Class groups are essential in our life

Alex Gélin

Laboratoire de Mathématiques de Versailles
Paris-Saclay – UVSQ – CNRS

ANTS Summer School – *at home* ☹

2020/06/25

Why do we study class groups?

Why do we study class groups?

Why do we study class groups?

- Because Gauss did!

Why do we study class groups?

- Because Gauss did!
- Class groups are everywhere

Why do we study class groups?

- Because Gauss did!
- Class groups are everywhere
- Beautiful mathematical challenge

Why do we study class groups?

- Because Gauss did!
- Class groups are everywhere
- Beautiful mathematical challenge
- Finite group $\implies$ Applications in Cryptology

Why do we study class groups?

- Because Gauss did!
- Class groups are everywhere
- Beautiful mathematical challenge
- Finite group $\implies$ Applications in Cryptology
- Make use of trendy structures

FROM ALEX GELIN'S

MATHEMATICAL WORLD

CLASS GROUPS

AND WHERE TO FIND THEM

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T\rangle$$

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow \exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] \big/ \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow \exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] \big/ \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Two manners for representing elements:

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow \exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Two manners for representing elements:

- The minimal polynomial

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow \exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Two manners for representing elements:

- The minimal polynomial
  A polynomial modulo T

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow \exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Two manners for representing elements:

- The minimal polynomial

  A polynomial modulo T

- The conjugates

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$

Primitive Element Theorem $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic such that

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

T is a defining polynomial of $\mathbf{K}$ and there exist infinitely many of them

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$

Two manners for representing elements:

- The minimal polynomial

  A polynomial modulo T

- The conjugates

  Vector of $[\mathbf{K}:\mathbf{Q}]$ complex coordinates $\Longrightarrow$ Vector of $[\mathbf{K}:\mathbf{Q}]$ real coordinates

Definitions

Two interesting structures in number fields:

Definitions

Two interesting structures in number fields:

- Group of fractional ideals

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

$$1 \longrightarrow P(\mathbf{K}) \longrightarrow I(\mathbf{K}) \longrightarrow Cl(\mathbf{K}) \longrightarrow 1$$

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

$$1 \longrightarrow P(\mathbf{K}) \longrightarrow I(\mathbf{K}) \longrightarrow Cl(\mathbf{K}) \longrightarrow 1$$

- Group of units

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

$$1 \longrightarrow P(\mathbf{K}) \longrightarrow I(\mathbf{K}) \longrightarrow Cl(\mathbf{K}) \longrightarrow 1$$

- Group of units $\longrightarrow$ finitely generated

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

$$1 \longrightarrow P(\mathbf{K}) \longrightarrow I(\mathbf{K}) \longrightarrow Cl(\mathbf{K}) \longrightarrow 1$$

- Group of units $\longrightarrow$ finitely generated

  Generators $\Longrightarrow$ fundamental units

Definitions

Two interesting structures in number fields:

- Group of fractional ideals $\longrightarrow$ contains subgroup of principal ideals

  Quotient $\Longrightarrow$ class group $Cl(\mathbf{K})$

$$1 \longrightarrow P(\mathbf{K}) \longrightarrow I(\mathbf{K}) \longrightarrow Cl(\mathbf{K}) \longrightarrow 1$$

- Group of units $\longrightarrow$ finitely generated

  Generators $\Longrightarrow$ fundamental units

$$1 \longrightarrow U(\mathbf{K}) \longrightarrow \mathbf{K}^* \longrightarrow P(\mathbf{K}) \longrightarrow 1$$

[Coh93], p.210

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & U(\mathbf{K}) \arrow[r] \arrow[d] & J_{S_\infty}(\mathbf{K}) \arrow[r] \arrow[d] & C_{S_\infty}(\mathbf{K}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbf{K}^* \arrow[r] \arrow[d] & J(\mathbf{K}) \arrow[r] \arrow[d] & C(\mathbf{K}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & P(\mathbf{K}) \arrow[r] \arrow[d] & I(\mathbf{K}) \arrow[r] \arrow[d] & Cl(\mathbf{K}) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$

$$\Delta_{\mathbf{K}} = \det\left(\sigma_i(\omega_j)\right)^2$$

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\quad$ $\left(H(T) = \max|t_k|\right.$ and $\left.n = [\mathbf{K}:\mathbf{Q}]\right)$

$$\Delta_{\mathbf{K}} = \det\left(\sigma_i(\omega_j)\right)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\quad$ ($H(T) = \max|t_k|$ and $n = [\mathbf{K}:\mathbf{Q}]$)

$$\Delta_{\mathbf{K}} = \det\big(\sigma_i(\omega_j)\big)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \le n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\big(H(T) = \max|t_k|$ and $n = [\mathbf{K} : \mathbf{Q}]\big)$

$$\Delta_{\mathbf{K}} = \det\big(\sigma_i(\omega_j)\big)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

- Polynomial: $\big(\log|\Delta_{\mathbf{K}}|\big)^c$ operations

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\quad$ ($H(T) = \max|t_k|$ and $n = [\mathbf{K} : \mathbf{Q}]$)

$$\Delta_{\mathbf{K}} = \det\left(\sigma_i(\omega_j)\right)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

- Polynomial: $\left(\log|\Delta_{\mathbf{K}}|\right)^c$ operations
- Exponential: $|\Delta_{\mathbf{K}}|^c$ operations

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\quad$ ($H(T) = \max|t_k|$ and $n = [\mathbf{K}:\mathbf{Q}]$)

$$\Delta_{\mathbf{K}} = \det\big(\sigma_i(\omega_j)\big)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

- Polynomial: $(\log|\Delta_{\mathbf{K}}|)^c$ operations
- Exponential: $|\Delta_{\mathbf{K}}|^c$ operations
- Between?

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\left(H(T) = \max|t_k| \text{ and } n = [\mathbf{K}:\mathbf{Q}]\right)$

$$\Delta_{\mathbf{K}} = \det\big(\sigma_i(\omega_j)\big)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

- Polynomial: $\left(\log|\Delta_{\mathbf{K}}|\right)^c$ operations
- Exponential: $|\Delta_{\mathbf{K}}|^c$ operations
- Between?

Subexponential L-notation :

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

Number fields

Number-field *size* is given by the discriminant $\Delta_{\mathbf{K}}$ $\qquad$ $(H(T) = \max|t_k|$ and $n = [\mathbf{K}:\mathbf{Q}])$

$$\Delta_{\mathbf{K}} = \det\big(\sigma_i(\omega_j)\big)^2 \quad \text{and} \quad |\Delta_{\mathbf{K}}| \;\leq\; n^{2n} H(T)^{2n-2}$$

Algorithm complexities are given according to the size of $|\Delta_{\mathbf{K}}|$

- Polynomial: $(\log|\Delta_{\mathbf{K}}|)^c$ operations
- Exponential: $|\Delta_{\mathbf{K}}|^c$ operations
- Between?

Subexponential L-notation : $\qquad$ $L_{|\Delta_{\mathbf{K}}|}(0,c) \approx (\log|\Delta_{\mathbf{K}}|)^c \mid L_{|\Delta_{\mathbf{K}}|}(1,c) \approx |\Delta_{\mathbf{K}}|^c$

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

Complexity history

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

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

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

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

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


how i
compute class
groups

Complexity history

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

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

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

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

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

Index Calculus Method

Well-known, used for discrete logarithms

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

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

B is determined such that $\mathscr{B}$ **generates the whole class group**

The factor base

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

B is determined such that $\mathscr{B}$ **generates the whole class group**

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

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

The factor base

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

B is determined such that $\mathscr{B}$ **generates the whole class group**

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

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

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

The factor base

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

B is determined such that $\mathscr{B}$ **generates the whole class group**

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

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

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

Practically

$$B = L_{|\Delta_{\mathbf{K}}|}\left(\beta, c_b\right)$$

Relation collection

$$\mathscr{B} = \left(\mathfrak{p}_1, \ldots, \mathfrak{p}_N\right)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbf{Z}^N & \longrightarrow & I & \longrightarrow & Cl(K) \\ (e_1, \ldots, e_N) & \longmapsto & \prod\limits_i \mathfrak{p}_i^{e_i} & \longmapsto & \left[\prod\limits_i \mathfrak{p}_i^{e_i}\right] \end{array}$$

$$Cl(\mathbf{K}) \quad \simeq \quad \mathbf{Z}^N \Big/ \left\{(e_1, \ldots, e_N) \in \mathbf{Z}^N \mid \prod \mathfrak{p}_i^{e_i} = (\alpha)\mathscr{O}_{\mathbf{K}}\right\}$$

Relation collection

$$\mathscr{B} = (\mathfrak{p}_1, \ldots, \mathfrak{p}_N)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbf{Z}^N & \longrightarrow & I & \longrightarrow & Cl(K) \\ (e_1, \ldots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \left[\prod_i \mathfrak{p}_i^{e_i}\right] \end{array}$$

$$Cl(\mathbf{K}) \quad \simeq \quad \mathbf{Z}^N / \left\{(e_1, \ldots, e_N) \in \mathbf{Z}^N \mid \prod \mathfrak{p}_i^{e_i} = (\alpha)\mathscr{O}_{\mathbf{K}}\right\}$$

Idea:

1. Pick at random $\mathfrak{a} = \prod \mathfrak{p}_i^{a_i}$
2. Find a *reduced* ideal $\mathfrak{b}$ in the same class
3. If $\mathfrak{b}$ splits over $\mathscr{B}$ $\left(\iff \mathfrak{b} = \prod \mathfrak{p}_i^{b_i}\right)$ then

$$\mathfrak{a} \cdot \mathfrak{b}^{-1} = \prod \mathfrak{p}_i^{a_i - b_i} \quad \text{is principal}$$

Ideal Reduction

Correspondence between ideals and lattices:

$$\mathfrak{a} \longleftrightarrow \sigma(\mathfrak{a}) = \left(\sigma_i\left(\mathfrak{a}_j\right)\right)_{i,j}$$

Ideal Reduction

Correspondence between ideals and lattices: *ideal-lattices*

$$\mathfrak{a} \longleftrightarrow \sigma(\mathfrak{a}) = \left(\sigma_i(\mathfrak{a}_j)\right)_{i,j}$$

Ideal Reduction

Correspondence between ideals and lattices: *ideal-lattices*

$$\mathfrak{a} \longleftrightarrow \sigma(\mathfrak{a}) = \left(\sigma_i(\mathfrak{a}_j)\right)_{i,j}$$

Buchmann's reduction:

- Shortest Vector
- Exponential in the extension degree

Ideal Reduction

Correspondence between ideals and lattices: *ideal-lattices*

$$\mathfrak{a} \longleftrightarrow \sigma(\mathfrak{a}) = \left(\sigma_i\left(\mathfrak{a}_j\right)\right)_{i,j}$$

Buchmann's reduction:

- Shortest Vector
- Exponential in the extension degree

Biasse-Fieker's reduction:

- BKZ
- Trade-off between time spent and approximation factor
- Subexponential complexity

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 $Cl(\mathbf{K})$ may be only a quotient of H
$\Longrightarrow$ Need an approximation of the class number $h_{\mathbf{K}} = |Cl(\mathbf{K})|$

Verification

We find a tentative class group H, but the class group $Cl(\mathbf{K})$ may be only a quotient of H
$\Longrightarrow$ Need an approximation of the class number $h_{\mathbf{K}} = |Cl(\mathbf{K})|$

Class Number Formula + Euler Product:

$$h_{\mathbf{K}} \cdot Reg_{\mathbf{K}} \approx EP \cdot \frac{w_{\mathbf{K}} \cdot \sqrt{|\Delta_{\mathbf{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}$$

Verification

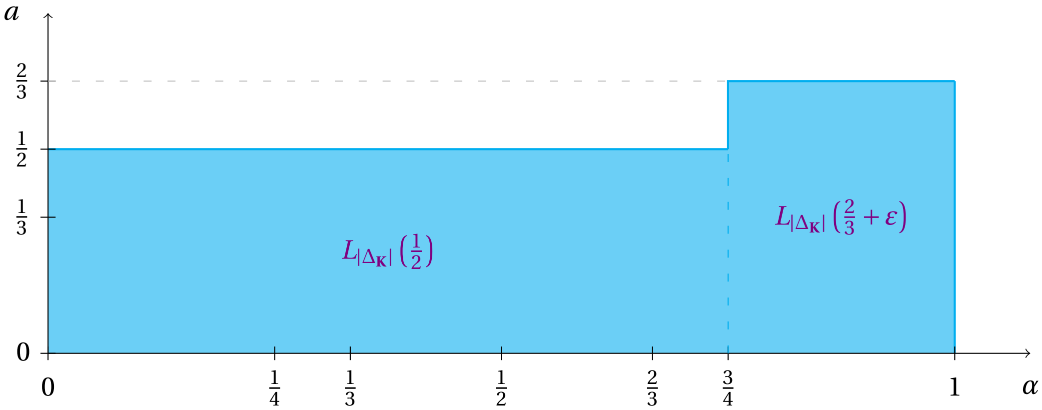
We find a tentative class group H, but the class group $Cl(\mathbf{K})$ may be only a quotient of H
$\Longrightarrow$ Need an approximation of the class number $h_{\mathbf{K}} = |Cl(\mathbf{K})|$

Class Number Formula + Euler Product:

$$h_{\mathbf{K}} \cdot Reg_{\mathbf{K}} \approx EP \cdot \frac{w_{\mathbf{K}} \cdot \sqrt{|\Delta_{\mathbf{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}$$

From the relations, we can also deduce a candidate for an approximation of $Reg_{\mathbf{K}}$ and perform the verification step

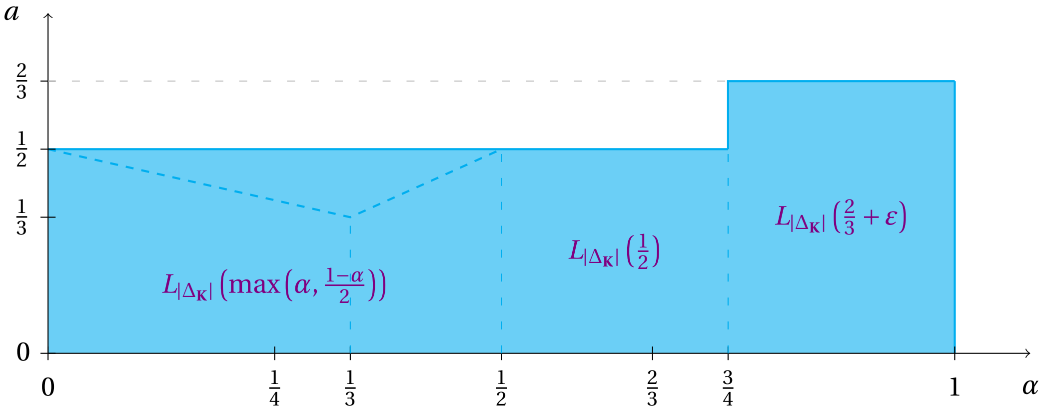
General case:



First general subexponential algorithm

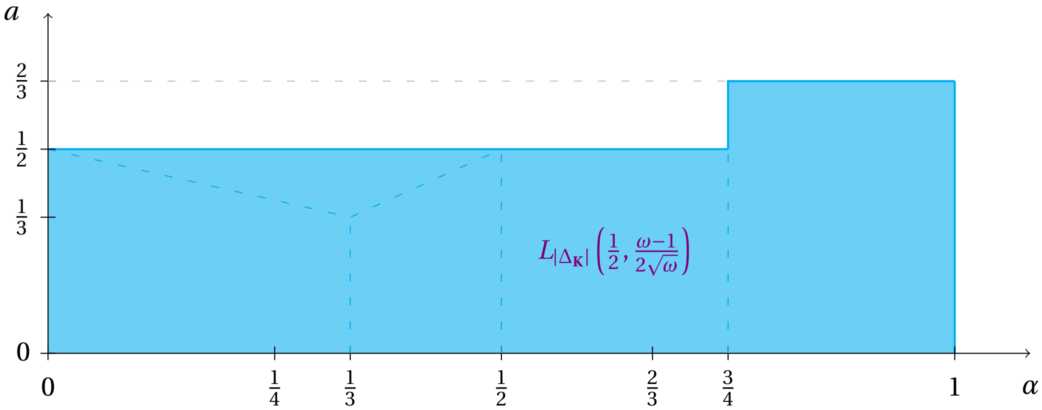
State of the art [BF14]

Special case:



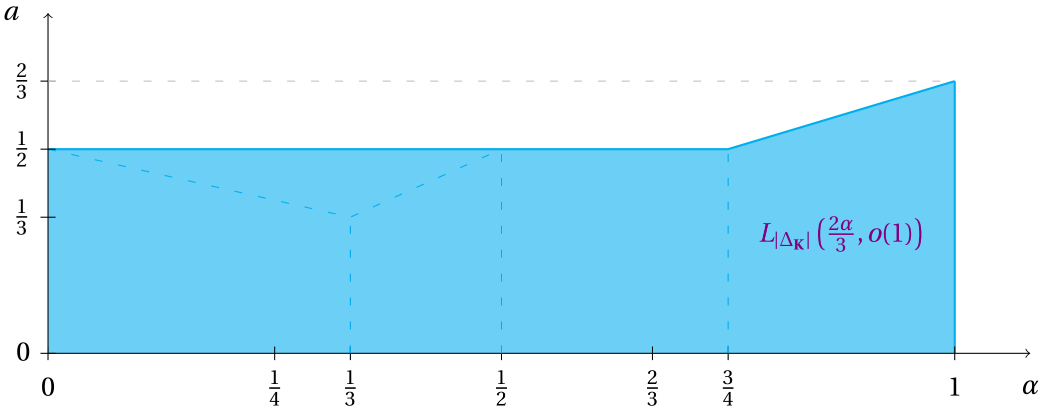
Only if $\mathbf{K}$ is defined by T such that $H(T) = L_{|\Delta_{\mathbf{K}}|}(1-\alpha)$

General case:



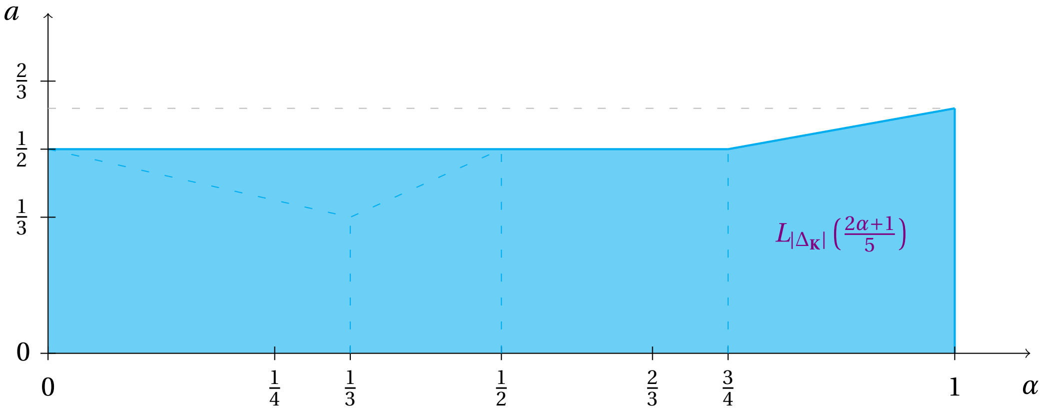
Refinement on the complexity analysis

General case:



Improvement through a better parameters choice

General case:



Improvement using special lattice-reduction algorithm

Complexity history

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

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

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

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

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

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

For $T = \sum a_k X^k \in \mathbf{Z}[X]$, the height is the maximal norm of its coefficients

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

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

For $T = \sum a_k X^k \in \mathbf{Z}[X]$, the height is the maximal norm of its coefficients

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

For every degree-n number field $\mathbf{K}$ and every defining polynomial T of $\mathbf{K}$,

$$|\Delta_{\mathbf{K}}| \leq n^{2n} H(T)^{2n-2}$$

Why minimizing the height?

Idea: Look at small algebraic integers $x \in \mathcal{O}_{\mathbf{K}}$ such that $x = A(\theta)$ with $\deg A \leq c_d$ and $H(A) \leq C_H$.

Why minimizing the height?

Idea: Look at small algebraic integers $x \in \mathcal{O}_{\mathbf{K}}$ such that $x = A(\theta)$ with $\deg A \leq c_d$ and $H(A) \leq C_H$. Then

$$\mathcal{N}\left(\langle x \rangle\right) \quad \leq \quad f(n, c_d) \cdot C_H^n \cdot H(T)^{c_d}$$

Why minimizing the height?

Idea: Look at small algebraic integers $x \in \mathscr{O}_{\mathbf{K}}$ such that $x = A(\theta)$ with $\deg A \leq c_d$ and $H(A) \leq C_H$. Then

$$\mathcal{N}\left(\langle x \rangle\right) \quad \leq \quad f(n, c_d) \cdot C_H^n \cdot H(T)^{c_d}$$

How: A tricky reduction of the lattice $\sigma(\mathscr{O}_{\mathbf{K}})$.

- Classic reduction: same magnitude for all the coordinates
- Tricky reduction: one dominant coordinate

Why minimizing the height?

Idea: Look at small algebraic integers $x \in \mathcal{O}_{\mathbf{K}}$ such that $x = A(\theta)$ with $\deg A \le c_d$ and $H(A) \le C_H$. Then

$$\mathcal{N}(\langle x \rangle) \quad \le \quad f(n, c_d) \cdot C_H^n \cdot H(T)^{c_d}$$

How: A tricky reduction of the lattice $\sigma(\mathcal{O}_{\mathbf{K}})$.

- Classic reduction: same magnitude for all the coordinates
- Tricky reduction: one dominant coordinate

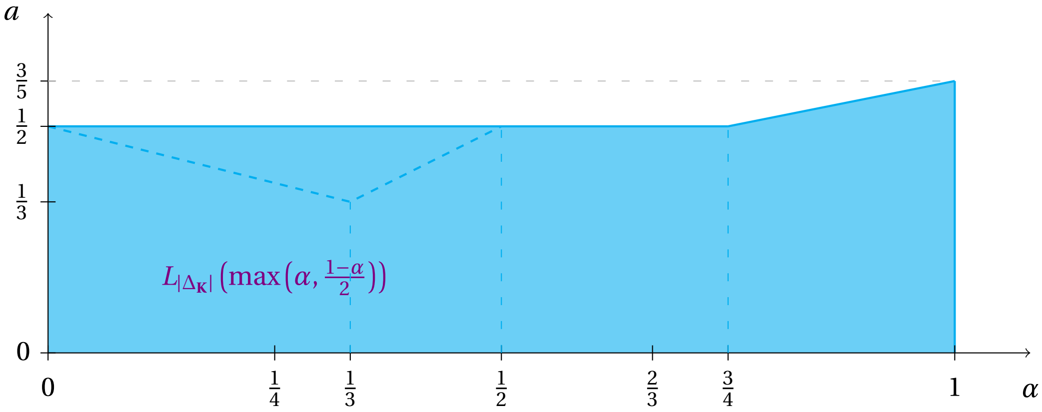
Example: Number field defined by $T = x^5 - 5843635x^4 + 931633x^2 + 6577x - 8570$

- Rounded conjugates: $[-0.38, -0.10, 0.095, 0.39, 5843634.99999997]$
- Rounded shortest vector: $[-84411, -23707, -1315, 20616, 88819]$

$x^5 - 2x^4 - 8001397580x^3 - 31542753393650x^2 + 36366533024511131875x + 48185475294252800675 00$

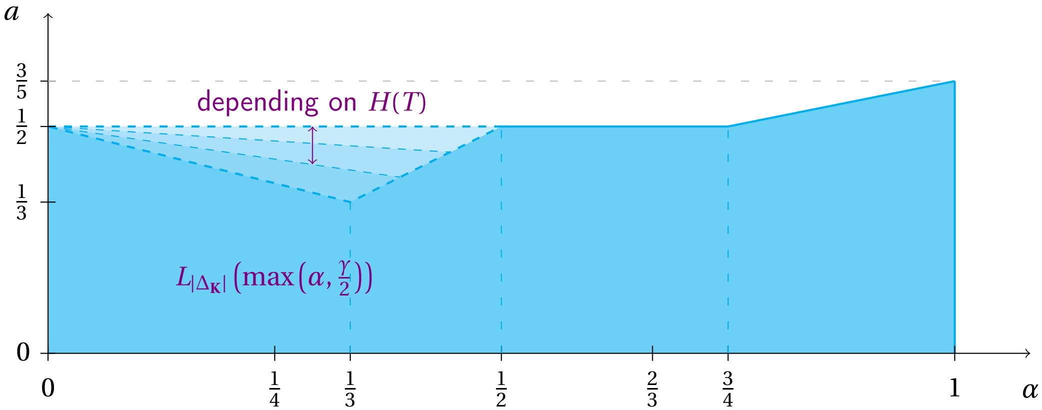
State of the art [BF14]

Special case:



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

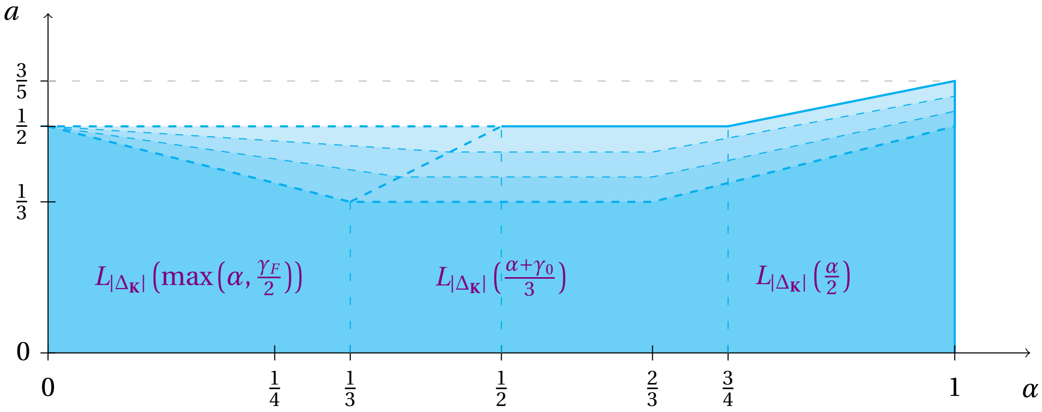
General case:



Without any condition

State of the art [G17]

Special case:



Only when it is better than the method based on ideal reductions

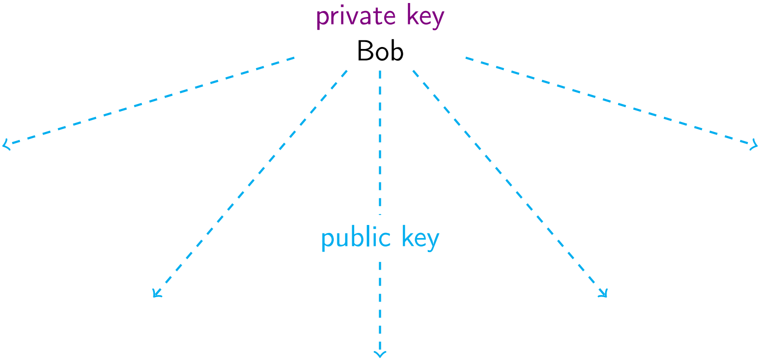
CLASS GROUPS AND CRYPTOLOGY

Public Key Cryptography

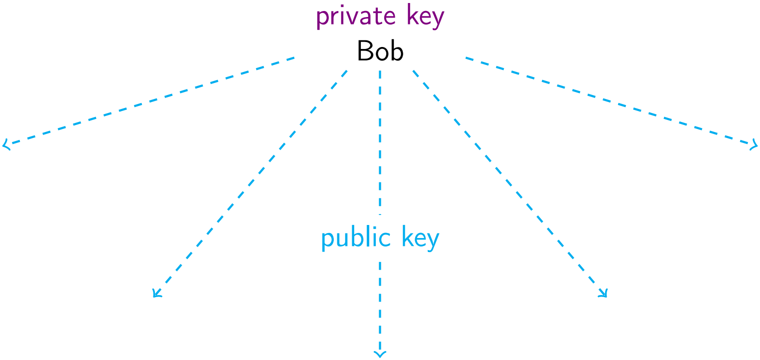
private key

Bob

Public Key Cryptography

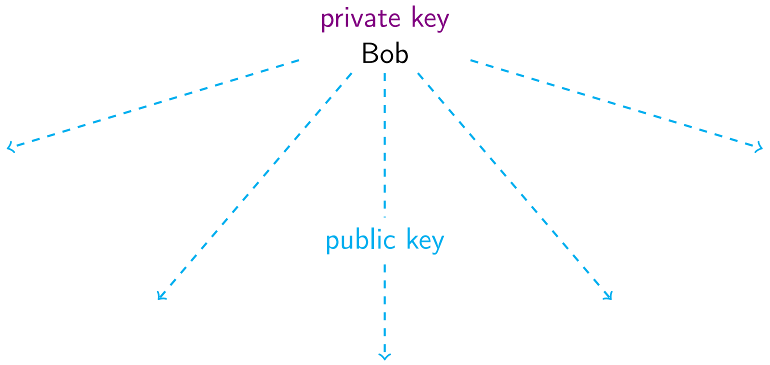


Public Key Cryptography



- Everyone uses the public key to encrypt

Public Key Cryptography



- Everyone uses the public key to encrypt
- Only Bob can decrypt thanks to his private key

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

2014 - Campbell, Groves, and Sheperd:
Reduction in polynomial time for power-of-two cyclotomic fields

2016 - Cramer, Ducas, Peikert, and Regev:
Proof and extension to prime-power cyclotomic fields

Key Generation:

1. Fix the security parameter $N = 2^n$
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbf{K} = \mathbf{Q}(\zeta_{2N})$
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 $\mathcal{N}(\langle G(\zeta_{2N})\rangle)$ is prime
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbf{K}}$
5. Return the private key $\mathrm{sk} = \boldsymbol{g}$ and the public key $\mathrm{pk} = HNF(\langle \boldsymbol{g} \rangle)$

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 $\mathbf{K} = \mathbf{Q}(\zeta_{2N})$
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 $\mathcal{N}(\langle G(\zeta_{2N})\rangle)$ is prime
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbf{K}}$
5. Return the private key $\mathrm{sk} = \boldsymbol{g}$ and the public key $\mathrm{pk} = HNF(\langle \boldsymbol{g} \rangle)$

Goal: Recover the private 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 sizes 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

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 sizes 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

All the complexities are expressed as a function of the field discriminant $\Delta_{\mathbf{Q}(\zeta_{2N})} = N^N$, for $N = 2^n$. For instance,

$$L_{|\Delta_{\mathbf{K}}|}(\alpha) = 2^{N^{\alpha+o(1)}}$$

1. Reduction to the totally real subfield

Goal: Halve the dimension of the ambient field

1. Reduction to the totally real subfield

Goal: Halve the dimension of the ambient field

- Based on the algorithm of Gentry and Szydlo

1. Reduction to the totally real subfield

Goal: Halve the dimension of the ambient field

- Based on the algorithm of Gentry and Szydlo
- Polynomial complexity

1. Reduction to the totally real subfield

Goal: Halve the dimension of the ambient field

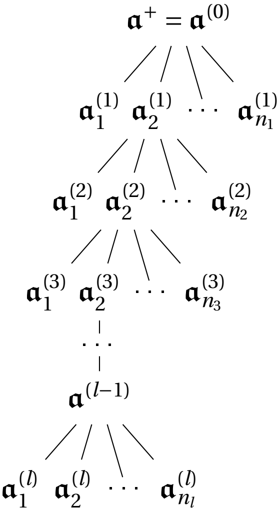
- Based on the algorithm of Gentry and Szydlo
- Polynomial complexity
- **Input:** a $\mathbf{Z}$-basis of $\mathfrak{a} = \langle g \rangle$

1. Reduction to the totally real subfield

Goal: Halve the dimension of the ambient field

- Based on the algorithm of Gentry and Szydlo
- Polynomial complexity
- **Input:** a $\mathbf{Z}$-basis of $\mathfrak{a} = \langle \boldsymbol{g} \rangle$
- **Output:** a $\mathbf{Z}$-basis of $\mathfrak{a}^+ = \langle \boldsymbol{g} + \bar{\boldsymbol{g}} \rangle \subset \mathbf{Q}(\zeta + \zeta^{-1})$ and $\boldsymbol{g} \cdot \bar{\boldsymbol{g}}^{-1}$ to recover $\boldsymbol{g}$ from $\boldsymbol{g} + \bar{\boldsymbol{g}}$

2. The descent



Input ideal – Norm arbitrary large

2. The descent

$$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$$

Input ideal – Norm arbitrary large

$$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$$

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

$$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$$

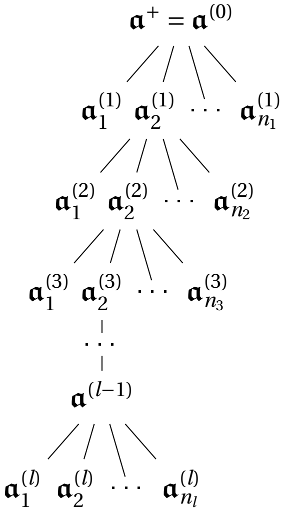
$$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$$

$$\cdots$$

$$\mathfrak{a}^{(l-1)}$$

$$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$$

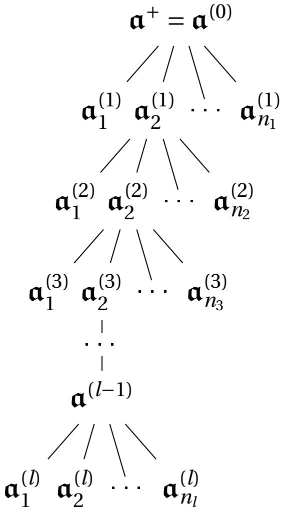
2. The descent



Input ideal – Norm arbitrary large

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

2. The descent

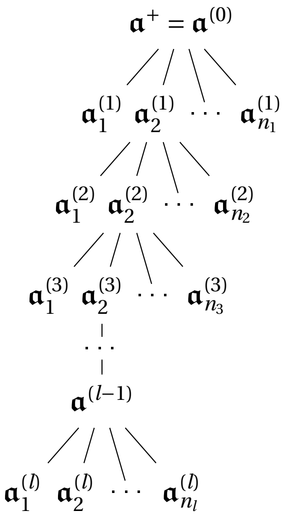


Input ideal – Norm arbitrary large

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

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

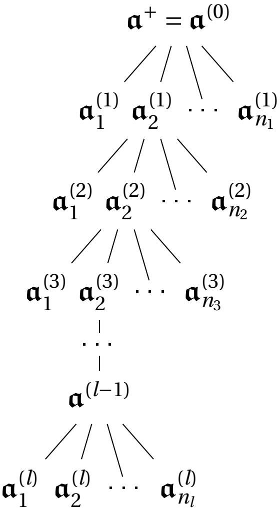
2. The descent



Input ideal – Norm arbitrary large

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

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

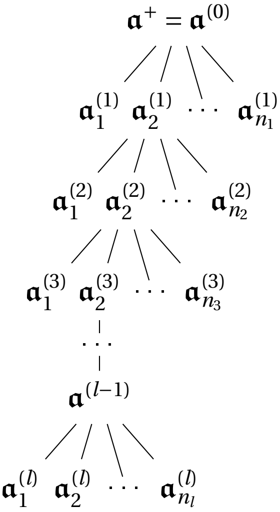


Input ideal – Norm arbitrary large

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

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

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



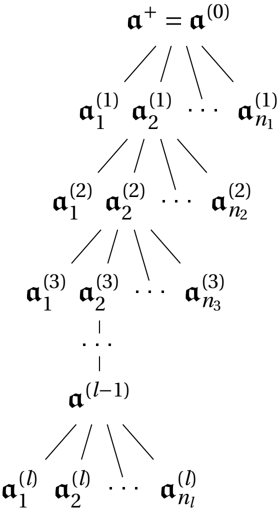
Input ideal – Norm arbitrary large

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

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

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

2. The descent



Input ideal – Norm arbitrary large

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

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

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

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

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$ Input ideal – Norm arbitrary large

$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$ Initial reduction – $L_{|\Delta_\mathbf{K}|}(1)$-smooth

$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$ First step – $L_{|\Delta_\mathbf{K}|}\left(\frac{3}{4}\right)$-smooth

$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$ Second step – $L_{|\Delta_\mathbf{K}|}\left(\frac{5}{8}\right)$-smooth

$\cdots$

$\mathfrak{a}^{(l-1)}$ Last but one step – $\approx L_{|\Delta_\mathbf{K}|}\left(\frac{1}{2}\right)$-smooth

$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$	Input ideal – Norm arbitrary large
$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$	Initial reduction – $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$-smooth
$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$	First step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{3}{4}\right)$-smooth
$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$	Second step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{5}{8}\right)$-smooth
$\cdots$	
$\mathfrak{a}^{(l-1)}$	Last but one step – $\approx L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{1}{2}\right)$-smooth
$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$	Last step – Norm: $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$	Input ideal – Norm arbitrary large
$\mathfrak{a}_1^{(1)}\ \mathfrak{a}_2^{(1)}\ \cdots\ \mathfrak{a}_{n_1}^{(1)}$	Initial reduction – $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$-smooth
$\mathfrak{a}_1^{(2)}\ \mathfrak{a}_2^{(2)}\ \cdots\ \mathfrak{a}_{n_2}^{(2)}$	First step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{3}{4}\right)$-smooth
$\mathfrak{a}_1^{(3)}\ \mathfrak{a}_2^{(3)}\ \cdots\ \mathfrak{a}_{n_3}^{(3)}$	Second step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{5}{8}\right)$-smooth
$\cdots$	
$\mathfrak{a}^{(l-1)}$	Last but one step – $\approx L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{1}{2}\right)$-smooth
$\mathfrak{a}_1^{(l)}\ \mathfrak{a}_2^{(l)}\ \cdots\ \mathfrak{a}_{n_l}^{(l)}$	Last step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{1}{2}\right)$-smooth

3. Solution for smooth ideals

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

3. Solution for smooth ideals

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

3. Solution for smooth ideals

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base.
  Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_{\mathbf{K}}|$

3. Solution for smooth ideals

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base.
  Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_{\mathbf{K}}|$

  Norm below $L_{|\Delta_{\mathbf{K}}|}(1) \implies L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$-smooth ideals in $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_{Q|\mathscr{B}|} \end{pmatrix} \begin{matrix} \rightarrow \\ \rightarrow \\ \vdots \\ \rightarrow \end{matrix} \begin{pmatrix} M_{1,1} & \cdots & M_{1,|\mathscr{B}|} \\ M_{2,1} & \cdots & M_{2,|\mathscr{B}|} \\ \vdots & & \vdots \\ M_{Q|\mathscr{B}|,1} & \cdots & M_{Q|\mathscr{B}|,|\mathscr{B}|} \end{pmatrix} \Longrightarrow \forall\, i, \langle \boldsymbol{v}_i \rangle = \prod_{j=1}^{|\mathscr{B}|} \mathfrak{p}_j^{M_{i,j}}$$

3. Solution for smooth ideals

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

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$

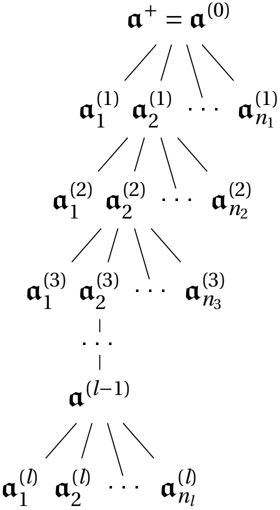
3. Solution for smooth ideals

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

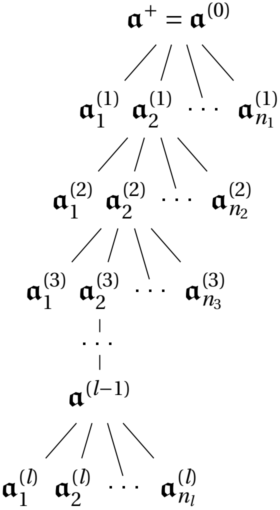
Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$
- A solution of $MX = Y$ provides a generator of the product of the $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

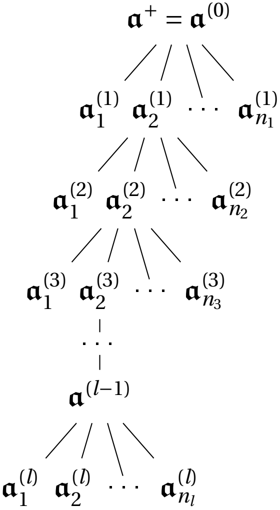
4. The backtracking



A generator for the product



A generator for the product

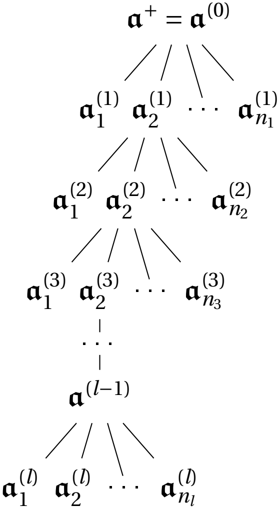


A generator for the initial ideal

$\Uparrow$

A generator for the product

4. The backtracking



A generator for the initial ideal

A generator for the product

Thanks

Kia ora

Illustrations by Alexia R. (@a_draw_r)