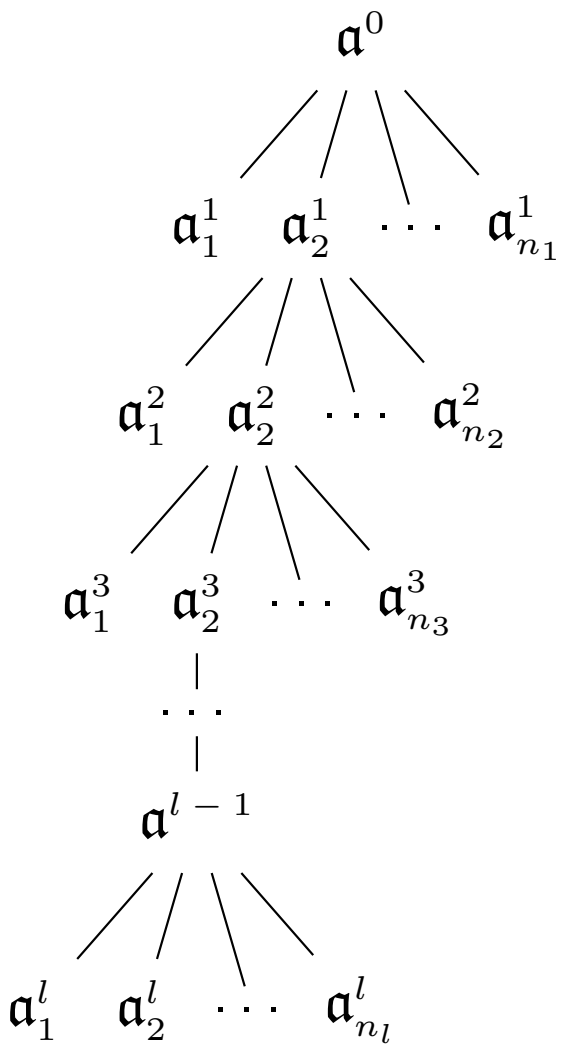
Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

The descent strategy



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

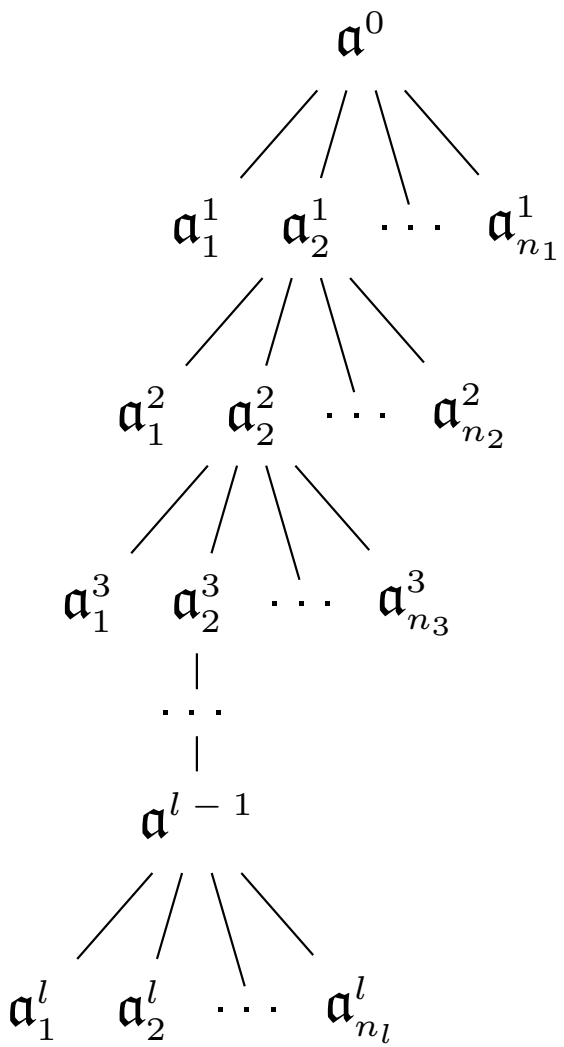
First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Last step – Norm: $L_{|\Delta_{\mathbb{K}}|}(1)$

The descent strategy



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

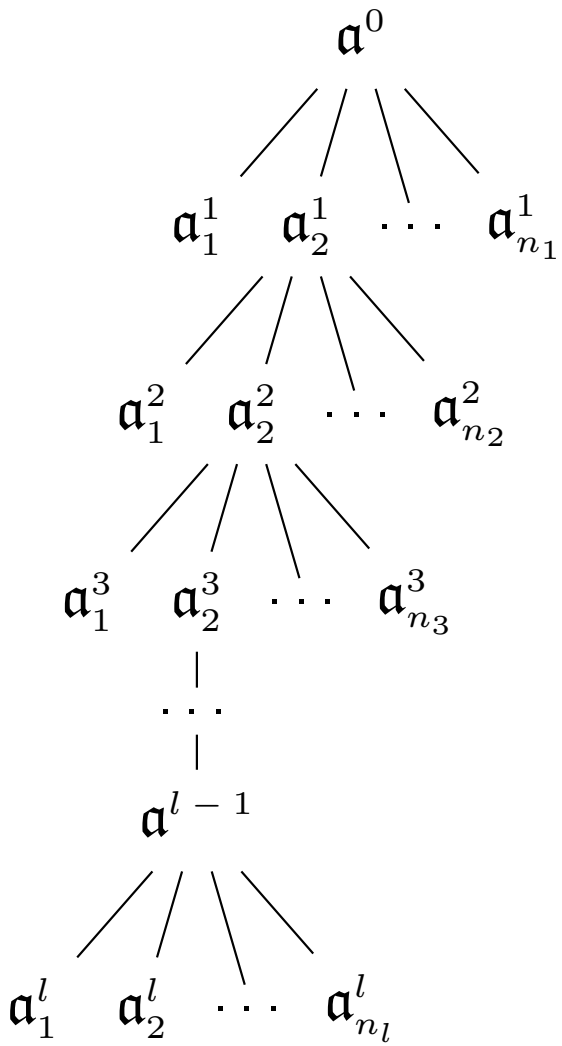
First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Last step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

The descent strategy



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Last step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Solution for $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Solution for $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

- As for class group computations, factor base: set of all prime ideals with norm below B $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$

Solution for $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

- As for class group computations, factor base: set of all prime ideals with norm below B $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$
- Construction of a full-rank matrix of relations M using the same process (relation collection)

Solution for $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

- As for class group computations, factor base: set of all prime ideals with norm below B $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$
- Construction of a full-rank matrix of relations M using the same process (relation collection)
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$

Solution for $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

- As for class group computations, factor base: set of all prime ideals with norm below B $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$
- Construction of a full-rank matrix of relations M using the same process (relation collection)
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$
- A solution X of $MX = Y$ provides a generator of the product of the $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Thanks

Merci