# COMPUTATION OF THE EUCLIDEAN MINIMUM OF ALGEBRAIC NUMBER FIELDS

PIERRE LEZOWSKI

Abstract. We present an algorithm to compute the Euclidean minimum of an algebraic number field, which is a generalization of the algorithm restricted to the totally real case described by Cerri ([7]). With a practical implementation, we obtain unknown values of the Euclidean minima of algebraic number fields of degree up to 8 in any signature, especially for cyclotomic fields, and many new examples of norm-Euclidean or non-norm-Euclidean algebraic number fields. Then, we show how to apply the algorithm to study extensions of norm-Euclideanity.

We consider an algebraic number field $K$. Let $\mathbf{Z}_K$ be its ring of integers. We write $r_1$ for its number of real places, $2r_2$ for its number of imaginary places and $n = r_1 + 2r_2$ for its degree. We denote by $\mathbf{N}_{K/\mathbf{Q}}$ the usual norm. The pair $(r_1, r_2)$ is called the signature of $K$. We write $d(K)$ for the discriminant of $K$, $\mathrm{h}_K$ for the class number of $K$, $\mathbf{Z}_K^\times$ for the group of units of $K$ and $r = r_1 + r_2 - 1$ for its rank.

*Definition* (Euclideanity with respect to the norm). We say that $\mathbf{Z}_K$ is Euclidean with respect to the norm if and only if for every $(a, b) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, there exists some $c \in \mathbf{Z}_K$ such that

$$\left|\mathbf{N}_{K/\mathbf{Q}}(a - bc)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|.$$

If the property written above holds, we also say that $K$ *is norm-Euclidean* or that $\mathbf{N}_{K/Q}$ is an Euclidean algorithm for $K$. There is no reason to choose the norm instead of another Euclidean algorithm, but the multiplicative property of the norm makes it (relatively) easier to test if $\mathbf{N}_{K/\mathbf{Q}}$ is an Euclidean algorithm for $\mathbf{Z}_K$. Indeed, checking if $\mathbf{Z}_K$ is norm-Euclidean is equivalent to checking if for any $\xi \in K$, there exists some $z \in \mathbf{Z}_K$ such that $\left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right| < 1$. Therefore, the determination of norm-Euclideanity can be seen in a geometric setting. The notion of Euclidean minimum will be introduced to indicate the "distance" between $K$ and the lattice $\mathbf{Z}_K$.

This notion of Euclideanity was extensively studied for several purposes. First, the existence of an Euclidean algorithm provides a technique to compute greatest common divisors in $\mathbf{Z}_K$. Besides, if $\mathbf{Z}_K$ is Euclidean, then it is a principal ideal domain and therefore a unique factorisation domain. Consequently, in the $19^{\text{th}}$ century, Wantzel tried to fill one gap in Lamé's "proof" of Fermat's Last Theorem by using some properties of norm-Euclideanity. Following and correcting his ideas, Cauchy and Kummer studied cyclotomic fields and proved that some of them are norm-Euclidean (see [15] for both mathematical and historical details).

---

*Date*: 2nd October 2012.

2010 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11R04, 11A05, 13F07.

*Key words and phrases.* Euclidean number fields, Euclidean minimum, inhomogeneous minimum.

Many attempts were made to find norm-Euclidean quadratic number fields, and if the imaginary case is easy, the complete list of the real ones was not found until the middle of the $20^{\text{th}}$ century (see [11] for a complete proof in one paper). Later, Lenstra ([14]) found a technique to prove that many number fields of large degree ($5 \leqslant n \leqslant 10$) are norm-Euclidean. For a more complete description of the subject, Lemmermeyer ([13]) wrote a very interesting and thorough survey.

More recently, Cerri ([7]) described an algorithm, which – among other properties – can determine whether or not a totally real number field (such that $r_2 = 0$) is norm-Euclidean. It allowed him to find many new examples of totally real norm-Euclidean fields. Our purpose here will be to extend his algorithm to general number fields.

First, we will define properly the different notions of Euclidean minimum and see their properties. Afterwards, we will present all the tools required for the algorithm. In the third section, we will see the algorithm itself. Then, we will present some applications of the algorithm. Finally, we will deal with the complexity of the procedures and the approximations of computation.

## 1. Euclidean and inhomogeneous minimum of $K$

### 1.1. Euclidean minimum of $K$.

*Definition* 1.1 (local Euclidean minimum). For any $\xi \in K$, we call *Euclidean minimum of $K$ at $\xi$* the nonnegative real number $m_K(\xi) := \inf_{z \in \mathbf{Z}_K} \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right|$.

With such a definition, we see immediately that the Euclidean minimum at $\xi$ is reached for any $\xi \in K$, that is to say there exists $z \in \mathbf{Z}_K$ such that $m_K(\xi) = \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right|$. However, it is not so obvious that we can compute it. To achieve this in the general case, we will need to know the units $\mathbf{Z}_K^\times$ of $K$. We will see how to do it in details in Section 2.1.

Definition 1.1 allows us to reformulate the definition of norm-Euclideanity: $K$ is norm-Euclidean if and only if for any $\xi \in K$, $m_K(\xi) < 1$.

*Definition* 1.2 (Euclidean minimum). We set $M(K) := \sup_{\xi \in K} m_K(\xi)$ and we call it the *Euclidean minimum* of $K$.

We will see that $M(K)$ is finite in Section 1.3. Our purpose is to compute this positive number, given the following basic observation.

(1) If $M(K) < 1$, then $K$ is norm-Euclidean.
(2) If $M(K) > 1$, then $K$ is not norm-Euclidean.

We will see a sharper result (Proposition 1.7) in Section 1.3.

### 1.2. Embedding of $K$.

We denote by $(\sigma_i)_{1 \leqslant i \leqslant n}$ the embeddings of $K$ into $\mathbf{C}$. We suppose that the $r_1$ first ones are real and that for any $r_1 < i \leqslant r_1 + r_2$,

$$\sigma_{i+r_2} = \overline{\sigma_i}.$$

We put
$$\Phi : \begin{cases} K & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & \Big(\sigma_1(x), \dots, \sigma_{r_1}(x), \ \Re\sigma_{r_1+1}(x), \dots, \Re\sigma_{r_1+r_2}(x), \\ & & \qquad \Im\sigma_{r_1+1}(x), \dots, \Im\sigma_{r_1+r_2}(x)\Big) \end{cases}.$$

We will infer properties of $K$ from results on $\Phi(K)$. To do this, we extend the product defined on $K$ to $\mathbf{R}^n$ through $\Phi$: for $x = (x_i)_{1\leqslant i\leqslant n}$ and $y = (y_i)_{1\leqslant i\leqslant n}$, we put $x \cdot y := (z_i)_{1\leqslant i\leqslant n}$ where

$$z_i = \begin{cases} x_i y_i & \text{if } 1 \leqslant i \leqslant r_1, \\ x_i y_i - x_{i+r_2} y_{i+r_2} & \text{if } r_1 < i \leqslant r_1 + r_2, \\ x_{i-r_2} y_i + x_i y_{i-r_2} & \text{if } r_1 + r_2 < i \leqslant n. \end{cases}$$

Therefore, for any $\xi, \upsilon \in K$, $\Phi(\xi\upsilon) = \Phi(\xi) \cdot \Phi(\upsilon)$.

To practical purposes, we introduce $H = K \otimes_{\mathbf{Q}} \mathbf{R}$, which we identify with $\mathbf{R}^n$ equipped with the product previously defined and we see $\Phi$ as a map from $K$ to $H$. We can extend the norm to $H$ by setting

$$\mathcal{N} : \begin{cases} H & \longrightarrow & \mathbf{R} \\ x = (x_i)_{1\leqslant i\leqslant n} & \longmapsto & \prod_{i=1}^{r_1} x_i \prod_{i=r_1+1}^{r_1+r_2} (x_i^2 + x_{i+r_2}^2) \end{cases}.$$

We see that for any $x, y \in H$, $\mathcal{N}(x \cdot y) = \mathcal{N}(x)\mathcal{N}(y)$ and that for any $\xi \in K$, $\mathbf{N}_{K/\mathbf{Q}}(\xi) = \mathcal{N}(\Phi(\xi))$. This leads to the definition of the following notion.

### 1.3. **Inhomogeneous minimum of $K$.**

*Definition* 1.3 (inhomogeneous minimum). For any $x \in H$, we define the *inhomogeneous minimum of $K$ at $x$* by $m_{\overline{K}}(x) := \inf_{z\in\mathbf{Z}_K} |\mathcal{N}(x - \Phi(z))|$.

Notice that for every $x \in K$, $m_{\overline{K}}(\Phi(x)) = m_K(x)$. Besides, $m_{\overline{K}}$ is the inhomogeneous minimum with respect to the lattice $\Phi(\mathbf{Z}_K)$ for the map $\mathcal{N}$. Consequently, we can deduce results on $m_{\overline{K}}$ from these remarks.

**Proposition 1.4.** *The map $m_{\overline{K}}$ has the following properties.*

*(1) For every $\varepsilon \in \mathbf{Z}_K^\times$, $Z \in \Phi(\mathbf{Z}_K)$, we have $m_{\overline{K}}(\Phi(\varepsilon) \cdot x - Z) = m_{\overline{K}}(x)$.*
*(2) $m_{\overline{K}}$ induces a map (also denoted by $m_{\overline{K}}$) on the quotient space $H/\Phi(\mathbf{Z}_K)$.*
*(3) $m_{\overline{K}}$ is upper semi-continuous on $H$ and on $H/\Phi(\mathbf{Z}_K)$.*

*Proof.* See [7, Proposition 2.1]. □

It is now natural to introduce the following notion.

*Definition* 1.5 (inhomogoneous minimum of $K$). $M(\overline{K}) := \sup_{x\in H} m_{\overline{K}}(x)$.

We immediately see that $M(K) \leqslant M(\overline{K})$. By the compactness of $H/\Phi(\mathbf{Z}_K)$, Proposition 1.4 (3) implies that $M(\overline{K})$ is finite and that there exists some $x \in H$ such that $m_{\overline{K}}(x) = M(\overline{K})$. Moreover, since $M(K) \leqslant M(\overline{K})$, $M(K)$ is finite too. However, it is more interesting to know if there is some $\xi \in K$ such that $m_{\overline{K}}(\Phi(\xi)) = M(\overline{K})$. Of course, it is true in the trivial cases $r = 0$. Besides, the following theorem provides a positive answer in many cases.

**Theorem 1.6.** *We recall that the unit rank is denoted by $r$.*

*a. If $r = 1$, then $M(K) = M(\overline{K})$.*
*b. If $r > 1$, then there exists some $\xi \in K$, such that $M(\overline{K}) = m_K(\xi)$. In particular, $M(K) = M(\overline{K}) \in \mathbf{Q}$.*

The statement (a) is due to [1] in the case $r_1 = 2$, $r_2 = 0$. This result was extended by [19] in the case $r = 1$. The statement (b) is proved in [6].

If $r = 1$, we do not have a result as strong as (b). However, there is no counterexample known, and the fact that this still holds was conjectured in the real quadratic case by Barnes and Swinnerton-Dyer [1].

Thus, the computation of $M(K)$ answers the question of whether or not $K$ is norm-Euclidean if $r > 1$. The following proposition sums up the criterion to decide norm-Euclideanity if we know the value of $M(K)$.

**Proposition 1.7.** *Let $K$ be an algebraic number field.*

*(1) If $M(K) < 1$, then $K$ is norm-Euclidean.*
*(2) If $M(K) > 1$, then $K$ is not norm-Euclidean.*
*(3) If $M(K) = 1$ and the rank of $\mathbf{Z}_K^\times$ is $r > 1$, then $K$ is not norm-Euclidean.*

Consequently, $M(K) = 1$ implies that $K$ is not norm-Euclidean, except maybe for number fields with unit rank 1. For such fields, it is known that there are only finitely many of them such that $M(K) \leqslant 1$, allowing us in principle to compute all of them and to check that Proposition 1.7 (3) also holds for $r = 1$.

In the case $n = 2$, we know (see [11, Lemma 11]) that $M(K) \leqslant 1$ implies that $d(K) \leqslant \kappa^2$, where $\kappa = 16 + 6\sqrt{6}$. Then, we can use the technique of [11] to study all number fields with such a discriminant satisfying $M(K) \geqslant 1$: most of them can be proved to verify $M(K) > 1$ thanks to a classical congruence lemma described in [3]. Besides, the critical points given in [11] show that the only real quadratic field with $M(K) = 1$ is $K = \mathbf{Q}\left(\sqrt{65}\right)$, which is not norm-Euclidean because its class number is 2.

## 1.4. Bounds for the Euclidean minimum.

1.4.1. *Lower bounds.* For any ideal $I$ of $\mathbf{Z}_K$, we denote by $\mathbf{N}I$ the cardinality of $\mathbf{Z}_K/I$. We define the integer

$$\Lambda(K) = \min\left\{\mathbf{N}I, I \text{ integral ideal}, \{0\} \subsetneq I \subsetneq \mathbf{Z}_K\right\}.$$

Then, we have $M(K) \geqslant \frac{1}{\Lambda(K)}$. In fact, if $K$ is principal, then there exists some $x \in \mathbf{Z}_K \setminus \left(\mathbf{Z}_K^\times \cup \{0\}\right)$ such that $\Lambda(K) = \mathbf{N}((x)) = \left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|$. Therefore, $m_K\left(\frac{1}{x}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|} = \frac{1}{\Lambda(K)}$. Obviously, if $K$ is not principal, we have the better bound $M(K) \geqslant 1$.

In the case $r = 1$, we also have special bounds of $M(K)$ in function of the discriminant $d(K)$ of $K$.

1.4.2. *Upper bounds.* Even though some explicit bounds are known in the general case [10] or in particular cases [2], none of these are really useful for the execution of the algorithm, because they are not very good in the cases of small discriminants.

# 2. Tools for the algorithm

The purpose of this section is to describe *practical* procedures which will be relied on for the general algorithm to compute the Euclidean minimum of a number field. First, we will deal with the local Euclidean minimum.

2.1. **Computation of the local Euclidean minimum.** The technique is the one described in [7], written in the general case. The ideas and arguments are standard.

Recall that we write $r = r_1 + r_2 - 1$ for the rank of $\mathbf{Z}_K^\times$. As the case $r = 0$ is easy, we will assume that $r \geqslant 1$, so $\mathbf{Z}_K^\times$ is infinite. The group $\mathbf{Z}_K^\times$ is determined by $r$ fundamental units, which will be written as $\{\varepsilon_1, \dots, \varepsilon_r\}$, and the roots of unity in $K$.

The units act on $K$ by multiplication and we can extend this action to $H$ by

$$\left\{ \begin{array}{ccc} \mathbf{Z}_K^\times \times H & \longrightarrow & H \\ (\varepsilon, x) & \longmapsto & \Phi(\varepsilon)\cdot x \end{array} \right. .$$

Thanks to Proposition 1.4 (1), we know that $m_{\overline{K}}$ is constant on the orbits of this action. For $x \in H$, we denote by $\mathrm{Orb}(x)$ the elements of the fundamental domain $\mathcal{F}$ which are translates by $\Phi(\mathbf{Z}_K)$ of elements of the orbit of $x$ under the action of units.

*Remark* 2.1. For $x \in H$, the set $\mathrm{Orb}(x)$ is finite if and only if $x \in \Phi(K)$.

For any $1 \leqslant i \leqslant n$, we set $\Gamma_i := \displaystyle\prod_{j=1}^{r} \max\left\{ |\sigma_i(\varepsilon_j)|, \frac{1}{|\sigma_i(\varepsilon_j)|} \right\}$, which allows us to define

$$\Gamma(k) := \left\{ \begin{array}{ll} \left(\prod_{j=1}^{n-1}\Gamma_j\right)^{\frac{1}{n}} k^{\frac{1}{n}} & \text{if } K \text{ is totally real,} \\ \left(\prod_{j=1}^{r_1}\Gamma_j \prod_{j=1}^{r_1+r_2-1}\Gamma_j\Gamma_{j+r_2}\right)^{\frac{1}{n}} k^{\frac{1}{n}} & \text{otherwise.} \end{array} \right.$$

**Lemma 2.2.** *For any $(c_i)_{1\leqslant i\leqslant r} \in (\mathbf{R}_{>0})^r$, there exists a unit $\nu \in \mathbf{Z}_K^\times$ such that for all $1 \leqslant i \leqslant r$,*

$$c_i \leqslant |\sigma_i(\nu)| \leqslant c_i\Gamma_i.$$

*Proof.* The proof is the same as in the real case ([7]). We consider the logarithmic embedding of $K$:

$$\mathcal{L} : \left\{ \begin{array}{ccc} K\setminus\{0\} & \longrightarrow & \mathbf{R}^{r_1+r_2} \\ x & \longmapsto & (\ln|\sigma_i(x)|)_{1\leqslant i\leqslant r_1+r_2} \end{array} \right. ,$$

we notice that $\mathcal{R} = \mathcal{L}(\mathbf{Z}_K)$ is a lattice of

$$\mathcal{H} = \left\{ (x_i)_{1\leqslant i\leqslant r_1+r_2}, \sum_{i=1}^{r_1} x_i + 2\sum_{i=r_1+1}^{r_1+r_2} x_i = 0 \right\}$$

and we use the fact that $(\mathcal{L}(\varepsilon_i))_{1\leqslant i\leqslant r}$ is a $\mathbf{Z}$-basis of $\mathcal{R}$. □

**Proposition 2.3.** *Let $x \in \Phi(K)\setminus\Phi(\mathbf{Z}_K)$ and $k > 0$. If there exists $X \in \Phi(\mathbf{Z}_K)$ such that $0 < |\mathcal{N}(x - X)| < k$, then there exist $\nu \in \mathbf{Z}_K^\times$ and $Y \in \Phi(\mathbf{Z}_K)$ such that*

$$|\mathcal{N}(\nu\cdot x - Y)| < k \qquad \text{and} \qquad |Y_i| \leqslant \Gamma(k) \text{ for all } 1 \leqslant i \leqslant n.$$

*Proof.* Apply Lemma 2.2 with $c_i = \frac{\Gamma(k)}{\Gamma_i|x_i - X_i|}$ for every $1 \leqslant i \leqslant r$. □

**Theorem 2.4.** *Let $x \in \Phi(K)$ and $k > 0$. For any $z \in \mathrm{Orb}(x)$, we set*

$$\mathcal{I}_{z,k} := \{Z \in \Phi(\mathbf{Z}_K), |z_i - Z_i| \leqslant \Gamma(k) \text{ for all } 1 \leqslant i \leqslant n\}.$$

*We consider the nonnegative rational*

$$\mathcal{M}_k = \min_{z\in\mathrm{Orb}(x)}\left(\min_{Z\in\mathcal{I}_{z,k}} |\mathcal{N}(z - Z)|\right).$$

*If $\mathcal{M}_k \leqslant k$, then $m_{\overline{K}}(x) = \mathcal{M}_k$.*

*Proof.* The proof is exactly the same as in the real case ([7]). □

As the function $k \longmapsto \mathcal{M}_k$ is non-decreasing, Theorem 2.4 implies that the following algorithm requires at most one execution of the loop to obtain $m_{\overline{K}}(x)$.

**Algorithm 2.1** Computation of the local Euclidean minimum

INPUT: a number field $K$, a point $x \in \Phi(K)$, the orbit $\operatorname{Orb}(x)$ of $x$, $k > 0$
OUTPUT: $m_K(x)$

```
Compute Γ(k), M_k
while M_k > k do
    k ← M_k, compute Γ(k), M_k
end while
return M_k
```

*Remarks* 2.5. i. This algorithm only applies to elements of $\Phi(K)$, because the orbits of other elements of $H$ are infinite (Remark 2.1).

ii. If $x = \frac{1}{\xi}$ where $\xi \in \mathbf{Z}_K \setminus \mathbf{Z}_K^\times \cup \{0\}$, then $m_K(x) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(\xi)\right|}$ and applying Algorithm 2.1 is unnecessary.

iii. Algorithm 2.1 requires the knowledge of the orbit $\operatorname{Orb}(x)$. We will see how to compute it in Section 3.2.4.

2.2. **Embedding and absorption test of $K$ by $\mathbf{Z}_K$.** Now, we are interested in the Euclidean minimum $M(K)$. The general idea will be to prove that $m_K(\xi) < k$ for some $k$ except for a finite set of points $(\xi_i)_{1 \leqslant i \leqslant l}$ of $K$. If we find that $m_K(\xi_i) \geqslant k$ for some $i$, then $M(K) = \max_{1 \leqslant i \leqslant l} m_K(\xi_i)$.

2.2.1. *Presentation and general ideas.* The computations will require some information on $K$. In fact, we assume that we know a $\mathbf{Z}$-basis $(z_i)_{1 \leqslant i \leqslant n}$ of $\mathbf{Z}_K$ and (good) approximations of $\sigma_j(z_i)$ for all $1 \leqslant i, j \leqslant n$. This allows us to identify $\mathbf{Q}^n$ and $K$ through the isomorphism of $\mathbf{Q}$-vector spaces

$$\Psi : \left\{ \begin{array}{ccc} \mathbf{Q}^n & \longrightarrow & K \\ (q_i)_{1 \leqslant i \leqslant n} & \longmapsto & \sum_{i=1}^n q_i z_i \end{array} \right. .$$

As both $\Phi$ and $\Psi$ are linear, $\Phi \circ \Psi : \mathbf{Q}^n \longrightarrow H$ is linear and we can extend it by continuity to a linear map $\phi : \mathbf{R}^n \longrightarrow H$ such that the following diagram commutes.

$$\begin{tikzcd} \mathbf{Q}^n \arrow[r, hook, "i"] \arrow[d, "\Psi"] & \mathbf{R}^n \arrow[d, "\phi", "\wr"'] \\ K \arrow[r, "\Phi"] & H \end{tikzcd}$$

Since $\Phi$ and $\Psi$ are injective, $\phi$ is injective, so $\phi$ is an isomorphism and its matrix $\mathcal{M}$ is invertible. We can give an explicit expression of $\mathcal{M} = (m_{i,j})_{1 \leqslant i,j \leqslant n}$: for all $1 \leqslant j \leqslant n$,

$$m_{i,j} = \left\{ \begin{array}{ll} \sigma_i(z_j) & \text{if } 1 \leqslant i \leqslant r_1, \\ \Re\sigma_i(z_j) & \text{if } r_1 < i \leqslant r_1 + r_2, \\ \Im\sigma_{i-r_2}(z_j) & \text{if } r_1 + r_2 < i \leqslant n. \end{array} \right. \tag{2.a}$$

Besides, $\Psi$ identifies $\mathbf{Z}^n$ and $\mathbf{Z}_K$, so the lattice $\mathcal{M}\mathbf{Z}^n$ in $H$ is used to describe the integers of $K$.

All the computations are performed in $H/\mathcal{M}\mathbf{Z}^n$. We identify the fundamental domain of $\mathcal{M}\mathbf{Z}^n$ with $\mathcal{F} = \mathcal{M}[0,1)^n$. We cover $\mathcal{F}$ and cut it into parallelotopes. The facets of the parallelotopes are orthogonal to the axes of $H$. A different cutting

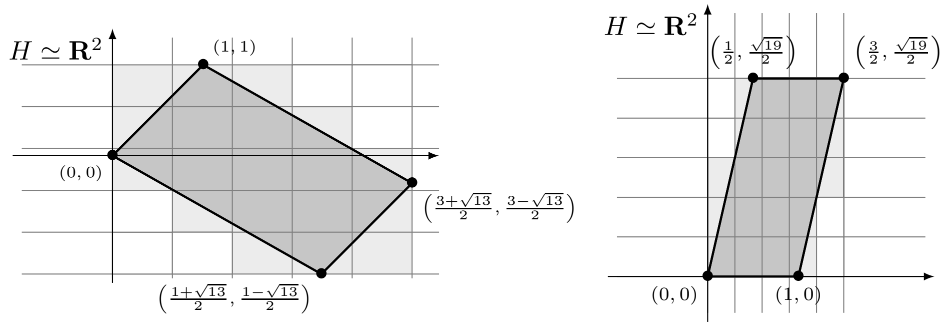



FIGURE 1. Example of covering and cutting of the fundamental domain: $K = \mathbf{Q}(\sqrt{13})$ and $K = \mathbf{Q}(\sqrt{-19})$.

was used by [4] to study cubic number fields. The one used here seems to be getting better results because it allows us to use an optimal test (see remark 2.8).

In practice, we apply an LLL-reduction (see [8, Section 2.6]) to $\mathcal{M}$ in order to control the size of coefficients of $\mathcal{M}$ and $\mathcal{M}^{-1}$ (see Section 5.2)

We show examples of covering and cutting of the fundamental domain for quadratic real and imaginary cases in Figure 1. Obviously, we keep only the parallelotopes which intersect the fundamental domain. Algorithm 2.2 sums up the data collected and the steps of this procedure.

**Algorithm 2.2** Initialisation of data

INPUT: a number field $K$ of degree $n$, a $n$-tuple $(N_i)_{1\leqslant i\leqslant n}$ of integers, $l$: the number of units we will use later

OUTPUT: matrix $\mathcal{M}$, the image by $\Phi$ of $l$ units, a list of parallelotopes which cover the fundamental domain $\mathcal{F}$

```
T ← ∅, compute the matrix M (2.a)
LLL-reduction of M
compute the embeddings of l units 𝔈 = {υ_1, ···, υ_l}
in each direction i, cut [a_i, b_i] (see (2.b)) into N_i segments (of same length) [c_i, d_i]
for each P = ∏_{i=1}^n [c_i, d_i] do
   if P ∩ F ≠ ∅ (see Lemma 3.3) then
      T ← T ∪ {P}
   end if
end for
return M, 𝔈, T
```

*Remark* 2.6. To perform computations in $H$, we use floating-point numbers, and an approximation of $\mathcal{M}$ is required.

2.2.2. *Absorption condition.* We choose $k > 0$ and we recall that the purpose is to know which points $x$ of $H$ satisfy $m_{\overline{K}}(x) < k$. To this end, we use the cutting described in 2.2.1. We choose a parallelotope $\mathcal{P}$ and we try to know if there exists some $z \in \Phi(\mathbf{Z}_K)$ such that for all $x \in \mathcal{P}$, $|\mathcal{N}(x-z)| < k$. In this case, we say that $\mathcal{P}$ is *absorbed* by $z$.

Each integer defines an open zone in which all points $x$ have an inhomogeneous minimum strictly smaller than $k$. In the real quadratic case, these zones are hyperbolic, in the imaginary quadratic case, they are disks, cf. Figure 2.

A parallelotope $\mathcal{P}$ is described by its *centre* $c = (c_1, \dots, c_n)$ and its *step* $h = (h_1, \dots, h_n) \in (\mathbf{R}_{>0})^n$:

$$\mathcal{P} = \left\{(x_1, \dots, x_n) \in H, \text{ for any } 1 \leqslant i \leqslant n, |c_i - x_i| \leqslant h_i\right\}.$$

**Proposition 2.7.** *The parallelotope $\mathcal{P}$ of centre $c = (c_1, \dots, c_n)$ and of step $h = (h_1, \dots, h_n)$ is absorbed by $z = (z_1, \dots, z_n)$ if*

$$\prod_{i=1}^{r_1} (|c_i - z_i| + h_i) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left( (|c_i - z_i| + h_i)^2 + (|c_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 \right) < k.$$

*Proof.* Let $x = (x_1, \dots, x_n)$ be a point of $\mathcal{P}$, fix an integer $1 \leqslant i \leqslant n$, then the triangle inequality implies $|x_i - z_i| \leqslant |c_i - z_i| + h_i$. Now, take $r_1 < i \leqslant r_1 + r_2$, then

$$(x_i - z_i)^2 + (x_{i+r_2} - z_{i+r_2})^2 \leqslant (|x_i - z_i| + h_i)^2 + (|x_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2.$$

Consequently, if the condition of Proposition 2.7 holds, the point $x$ is absorbed by $z$. □

*Remark* 2.8. The condition of Proposition 2.7 is optimal. Indeed, it is exactly the test $|\mathcal{N}(x-z)| < k$ where $x$ is some vertex of the parallelotope $\mathcal{P}$.

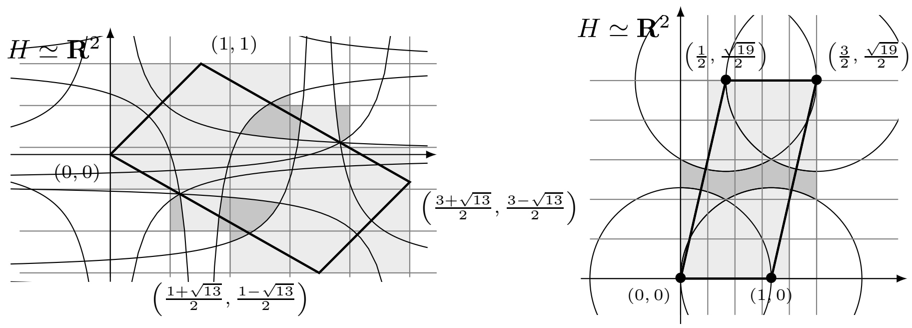
We choose a fixed list of integers $\mathcal{L}$ and we apply the test described in Proposition 2.7 for all parallelotopes and all elements of $\mathcal{L}$. All the parallelotopes which are not absorbed by integers are called *problematic*. Algorithm 2.3 tests if a parallelotope $\mathcal{P}$ can be absorbed by $\mathcal{L}$.

**Algorithm 2.3** Absorption test

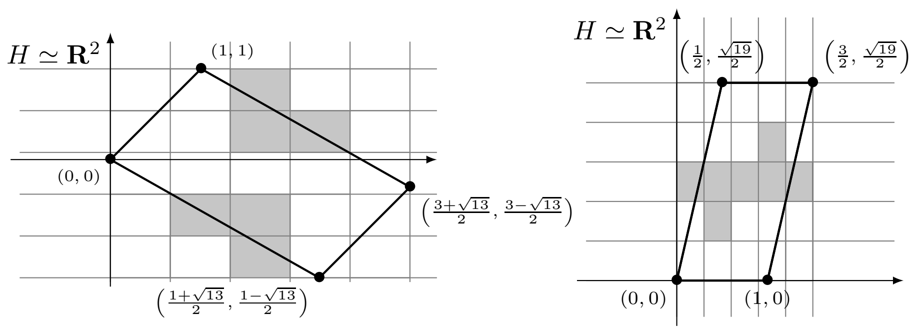
INPUT: a parallelotope $\mathcal{P}$ of centre $c$ and step $h$, a finite list $\mathcal{L} \subseteq \Phi(\mathbf{Z}_K)$, $k \in \mathbf{R}$.
OUTPUT: if $\mathcal{P}$ can be absorbed for $k$ by an element of $\mathcal{L}$.

**for** each element $z \in \mathcal{L}$ **do**
  $m \leftarrow \prod_{i=1}^{r_1} (|c_i - z_i| + h_i) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left( (|c_i - z_i| + h_i)^2 + (|c_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 \right)$
  **if** $m < k$ **then**
    **return true**
  **end if**
**end for**
**return false**

2.2.3. *Choice of integers.* We have to decide which integers are going to be used to absorb the parallelotopes. We choose some rational integer $B > 0$ and we compute $\mathcal{M}x$ for any vector $x \in \mathbf{Z}^n$ such that $\|x\|_\infty \leqslant B$. Ideally, $B$ must be chosen not too small as we want to absorb as many parallelotopes as possible, but not too big either, as we test the absorption by *all* these elements for a parallelotope $\mathcal{P}$ which cannot be absorbed.




(A) Domains absorbed by integers. In both cases, we use the four integers corresponding to the vertices of $\mathcal{F}$, but we can take other integers, especially in the real case.




(B) Problematic parallelotopes remaining, only totally covered parallelotopes are eliminated.

FIGURE 2. Absorption of parallelotopes by integers, $K = \mathbf{Q}(\sqrt{13})$ and $K = \mathbf{Q}(\sqrt{-19})$ for $k = \frac{1}{3}$ and $k = 1$ respectively. The choice of integers is crucial, for instance, in the first case, we could absorb more parallelotopes with more integers.

However, we can easily determine beforehand that some elements $\mathcal{M}x$ are useless for the absorption of parallelotopes. With the notation $\mathcal{M} = (m_{i,j})_{1 \leqslant i,j \leqslant n}$, let us put for any $i \in \{1, \ldots, n\}$,

$$a_i = \sum_{\substack{j=1 \\ m_{i,j} \leqslant 0}}^{n} m_{i,j} \qquad \text{and} \qquad b_i = \sum_{\substack{j=1 \\ m_{i,j} > 0}}^{n} m_{i,j}, \tag{2.b}$$

so that $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. Besides if for some $X = (X_i)_{1 \leqslant i \leqslant n} \in \Phi(\mathbf{Z}_K)$ and $x \in \mathcal{F}$, we have $|\mathcal{N}(x - X)| < k$, then there exists an integer $i \in \{1, \ldots, r_1 + r_2\}$ such that

$$\begin{cases} \text{either } 1 \leqslant i \leqslant r_1 \text{ and } X_i \in \left(a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}\right), \\ \text{or } r_1 < i \leqslant r_1 + r_2 \text{ and } \begin{cases} X_i \in \left(a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}\right), \\ X_{i+r_2} \in \left(a_{i+r_2} - k^{\frac{1}{n}}, b_{i+r_2} + k^{\frac{1}{n}}\right) \end{cases} \end{cases}. \tag{2.c}$$

These estimates may seem rough, but they are very useful in practice. We apply them in Algorithm 2.4.

**Algorithm 2.4** Computation of the list of integers

INPUT: the matrix $\mathcal{M}$, a bound $B$
OUTPUT: a list of elements of $\Phi(\mathbf{Z}_K)$ which may absorb parallelotopes

$\mathcal{L} \leftarrow \emptyset$
**for** each vector $Z \in \mathbf{Z}^n$ such that $-B \leqslant Z_i \leqslant B$ **do**
  compute $X = \mathcal{M}Z^n$
  **if** condition (2.c) is valid **then**
    $\mathcal{L} \leftarrow \mathcal{L} \cup \{X\}$
  **end if**
**end for**
**return** $\mathcal{L}$

### 2.3. Action of the units $\mathbf{Z}_K^\times$ on $K$.

2.3.1. *General ideas.* The purpose is to try to absorb problematic parallelotopes without using more integers. Let us choose a unit $\varepsilon$. We write $\nu = (\nu_i)_{1 \leqslant i \leqslant n} = \Phi(\varepsilon)$. In practice, we work directly with $\nu$, which is one the embeddings of the units precomputed in $\mathfrak{E}$ by Algorithm 2.2. We suppose that we have a cutting of the fundamental domain $\mathcal{F}$ into parallelotopes. Some of them are absorbed by integers, but not all of them. We consider a problematic parallelotope $\mathcal{P}$ and its image under the action of $\nu$:

$$\nu \cdot \mathcal{P} = \{\nu \cdot x,\, x \in \mathcal{P}\}.$$

We write $c$ for the centre of $\mathcal{P}$ and $h$ for the step of $\mathcal{P}$.

**Lemma 2.9.** *Let $c' = \nu \cdot c = (c'_i)_{1 \leqslant i \leqslant n}$, then $\nu \cdot \mathcal{P}$ is contained in the following domain:*

$$\mathcal{B} = \left\{ (x_i)_{1\leqslant i \leqslant n} \in H, \left\{ \begin{array}{l} \textit{for } 1 \leqslant i \leqslant r_1, |x_i - c'_i| \leqslant h'_i \\ \textit{for } r_1 < i \leqslant r_1 + r_2, (x_i - c'_i)^2 + (x_{i+r_2} - c'_{i+r_2})^2 \leqslant {h'_i}^2 \end{array} \right. \right\},$$

*where the $n$-tuple $h' = (h'_i)_{1 \leqslant i \leqslant n}$ is defined by*

$$h'_i = \left\{ \begin{array}{ll} h_i\,|\nu_i| & \textit{if } 1 \leqslant i \leqslant r_1, \\ \sqrt{(\nu_i^2 + \nu_{i+r_2}^2)(h_i^2 + h_{i+r_2}^2)} & \textit{if } r_1 < i \leqslant r_1 + r_2, \\ h'_{i-r_2} & \textit{if } r_1 + r_2 < i \leqslant n. \end{array} \right.$$

*Proof.* It is a straightforward verification. □

We want to know if for any $x \in \mathcal{P}$, there is some $z_x \in \Phi(\mathbf{Z}_K)$ such that $m_{\overline{K}}(\nu \cdot x - z_x) < k$. If we find such elements $z_x$, then we can discard $\mathcal{P}$, since for any $x \in \mathcal{P}$,

$$m_{\overline{K}}(x) = m_{\overline{K}}(\nu \cdot x - z_x).$$

However, we do not want to compute again many norms for a huge list of elements $z \in \Phi(\mathbf{Z}_K)$. Instead, we translate $\nu \cdot \mathcal{P}$ into the fundamental domain $\mathcal{F}$ and we see if it is contained in $\{x \in \mathcal{F},\, m_{\overline{K}}(x) < k\}$.

We suppose that $\{\mathcal{Q}_i,\, 1 \leqslant i \leqslant l\}$ is a covering of $\mathcal{F}$ such that for all $1 \leqslant i \leqslant l$, $\mathcal{Q}_i$ is a parallelotope of centre $c^{(i)}$ and of step $h^{(i)}$. We assume that there exists

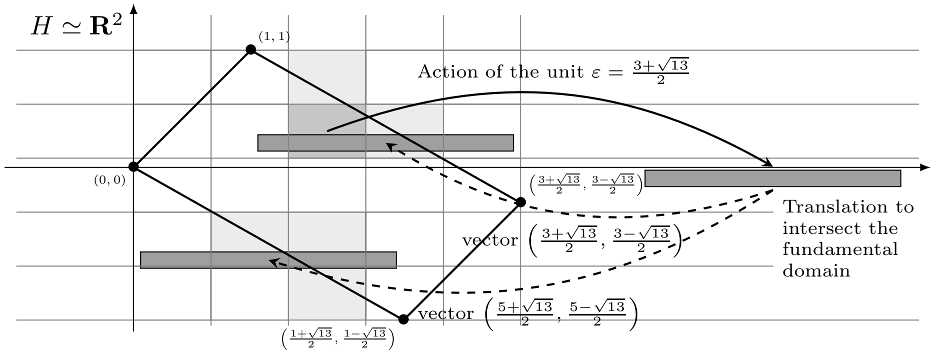



FIGURE 3. Action of the unit $\frac{3+\sqrt{13}}{2}$ on a problematic parallelotope. The two translates of the image in the fundamental domain intersect problematic parallelotopes, we keep this problem.

some integer $1 \leqslant m \leqslant l$ such that all parallelotopes $\mathcal{Q}_i$ for $m < i \leqslant l$ are absorbed by integers.

*Definition* 2.10. We call $z \in \Phi(\mathbf{Z}_K)$ a *translation vector* of $\mathcal{B}$ into $\mathcal{F}$ if we have $(\mathcal{B} - z) \cap \mathcal{F} \neq \emptyset$.

**Lemma 2.11.** *Let $\{z^{(j)}, 1 \leqslant j \leqslant k\} \subseteq \Phi(\mathbf{Z}_K)$ be the list of all possible translation vectors of $\mathcal{B}$ into $\mathcal{F}$. If for all $1 \leqslant j \leqslant k$, $1 \leqslant i \leqslant m$, $\left(\mathcal{B} - z^{(j)}\right) \cap \mathcal{Q}_i = \emptyset$, then $\mathcal{P}$ can be discarded from the list of problematic parallelotopes.*

The proof is obvious, but notice that we need to consider *all* translation vectors because a translate of $\mathcal{B}$ which intersects the fundamental domain is not necessarily included in the fundamental domain. Figure 3 shows an example of action of a unit in the quadratic real case: two translation vectors are possible. Both translates intersect the problematic parallelotopes.

Therefore, we are led to compute all translation vectors of $\mathcal{B}$ into $\mathcal{F}$.

2.3.2. *Translations into the fundamental domain.* Let us recall that we write $\mathcal{M} = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ and set $(a_i)_{1 \leqslant i \leqslant n}$ and $(b_i)_{1 \leqslant i \leqslant n}$ as in 2.2.3. With this notation, $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. Therefore, if $(\mathcal{B} - z) \cap \mathcal{F} \neq \emptyset$, then for all $1 \leqslant i \leqslant n$,

$$([c'_i - h'_i, c'_i + h'_i] - z_i) \cap [a_i, b_i] \neq \emptyset,$$

with the notation of Lemma 2.9. Consenquently, we get the following criterion.

**Lemma 2.12.** *Let $z \in H$ be a translation vector of $\mathcal{B}$ into $\mathcal{F}$. Then*

(1) *there exists $Z \in \mathbf{Z}^n$ such that $z = \mathcal{M}Z$,*
(2) *for all $1 \leqslant i \leqslant n$, $c'_i - b_i - h'_i \leqslant z_i \leqslant c'_i - a_i + h'_i$.*

Therefore, we can compute all translation vectors. Now, given such a vector $z$, we need a criterion to decide if $\mathcal{B} - z$ intersects the problematic parallelotope $\mathcal{Q}_j$, of centre $c^{(j)}$ and step $h^{(j)}$.

**Lemma 2.13.** *If $(\mathcal{B} - z) \cap \mathcal{Q}_j \neq \emptyset$, then for all $1 \leqslant i \leqslant n$,*

$$c'_i - c_i^{(j)} - h_i^{(j)} - h'_i \leqslant z_i \leqslant c'_i - c_i^{(j)} + h_i^{(j)} + h'_i. \tag{2.d}$$

*Proof.* It comes from the fact that for all $x \in \mathcal{B}$, for all $1 \leqslant i \leqslant n$, $|x_i - c'_i| \leqslant h'_i$. $\square$

With Lemma 2.12, we may find a set of vectors which strictly contains the translation vectors, however even if we use too many vectors, we can only discard non-problematic parallelotopes.

**Algorithm 2.5** Action of a unit to discard parallelotopes

INPUT: a list of problematic parallelotopes $\mathcal{T}$, an embedding of a unit $\nu \in \mathfrak{E} \subseteq \Phi(\mathbf{Z}_K^\times)$

OUTPUT: a list of problematic parallelotopes $\mathcal{T}' \subseteq \mathcal{T}$

$\mathcal{T}' \leftarrow \emptyset$, $\mathcal{T}_0 \leftarrow \mathcal{T}$
**while** $\#\mathcal{T}' < \#\mathcal{T}_0$ **do**
  **for** each $\mathcal{P} \in \mathcal{T}_0$ **do**
    compute the image $\mathcal{B}$ of $\mathcal{P}$ under the action of $\nu$ and a list $\mathcal{V}$ of all possible translation vectors of $\mathcal{B}$ into $\mathcal{F}$
    **for** each $v \in \mathcal{V}$ **do**
      **if** there exists $\mathcal{Q}_j \in \mathcal{T}_0$, such that for all $1 \leqslant i \leqslant n$ (2.d) holds **then**
        $\mathcal{T}' \leftarrow \mathcal{T}' \cup \{\mathcal{P}\}$
      **end if**
    **end for**
  **end for**
  **if** $\#\mathcal{T}' < \#\mathcal{T}_0$ **then**
    $\mathcal{T}_0 \leftarrow \mathcal{T}'$, $\mathcal{T}' \leftarrow \emptyset$
  **end if**
**end while**
**return** $\mathcal{T}'$

**Proposition 2.14.** *Algorithm 2.5 returns a list a parallelotopes $\mathcal{T}'$ such that for all $x \in \mathcal{F}$ such that $m_{\overline{K}}(x) \geqslant k$, there exists $\mathcal{P}' \in \mathcal{T}'$ such that $x \in \mathcal{P}'$.*

*Proof.* It is an easy consequence of Lemma 2.13. $\square$

We can repeat the procedure for every element of the set $\mathfrak{E}$, which was computed by Algorithm 2.2. We apply these tests until they no problematic parallelotopes are eliminated.

The absorption test and the test of units allow us to prove with a computer that $M(\overline{K}) < k$ for some given $k$. However, we would like to compute $M(K)$ exactly. To achieve this, we will use a value of $k$ for which not all parallelotopes are absorbed.

2.4. **Problematic parallelotopes and Euclidean minimum.** At this step, we suppose that for some $k > 0$, there remains $m$ problematic parallelotopes. Let us write them $\mathcal{Q}_i$ for $1 \leqslant i \leqslant m$. We choose a unit $\varepsilon$ which is not a root of unity and such that for all $1 \leqslant i \leqslant r_1 + r_2$,

$$|\sigma_i(\varepsilon)| \neq 1.$$

2.4.1. *Action of the units (revisited).* The action of $\varepsilon$ does not allow us to eliminate parallelotopes, because for all $1 \leqslant i \leqslant m$, there exists at least one translation vector $z \in \Phi(\mathbf{Z}_K)$ such that $(\varepsilon \cdot \mathcal{Q}_i - z) \cap \mathcal{Q}_j$ can be non-empty, for some problematic parallelotope $\mathcal{Q}_j$.

We construct a directed graph $\mathcal{G}$ whose vertices are the problematic parallelotopes $(\mathcal{Q}_i)_{1\leqslant i\leqslant m}$ and whose directed edges are

$$\mathcal{Q}_i \xrightarrow{z} \mathcal{Q}_j$$

if $(\varepsilon \cdot \mathcal{Q}_i - z) \cap \mathcal{Q}_j$ may be non-empty for some $z \in \Phi(\mathbf{Z}_K)$.

2.4.2. *Convenient graphs.*

*Definition* 2.15. A directed graph is called *convenient* if every infinite path is ultimately periodic or, equivalently, if its simple cycles are disjoint.

We assume that we can obtain a convenient graph $\mathcal{G}$ of problematic parallelotopes. We denote by $(\mathcal{C}_i)_{1\leqslant i\leqslant l}$ the simple cycles of $\mathcal{G}$.

To any simple cycle $\mathcal{C}$ of $\mathcal{G}$, the following theorem will associate a critical point $t_{\mathcal{C}} \in \Phi(K)$ such that for any element $x$ in the parallelotopes corresponding to the vertices of $\mathcal{C}$, $m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t_{\mathcal{C}})$ and $k < m_{\overline{K}}(t_{\mathcal{C}})$. As a result, we will be able to compute the Euclidean minimum of $K$, provided we can obtain a convenient graph.

**Theorem 2.16.** *Let $\mathcal{C}$ be a simple cycle of $\mathcal{G}$. We denote by $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ the vertices of $\mathcal{C}$ and $m$ elements $z_1 = \Phi(Z_1), \ldots, z_m = \Phi(Z_m)$ of $\Phi(\mathbf{Z}_K)$ such that*

$$\mathcal{C} = \begin{tikzcd} & \mathcal{Q}_2 \arrow[r, "z_2"] & \cdot \arrow[dr, bend left] & \\ \mathcal{Q}_1 \arrow[ur, bend left, "z_1"] & & & \vdots \arrow[dl, bend left] \\ & \mathcal{Q}_m \arrow[ul, bend left, "z_m"] & \cdot \arrow[l, "z_{m-1}"'] & \end{tikzcd}$$

*Then, if we define $\Omega_{\mathcal{C}} = \displaystyle\sum_{j=0}^{m} \varepsilon^j z_{m-j} \in \mathbf{Z}_K$, $\xi_{\mathcal{C}} = \dfrac{\Omega_{\mathcal{C}}}{\varepsilon^m - 1}$ and $t_{\mathcal{C}} = \Phi(\xi_{\mathcal{C}})$, we have for all $x \in Q_1$ such that $m_{\overline{K}}(x) > k$,*

*(1) $k < m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t_{\mathcal{C}})$,*
*(2) if $x \in \Phi(K)$, then $x = t_{\mathcal{C}}$.*

*Proof.* This a straightforward generalization of [7, Theorem 4.1]. □

**Theorem 2.17.** *We assume that the graph $\mathcal{G}$ is convenient. If $x \in K$ is such that $m_K(x) > k$, then there exist a simple cycle $\mathcal{C}$ of $\mathcal{G}$ and $\varepsilon \in \mathbf{Z}_K^\times$ such that $x \equiv \varepsilon\xi_{\mathcal{C}}$ $(\mathrm{mod}\ \mathbf{Z}_K)$.*

*Proof.* See [7, Theorem 4.5]. □

*Remarks* 2.18.
- In fact, if we apply the algorithm with the value $k$ and if the graph obtained is convenient, Theorem 2.17 allows us to find all elements $x \in K$ (modulo $\mathbf{Z}_K$) so that $m_K(x) > k$.
- In the examples considered, we can always find an initial cutting such that the graph is convenient.
- The fact that we deal with parallelotopes is irrelevant, consequently, we can merge parallelotopes to obtain a convenient graph. We will see how we proceed in practice in 3.2.2.

**Algorithm 2.6** Computation of the minimum associated to a cycle

INPUT: a simple cycle $\mathcal{C}$, a unit $\varepsilon$
OUTPUT: an orbit of points $\mathcal{O} \subseteq K$, $m_K(x)$ (for any $x \in \mathcal{O}$)
1: compute $\xi_{\mathcal{C}}$ (see Theorem 2.16), $\mathcal{O} \leftarrow \mathrm{Orb}\,(\xi_{\mathcal{C}})$ (see Section 3.2.4)
2: compute $m_K\,(\xi_{\mathcal{C}})$ with Algorithm 2.1
3: **return** $\mathcal{O}, m_K\,(\xi_{\mathcal{C}})$

## 3. Description of the algorithm

3.1. **General algorithm.** Now we can describe a general procedure to compute the Euclidean minimum of a number field $K$. At each step, we are considering three real numbers $k_0, k$ and $k_1$ such that

(1) $k_0 < k < k_1$,
(2) $M(K) < k_1$,
(3) probably, $k_0 < M(K)$.

Initially, we choose $k_0 < \frac{1}{\Lambda(K)}$ such that $k_0 < M(K)$ and $k_1 > M(K)$, then we apply the absorption and units tests for some $k$ such that $k_0 < k < k_1$. If they discard all problems, then $M(K) < k$, and we can start over with $k_1 = k$, else, we cannot be sure that $k < M(K)$. Nevertheless, we try to form a convenient graph. If this fails, we repeat the tests with $k_0 = k$ (so we know that *probably* $k_0 < M(K)$ but not definitely).

This procedure requires an initial value $\mathcal{K}$ for $k$. As the absorption test (Algorithm 2.3) can be very long if many problematic parallelotopes remain, we choose a "big" value for $\mathcal{K}$.

After this step, we fix a value of $k$ between $k_0$ and $k_1$. To achieve this, we choose $d \in (0, 1)$ and take $k = (1-d)k_0 + dk_1$. Again, we do not want $k$ to decrease too fast, so we choose $d$ closer to 1 (for instance $d = \frac{2}{3}$). The Euclidean minimum $M(K)$ may be equal to $\frac{1}{\Lambda(K)}$. In this case, we have to apply the procedure with $k < \frac{1}{\Lambda(K)}$ to prove it. That explains why we start with an initial $k_0 < \frac{1}{\Lambda(K)}$.

Then we determine a list $\mathcal{T}$ of problematic parallelotopes and we repeat the following loop:

- replace $\mathcal{T}$ by the list of parallelotopes obtained by cutting each parallelotope of $\mathcal{T}$ in two in each direction,
- try to reduce $\mathcal{T}$ with the absorption test,
- try to reduce $\mathcal{T}$ with the action of units.

We decide when we stop this loop as follows: we fix an integer $I$ and we ensure that we perform at most $I$ consecutive cuttings without improving the smallest number of problematic parallelotopes found at the end of the loop. In practice, we choose $I = 5$.

Afterwards, we try to build a convenient graph for the smallest list of problematic parallelotopes found. If we succeed for the value $k$, we can use the upper bound $k_1$ of $M(K)$ to compute the local Euclidean minimum of points associated to the simple cycles. If the greatest value found is greater than $k$, then it is $M(K)$. In the other case, we start over with $k = m - \eta$ for some small $\eta$. Besides, if at any step we obtain $k_1 < 1$, then we can conclude that $K$ is norm-Euclidean.

**Algorithm 3.1** General algorithm for computing the Euclidean minimum

INPUT: an irreducible polynomial $p \in \mathbf{Z}[X]$ (defining the number field $K$)
OUTPUT: $M(K)$ or failure

1: initialisation of data $\rightarrow$ matrix $\mathcal{M}$, list of parallelotopes $\mathcal{T}$, list of embbeddings of units $\mathfrak{E} = \{\upsilon_1, \dots, \upsilon_l\}$ (Algorithm 2.2 )
2: computation of a list of integers $\mathcal{L}$ (Algorithm 2.4)
3: $k_0 \leftarrow \texttt{0.9} \cdot \frac{1}{\Lambda(K)}$, $k \leftarrow \mathcal{K}$, $k_1 \leftarrow \infty$, $i \leftarrow 0$,
4: **for** each unit $\nu \in \mathfrak{E}$ **do**
5:     $\mathcal{T} \leftarrow$ action of the unit $\nu$ on $\mathcal{T}$ (Algorithm 2.5)
6: **end for**
7: $\mathcal{T}_{\min} \leftarrow \mathcal{T}$
8: **repeat**
9:     $\mathcal{T} \leftarrow$ list obtained by cutting each $\mathcal{P} \in \mathcal{T}$ in two in each direction $1 \leqslant i \leqslant n$
10:     **for** each parallelotope $\mathcal{P} \in \mathcal{T}$ **do**
11:         **if** $\mathcal{P}$ can be absorbed for $k$ by $\mathcal{L}$ (Algorithm 2.3) **then**
12:             $\mathcal{T} \leftarrow \mathcal{T} \setminus \mathcal{P}$ (Algorithm 2.5)
13:         **end if**
14:     **end for**
15:     **for** each unit $\nu \in \mathfrak{E}$ **do**
16:         $\mathcal{T} \leftarrow$ action of the unit $\nu$ on $\mathcal{T}$ (Algorithm 2.5)
17:     **end for**
18:     **if** $\#\mathcal{T}_{\min} < \#\mathcal{T}$ **then**
19:         $i \leftarrow i + 1$
20:     **else**
21:         $\mathcal{T}_{\min} \leftarrow \mathcal{T}$
22:     **end if**
23: **until** $\mathcal{T} = \emptyset$ **or** $i > I$
24: **if** $\mathcal{T} = \emptyset$ **then**
25:     $k_1 \leftarrow k$, $k \leftarrow (1-d) \cdot k_0 + d \cdot k$, $i \leftarrow 0$, $\mathcal{T}_{\min} \leftarrow \mathcal{T}$, **go to** step 8
26: **end if**
27: choose $\nu \in \mathcal{E}$ and compute the graph $\mathcal{G}$ associated to the action of $\nu$ on $\mathcal{T}_{\min}$
28: **if** $\mathcal{G}$ is convenient **then**
29:     **for** each simple cycle $\mathcal{C}$ of $\mathcal{G}$ **do**
30:         compute the orbit $\mathcal{O}_{\mathcal{C}}$ and the minimum $m_{\mathcal{C}}$ (Algorithm 2.6)
31:     **end for**
32:     $m \leftarrow \max_{\mathcal{C}} m_{\mathcal{C}}$
33:     **if** $m > k$ **then**
34:         **return** $m$ and the orbits associated
35:     **else**
36:         $k \leftarrow m - \eta$, **go to** step 8
37:     **end if**
38: **else**
39:     **if** $k_1 - k_0 < \epsilon$ **then**
40:         **return** failure
41:     **else**
42:         $k_0 \leftarrow k$, $k \leftarrow \min\left\{\frac{k+k_1}{2}, k+2\right\}$, $i \leftarrow 0$, **go to** step 8
43:     **end if**
44: **end if**

**Theorem 3.1.** *Algorithm 3.1 computes the Euclidean minimum of $K$ and the critical points when it does not return* failure.

*Remark* 3.2. The procedure may fail when we do not succeed in building a convenient graph. In this case, there is a threshold $k_2$ such that

- for $k > k_2$, all problems are absorbed,
- for $k < k_2$, some problems remain and no convenient graph is found.

Then $k_0$ and $k_1$ will be close to $k_2$. To prevent the procedure from never ending, we fix $\epsilon > 0$ such that if $k_1 - k_0 < \epsilon$, then we stop the procedure and say that the algorithm fails. In practice, $\epsilon$ is equal to the precision of the absorption test (see Table 6).

In the rare cases where Algorithm 3.1 returns *failure*, we cut more initially in each direction in Algorithm 2.2 and we increase the size of the list of integers $\mathcal{L}$ in Algorithm 2.4. Generally, it allows a further running of Algorithm 3.1 to be successful.

In fact, if the unit rank is strictly greater than 1 and $K$ is not a CM-field, then the results of [5, Proposition 4.25] can be extended to the general case: if our cutting is sharp enough and if we use enough integers, we will obtain a convenient graph. Nevertheless, this property is not effective: we do not know which parameters will give such a result and we do not take into account the precision problems.

Besides, this theoretical argument is no longer valid for $r = 1$, but it turns out that Algorithm 3.1 is successful, even when there are infinitely many points $x \in H \setminus \Phi(K)$ modulo $\Phi(\mathbf{Z}_K)$ with $m_{\overline{K}}(x) = M(\overline{K}) = M(K)$: see the example $K = \mathbf{Q}(\sqrt{13})$ described in [7, Section 5.10].

## 3.2. **Practical aspects.**

### 3.2.1. *Covering of the fundamental domain and cuttings.*

*Covering of the fundamental domain.* Let us write $\mathcal{M}$, $(a_i)_{1\leqslant i\leqslant n}$ and $(b_i)_{1\leqslant i\leqslant n}$ as in Section 2.2.3. Then $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. Let us assume the parallelotope $\mathcal{P}$ of centre $c = (c_i)_{1\leqslant i\leqslant n}$ and of step $h = (h_i)_{1\leqslant i\leqslant n}$ is such that $\mathcal{P} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. We keep $\mathcal{P}$ if and only if $\mathcal{P} \cap \mathcal{F} \neq \emptyset$. As $\Phi$ is a bijection, that is equivalent to $\Phi^{-1}(\mathcal{P}) \cap [0,1)^n \neq \emptyset$.

By definition, for all $(x_i)_{1\leqslant i\leqslant n} \in \mathcal{P}$, $1 \leqslant i \leqslant n$, $c_i - h_i \leqslant x_i \leqslant c_i + h_i$. We write $\mathcal{M}^{-1} = \left(m'_{i,j}\right)_{1\leqslant i,j\leqslant n}$. Then for all $(x_i)_{1\leqslant i\leqslant n} \in \mathcal{P}$,

$$\sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j + h_j) + \sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j - h_j) \leqslant \sum_{j=1}^{n} m'_{i,j} x_j,$$

$$\text{and } \sum_{j=1}^{n} m'_{i,j} x_j \leqslant \sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j - h_j) + \sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j + h_j).$$

Therefore, we immediately obtain the following result.

**Lemma 3.3.** *If $\mathcal{P} \cap \mathcal{F} \neq \emptyset$, then* $\displaystyle\sum_{\substack{j=1 \\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j + h_j) + \sum_{\substack{j=1 \\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j - h_j) \leqslant 1$ *and*

$$\sum_{\substack{j=1 \\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j - h_j) + \sum_{\substack{j=1 \\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j + h_j) \geqslant 0.$$

*Initial cutting*. For any direction $1 \leqslant i \leqslant n$, we choose a positive integer $N_i$ and we cut $\mathcal{F}$ into $N_i$ parts in the direction $i$. As seen in Figure 2, the cutting must be quite sharp in order to absorb parallelotopes. We get rid of the parallelotopes which do not intersect $\mathcal{F}$ with Lemma 3.3. Besides, as we can notice in Figure 3, the action of units is different according to the coordinates. Therefore, it can be interesting to cut more precisely in the directions corresponding to "big" coordinates of the embedding of the unit.
*Further cutting*. We cut each parallelotope in two in each direction, the number of problematic parallelotopes is at most multiplied by $2^n$, however after absorption by integers and action of the units, we expect the number of problematic parallelotopes not to grow. Once again, we discard parallelotopes which do not intersect $\mathcal{F}$ thanks to Lemma 3.3.

3.2.2. *Simplification of the graph.* For the construction described in 2.4.2, the fact that we deal with parallelotopes is not important, we can merge some parallelotopes and Theorem 2.17 still holds. To identify convenient graphs, we can do some simplifications of the graph $\mathcal{G}$.

First we can get rid of some useless vertices. Indeed, if a vertex $\mathcal{V}$ is not reached by any edge, we can discard it from the list of vertices.

*Definition* 3.4. Let $\mathcal{V}$ and $\mathcal{V}'$ be two vertices of the graph $\mathcal{G}$. $\mathcal{V}$ is said to be *compatible* with $\mathcal{V}'$ if for any edge $\mathcal{V} \xrightarrow{a} \mathcal{X}$, there exists an edge $\mathcal{V}' \xrightarrow{a} \mathcal{X}$.

Now, if the vertex $\mathcal{V}$ is compatible with $\mathcal{V}'$, we merge $\mathcal{V}$ and $\mathcal{V}'$ into a new vertex $\mathcal{W}$ such that

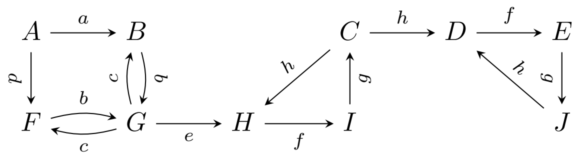
$$\begin{cases} \mathcal{U} \xrightarrow{c} \mathcal{W} & \text{if } \mathcal{U} \xrightarrow{c} \mathcal{V} \text{ or } \mathcal{U} \xrightarrow{c} \mathcal{V}', \\ \mathcal{W} \xrightarrow{d} \mathcal{X} & \text{if } \mathcal{V}' \xrightarrow{d} \mathcal{X}. \end{cases}$$

Then we consider the vertices from which at least two edges are starting. Let $\mathcal{V}$ be such a vertex. We denote by $\mathcal{V} \xrightarrow{a_i} \mathcal{W}_i$ for $1 \leqslant i \leqslant l$ the egdes starting from $\mathcal{V}$. For $1 \leqslant i \neq j \leqslant l$, we merge $\mathcal{W}_i$ and $\mathcal{W}_j$ if $a_i = a_j$. Obviously, we obtain a new vertex $\mathcal{W}_{i,j}$ whose edges are obtained by merging of the edges of $\mathcal{W}_i$ and $\mathcal{W}_j$.

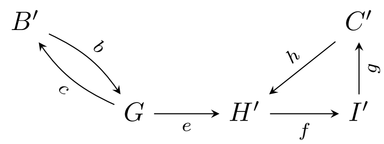
These simplifications are illustrated by Figure 4.

Finally, to check if the simplified graph is convenient, we compute its strongly connected components (using for instance Tarjan's algorithm, [17]) and check that they are cycles. In this case, we also get the simple cycles of the graph.

3.2.3. *Translations of the fundamental domain.* In some cases, the Euclidean minimum can be reached at points which are on the edge of the fundamental domain. For instance, for $K = \mathbf{Q}(\sqrt{13})$, $M(K) = m_K\left(\frac{\pm 1+\sqrt{13}}{6}\right) = m_K\left(\frac{\pm 1+\sqrt{13}}{3}\right) = \frac{1}{3}$. Two of the four critical points in $K$ are close to the edge of the fundamental domain used in Figure 2. Consequently, a problematic point and its translate by a vector in $\Phi(\mathbf{Z}_K)$ may be contained in the covering of the fundamental domain. If this happens, we cannot obtain a convenient graph.



(A) Initial graph which is not convenient, there is an infinite path between $B$ and $F$ (through $G$) which is not ultimately periodic.



(B) We can delete vertex $A$ which is not reached and merge $B$ and $F$, which are compatible. Further simplications can be performed on the right-hand side of the graph to merge the two three-cyles. The new graph is convenient.

FIGURE 4. Example of simplification of a graph to make it convenient.

Therefore, we translate the covering of the fundamental domain to avoid this situation: in the directions where problematic parallelotopes are close to the edge, we translate by $-\eta$ where $\eta > 0$. The domain considered will still contain a fundamental domain, but will not contain two critical points which are translates of each other by a vector of $\Phi(\mathbf{Z}_K)$.

3.2.4. *Computation of the orbit of a point.* Given a point $\xi \in K$, we want to compute the finite set $\mathrm{Orb}(\Phi(x))$. In practice, the computations are performed with elements of $K$, so we compute with elements of $K$ of coordinates in $\mathbf{Q} \cap [0, 1)$ in the basis $(z_i)_{1 \leqslant i \leqslant n}$ of $\mathbf{Z}_K$. Let us write this reduction as

$$\left\{ \begin{array}{ccc} K & \longrightarrow & K \\ x = \sum_{i=1}^{n} q_i z_i & \longmapsto & \overline{x} = \sum_{i=1}^{n} \left(q_i - \lfloor q_i \rfloor\right) z_i \end{array} \right. .$$

Then, we want to compute $\mathcal{O} = \left\{ \overline{\varepsilon \cdot \xi}, \, \varepsilon \in \mathbf{Z}_K^\times \right\}$. We denote by $(\varepsilon_i)_{1 \leqslant i \leqslant r}$ the fundamental units of $K$ and by $\nu$ a generator of the roots of unity of $K$. We suppose that the order of $\nu$ is $l$. For any $1 \leqslant i \leqslant r$, there exists a positive integer $m$ such that $\overline{\varepsilon_i}^m \cdot \overline{\xi} = \overline{\xi}$ (Lemma 2.1), we write $l_i$ the smallest such element.

With this notation, it is easy to see that

$$\mathcal{O} = \left\{ \overline{\nu}^m \cdot \prod_{i=1}^{r} \overline{\varepsilon_i}^{m_i} \cdot \overline{\xi}, \, 0 \leqslant m < l, \text{ for any } 1 \leqslant i \leqslant n, \, 0 \leqslant m_i < l_i \right\}.$$

We use this description of $\mathcal{O}$ to compute it.

3.2.5. *Implementation.* The general algorithm is written in `C` and is available at [16]. Exact computations involve the PARI library ([18]). With the tricks described in Section 3.2.2, Algorithm 3.1 can compute the Euclidean minimum of a number field of degree at most 8 and of small discriminant given simply its minimal polynomial. For greater degrees, lack of precision (see 5.1) and time of execution (see 5.3) make the application of Algorithm 3.1 harder.

3.3. **Example.** The algorithm runs as follows.

We consider $p(x) = x^4 - x^3 + 2x^2 - 6x + 3$, $\alpha$ a root of $p$ and $K = \mathbf{Q}(\alpha)$. Then $n = 4$, $r_1 = 2$, $r_2 = 1$, $d(K) = -8787$, $\Lambda(K) = 3$, $K$ is principal.

With such an input, we obtain an LLL-reduced matrix $\mathcal{M}$ as defined in (2.a).

| value of $k$ | 3 | 2.1 | 1.5 | 1.1 | 0.83 | 0.66 | 0.54 | 0.46 |
|---|---|---|---|---|---|---|---|---|
| after the initial cutting | 0 | 0 | 0 | 0 | 4 | 256 | 2384 | 7908 |
| after the first action of units | – | – | – | – | 0 | 38 | 522 | 5028 |
| after the second cutting | – | – | – | – | – | 0 | 64 | 4092 |
| after the second action of units | – | – | – | – | – | – | 22 | 1076 |
| after the third cutting | – | – | – | – | – | – | 34 | 1174 |
| after the third action of units | – | – | – | – | – | – | 0 | 426 |
| after the fifth cutting and action of units | – | – | – | – | – | – | – | 322 |

TABLE 1. Problematic parallelotopes in the different steps of the execution of Algorithm 3.1.

We choose the initial value $\mathcal{K} = \mathtt{3}$ and we decide to use for $\mathcal{L}$ all useful integers $\mathcal{M}Z$, where $Z = (Z_i)_{1\leqslant i\leqslant 4} \in \mathbf{Z}^4$ and $\max_{1\leqslant i\leqslant 4} |Z_i| \leqslant 25$. There are 1520365 such vectors ($\simeq 22\%$ of $51^4$). Table 1 presents the number of problematic parallelotopes remaining at each step of the algorithm according to the value of $k$. For $k = \mathtt{0.46}$, we obtain 322 problematic parallelotopes in the best case.

After simplification, we obtain the following convenient graph with 8 vertices. The elements written $(z_i)_{1\leqslant i\leqslant 6} \subseteq \Phi(\mathbf{Z}_K)$ are explicit.

$$\begin{tikzcd} 0 \arrow[r, bend left, "z_1"] & 1 \arrow[d, bend left, "z_2"] \\ 2 \arrow[u, bend left, "z_4"] & 3 \arrow[l, bend left, "z_3"] \end{tikzcd} \qquad \begin{tikzcd} 4 \arrow[r, bend left, "z_5"] & 5 \arrow[d, bend left, "z_2"] \\ 6 \arrow[u, bend left, "z_6"] & 7 \arrow[l, bend left, "z_4"] \end{tikzcd}$$

We associate the point $t = \frac{16}{41}\alpha^3 + \frac{21}{41}\alpha^2 + \frac{37}{41}\alpha + \frac{28}{41} \in K$ to the first cycle. The orbit $\mathrm{Orb}(\Phi(t))$ has eight elements, including the point associated to the other cycle. As a result, $M(K) = m_K(t) = \frac{21}{41}$ and this minimum is reached at eight points of $K$ (modulo $\mathbf{Z}_K$).

This example was tested on an Intel®Xeon®CPU X5570 @ 2.93GHz (with 4 cores). The Euclidean minimum was computed in 7 minutes and 13 seconds.

## 4. Results obtained

Algorithm 3.1 was used to compute many Euclidean minima. Many values were already known and listed in [13], which enabled us to test the correctness of the algorithm.

4.1. **General observations.** The number fields of degree less than 8 of "small" discriminant are norm-Euclidean and their minimum is $\frac{1}{\Lambda(K)}$. Besides, as the degree grows, more examples of number fields with such a property are known.

4.2. **Cyclotomic fields.** With the algorithm, we can compute some previously unknown values of Euclidean minima of cyclotomic fields. Let $n$ be a positive integer such that $n \not\equiv 2 \mod 4$, we denote $K_n = \mathbf{Q}(\zeta_n)$, where $\zeta_n$ is a primitive $n^{\text{th}}$ root of unity.

Table 2 lists all known values of $M(K_n)$. They correspond to the cases when the cyclotomic polynomial is of degree at most 8. In all these cases, the Euclidean minimum coincides with $\frac{1}{\Lambda(K)}$. The bold values were unknown.

| $n$ | 1 | 3 | 4 | ***5*** | ***7*** | 8 | ***9*** | 12 | ***15*** | ***16*** | ***20*** | ***24*** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $M(K_n)$ | $\frac{1}{2}$ | $\frac{1}{3}$ | $\frac{1}{2}$ | $\mathbf{\frac{1}{5}}$ | $\mathbf{\frac{1}{7}}$ | $\frac{1}{2}$ | $\mathbf{\frac{1}{3}}$ | $\frac{1}{4}$ | $\mathbf{\frac{1}{16}}$ | $\mathbf{\frac{1}{2}}$ | $\mathbf{\frac{1}{5}}$ | $\mathbf{\frac{1}{4}}$ |

TABLE 2. Values of Euclidean minimum of some cyclotomic fields.

### 4.3. **Successive minima.**

*Definition* 4.1. We can define further Euclidean minima and inhomogeneous minima. If we put $M_1(K) = M_1\left(\overline{K}\right) = M(K) = M\left(\overline{K}\right)$, then we define by induction for any $p > 1$ the $p^{\text{th}}$ Euclidean and inhomogeneous minima by

$$\begin{cases} M_p(K) = \sup\left\{m_K(\xi),\, \xi \in K,\, m_K(\xi) < M_{p-1}(K)\right\}, \\ M_p\left(\overline{K}\right) = \sup\left\{m_{\overline{K}}(x),\, x \in H,\, m_{\overline{K}}(x) < M_{p-1}\left(\overline{K}\right)\right\}. \end{cases}$$

As in the case of the first minimum, we have some precise link between these notions in most cases (cf. [6]).

**Theorem 4.2.** *If $r > 1$ and $K$ is not CM, then, for all $p > 0$,*
*(1) $M_p(K) = M_p\left(\overline{K}\right) \in \mathbf{Q}$,*
*(2) $M_{p+1}(K) < M_p(K)$,*
*(3) in particular, $M(\overline{K})$ is isolated, that is to say $M_2\left(\overline{K}\right) < M\left(\overline{K}\right)$.*
*(4) $\lim_{p\to+\infty} M_p(K) = 0$.*

In the other cases and in particular when $r = 1$, (3) is conjectured to hold.

With Algorithm 3.1, we may try to compute $M_p(K)$, for some values of $p > 0$. To achieve this, we choose $k > 0$. If the execution of the algorithm succeeds, we find a convenient graph, from which we deduce all points $x \in K$ such that $m_K(x) \geqslant k$ (thanks to Theorem 2.17).

*Example* 4.3. Let us consider the cubic number field of mixed signature $K = \mathbf{Q}(\alpha)$ where $\alpha = \sqrt[3]{-7}$. We apply the Algorithm 3.1 for $k = 2.39$, we obtain the following three orbits of critical points.

- $\mathcal{O}_1 = \left\{\frac{2}{5}x^2 + \frac{1}{5}x - \frac{2}{5}, \frac{3}{5}x^2 + \frac{4}{5}x - \frac{3}{5}\right\}$ of minimum $\frac{12}{5}$,
- $\mathcal{O}_2 = \left\{\frac{11}{20}x^2 + \frac{13}{20}x - \frac{1}{20}, \frac{9}{20}x^2 + \frac{7}{20}x + \frac{1}{20}\right\}$ of minimum $\frac{49}{20}$,
- $\mathcal{O}_3 = \left\{\frac{1}{2}x^2 + \frac{1}{2}x - \frac{1}{2}\right\}$ of minimum $\frac{5}{2}$.

As a result, $M(K) = M\left(\overline{K}\right) = \frac{5}{2}$, $M_2(K) = \frac{49}{20}$, $M_3(K) = \frac{12}{5}$.

4.4. **Principal and non-norm-Euclidean number fields.** For small degrees, we can compute extensive values of Euclidean minima for small discriminants. This allows us to find principal and non-norm-Euclidean number fields. Here, we list in Table 3 principal and non-norm-Euclidean number fields of small discriminant. In fact, if the signature is different from $(6,0)$, $(4,1)$ and $(2,2)$, then the table provides such a number field of smallest discriminant (in absolute value).

Consequently, all principal number fields of such signature whose discriminant is smaller than the discriminant given (in absolute value) are in fact norm-Euclidean.

4.5. **Non-norm-Euclidean number fields with unit rank 1 of minimum 1.** If we assume that the signature $(r_1, r_2) \notin \{(1,1),(0,2)\}$, then $M(K) = 1$ implies that $K$ is not norm-Euclidean. In the other cases, we can list some examples of number fields whose Euclidean minimum is 1. All of these are not norm-Euclidean.

| $n$ | $(r_1, r_2)$ | a minimal polynomial such that $K = \mathbf{Q}(x)$ | $d(K)$ | $M(K)$ | critical point(s) |
|---|---|---|---|---|---|
| 2 | $(2,0)$ | $x^2 - 53$ | 53 | $\frac{9}{7}$ | $\left\{\frac{2x+3}{7}, \frac{3x+1}{14}\right\}$ |
| | $(0,1)$ | $x^2 + 19$ | $-19$ | $\frac{25}{19}$ | $\left\{\frac{5}{19}x, \frac{14}{19}x\right\}$ |
| 3 | $(3,0)$ | $x^3 - x^2 - 6x + 1$ | 985 | 1 | $\left\{\frac{2x^2+x+2}{5}, \frac{3x^2+4x+3}{5}\right\}$ |
| | $(1,1)$ | $x^3 - x^2 + 4x - 1$ | $-199$ | 1 | $\left\{\frac{3x^2+x+4}{7}, \frac{4x^2+6x+3}{7}\right\}$ |
| 4 | $(4,0)$ | $x^4 - 12x^2 + 18$ | 18432 | $\frac{7}{4}$ | $\left\{\frac{x^3+x^2}{6}\right\}$ |
| | $(2,1)$ | $x^4 - x^3 - 5x + 1$ | $-4564$ | 1 | $\left\{\frac{x^2+x+1}{2}\right\}$ |
| | $(0,2)$ | $x^4 - 4x^2 + 5$ | 1280 | $\frac{5}{4}$ | $\left\{\frac{x^3+x}{2}\right\}$ |
| 5 | $(5,0)$ | $x^5 - 10x^3 - 5x^2 + 10x - 1$ | 390625 | $\frac{7}{5}$ | $\left\{\frac{3x^4+3x^3+3x^2+3x+3}{5}, \frac{9x^4+29x^3+19x^2+24x+4}{35}\right\}$ |
| | $(3,1)$ | $x^5 - x^4 - 4x^3 + 6x^2 + 3x - 7$ | $-156848$ | $\frac{5}{4}$ | $\left\{\frac{x^4+x^3+x^2+x}{2}\right\}$ |
| | $(1,2)$ | $x^5 + 2x^3 - x^2 + 2x + 1$ | 36025 | 1 | $\left\{\frac{2x^4+2x^3+x^2+4x+3}{5}, \frac{3x^4+3x^3+4x^2+x+2}{5}\right\}$ |
| 6 | $(6,0)$ | $x^6 - 12x^4 - 2x^3 + 36x^2 + 12x - 20$ | 108020304 | $\frac{16}{9}$ | $\left\{\frac{x^5+2x^3+2x^2+1}{3}, \frac{x^5+2x^3+2x^2+4}{6}\right\}$ |
| | $(4,1)$ | $x^6 - 2x^5 - 9x^4 + 18x^3 + 13x^2 - 48x + 17$ | $-10163456$ | $\frac{5}{4}$ | $\left\{\frac{17x^5+6x^4+12x^3+6x^2+17x+16}{18}\right\}$ |
| | $(2,2)$ | $x^6 - 2x^5 - 4x^4 + 6x^3 + 6x^2 + 11x - 27$ | 1281013 | 1 | $\left\{\frac{59x^5+14x^4+53x^3+4x^2+30x+56}{69}, \frac{56x^5+9x^4+62x^3+42x^2+7x+13}{69}\right\}$ |
| | $(0,3)$ | $x^6 + x^4 - x^3 + 2x^2 + x + 1$ | $-165611$ | 1 | $\left\{\frac{3x^5+2x^4+x^3+x^2+3}{5}, \frac{2x^5+3x^4+4x^3+4x^2+3}{5}\right\}$ |

TABLE 3. Principal and non-norm-Euclidean number fields of small discriminant for a given signature. All the number fields listed here have a unique critical orbit.

*Example* 4.4. The cubic number fields of discriminant $-199$, $-335$, $-351$, $-367$, $-755$ have an Euclidean minimum equal to 1. Besides, there are at least 27 number fields of signature $(0,2)$ which have an Euclidean minimum equal to 1.

4.6. **Two-stage Euclideanity and Generalized Euclideanity.** Several notions were introduced to generalize Euclideanity. In this paragraph, we present two of them and show how Algorithm 3.1 can help us tackle these notions.

4.6.1. *Two-stage norm-Euclideanity.* Cooke introduced this generalization of Euclideanity in [9].

*Definition* 4.5. We say that $\mathbf{Z}_K$ is *two-stage norm-Euclidean* if for any $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, either there exists $(\gamma_1, \delta_1) \in \mathbf{Z}^2$ such that $\alpha - \beta\gamma_1 = \delta_1$ and $\left|\mathbf{N}_{K/\mathbf{Q}}(\delta_1)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, or there exists $(\gamma_1, \gamma_2, \delta_1, \delta_2) \in \mathbf{Z}_K^4$ such that

$$\left\{ \begin{array}{ccc} \alpha - \beta\gamma_1 & = & \delta_1, \\ \beta - \delta_1\gamma_2 & = & \delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \end{array} \right.$$

Clearly, if $K$ is norm-Euclidean, then it is also two-stage norm-Euclidean. Besides, any two-stage norm-Euclidean number field is principal.

To prove that a number field is two-stage norm-Euclidean, it is enough to

- compute all points $x \in K$ modulo $\mathbf{Z}_K$ such that $m_K(x) \geqslant 1$,
- choose one such point $x = \frac{\alpha}{\beta}$ where $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ by orbit and find a two-stage Euclidean division for $(\alpha, \beta)$. The existence of such a division is independent of the choice of $x$ and of $(\alpha, \beta)$.

*Example* 4.6. Let $K = \mathbf{Q}(s)$ where $s$ is a root of $X^3 - X^2 + 3X + 2$. Then $d(K) = -307$ and for any $t \in K$, $m_K(t) \geqslant 1$ if and only if $t \equiv \frac{1}{2}s^2 + \frac{1}{2} \mod \mathbf{Z}_K$. We consider $x = \frac{s^2+1}{2}$ and we have

$$\begin{cases} s^2 + 1 - 2(-s) & = & (s+1)^2, \\ 2 - (s+1)^2 \cdot (s^2 - 5s + 6) & = & 8s^2 - 11s - 8, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(8s^2 - 11s - 8)\right| = 2 & < & 8 = \left|\mathbf{N}_{K/\mathbf{Q}}(2)\right|. \end{cases}$$

This proves that $K$ is two-stage norm-Euclidean.

In some cases, if we know the critical points, it is not required to exhibit an explicit two-stage Euclidean division.

**Proposition 4.7.** *If $K$ is principal, $M(K) \geqslant 1$ and $K$ admits only one orbit of minimum greater than or equal to $\frac{1}{M(K)}$, then $K$ is two-stage norm-Euclidean.*

*Proof.* Let us write $\mathcal{O}$ the critical orbit and take $\frac{\alpha}{\beta} \in \mathcal{O}$, where $\alpha, \beta \in \mathbf{Z}_K \setminus \{0\}$ are coprime (this is possible as $K$ is principal). There exists $(\gamma, \tau) \in \mathbf{Z}_K \times \mathbf{Z}_K$ such that $\alpha - \beta\gamma = \tau$ and $\left|\mathbf{N}_{K/\mathbf{Q}}(\tau)\right| = M(K) \cdot \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$. Now, either $m_K\left(\frac{\beta}{\tau}\right) < \frac{1}{M(K)} = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(\tau)\right|}$ or $m_K\left(\frac{\beta}{\tau}\right) \geqslant \frac{1}{M(K)}$.

In the first case, there exists $\gamma \in \mathbf{Z}_K$ such that $\left|\mathbf{N}_{K/\mathbf{Q}}(\beta - \tau\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, which provides a two-stage division for $(\alpha, \beta)$.

In the latter case, as there is only one orbit of minimum greater than or equal to $\frac{1}{M(K)}$, $\frac{\beta}{\tau} \in \mathcal{O}$ and $m_K\left(\frac{\beta}{\tau}\right) = M(K)$. Consequently, there exist $\varepsilon \in \mathbf{Z}_K^\times$ and $z \in \mathbf{Z}_K$ such that

$$\frac{\beta}{\tau} = \varepsilon \cdot \frac{\alpha}{\beta} - z.$$

This implies that $\beta$ divides $\tau(\varepsilon\alpha - \beta z)$, so $\beta$ divides $\tau\alpha$ and then $\tau$. Therefore, we may write $\frac{\beta}{\tau} = \frac{1}{\kappa}$ where $\kappa \in \mathbf{Z}_K \setminus \{0\}$. As $\frac{\beta}{\tau} \notin \mathbf{Z}_K^\times$, we have $M(K) = m_K\left(\kappa^{-1}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(\kappa)\right|} < 1$, which is impossible. □

*Remark* 4.8. In particular, if $M(K) = 1$, $K$ is principal and admits one critical orbit, then $K$ is two-stage norm-Euclidean.

Table 4 lists some examples of two-stage norm-Euclidean number fields.

4.6.2. *Generalized Euclideanity.* Johnson, Queen and Sevilla ([12]) extended Euclideanity in another direction. Their definition is equivalent to the following one.

*Definition* 4.9. We say that $K$ is *Generalized Euclidean* (*G.E.* for short) if for any $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ such that the ideal $(\alpha, \beta)$ is principal,

$$m_K\left(\frac{\alpha}{\beta}\right) < 1.$$

| $n$ | $(r_1, r_2)$ | minimal polynomial, $K = \mathbf{Q}(x)$ | $d(K)$ | $M(K)$ | $N$ |
|---|---|---|---|---|---|
| 3 | $(3,0)$ | $x^3 - x^2 - 6x + 1$ | 985 | 1 | 1 |
| | $(1,1)$ | $x^3 - x^2 + 4x + 1$ | $-335$ | 1 | 2 |
| 4 | $(4,0)$ | $x^4 - 2x^3 - 6x^2 + 3x + 5$ | 42341 | $\frac{7}{5}$ | 1 |
| | $(2,1)$ | $x^4 - x^3 + 6x^2 - x - 1$ | $-5732$ | 1 | 1 |
| | $(0,2)$ | $x^4 - x^3 + 3x^2 + 2$ | 1436 | 1 | 1 |
| 5 | $(5,0)$ | $x^5 - 2x^4 - 6x^3 + 7x^2 + 6x - 5$ | 1719625 | 1 | 1 |
| | $(3,1)$ | $x^5 - x^3 - 5x^2 + 7$ | $-271292$ | 1 | 1 |
| | $(1,2)$ | $x^5 - x^4 + x^3 - 2x - 2$ | 37156 | 1 | 1 |
| 6 | $(6,0)$ | $x^6 - 3x^5 - 11x^4 + 27x^3 + 43x^2 - 57x - 57$ | 115745625 | $\frac{27}{25}$ | 1 |
| | $(4,1)$ | $x^6 - 5x^3 + 4x + 2$ | $-12781568$ | $\frac{11}{8}$ | 1 |
| | $(2,2)$ | $x^6 - x^4 - 3x^2 - 2$ | 1465472 | 1 | 1 |
| | $(0,3)$ | $x^6 - x^5 - 2x^4 - x^3 + 3x^2 + 2x + 2$ | $-275560$ | 1 | 1 |

TABLE 4. Examples of two-stage norm-Euclidean number fields. $N$ stands for the number of orbits whose Euclidean minimum is greater than or equal to 1.

We see immediately that any number field of class number 1 is G.E. if and only if it is norm-Euclidean. Besides, to prove that $K$ is G.E. when $\mathbf{Z}_K$ is not a principal ideal domain, it is sufficient to show that for any $x = \frac{\alpha}{\beta} \in K$, where $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, such that $m_K(x) \geqslant 1$, the ideal $(\alpha, \beta)$ is not principal. In fact, this property does not depend on the choice of $(\alpha, \beta)$, and we easily see it is enough to prove it for one point of each orbit of Euclidean minimum greater than or equal to 1.

*Example* 4.10. $K = \mathbf{Q}(x)$ where $x^4 - 2x^3 + 3x^2 + 8x - 14 = 0$, $d(K) = -11200$, $r_1 = 2$, $r_2 = 1$, $\mathrm{h}_K = 2$. For all $\xi \in K$, we have $m_K(\xi) \geqslant 1$ if and only if $\xi \equiv \frac{\alpha}{\beta} \bmod \mathbf{Z}_K$ or $\xi \equiv \frac{\alpha'}{\beta} \bmod \mathbf{Z}_K$ where $\alpha, \alpha', \beta \in \mathbf{Z}_K$ are defined by

$\alpha = \dfrac{1}{8}x^3 - \dfrac{7}{8}x^2 - \dfrac{1}{4}x + \dfrac{5}{4}$, $\alpha' = \dfrac{1}{4}x^3 - \dfrac{3}{4}x^2 - \dfrac{1}{2}x + \dfrac{3}{2}$ and $\beta = \dfrac{1}{8}x^3 + \dfrac{1}{8}x^2 - \dfrac{1}{4}x - \dfrac{3}{4}$.
Neither $(\alpha, \beta)$, nor $(\alpha', \beta)$ is principal, so $K$ is G.E..

We can find other examples of non-Euclidean G.E. number fields, some of them are listed in Table 5. We can also provide an example of non-principal number field which is not G.E..

*Example* 4.11. Consider $K = \mathbf{Q}(x)$ where $x^4 - 3x^2 - 29 = 0$. Then $d(K) = -11600$, $\mathrm{h}_K = 2$. We find two critical orbits $\mathcal{O}_1$ of length 3 and of minimum $\frac{5}{4}$ and $\mathcal{O}_2$ of length 6 and of minimum $\frac{19}{16}$. Besides, $\frac{x^2+5x+1}{10} \in \mathcal{O}_1$ and $\frac{x^3+x}{10} \in \mathcal{O}_2$.

| $n$ | $(r_1, r_2)$ | minimal polynomial, $K = \mathbf{Q}(x)$ | $d(K)$ | $M(K)$ | $N$ | $\mathrm{h}_K$ |
|---|---|---|---|---|---|---|
| 3 | $(3,0)$ | $x^3 - 12x - 1$ | 6885 | $\frac{67}{40}$ | 6 | 3 |
| | $(1,1)$ | $x^3 + 4x - 1$ | $-283$ | $\frac{3}{2}$ | 1 | 2 |
| 4 | $(4,0)$ | $x^4 - 9x^2 - 5x + 9$ | 56025 | $\frac{3}{2}$ | 1 | 2 |
| | $(2,1)$ | $x^4 - 2x^3 + 5x^2 - 2x - 1$ | $-6848$ | $\frac{4}{3}$ | 1 | 2 |
| | $(0,2)$ | $x^4 - x^3 + 4x^2 + 3x + 9$ | 1521 | 1 | 1 | 2 |
| 5 | $(5,0)$ | $x^5 - 11x^3 - 9x^2 + 14x + 9$ | 4010276 | $\frac{3}{2}$ | 1 | 2 |
| | $(3,1)$ | $x^5 - 2x^4 + 2x^3 - 12x^2 + 21x - 9$ | $-243219$ | 1 | 2 | 2 |
| | $(1,2)$ | $x^5 - x^4 - 2x^2 + 4x - 1$ | 41381 | $\frac{4}{3}$ | 1 | 2 |
| 6 | $(6,0)$ | $x^6 - 13x^4 - 2x^3 + 21x^2 + 13x + 1$ | 49744125 | $\frac{7}{3}$ | 1 | 2 |
| | $(4,1)$ | $x^6 - 3x^5 + x^4 + 3x^3 - 7x^2 + 5x + 1$ | $-9243375$ | $\frac{5}{3}$ | 2 | 2 |
| | $(2,2)$ | $x^6 - 3x^5 + 7x^4 - 9x^3 + 5x^2 - x - 1$ | 1856465 | 1 | 3 | 2 |
| | $(0,3)$ | $x^6 - 2x^5 + 3x^4 + 4x^2 + 2x + 1$ | $-392000$ | 1 | 3 | 2 |

TABLE 5. Examples of non-principal Generalized Euclidean number fields. $N$ is the number of orbits of minimum greater than or equal to 1.

But $\left(x^2+5x+1, 10\right) = \left(x^3+x, 10\right) = \mathbf{Z}_K$, which is obviously a principal ideal. Therefore, $K$ is not G.E..

## 5. On complexity and approximations of computation

For any square matrix $\mathcal{A} = (a_{i,j})_{1\leqslant i,j\leqslant l}$ of size $l$, we will write

$$\|\mathcal{A}\|_\infty := \max_{1\leqslant i\leqslant l} \sum_{j=1}^{l} |a_{i,j}| \,.$$

5.1. **About the approximations of computation.** The procedures described use some floating-point approximations of real numbers. In this section, we will see how to obtain exact and correct results with these approximations.

5.1.1. *Properties of the matrix $\mathcal{M}$.* Let us recall that $\mathcal{M}$ is obtained by LLL-reduction of the matrix defined by (2.a). Classical properties allow to state the following properties of $\mathcal{M}$.

**Lemma 5.1.** $\|\mathcal{M}\|_\infty \leqslant n\left(\frac{2^{\frac{n}{4}}}{\sqrt{n}}\right)^{n-1}\frac{\sqrt{|d(K)|}}{2^{r_2}}$ *and* $\left\|\mathcal{M}^{-1}\right\|_\infty \leqslant \sqrt{n}\cdot 2^{\frac{n(n-1)}{4}}$.

*Remark* 5.2. These upper bounds are generic and much greater than the practical ones. In the examples considered, we always have $\left\|\mathcal{M}^{-1}\right\|_\infty < \|\mathcal{M}\|_\infty < 20$. For instance, in the example described in Section 3.3, we have

$$\|\mathcal{M}\|_\infty \simeq \texttt{5.59} \qquad \text{and} \qquad \left\|\mathcal{M}^{-1}\right\|_\infty \simeq \texttt{1.18}.$$

5.1.2. *Exact computation of the local Euclidean minimum.* When we deal with points of $K$, we can compute *exactly* the local Euclidean minimum. The only approximations required are for the real number $\Gamma(k)$, therefore, it is enough to find $\Gamma'(k) \geqslant \Gamma(k)$ regardless of errors of computation.

However, the precision is not the actual problem here. In fact, if $\Gamma(k)$ is too big (which happens when the absolute value of an embedding of the unit $\varepsilon$ used is too big or too small), then the computation of the local Euclidean minimum may require too many estimates of norms. In practice, we use the PARI library [18], which features a built-in function to compute the norm of elements of number fields.

5.1.3. *Covering and cutting of the fundamental domain.* All the computations are performed using the matrix $\mathcal{M}$. But we know an approximation denoted by $\widetilde{\mathcal{M}} = (\widetilde{m}_{i,j})_{1 \leqslant i,j \leqslant n}$ of $\mathcal{M} = (m_{i,j})_{1 \leqslant i \leqslant n}$. We assume that for any $1 \leqslant i, j \leqslant n$, we have $|\widetilde{m}_{i,j} - m_{i,j}| < \epsilon$.
*Errors on $(a_i)_{1 \leqslant i \leqslant n}$ and $(b_i)_{1 \leqslant i \leqslant n}$.* To define $(a_i)_{1 \leqslant i \leqslant n}$ and $(b_i)_{1 \leqslant i \leqslant n}$, we need to know the sign of the coefficient of the matrix $\mathcal{M}$. However, as these coefficients are not exactly computed, this is not necessarily so easy. Nevertheless, to perform the computations, it is enough to determine some $n$-tuples $\widetilde{a} = (\widetilde{a}_i)_{1 \leqslant i \leqslant n}$ and $\widetilde{b} = (\widetilde{b}_i)_{1 \leqslant i \leqslant n}$ such that for any $1 \leqslant i \leqslant n$, $\widetilde{a}_i \leqslant a_i < b_i \leqslant \widetilde{b}_i$. whatever the errors on $a_i$ and $b_i$ are. So we simply define for $1 \leqslant i \leqslant n$,

$$\widetilde{a}_i = \sum_{\substack{j=1 \\ \widetilde{m}_{i,j} < \epsilon}}^{n} (\widetilde{m}_{i,j} - \epsilon) \qquad \text{and} \qquad \widetilde{b}_i = \sum_{\substack{j=1 \\ \widetilde{m}_{i,j} > -\epsilon}}^{n} (\widetilde{m}_{i,j} + \epsilon)\,.$$

All the computations are performed in $\widetilde{\mathcal{F}} = \left[\widetilde{a}_1, \widetilde{b}_1\right] \times \cdots \times \left[\widetilde{a}_n, \widetilde{b}_n\right]$ which contains $\mathcal{F}$.
*Cutting*. We choose a $n$-tuple of integers $(N_i)_{1 \leqslant i \leqslant n}$ and we decide to cut the fundamental domain in $N_i$ parts in the $i^{\text{th}}$ direction. The centres and steps of the parallelotopes are determined by $\widetilde{\mathcal{M}}$, but even if they differ from the theoretic ones (defined by $\mathcal{M}$), there is no error at this step: we have a covering of $\mathcal{F}$ by parallelotopes.

5.1.4. *Floating-point computations for the absorption test.* At this step, we have a problematic parallelotope $\widetilde{\mathcal{P}}$ of centre $\widetilde{c} = (\widetilde{c}_i)_{1 \leqslant i \leqslant n}$ and of step $\widetilde{h} = \left(\widetilde{h}_i\right)_{1 \leqslant i \leqslant n}$.
We want to know if the element $Z = (Z_i)_{1 \leqslant i \leqslant n} = \mathcal{M}z$ (where $z \in \mathbf{Z}^n$) absorbs $\widetilde{\mathcal{P}}$ for the value $k > 0$, which occurs (Lemma 2.7) when $\mathcal{S} < k$, where

$$\mathcal{S} := \prod_{i=1}^{r_1} \left(|\widetilde{c}_i - Z_i| + \widetilde{h}_i\right) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left(\left(|\widetilde{c}_i - Z_i| + \widetilde{h}_i\right)^2 + \left(|\widetilde{c}_{i+r_2} - Z_{i+r_2}| + \widetilde{h}_{i+r_2}\right)^2\right).$$

However, we do not know $Z$ exactly, but rather $\widetilde{Z} = \left(\widetilde{Z}_i\right)_{1\leqslant i\leqslant n} = \widetilde{M}z$. Instead of $\mathcal{S}$, we will compute

$$\widetilde{\mathcal{S}} := \prod_{i=1}^{r_1}\left(\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i\right)\cdot \prod_{i=r_1+1}^{r_1+r_2}\left(\left(\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i\right)^2 + \left(\left|\widetilde{c}_{i+r_2} - \widetilde{Z}_{i+r_2}\right| + \widetilde{h}_{i+r_2}\right)^2\right).$$

The purpose is to find a real number $k' > 0$ such that the condition $\widetilde{\mathcal{S}} < k'$ implies $\mathcal{S} < k$. We also suppose that the list of integers $\mathcal{L}$ is such that $\mathcal{L} \subseteq \mathcal{M}[-B, B]^n$. With this notation, we can estimate the error of computation.

**Lemma 5.3.**

$$\left|\widetilde{\mathcal{S}} - \mathcal{S}\right| < 2^{r_2}\left((B+1)\|\widetilde{\mathcal{M}}\|_\infty + n\epsilon\right)^n \left[\left(1 + \frac{nB\epsilon}{(B+1)\|\widetilde{\mathcal{M}}\|_\infty + n\epsilon}\right)^n - 1\right].$$

To prove it, we will use the following easy lemma.

**Lemma 5.4.** *We have the following properties.*

(1) *Let $a, b, c, d \in \mathbf{C}$, then $2(ab - cd) = (a - c)(b + d) + (a + c)(b - d)$.*
(2) *Let $l$ be a positive integer, $a = (a_1, \ldots, a_l) \in \mathbf{C}^l$ and $b = (b_1, \ldots, b_l) \in \mathbf{C}^l$. We assume that there exists some real number $\rho > 0$ such that for any $1 \leqslant i \leqslant l$, $|b_i - a_i| < \rho$. Besides, let $A$ be a positive real number such that for any $1 \leqslant i \leqslant l$, $|a_i| \leqslant A$. Then*

$$\left|\prod_{i=1}^{l} b_i - \prod_{i=1}^{l} a_i\right| < (A + \rho)^l - A^l.$$

*Proof of Lemma 5.3.* Let us write $D = \|\widetilde{\mathcal{M}}\|_\infty$ and $\mathcal{I} = \sqrt{-1}$. The $n$-tuple $a = (a_i)_{1\leqslant i\leqslant n}$ is given by

$$a_i := \begin{cases} \left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i & \text{if } 1 \leqslant i \leqslant r_1, \\ \left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i + \mathcal{I}\left(\left|\widetilde{c}_{i+r_2} - \widetilde{Z}_{i+r_2}\right| + \widetilde{h}_{i+r_2}\right) & \text{if } r_1 < i \leqslant r_1 + r_2, \\ \left|\widetilde{c}_{i-r_2} - \widetilde{Z}_{i-r_2}\right| + \widetilde{h}_{i-r_2} - \mathcal{I}\left(\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i\right) & \text{if } r_1 + r_2 < i \leqslant n. \end{cases} \tag{5.e}$$

Similarly, we define $b = (b_i)_{1\leqslant i\leqslant n}$ by replacing $\widetilde{Z}$ by $Z$ in (5.e). We write $\widetilde{\mathcal{S}}^{(1)} := \prod_{i=1}^{r_1} a_i$, $\widetilde{\mathcal{S}}^{(2)} := \prod_{i=r_1+1}^{n} a_i$, $\mathcal{S}^{(1)} := \prod_{i=1}^{r_1} b_i$ and $\mathcal{S}^{(2)} := \prod_{i=r_1+1}^{n} b_i$, so that $\widetilde{\mathcal{S}} - \mathcal{S} = \widetilde{\mathcal{S}}^{(1)}\widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(1)}\mathcal{S}^{(2)}$. Thanks to Lemma 5.4, (1), we see that

$$\begin{aligned} 2\left|\widetilde{\mathcal{S}} - \mathcal{S}\right| \leqslant \left|\widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)}\right| \left(2\left|\widetilde{\mathcal{S}}^{(2)}\right| + \left|\widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)}\right|\right) \\ + \left(2\left|\widetilde{\mathcal{S}}^{(1)}\right| + \left|\widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)}\right|\right)\left|\widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)}\right|. \end{aligned}$$

Let us notice that $\left|\widetilde{\mathcal{S}}^{(1)}\right| \leqslant (D(B+1) + n\epsilon)^{r_1}$ and $\left|\widetilde{\mathcal{S}}^{(2)}\right| \leqslant 2^{r_2}(D(B+1) + n\epsilon)^{2r_2}$. For short, we will write

$$\mu := \frac{nB\epsilon}{D(B+1) + n\epsilon}.$$

| $n = [K : \mathbf{Q}]$ | rough value of $B$ | precision on the absorption test |
|---|---|---|
| 2 | 1000 | $10^{-7}$ |
| 3 | 200 | $10^{-5}$ |
| 4 | 30 | $5 \cdot 10^{-5}$ |
| 5 | 12 | $3 \cdot 10^{-4}$ |
| 6 | 6 | $3 \cdot 10^{-3}$ |
| 7 | 2 | $6 \cdot 10^{-4}$ |
| 8 | 2 | $4 \cdot 10^{-2}$ |

TABLE 6. Precision of the absorption test according to the degree and the size of the integers used.

Using Lemma 5.4, (2) twice with $A = D(B+1) + n\epsilon$, $\rho = nB\epsilon$ for $\widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)}$ and with $A = \sqrt{2}\,(D(B+1) + n\epsilon)$, $\rho = nB\epsilon\sqrt{2}$ for $\widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)}$, we get

$$\begin{aligned}\left|\widetilde{\mathcal{S}} - \mathcal{S}\right| <& 2^{r_2-1}(D(B+1)+n\epsilon)^n \\ & \times \left[((1+\mu)^{r_1} - 1)\left((1+\mu)^{2r_2} + 1\right) + ((1+\mu)^{r_1} + 1)\left((1+\mu)^{2r_2} - 1\right)\right],\end{aligned}$$

from which we easily deduce the result. □

In the examples considered $\|\widetilde{\mathcal{M}}\|_\infty < 10$, we use floating-point numbers with double-precision, the minimum is roughly 1, so $\epsilon \simeq 10^{-15}$ and we choose $B$ decreasing with the degree $n$. Table 6 provides some examples of the precision in the worst case of computation of extended norms. In practice, when we try to absorb parallelotopes by integers for some value $k > 0$, we replace $k$ by $k' := k - \eta$, where $\eta$ is the precision on the norms.

5.1.5. *Floating point computations for the action of units.* All computations described in 2.3 are explicit, but they are performed starting with approximations of the embeddings of the units, $\mathcal{M}$ and $\mathcal{M}^{-1}$. We assume that we know their coordinates up to $\epsilon > 0$. We denote by $\nu = (\nu_1, \ldots, \nu_n)$ the image by $\Phi$ of the unit used and $c = (c_1, \ldots, c_n) \in H$ the centre of the parallelotope $\mathcal{P}$ of step $h = (h_1, \ldots, h_n)$ considered.
*Error on the size of the image*. We included $\nu \cdot \mathcal{P}$ in a domain $\mathcal{B}$ defined with the step $h' = (h'_1, \ldots, h'_n) \in \mathbf{R}^n$. The error stems from the fact that we do not know $\nu$ exactly but only an approximation $\widetilde{\nu} = (\widetilde{\nu}_1, \ldots, \widetilde{\nu}_n)$ such that for any $1 \leqslant i \leqslant n$, $|\widetilde{\nu}_i - \nu_i| < \epsilon$. With this $n$-tuple $\widetilde{\nu}$, we compute the $n$-tuple $\widetilde{h'} = \left(\widetilde{h'}_i\right)_{1 \leqslant i \leqslant n}$ and we have the following straightforward bounds.

$$\left\{\begin{array}{lll} \left|\widetilde{h'}_i - h'_i\right| < h_i \cdot \epsilon & & \text{if } 1 \leqslant i \leqslant r_1 \\ \left|\widetilde{h'}_i - h'_i\right| < \epsilon\sqrt{h_i^2 + h_{i+r_2}^2} & & \text{if } r_1 < i \leqslant r_1 + r_2 \end{array}\right. . \tag{5.f}$$

*Remarks* 5.5. We have the same estimate for the step $\widetilde{h'}_{i+r_2} = \widetilde{h'}_i$ ($r_1 < i \leqslant r_1 + r_2$). In practice, we can increase $\widetilde{h'}_i$ to get through the error of computation. This error remains small as long as the initial step $h$ is small. In any case, the action of units eliminates problems only when the cutting is such that the steps are small.

*Error on the centre of the image*. The domain $\mathcal{B}$ is centred in $c' = \nu \cdot c$, but we use $\widetilde{\nu}$ instead of $\nu$. Therefore, we compute $\widetilde{c'} = \widetilde{\nu} \cdot c$ and as in (5.f), the error on the coordinates of the centre is $|c_i| \cdot \epsilon$ if $1 \leqslant i \leqslant r_1$ or $(|c_i| + |c_{i+r_2}|) \cdot \epsilon$ if $r_1 < i \leqslant r_1 + r_2$.

These errors are at most $2\|\widetilde{\mathcal{M}}\|\epsilon$, we can increase the step $\widetilde{h'}_i$ to make sure that the test with the unit is correct.
*Translation vectors*. We will use the following trivial lemma.

**Lemma 5.6.** *Let $x = (x_i)_{1\leqslant i\leqslant n}$, $\alpha = (\alpha_i)_{1\leqslant i\leqslant n}$ and $\beta = (\beta_i)_{1\leqslant i\leqslant n}$ be three $n$-tuples such that for any $1 \leqslant i \leqslant n$, we have $\alpha_i \leqslant z_i \leqslant \beta_i$. For any matrix $\mathcal{A} = (a_{i,j})_{1\leqslant i,j\leqslant n}$, if we write $y = \mathcal{A}x = (y_i)_{1\leqslant i\leqslant n}$, then for any $1 \leqslant i \leqslant n$,*

$$\sum_{\substack{j=1\\ a_{i,j}>-\epsilon}}^{n} (a_{i,j}+\epsilon)\alpha_j + \sum_{\substack{j=1\\ a_{i,j}<\epsilon}}^{n} (a_{i,j}-\epsilon)\beta_j \leqslant y_i \leqslant \sum_{\substack{j=1\\ a_{i,j}>-\epsilon}}^{n} (a_{i,j}+\epsilon)\beta_j + \sum_{\substack{j=1\\ a_{i,j}<\epsilon}}^{n} (a_{i,j}-\epsilon)\beta_j.$$

Here, we apply this lemma with $\alpha = a'$, $\beta = b'$ and $\mathcal{A} = \widetilde{\mathcal{M}}^{-1}$. We get correct bounds on $y_i$ for all $1 \leqslant i \leqslant n$ regardless of the errors of computations. We take the integers in these intervals to obtain all translation vectors.
*Intersection with other problems*. We assume that we use a translation vector $\widetilde{X}$ which is an approximation of the vector $X$. The error on each coordinate of $\widetilde{X}$ is at most $nB\epsilon$. We take into account this error to decide if $\nu\cdot\mathcal{P} - X$ can intersect a problematic parallelotope. By increasing the size of the domain containing $\nu\cdot\mathcal{P} - X$, we may not eliminate an unproblematic parallelotope, but we never discard a problematic one.

5.2. **Complexity of some procedures.** In this paragraph, we will give the complexity of the most expensive procedures previously described.

5.2.1. *Computation of the local Euclidean minimum.*

**Proposition 5.7.** *Let $x \in K$, Algorithm 2.1 requires at most*

$$\#\mathrm{Orb}\,(x)\cdot\left(2\Gamma\left(\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|\right)\left\|\mathcal{M}^{-1}\right\|_\infty + 1\right)^n$$

*computations of norms of elements of $K$.*

*Proof.* It is straightforward to notice that for any $k > 0$, computing $\mathcal{M}_k$ requires at most $\#\mathrm{Orb}\,(x)\cdot\left(2\Gamma(k)\left\|\mathcal{M}^{-1}\right\|_\infty + 1\right)^n$ computations of norms. □

5.2.2. *Test of units.* We consider the action of $\nu \in \Phi(\mathbf{Z}_K^\times)$ on any problematic parallelotope $\mathcal{P}$ of centre $c$ and step $h$.

**Proposition 5.8.** *There are at most $\left(\left\|\mathcal{M}^{-1}\right\|_\infty(\|\mathcal{M}\|_\infty(1+2\|\nu\|_\infty))+1\right)^n$ translation vectors of $\mathcal{P}$ in the fundamental domain $\mathcal{F}$.*

We want to have as few translation vectors as possible, consequently, it is interesting to choose $\nu \in \Phi(\mathbf{Z}_K^\times)$ such that $\|\nu\|_\infty$ is as small as possible. Besides, the upper bound uses the very bad inequality $|h'_i| \leqslant \|\nu\|_\infty\|\mathcal{M}\|_\infty$, for any $1 \leqslant i \leqslant n$ (with the notation of Section 2.3). We can obtain a better inequality (and better results) by cutting further in the directions $i$ where $\nu_i$ is “big”.

With the estimation on the number translation vectors, we can bound the number of operations required for the test of the unit $\nu$.

**Proposition 5.9.** *Algorithm 2.5 requires*

$$O\left(n\cdot(\#\mathcal{T})^3\cdot\left(\left\|\mathcal{M}^{-1}\right\|_\infty(\|\mathcal{M}\|_\infty(1+2\|\nu\|_\infty))+1\right)^n\right)$$

*floating-point operations.*

(A) Smallest discriminant.

| $(r_1, r_2)$ | $M(K)$ | $N$ | time |
|---|---|---|---|
| $(0, 2)$ | $\frac{1}{7}$ | 12 | 10 s |
| $(3, 1)$ | $\frac{1}{13}$ | 24 | 16min 23s |
| $(0, 3)$ | $\frac{1}{13}$ | 36 | 23min 10s |
| $(6, 0)$ | $\frac{1}{13}$ | 168 | 2h 13min 26s |
| $(7, 0)$ | $\frac{1}{7}$ | 6 | 1h 38min 52s |
| $(0, 4)$ | $\frac{1}{16}$ | 15 | 55h 54min 38s |

(B) Signature $(1, 2)$.

| $d(K)$ | $M(K)$ | $N$ | time |
|---|---|---|---|
| 4897 | $\frac{1}{5}$ | 4 | 3min 58s |
| 8705 | $\frac{1}{5}$ | 4 | 21 min 5 s |
| 10229 | $\frac{1}{2}$ | 1 | 1min 15s |
| 52813 | $\frac{1}{2}$ | 1 | 43min 8s |
| 163273 | $\frac{7}{5}$ | 2 | 11min 27s |
| 163300 | 1 | 1 | 22min 19s |

Table 7. Some timings for Algorithm 3.1. The number of critical points is denoted by $N$.

5.3. **Timings.** Running time of Algorithm 3.1 depends on the choice of the initial value $\mathcal{K}$. The dichotomy described in 3.1 may be the longest part of the execution. In Table 7, we give CPU time and we only describe the time required once we use $k = 0.97 \cdot M(K)$, for which we obtain a convenient graph in all cases.

To explain the timings observed, let us notice first that for a number field of degree $n$, a cutting in $n$ directions is required and if $M(K)$ is small, we have to choose $N_i$ large enough for every $1 \leqslant i \leqslant n$, in order to be efficient from the start of the algorithm.

Then, when we fix the signature, the following properties of $K$ may make some parts of Algorithm 3.1 costly.

- If $M(K)$ is small, then a precise initial cutting will be required.
- If the units of $K$ are big, then many translation vectors will be computed by Algorithm 2.5 and the final computation of the local Euclidean minimum by Algorithm 2.1 can turn out to be long.
- If there are many critical points, then there will be more problematic parallelotopes at each step and an execution of Algorithm 2.1 will be required for each critical orbit.

## Acknowledgements

I am very grateful to Jean-Paul Cerri for his invaluable help at each step of the redaction of this paper. I would also like to thank Karim Belabas for his advice and both anonymous referees, whose comments, corrections and suggestions helped me improve this article.

## References

1. Eric S. Barnes and H. Peter F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms (II)*, Acta Mathematica **88** (1952), 279–316.
2. Eva Bayer-Fluckiger, *Upper bounds for Euclidean minima of algebraic number fields*, Journal of Number Theory **121** (2006), 305–323.
3. Hermann Behrbohm and László Rédei, *Der Euklidische Algorithmus in quadratischen Zahlkörpern*, Journal für die reine und angewandte Mathematik **174** (1936), 192–205.

4. Stefania Cavallar and Franz Lemmermeyer, *The Euclidean algorithm in cubic number fields*, Proceedings of Number Theory Eger 1996 (Kálmán Győry, Attila Pethő, and Vera T. Sos, eds.), de Gruyter, 1998, pp. 123–146.
5. Jean-Paul Cerri, *Spectres euclidiens et inhomogènes des corps de nombres*, Ph.D. thesis, Université Nancy 1, 2005.
6. ———, *Euclidean and inhomogeneous spectra of number fields with unit rank strictly greater than 1*, Journal für die reine und angewandte Mathematik **592** (2006), 49–62.
7. ———, *Euclidean minima of totally real number fields. Algorithmic determination*, Mathematics of Computation **76** (2007), 1547–1575.
8. Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1996.
9. George E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I.*, Journal für die reine und angewandte Mathematik **282** (1976), 133–156.
10. Harold Davenport, *Linear forms associated with an algebraic number field*, Quarterly Journal of Mathematics **2** (1952), 32–41.
11. Veikko Ennola, *On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields*, Ph.D. thesis, University of Turku, 1958.
12. David H. Johnson, Clifford S. Queen, and Alicia N. Sevilla, *Euclidean real quadratic number fields*, Archiv der Mathematik **44** (1985), 340–347.
13. Franz Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Expositiones Mathematicae **13** (1995), 385–416, an updated version is available at `http://www.rzuser.uni-heidelberg.de/~hb3/publ/survey.pdf`.
14. Hendrik W. Lenstra, Jr., *Euclidean number fields of large degree*, Inventiones Mathematicae **38** (1976), no. 3, 237–254.
15. ———, *Euclidean number fields 1*, The Mathematical Intelligencer **2** (1979), no. 1, 6–15.
16. Pierre Lezowski, *euclid, version* `1.0`, 2012, available from `http://www.math.u-bordeaux1.fr/~lezowski/euclid/`.
17. Robert E. Tarjan, *Depth-first search and linear graph algorithms*, SIAM Journal on Computing **1** (1972), 146–160.
18. The PARI Group, Bordeaux, *PARI/GP, version* `2.4.3`, 2008, available from `http://pari.math.u-bordeaux.fr/`.
19. Franciscus Jozef van der Linden, *Euclidean rings with two infinite primes*, Ph.D. thesis, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.



Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
INRIA, LFANT, F-33400 Talence, France
*E-mail address*: `pierre.lezowski@math.u-bordeaux1.fr`