Computation of the Euclidean minimum of algebraic number fields

Pierre Lezowski

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 in [6]. With a practical implementation, we obtained 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. We also prove a result of independant interest concerning real quadratic fields whose Euclidean minimum is equal to 1.

We consider an algebraic number field K. Let $\mathbf{Z}_K$ be its ring of integers. We write r_1 its number of real places, $2r_2$ its number of imaginary places and $n = r_1 + 2r_2$ its degree. We denote by $\mathbf{N}_{K/\mathbf{Q}}$ the usual norm. The couple (r_1, r_2) is called the signature of K. We will write $\mathbf{Z}_K^\times$ the group of units of K and $r = r_1 + r_2 - 1$ its rank. For any square matrix $\mathcal{A} = (a_{i,j})_{1 \leqslant i,j \leqslant l}$ of size l, we will write

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

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^{th} century, Wantzel tried to prove Fermat's Last Theorem using some (false) 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: August 16, 2011.

1991 *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^{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 ([6]) 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 its properties. In particular, we will study real quadratic number fields whose Euclidean minimum is equal to 1. 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 of K). For any $\xi \in K$, we call *Euclidean minimum of* ξ 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 ξ 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 the paragraph 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 $M(K) := \sup_{\xi \in K} m_K(\xi)$, 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 paragraph 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 $\Phi : \left\{ \begin{array}{ccc} K & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & \Big(\sigma_1(x), \ldots, \sigma_{r_1}(x), \quad \Re\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \quad \Im\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_2}(x)\Big) \end{array} \right.$.

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 Φ: 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

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

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. We can extend the norm to H by setting

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

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 of K). For any $x \in H$, we put

$$m_{\overline{K}}(x) := \inf_{z \in \mathbf{Z}_K} |\mathcal{N}(x - \Phi(z))| .$$

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 [6], Proposition 2.1. □

It is now natural to introduce the following notion.

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

We immediately see that $M(K) \leqslant M(\overline{K})$. Besides, thanks to Proposition 1.4, 3, we know that there exists some $x \in H$ such that $M(\overline{K}) = m_{\overline{K}}(x)$. 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 $r = 0$. Moreover, the following theorem provides a positive answer in many cases.

Theorem 1.6. *We recall that the rank of the units $\mathbf{Z}_K^\times$ 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 $M(\overline{K}) = m_K(x)$. 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 [20] in the case $r = 1$. The statement (b) is proved in [5].

If $r = 1$, we do not have a result as strong as (b). However, there is no counter-example 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, if $r \neq 1$, then K is norm-Euclidean if and only if $M(K) < 1$. However, if $r = 1$ and $M(K) = 1$, we cannot conclude about the norm-Euclideanity of K. Nevertheless, if $r_1 = 2$ and $r_2 = 0$, we can check that $M(K) = 1$ if and only if K is $\mathbf{Q}(\sqrt{65})$, in which case K is not norm-Euclidean, thanks to the bound on $M(\overline{K})$ given in [11].

1.4. **Real quadratic fields of Euclidean minimum equal to 1.** In this paragraph, we deal with $K = \mathbf{Q}(\sqrt{m})$ where m is a squarefree integer greater than 1. We recall that $H \simeq \mathbf{R}^2$.

We will prove the following result.

Theorem 1.8. *A real quadratic field K is norm-Euclidean if and only if $M(K) < 1$.*

To prove this, we will find the cases when $M(K) = 1$ and prove that this may happen only for non-norm-Euclidean number fields.

1.4.1. *Ennola's bound.*

Theorem 1.9 ([11], Lemma 11)**.** *Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form, where $a, b, c \in \mathbf{Q}$ are such that $b^2 - 4ac > 0$. We suppose that f does not represent 0 for $(x, y) \neq (0, 0)$. Then there exist $h, k \in \mathbf{Q}$, such that*

$$|f(x + h, y + k)| \geqslant \kappa\sqrt{b^2 - 4ac},$$

for all integers x, y, where $\kappa = \dfrac{1}{16 + 6\sqrt{6}}$.

If $m \equiv 2, 3 \mod 4$, then $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\sqrt{m}$. For all $x, y \in \mathbf{R}$, we set $f(x, y) = \mathcal{N}(x + y\sqrt{m}, y - \sqrt{m}) = x^2 - my^2$. By applying Theorem 1.9, we obtain two rationals h and k such that

$$m_K(h + k\sqrt{m}) = m_{\overline{K}}(h + k\sqrt{m}, h - k\sqrt{m}) \geqslant \kappa\sqrt{4m}.$$

As a result, if $m > \frac{1}{4\kappa^2}$, then $M(K) > 1$. Consequently, if we are interested in the number fields K whose Euclidean minimum is not greater than 1, it is enough to consider $m \leqslant 235$, if $m \equiv 2, 3 \mod 4$.

If $m \equiv 1 \mod 4$, then $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{m}}{2}$ and we can apply Theorem 1.9 with $f(x, y) = \left(x + \frac{y}{2}\right)^2 - m\frac{y^2}{4} = x^2 + xy + \frac{1-m}{4}y^2$. Then it is enough to deal with $m \leqslant \frac{1}{\kappa^2}$, so with $m \leqslant 941$.

1.4.2. *A classical lemma.* Now we only have a finite number of cases to solve. In [11], the bound is used to determine Euclidean number fields, here, we want to know when $M(K) = 1$. To achieve this, as in [11], we use a classical lemma which goes at least back to [3].

Lemma 1.10 (Case $m \equiv 2, 3 \mod 4$)**.** *We assume that K is norm-Euclidean. If r is an integer such that $0 < r < m$ and is a square modulo m, then there exist $X, Y \in \mathbf{Z}$ such that $X^2 - mY^2 \in \{r, r - m\}$.*

Proof. Let Z be an integer such that $Z^2 \equiv r \mod m$. We perform the Euclidean division of $Z\sqrt{m}$ by $-m$: there exist $\alpha, \beta \in \mathbf{Z}$ such that

$$\left|\mathbf{N}_{K/\mathbf{Q}}\left(Z\sqrt{m} + m(\alpha + \beta\sqrt{m})\right)\right| < m^2.$$

Then, we divide by m to get

$$\left|m\alpha^2 - (\beta m + Z)^2\right| < m.$$

We write $X = \beta m + Z$ and $Y = \alpha$. Then, $X^2 - mY^2 \equiv r \mod m$. We deduce the result from the bound previously found. □

We can get a similar result in the other case.

Lemma 1.11 (Case $m \equiv 1 \mod 4$)**.** *We assume that K is norm-Euclidean. If r is an integer such that $0 < r < m$ and is a square modulo m, then there exist $X, Y \in \mathbf{Z}$ such that $X^2 - 4mY^2 \in \{4r, 4(r-m)\}$.*

Therefore, to show non-norm-Euclideanity, it is enough to find some r contradicting the conclusions of Lemmas 1.10 or 1.11. Besides, if we achieve this construction, then $M(K) \geqslant \min\left\{\frac{r+m}{m}, \frac{2m-r}{m}\right\} > 1$. In [11], it is used[1] in all but 7 cases, if $m \equiv 2, 3 \mod 4$ and in all but 22 cases if $m \equiv 1 \mod 4$.

For the remaining values of m, either they define norm-Euclidean number fields $K = \mathbf{Q}(\sqrt{m})$ or explicit values of $x \in K$ are known[2] such that $m_K(x) > 1$, except for $m = 65$, in which case $M(K) = m_K\left(\frac{1+\sqrt{65}}{4}\right) = 1$ and so K is not norm-Euclidean.

Consequently, in the case $r_1 = 2$, $r_2 = 0$, we know that no norm-Euclidean number field K is such that $M(K) = 1$. That achieves the proof of Theorem 1.8.

1.5. **Bounds for the Euclidean minimum.**

1.5.1. *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.

1.5.2. *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 the 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 [6], 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 $\{\varepsilon_1, \ldots, \varepsilon_r\}$, and the roots of unity in K.

The units act on K by multiplication, we can extend this action on 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 translated of elements of the orbit of x for the action of units by $\Phi(\mathbf{Z}_K)$.

[1] In the original proof of [11], some corollaries of Lemmas 1.10 and 1.11 are involved, but we can also construct directly counter-examples using Lagrange-Matthews-Mollin algorithm ([16], [17]) to show quickly that some Pell's equations do not admit solutions.

[2] see [11], pages 55-56, where points and original references are provided.

Lemma 2.1. *Let $x \in H$, $\mathrm{Orb}(x)$ is finite if and only if $x \in \Phi(K)$.*

Proof. If $\mathrm{Orb}(x)$ is finite, there exist $\varepsilon \neq \varepsilon' \in \mathbf{Z}_K^\times$ such that $\Phi(\varepsilon)\cdot x = \Phi(\varepsilon')\cdot x \mod \Phi(\mathbf{Z}_K)$, since $\mathbf{Z}_K^\times$ is infinite. As Φ is multiplicative, there exists some $z \in \mathbf{Z}_K$ such that

$$x = \Phi\left(\frac{z}{\varepsilon - \varepsilon'}\right) \in \Phi(K).$$

Conversely, if $\xi \in K$ and $x = \Phi(\xi)$, then we can write $\xi = \frac{\alpha}{\beta}$ with $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$. Then, we conclude that $\mathrm{Orb}(x)$ is finite, for $\mathbf{Z}_K/\beta\mathbf{Z}_K$ is finite of cardinality $\left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$. □

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

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

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 ([6]). We consider the logarithmic embedding of K:

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

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. It is an easy consequence of 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*

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

We consider the nonnegative rational

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

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 ([6]). □

Proposition 2.5. *Let $x \in K$, Algorithm 2.1 computes the local Euclidean minimum and requires at most $\#\mathrm{Orb}\,(x)\cdot\left(2\Gamma\left(\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|\right)\cdot\sqrt{2n}\cdot 2^{\frac{n(n-1)}{4}} + 1\right)^n$ computations of norms of elements of K.*

Algorithm 2.1 Computation of the local Euclidean minimum

INPUT: a number field K, a point $x \in \Phi(K)$, the orbit $\mathrm{Orb}(x)$ of x, $k > 0$
OUTPUT: $m_K(x)$
1: Compute $\Gamma(k)$, $\mathcal{M}_k$
2: **if** $\mathcal{M}_k \leqslant k$ **then**
3: **return** $\mathcal{M}_k$
4: **else**
5: $k \leftarrow \mathcal{M}_k$
6: **go to** 1
7: **end if**

Proof. As the function $k \longmapsto \mathcal{M}_k$ is non-decreasing, Theorem 2.4 implies that we need to repeat the loop at most twice to obtain $m_K(x)$. We postpone the evaluation of the complexity of this algorithm until the required tools and notations are introduced (see Corollary 5.4). □

Remarks 2.6. i. This algorithm only applies to elements of $\Phi(K)$, because the orbit of other elements of H is infinite (Lemma 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 not required.
iii. Algorithm 2.1 requires the knowledge of the orbit $\mathrm{Orb}(x)$, we will see how to compute it in paragraph 3.2.4.
iv. $\mathcal{M}_k$ is determined thanks to the computation of $\mathcal{N}(t)$ for some elements $t \in \Phi(K)$. In practice, instead of evaluating the extended norm (in $\Phi(K)$), we compute directly (and exactly) norms of the corresponding elements in K.
v. The complexity written here is in the very worst case when we have no idea on $m_K(x)$, in practice, if we have a better upper bound k_1 on $m_K(x)$, we can substitute k_1 to $\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|$.
vi. The norm of an element of K can be computed with a resultant using $\tilde{O}(n)$ operations in $\mathbf{Z}$.

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 $\Phi(K)$. 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 $\sigma_i(z_j)$ for all $1 \leqslant i, j \leqslant n$. This allows us to identify $\mathbf{Q}^n$ and K through the map

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

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

$$\begin{array}{ccc} \mathbf{Q}^n & \xhookrightarrow{\ i\ } & \mathbf{R}^n \\ \downarrow{\scriptstyle \Psi} & & \wr \downarrow{\scriptstyle \phi} \\ K & \xrightarrow{\ \Phi\ } & H \end{array}$$

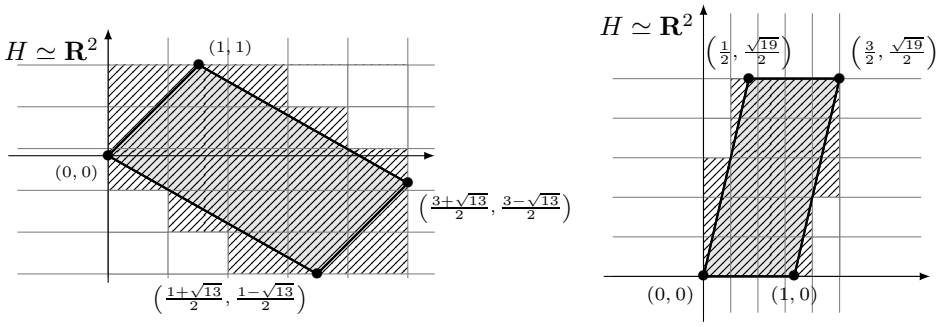


FIGURE 1. Example of covering and cutting of the fundamental domain: $K = \mathbf{Q}(\sqrt{13})$ and $K = \mathbf{Q}(\sqrt{-19})$.

Since Φ and Ψ are injective, ϕ is injective, so ϕ is an isomorphism, 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 $1 \leqslant j \leqslant n$,

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

Besides, Ψ 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 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 2.9).

In practice, we apply an LLL-reduction (see [7], section 2.6) to $\mathcal{M}$ in order to control the size of coefficients of $\mathcal{M}$ and $\mathcal{M}^{-1}$ (see section 5.1?

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.

Remark 2.7. To perform computations in H, we use floating-point numbers and an approximation of $\mathcal{M}$ is required. For questions of precision, see 5.2.3.

2.2.2. *Absorption condition.* We choose $k > 0$ and we recall that the purpose is to know which points x of H check $|m_{\overline{K}}(x)| < k$. To do this, 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 $c = (c_1, \ldots, c_n)$ and its step $h = (h_1, \ldots, h_n) \in (\mathbf{R}_{>0})^n$:

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

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 $\mathcal{M}$, l embeddings of units, a list of parallelotopes which cover the fundamental domain $\mathcal{F}$

1: $\mathcal{T} \leftarrow \emptyset$, compute the matrix $\mathcal{M}$ (2.a)
2: LLL-reduction of $\mathcal{M}$
3: compute l embeddings of units $\mathfrak{E} = \{\upsilon_1, \cdots, \upsilon_l\}$
4: in each direction i, cut $[a_i, b_i]$ (see 2.b) into N_i segments (of same length) $[c_i, d_i]$
5: **for** each $\mathcal{P} = \prod_{i=1}^{n}[c_i, d_i]$ **do**
6: **if** $\mathcal{P} \cap \mathcal{F} \neq \emptyset$ (see Lemma 3.2) **then**
7: $\mathcal{T} \leftarrow \mathcal{T} \cup \{\mathcal{P}\}$
8: **end if**
9: **end for**
10: **return** $\mathcal{M}$, $\mathfrak{E}$, $\mathcal{T}$

Lemma 2.8. *The parallelotope $\mathcal{P}$ of centre $c = (c_1, \ldots, c_n)$ and of step $h = (h_1, \ldots, h_n)$ is absorbed by $z = (z_1, \ldots, z_n)$ 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 $x = (x_1, \ldots, x_n)$ be a point of $\mathcal{P}$, fix an integer $1 \leqslant i \leqslant n$, then the triangle inequality easily 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 Lemma 2.8 is checked, the point x is absorbed by z. □

Remark 2.9. The condition of Lemma 2.8 is optimal, indeed, it is exactly the test $|\mathcal{N}(x - z)| < k$ where x is some vertex of the parallelotope $\mathcal{P}$.

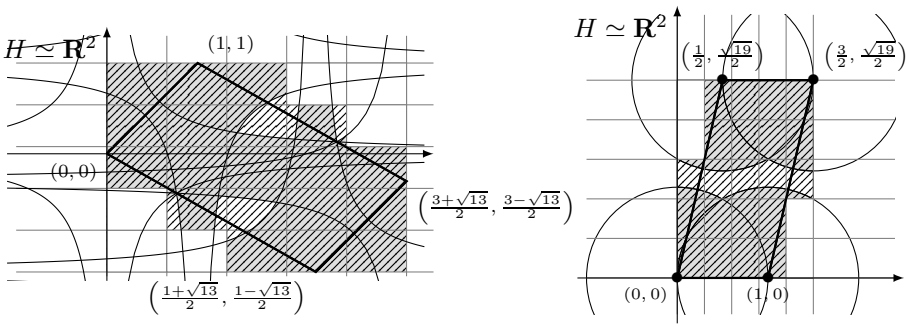
We choose a fixed list of integers $\mathcal{L}$ and we apply the test described in Lemma 2.8 for all parallelotopes and all elements of $\mathcal{L}$. All the parallelotopes which are not absorbed by integers are called *problematic*.

Algorithm 2.3 Absorption test

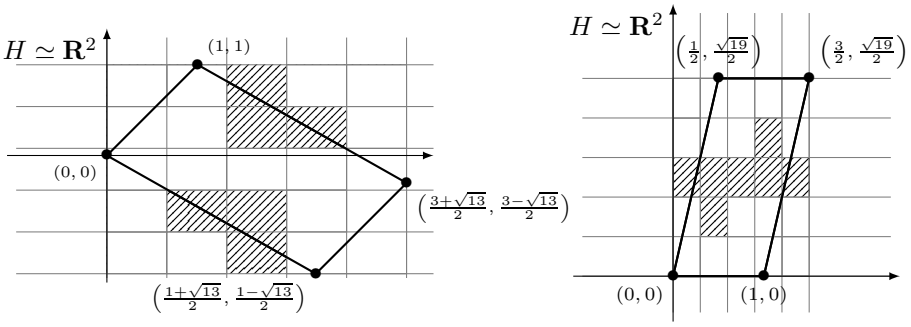
INPUT: a parallelotope $\mathcal{P}$ of centre c and step h, a finite list $\mathcal{L} \subseteq \Phi(\mathbf{Z}_K)$, $k \in \mathbf{R}$.
OUTPUT: if $\mathcal{P}$ can be absorbed for k by an element of $\mathcal{L}$.

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

Proposition 2.10. *Algorithm 2.3 tests if $\mathcal{P}$ can be absorbed by $\mathcal{L}$ and requires at most $O(\#\mathcal{L})$ floating-point operations.*



(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.

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.

However, we can easily determine beforehands 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 $i \in \{1, \dots, n\}$,

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

so that $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. Besides if $X = (X_i)_{1\leqslant i\leqslant n} \in \Phi(\mathbf{Z}_K)$ absorbs some element $x \in \mathcal{F}$, then we have $|\mathcal{N}(x - X)| < k$. Consequently, we obtain

immediately that there exists an integer $i \in \{1, \dots, r_1 + r_2\}$ such that

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

These estimations 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 N
OUTPUT: a list of elements of $\Phi(\mathbf{Z}_K)$ which may absorb parallelotopes

```
L ← ∅
for each vector Z ∈ Z^n such that −N ⩽ Z_i ⩽ N do
    compute X = MZ^n
    if condition (2.c) is checked then
        L ← L ∪ {X}
    end if
end for
```

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 ε. We write $\nu = (\nu_i)_{1 \leqslant i \leqslant n} = \Phi(\varepsilon)$. In practice, we work directly with ν, 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 ν:

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

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

Lemma 2.11. *Let $c' = \nu \cdot c = (c'_i)_{1 \leqslant i \leqslant n}$ be the image of the centre of $\mathcal{P}$ by the action of ν, then $\nu \cdot \mathcal{P}$ is contained in the following domain:*

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

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

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

Proof. It is a straightforward verification. In fact, $\nu \cdot \mathcal{P}$ is another parallelotope, but its directions can be rotated for the imaginary coordinates. □

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 $\{x \in \mathcal{F},\, m_{\overline{K}}(x) < k\}$.

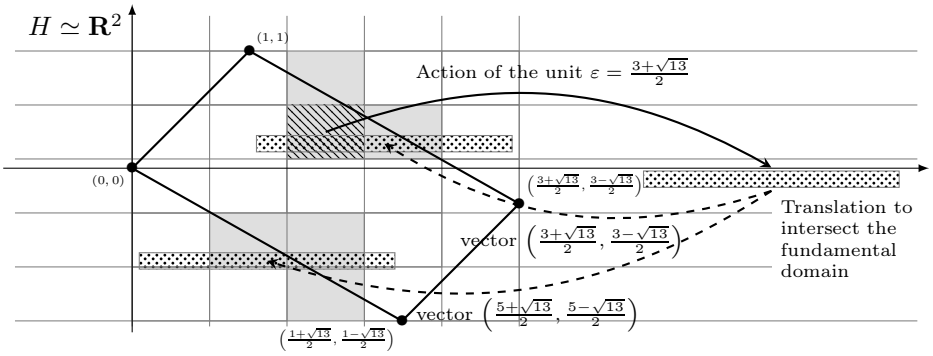


FIGURE 3. Action of the unit $\frac{3+\sqrt{13}}{2}$ on a problematic parallelotope. The two translates of the image in the fundamental domain intersect problematic parallelotopes, we keep this problem.

We suppose that $\{\mathcal{Q}^{(i)}, 1 \leqslant i \leqslant m\}$ 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 some integer $1 \leqslant m \leqslant l$ such that all parallelotopes $\mathcal{Q}^{(i)}$ for $m < i \leqslant l$ are absorbed by integers.

Definition 2.12. 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 2.13. *Let $\{z^{(j)}, 1 \leqslant j \leqslant k\} \subseteq \Phi(\mathbf{Z}_K)$ be the list of 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 interesects 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 these notations, $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$, 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 notations of Lemma 2.11. Consenquently, we get the following criterion.

Lemma 2.14. *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 a translation 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 2.15. *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 is enough to notice that

$$\mathcal{Q}^{(j)} \subseteq \left[c_1^{(j)} - h_1^{(j)}, c_1^{(j)} + h_1^{(j)}\right] \times \cdots \times \left[c_n^{(j)} - h_n^{(j)}, c_n^{(j)} + h_n^{(j)}\right].$$

□

With this lemma, 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.

For questions of precision regarding these computations with the units, see 5.2.4.

Algorithm 2.5 Action of a unit to discard parallelotopes

INPUT: a list of problematic parallelotopes $\mathcal{T}$, 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 all translation vectors $\mathcal{V}$
    for each $v \in \mathcal{V}$ **do**
      if for all $\mathcal{Q}^{(j)} \in \mathcal{T}_0$, there exists some $1 \leqslant i \leqslant n$ such that 2.d is *not* checked **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 2.16. *Algorithm 2.5 returns a list a parallelotopes $\mathcal{T}'$ such that for all $x \in \Phi(K)$ such that $m_{\overline{K}}(x) \geqslant k$, $x \in \mathcal{T}'$. The number of floating-point operations required is*

$$O\left(n^{\frac{n+2}{2}} \cdot (\#\mathcal{T})^3 \cdot \left(2^{\frac{n(n-1)}{4}} \cdot \left(n\left(\frac{2^{\frac{n+2}{4}}}{\sqrt{n}}\right)^{n-1} \frac{\sqrt{|d(K)|}}{2r_2}(1 + 2\|\nu\|_\infty)\right) + 1\right)^n\right).$$

Proof. Let us write $\mathcal{T}_0^{(j)}$ the list $\mathcal{T}_0$ at the j^{th} iteration of the loop. We assume that $x \in \mathcal{T}_0^{(j-1)} \setminus \mathcal{T}_0^{(j)}$. We prove by induction on j that for all $x \in \Phi(K)$ such that $m_{\overline{K}}(x) \geqslant k$, $x \in \mathcal{T}_0^{(j)}$. For $j = 0$, it is obvious. Then, we assume that $x \in \mathcal{T}_0^{(j)}$. If $x \notin \mathcal{T}_0^{(j+1)}$, then there exists a unique translation vector v such that $\varepsilon \cdot x - v \in \mathcal{F}$, and $\varepsilon \cdot x - v \notin \mathcal{T}_0^{(j)}$ since 2.d is not checked. Consequently, $m_K(x) = m_K(\varepsilon \cdot x - v) < k$.

As for the number of operations required, see Corollary 5.8. □

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

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

2.4. **Problematic parallelotopes and Euclidean minimum.** At this step, we suppose that for some $k > 0$, there remains the m problematic parallelotopes $(\mathcal{Q}_i)_{1\leqslant i\leqslant m}$. We choose a unit ε which is not a root of unity.

2.4.1. *Action of the units (revisited).* The action of ε does not allow us to eliminate parallelotopes, because for all $1 \leqslant i \leqslant m$, there exists at least one translation vector z of $\varepsilon \cdot \mathcal{Q}_i$ into $\mathcal{F}$ which intersects a 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 $(\varepsilon \cdot \mathcal{Q}_i - z) \cap \mathcal{Q}_j \neq \emptyset$ for some $z \in \Phi(\mathbf{Z}_K)$.

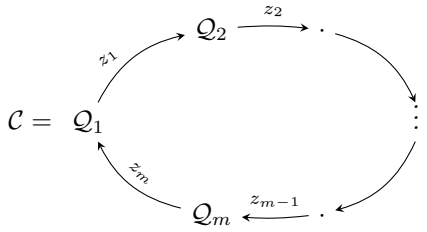
2.4.2. *Convenient graphs.*

Definition 2.17. 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 $t \in \Phi(K)$ such that for any element x in the regions described by the vertices of $\mathcal{C}$, $m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t)$ and $k < m_{\overline{K}}(t)$. As a result, we will be able to compute the Euclidean minimum of K, provided we can obtain a convenient graph.

Theorem 2.18. *Let $\mathcal{C}$ be a simple cycle of $\mathcal{G}$. We write $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ 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*



Then, if we define $\Omega_{\mathcal{C}} = \sum_{j=0}^{m} \varepsilon^j z_{m-j} \in \mathbf{Z}_K$, $\xi_{\mathcal{C}} = \dfrac{\Omega_{\mathcal{C}}}{\varepsilon^m - 1}$ and $t = \Phi(\xi)$, we have for all $x \in \cup_{i=1}^{m} \mathcal{Q}_i$ such that $m_{\overline{K}}(x) \geqslant k$,

(1) $k \leqslant m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t)$,
(2) if $x \in \Phi(K)$, then $x = t$.

Proof. This a straightforward generalization of [6]. □

Corollary 2.19. *We assume that the graph $\mathcal{G}$ is convenient. If $x \in K$ is such that $m_K(x) \geqslant k$, then there exist a simple cycle $\mathcal{C}$ of $\mathcal{G}$ such that $x \in \mathrm{Orb}\,(\xi_{\mathcal{C}})$.*

Remarks 2.20.

- The hypothesis "ε is not a root of unity" is crucial, but it is not a limitation as soon as the rank of units r is positive (and the case $r = 0$ is easy).
- If the algorithm succeeds in building a convenient graph, it will provide all the points $\xi \in K$ for which $M(K) = m_K(\xi)$. If such points do not exist, the algorithm will be unsuccessful.
- In fact, if we apply the algorithm with the value k, if the graph obtained is convenient, Corollary 2.19 allows us to find all elements $x \in K$ (modulo $\mathbf{Z}_K$) such that $m_K(x) \geqslant k$.

- 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 ε
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 2.18), $\mathcal{O} \leftarrow \mathrm{Orb}\,(\xi_{\mathcal{C}})$ (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 $k_0 < \frac{1}{\Lambda(K)}$.

We have yet to decide when we stop cutting further parallelotopes and applying the absorption and units tests. Concretely, we fix an integer $\mathcal{I}$ and we ensure that we perform at most $\mathcal{I}$ consecutive cuttings without improving the smallest number of problematic parallelotopes found. In practice, we choose $\mathcal{I} = 5$.

The procedure may fail when we do not succeed in building a conveniant 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, ϵ is equal to the precision of the absorption test (see Remark 5.12).

If we succeed in finding a convenient graph 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 (see Remarks 2.6, v). Besides, if at any step we obtain $k_1 < 1$, then we can conclude that K is norm-Euclidean.

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

Algorithm 3.1 General algorithm to compute 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 units $\mathfrak{E} = \{\upsilon_1, \dots, \upsilon_l\}$ (Algorithm 2.2)
2: computation of a list of integers $\mathcal{L}$ (Algorithm 2.4)
3: $k_0 \leftarrow \texttt{0.9} \cdot \frac{1}{\Lambda(K)}$, $k \leftarrow \mathcal{K}$, $k_1 \leftarrow \infty$
4: $i \leftarrow 0$, $\mathcal{T}_{\min} \leftarrow \mathcal{T}$
5: **repeat**
6: **for** each parallelotope $\mathcal{P} \in \mathcal{T}$ **do**
7: **if** $\mathcal{P}$ can be absorbed for k by $\mathcal{L}$ (Algorithm 2.3) **then**
8: $\mathcal{T} \leftarrow \mathcal{T} \setminus \mathcal{P}$ (Algorithm 2.5)
9: **end if**
10: **end for**
11: **for** each unit $\nu_i \in \mathfrak{E}$ **do**
12: $\mathcal{T} \leftarrow$ action of the unit ν_i on $\mathcal{T}$
13: **end for**
14: **if** $\#\mathcal{T}_{\min} < \#\mathcal{T}$ **then**
15: $i \leftarrow i + 1$
16: **else**
17: $\mathcal{T}_{\min} \leftarrow \mathcal{T}$
18: **end if**
19: **until** $\mathcal{T} = \emptyset$ **or** $i > I$
20: **if** $\mathcal{T} = \emptyset$ **then**
21: $k_1 \leftarrow k$, $k \leftarrow (1-d) \cdot k_0 + d \cdot k$, $i \leftarrow 0$, **go to** 5
22: **end if**
23: compute the graph $\mathcal{G}$ associated to the action of ν_1 on $\mathcal{T}_{\min}$
24: **if** $\mathcal{G}$ is convenient **then**
25: **for** each simple cycle $\mathcal{C}$ of $\mathcal{G}$ **do**
26: compute the orbit $\mathcal{O}_{\mathcal{C}}$ and the minimum $m_{\mathcal{C}}$ (Algorithm 2.6)
27: **return** greatest value $m_{\mathcal{C}}$ found and the orbits associated
28: **end for**
29: **else**
30: **if** $k_1 - k_0 < \epsilon$ **then**
31: **return** failure
32: **else**
33: $k_0 \leftarrow k$, $k \leftarrow \min\left\{\frac{k+k_1}{2}, k+2\right\}$, $i \leftarrow 0$, **go to** 5
34: **end if**
35: **end if**

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 paragraph 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 $h = (h_i)_{1 \leqslant i \leqslant n}$ 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 Φ 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 $(x_i)_{1\leqslant i\leqslant n} \in \mathcal{P}$,

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

Therefore, we immediately obtain the following result.

Lemma 3.2. *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 3.2. Besides, as we can notice in Figure 3, the action of units is different according to the coordinates, consequently, 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. Otherwise, we stop the cuttings and try to see if we have a convenient graph. Once again, we discard parallelotopes which do not intersect $\mathcal{F}$ thanks to Lemma 3.2.

3.2.2. *Simplification of the graph.* For the construction described in the previous paragraph, the fact that we deal with parallelotopes is not important, we can merge some parallelotopes and Theorem 2.19 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 3.3. 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 $\mathcal{V} \xrightarrow{a} \mathcal{W}$, there exists an edge $\mathcal{V}' \xrightarrow{a} \mathcal{W}$.

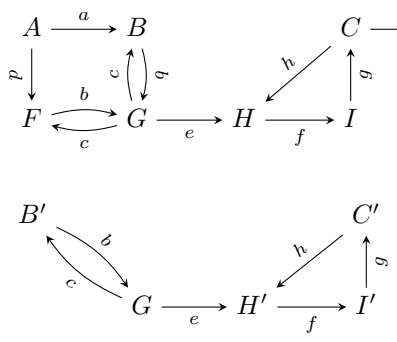
Now, if the vertex $\mathcal{V}$ is compatible with $\mathcal{V}'$, we merge $\mathcal{V}$ et $\mathcal{V}'$ into a new vertex $\mathcal{W}$ such that

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

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 form $\mathcal{V}$. 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 from the merge 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, [18]) and check that they are cycles. In this case, we also get the simple cycles of the 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.

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.

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 critical 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 $\begin{cases} K & \longrightarrow & K \\ x = \sum_{i=1}^n q_i z_i & \longmapsto & \overline{x} = \sum_{i=1}^n (q_i - \lfloor q_i \rfloor) z_i \end{cases}$. Then, we want to compute $\mathcal{O} = \left\{\overline{\varepsilon \cdot \xi},\, \varepsilon \in \mathbf{Z}_K^\times\right\}$. We denote by $(\varepsilon_i)_{1\leqslant i\leqslant r}$ for the fundamental units of K and ν for a generator of the roots of unity of K. We suppose that the order of ν 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 these notations, 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`. Exact computations involve the PARI library ([19]). With the tricks described in paragraph 3.2.2, the algorithm can compute the Euclidean minimum of a number field of degree at most 8 and of small discriminant given simply its minimal polynomial.

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

We consider $p(x) = x^4 - x^3 + 2x^2 - 6x + 3$, α 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.

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

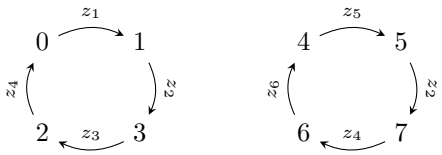
TABLE 1. Problematic parallelotopes in the different steps of the execution of Algorithm 3.1.

With such an input, we obtain a (LLL-reduced) matrix $\mathcal{M}$ such that

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

We choose the initial value $\mathcal{K} = 3$ and we decide to use for $\mathcal{L}$ all useful integers $\mathcal{M}Z$, where $Z \in \mathbf{Z}^n$ and $\|Z\|_\infty \leqslant 25$. 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 $k = 0.46$, 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.



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 8 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 new values of Euclidean minimum. 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 $\frac{1}{\Lambda(K)}$. The number of norm-Euclidean number fields seems to be growing with the degree n.

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 ζ_n is a primitive n^{th} root of unity.

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.

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.

4.3. **Successive minima.**

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

$$M_p(K) = \sup_{\substack{\xi\in K\\ m_K(\xi)<M_{p-1}(K)}} m_K(x) \qquad \text{and} \qquad M_p\left(\overline{K}\right) = \sup_{\substack{x\in H\\ m_{\overline{K}}(x)<M_{p-1}\left(\overline{K}\right)}} m_{\overline{K}}(x).$$

As in the case of the first minimum, we have some precise link between these notions in most cases (cf. [5]).

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, $M(K)$ 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.

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 Corollary 2.19).

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

Example 4.4. Consider $K = \mathbf{Q}(x)$ where x is a root of $X^3 - X^2 - 4X + 12$. Then $d(K) = -676$, $r_1 = r_2 = 1$, $\mathrm{h}_K = 3$. With the Algorithm 3.1, we obtain the orbits of points $t \in K$ such that $m_K(t) \geqslant 1$.

- $\mathcal{O}_1 = \left\{\frac{1}{4}x^2 + \frac{1}{2}x - 1, \frac{1}{4}x^2 + x - 1\right\}$ of minimum 1,
- $\mathcal{O}_2 = \left\{\frac{1}{2}x + \frac{1}{2}, \frac{1}{4}x^2 + \frac{3}{4}x - 1\right\}$ of minimum 1,
- $\mathcal{O}_3 = \left\{\frac{1}{4}x^2 + \frac{3}{4}x - \frac{1}{2}\right\}$ of minimum $\frac{7}{4}$,
- $\mathcal{O}_4 = \left\{\frac{1}{4}x^2 + \frac{1}{4}x - \frac{1}{2}\right\}$ of minimum $\frac{7}{4}$,
- $\mathcal{O}_5 = \left\{\frac{1}{2}x\right\}$ of minimum 1.

Consequently, $M(K) = M\left(\overline{K}\right) = \frac{7}{4}$, $M_2(K) = 1$. This example shows that we may have different orbits with the same Euclidean minimum.

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 smallest discriminant for a given signature. All the number fields listed here have a unique critical orbit.

4.4. **Principal and non-norm-Euclidean number fields.** For small degrees, we can compute extensive values of Euclidean minima of small discriminants. This allows us to find principal and non-norm-Euclidean number fields. Here, we list in Table 3 the principal and non-norm-Euclidean number fields of smallest discriminant. Consequently, all principal number fields of a given signature and of discriminant smaller than the discriminant given (in absolute value) are in fact norm-Euclidean.

4.5. **The case r=1.**

4.5.1. *Non-norm-Euclidean number fields 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.

Example 4.5.
- The cubic number fields of discriminant -199, -335, -351, -367, -755 have an Euclidean minimum equal to 1.
- There are at least 29 number fields of signature $(0,2)$ which have an Euclidean minimum equal to 1.

4.5.2. *A conjecture on cubic number fields.* Many values of Euclidean minima were already known and listed in [4]. These values were a good test for the validity of the

algorithm. In this very article, a conjecture regarding the value of the Euclidean minimum of some cubic fields of mixed signature was formulated: considering l an even positive integer such that $m = l^3 + 1$ is squarefree, we set $K_l = \mathbf{Q}(\alpha)$ where α is a root of $x^3 - m$, it was conjectured that $M(K_l) = m_K\left(\frac{1}{2}(\alpha^2 + \alpha + 1)\right)$ and we know that

$$m_K\left(\frac{1}{2}(\alpha^2+\alpha+1)\right) = \begin{cases} \frac{1}{64}\left(18l^4 - 9l^3 + 12l^2 + 12l\right) & \text{if } l \equiv 2 \mod 4, \\ \frac{1}{64}\left(18l^4 - 9l^3 + 30l^2 + 24l - 32\right) & \text{if } l \equiv 0 \mod 4. \end{cases}$$

Thanks to Algorithm 3.1, we can compute some of these values of $M(K_l)$ and the corresponding critical points.

l	m	$M(K_m)$	critical points
4	65	$\frac{143}{2}$	$\left\{\frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + \frac{1}{2}\right\}$
6	217	$\frac{2451}{92}$	$\left\{\frac{19}{92}\alpha^2 + \frac{3}{92}\alpha + \frac{15}{92}, \frac{35}{276}\alpha^2 + \frac{83}{276}\alpha + \frac{47}{276}\right\}$
10	1001	$\frac{5385}{2}$	$\left\{\frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + \frac{1}{2}\right\}$
12	1729	$\frac{75253}{199}$	$\left\{\frac{40}{199}\alpha^2 + \frac{42}{199}\alpha + \frac{64}{199}, \frac{79}{597}\alpha^2 + \frac{73}{597}\alpha + \frac{7}{597}\right\}$

These values contradict the conjecture in both cases $l \equiv 0 \mod 4$ and $l \equiv 2 \mod 4$.

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 the articles [8] and [9].

Definition 4.6. We say that $\mathbf{Z}_K$ is *two-stage norm-Euclidean* if for any $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, there exist $(\gamma_1, \gamma_2, \delta_1, \delta_2) \in \mathbf{Z}_K^2$ such that

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

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 $m_K(x) \geqslant 1$,
- for any of these points $x = \frac{\alpha}{\beta}$ where $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, find a two-stage Euclidean division for (α, β). The existence of such a division is independant of the choice of (α, β).

Examples 4.7.

- $K = \mathbf{Q}(s)$ 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.
- $K = \mathbf{Q}(s)$ where s is a root of $X^4 - 4X^2 + 5$. Then $d(K) = 1280$ and for any $t \in K$, $m_K(t) \geqslant 1$ if and only if $t \equiv \frac{1}{2}s^3 - \frac{1}{2} \mod \mathbf{Z}_K$.

We consider $\alpha = s^3 - s$, $\beta = 2$, $\gamma_1 = s^3 + s^2$, $\delta_1 = -s^3 - 2s^2 - s$, $\gamma_2 = s^3 - 2s^2 - 2s + 4$ and $\delta_2 = -2s^3 - 3s^2 + 4s + 7$ to prove that K is two-stage Euclidean since $\left|\mathbf{N}_{K/Q}(-2s^3 - 3s^2 + 4s + 7)\right| = 4 < 16 = \left|\mathbf{N}_{K/\mathbf{Q}}(2)\right|$.

- $K = \mathbf{Q}(s)$ where s is a root of $x^6 - 5x^3 + 4x + 2$. Then $d(K) = -12781568$, $M(K) = \frac{11}{8}$ and for any $t \in K$, $m_K(t) \geqslant 1$ if and only if $t \equiv \frac{s^5+s^2}{2} \bmod \mathbf{Z}_K$.

  We consider $\alpha = s^5 + s^2$, $\beta = 2$, $\gamma_1 = s^3$, $\delta_1 = s^5 - 2s^3 + s^2$, $\gamma_2 = -x^3 + 4x$, $\delta_2 = s^5 - s^4 - 4s^3 + 2s^2 + 4$. As $\left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| = 16 < 64 = \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, we can conclude 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 4.8. *If K is principal, $M(K) \geqslant 1$ and K admits only one orbit of minimum greater of 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). Obviously, $\frac{\alpha}{\beta}$ is not a unit. We know that $m_K\left(\frac{\alpha}{\beta}\right) = M(K)$, so 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 $m_K\left(\frac{\beta}{\tau}\right) < \frac{1}{M(K)} = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(\tau)\right|}$ and K is two-stage norm-Euclidean, or $m_K\left(\frac{\beta}{\tau}\right) \geqslant \frac{1}{M(K)}$.

In this case, as there is only one orbit of minimum greater 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 β divides $\tau(\varepsilon\alpha - \beta z)$, so β divides $\tau\alpha$. Since β and α are coprime, β divides τ. Therefore, we may write $\frac{\beta}{\tau} = \frac{1}{\kappa}$ where $\kappa \in \mathbf{Z}_K \setminus \{0\}$. As $\kappa = \left(\frac{\alpha}{\beta}\right)^{-1}$ is not a unit, we have $m_K\left(\kappa^{-1}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(\kappa)\right|} < 1$. Finally, $M(K) = m_K\left(\frac{\beta}{\tau}\right) < 1$, which is impossible. □

Remark 4.9. 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 4.10. 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 (α, β) is principal,

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

We see immediately that any number field of class number 1 is Generalized Euclidean 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 (α, β) is not principal. In fact, this property does not depend on the choice of (α, β), and we easily see it is enough to prove it for one point of each orbit of Euclidean minimum greater or equal to 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
	$(2,2)$	$x^6 - x^4 - x^2 - 2$	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 or equal to 1.

Example 4.11. $K = \mathbf{Q}(x)$ where $x^4 - 2x^3 + 3x^2 + 8x - 14$, $d(K) = -11200$, $r_1 = 2$, $r_2 = 1$, $\mathrm{h}_K = 2$. For all $\xi \in K$, we have $m_K(\xi) \geqslant 1$ if and only if $\xi \equiv \frac{\alpha}{\beta} \mod \mathbf{Z}_K$ of $\xi \equiv \frac{\alpha'}{\beta} \mod \mathbf{Z}_K$ where $\alpha, \alpha', \beta \in \mathbf{Z}_K$ are defined by

$$\alpha = \frac{1}{8}x^3 - \frac{7}{8}x^2 - \frac{1}{4}x + \frac{5}{4},\ \alpha' = \frac{1}{4}x^3 - \frac{3}{4}x^2 - \frac{1}{2}x + \frac{3}{2} \text{ and } \beta = \frac{1}{8}x^3 + \frac{1}{8}x^2 - \frac{1}{4}x - \frac{3}{4}.$$

Then $\mathbf{N}_{K/\mathbf{Q}}(\alpha) = 14$, $\mathbf{N}_{K/\mathbf{Q}}(\beta) = 4$. Consequently, if we write $I = (\alpha, \beta)$, $\mathbf{N}I$ divides $\gcd(4, 14) = 2$. As $I \neq \mathbf{Z}_K$ and there exists no $z \in \mathbf{Z}_K$ such that $\mathbf{N}_{K/\mathbf{Q}}(z) = \pm 2$, we find that I is not principal. Similarly, $I' = (\alpha', \beta)$ is not principal.

Remark 4.12. We can also use PARI ([19]) to check whether or not these ideals are principal.

We can find other examples of non-Euclidean Generalized Euclidean number fields, some of them are listed in Table 5.

We can also provide an example of non-principal number field which is not Generalized Euclidean.

Example 4.13. 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 $\frac{x^3+x}{10} \in \mathcal{O}_2$. 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

n	(r_1, r_2)	minimal polynomial, $K = \mathbf{Q}(x)$	$d(K)$	$M(K)$	N	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 or equal to 1.

5.1. **Proofs of complexity of some procedures.** Previously, we gave the number of operations required for some procedures. In this paragraph, we will prove these results.

5.1.1. *Properties of the matrix $\mathcal{M}$.*

Lemma 5.1. *Let us recall that $\mathcal{M}$ is the LLL-reduction of the matrix defined by 2.a, then*

(1) $|\det \mathcal{M}| = \frac{\sqrt{|d(K)|}}{2^{r_2}}$,

(2) $\|\mathcal{M}\|_\infty \leqslant n \left(\frac{2^{\frac{n+2}{4}}}{\sqrt{n}} \right)^{n-1} |\det \mathcal{M}|$,

(3) $\left\|\mathcal{M}^{-1}\right\|_\infty \leqslant \sqrt{2n} \cdot 2^{\frac{n(n-1)}{4}}$.

Remark 5.2. These upper bounds are generic and much greater than the practical ones. Concretely, in the examples considered, we always have $\|\mathcal{M}\|_\infty < 20$.

Proof. (1) This is an easy consequence of the fact that $\mathcal{M} = \mathcal{N}\mathcal{M}_2$ where

$$\mathcal{N} = \begin{pmatrix} \mathcal{I}_{r_1} & 0 & 0 \\ 0 & \mathcal{I}_{r_2} & \mathcal{I}_{r_2} \\ 0 & \mathcal{I}_{r_2} & -\mathcal{I}_{r_2} \end{pmatrix} \qquad \text{and} \qquad \mathcal{M}_2 = \left(\sigma_i\left(z_j\right)\right)_{1 \leqslant i,j \leqslant n}$$

if we denote by $\mathcal{I}_l$ the identity matrix of size l.

(2) For any l and any vector $v \in \mathbf{R}^l$, we will write $|v| := \sqrt{\sum_{i=1}^{l} v_i^2}$. For any $1 \leqslant j \leqslant n$, $\mathcal{M}_j$ is the j^{th} row of $\mathcal{M}$. First, we will prove that $|\mathcal{M}_j| \geqslant \sqrt{\frac{n}{2}}$ for any $1 \leqslant j \leqslant n$.

For such a j, from the definition of $\mathcal{M}$, we know that there exists some $z_j \in \mathbf{Z}_K \setminus \{0\}$ such that

$$|\mathcal{M}_j|^2 = \sum_{i=1}^{r_1+r_2} |\sigma_i(z_j)|^2 \geqslant \sum_{i=1}^{n} |\sigma_i(z_j)|^2 .$$

This property still holds after LLL-reduction (even though the z_j might be changed). Therefore, thanks to the inequality of arithmetic and geometric means,

$$|\mathcal{M}_j|^2 \geqslant \frac{n}{2} \left(\prod_{i=1}^{n} |\sigma_i(z_j)| \right)^{\frac{2}{n}} .$$

But $\prod_{i=1}^{n} |\sigma_i(z_j)|\, 2 = \left|\mathbf{N}_{K/\mathbf{Q}}(z_j)\right| \geqslant 1$, consequently,

$$|\mathcal{M}_j|^2 \geqslant \frac{n}{2},$$

which proves $|\mathcal{M}_j| \geqslant \sqrt{\frac{n}{2}}$.

Now, as $\mathcal{M}$ is LLL-reduced, $\prod_{j=1}^{n} |\mathcal{M}_j| \leqslant 2^{\frac{n(n-1)}{4}} |\det \mathcal{M}|$, therefore, for any $1 \leqslant j \leqslant n$,

$$|\mathcal{M}_j| \leqslant \left(\frac{2^{\frac{n+2}{4}}}{\sqrt{n}} \right)^{n-1} |\det \mathcal{M}| .$$

This allows us to bound each coefficient of $\mathcal{M}$, then we can easily find the upper bound on $\|\mathcal{M}\|_\infty$ stated.

(3) For any $1 \leqslant i, j \leqslant n$, let us write $\mathcal{M}_{i,j}$ the submatrix obtained by removing the i^{th} row and j^{th} column from $\mathcal{M}$ and $n_{i,j} = (-1)^{i+j} \det \mathcal{M}_{i,j}$ the (i,j) cofactor of $\mathcal{M}$. Then, as $\mathcal{M}^{-1} = \frac{1}{\det \mathcal{M}} (n_{j,i})_{1 \leqslant i,j \leqslant n}$, we will find an upper bound on $|n_{j,i}|$.

Let us write $(C_k)_{1 \leqslant k \leqslant n-1}$ the columns of $\mathcal{M}_{j,i}$. Thanks to Hadamard's inequality,

$$|n_{j,i}| = |\det \mathcal{M}_{j,i}| \leqslant \prod_{k=1}^{n-1} |C_k| .$$

But $|C_k| \leqslant |\mathcal{M}_r|$, where $r = \begin{cases} k & \text{if } k < i \\ k+1 & \text{if } k \geqslant i \end{cases}$. Consequently,

$$|n_{j,i}| \leqslant \frac{\prod_{r=1}^{n} |\mathcal{M}_r|}{|\mathcal{M}_i|}.$$

Then, as $\mathcal{M}$ is LLL-reduced, $\prod_{r=1}^{n} |\mathcal{M}_r| \leqslant 2^{\frac{n(n-1)}{4}} |\det \mathcal{M}|$ and we already saw that $|M_i| \geqslant \sqrt{\frac{n}{2}}$, therefore we find

$$\left| \frac{n_{j,i}}{\det \mathcal{M}} \right| \leqslant \sqrt{\frac{2}{n}} \cdot 2^{\frac{n(n-1)}{4}},$$

from which we easily deduce the result.

□

Now, we can establish the complexity of Algorithm 2.1, which computes the local Euclidean minimum.

5.1.2. *Computation of the local Euclidean minimum.*

Proposition 5.3. *Suppose that k is fixed. The computation of $\mathcal{M}_k$ in Algorithm 2.1 requires at most $\#\mathrm{Orb}\,(x)\cdot\left(2\Gamma(k)\left\|\mathcal{M}^{-1}\right\|_\infty+1\right)^n$ computations of norms.*

Proof. Given $z\in\mathrm{Orb}\,(x)$, we want to know the size of $\mathcal{I}_z$. If $Z\in\mathcal{I}_z$, then $\left\|\mathcal{M}^{-1}z-\mathcal{M}^{-1}Z\right\|_\infty\leqslant\left\|\mathcal{M}^{-1}\right\|_\infty\Gamma(k)$. Consequently,

$$\#\mathcal{I}_z\leqslant\left(2\Gamma(k)\left\|\mathcal{M}^{-1}\right\|_\infty+1\right)^n.$$

□

Corollary 5.4. *Let $x\in K$, Algorithm 2.1 requires at most*

$$\#\mathrm{Orb}\,(x)\cdot\left(2\Gamma\left(\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|\right)\cdot\sqrt{2n}\cdot2^{\frac{n(n-1)}{4}}+1\right)^n$$

computations of norms of elements of K.

Proof. We know that $m_K(x)\leqslant\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|$, consequently, $\mathcal{M}_{\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|}=m_K(x)$. Applying Proposition 5.3 with $k=\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|$ and using Lemma 5.1, (3) give us the result. □

5.1.3. *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. We use the notations of paragraph 2.3.2 to define c' and h', we want to count the maximum number of translation vectors.

Proposition 5.5. *There are at most $\left(\left\|\mathcal{M}^{-1}\right\|_\infty\left(\|\mathcal{M}\|_\infty\left(1+2\|\nu\|_\infty\right)\right)+1\right)^n$ translation vectors of $\mathcal{P}$.*

Proof. Let us consider a translation vector $z=(z_i)_{1\leqslant i\leqslant n}$ of $\mathcal{P}$. Notice that for all $1\leqslant i\leqslant n$,

$$\frac{a_i-b_i-2h_i'}{2}\leqslant z_i-c_i'-\frac{a_i+b_i}{2}\leqslant\frac{b_i-a_i+2h_i'}{2}.$$

As a result, if we write $(c_i'')_{1\leqslant i\leqslant n}=\mathcal{M}^{-1}c'$ and $d=\mathcal{M}^{-1}\left(a_i+b_i\right)_{1\leqslant i\leqslant n}$, then $\|Z-c''-d\|_\infty\leqslant\left\|\mathcal{M}^{-1}\right\|_\infty\left(\|\mathcal{M}\|_\infty\left(1+2\|\nu\|_\infty\right)+1\right)$, which leads easily to the conclusion. □

Remark 5.6. We want to have as few translation vectors as possible, consequently, it is interesting to choose $\varepsilon\in\Phi(\mathbf{Z}_K^\times)$ such that $\|\varepsilon\|_\infty$ is as small as possible. Besides, the upper bound uses the very bad inequality $|h_i'|\leqslant\|\varepsilon\|_\infty\|\mathcal{M}\|_\infty$, for any $1\leqslant i\leqslant n$, we can obtain a better inequality (and better results) by cutting further in the directions i where ε_i is "big".

Proposition 5.7. *Algorithm 2.5 requires*

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

floating-point operations.

Proof. Each step of the while-loop (lines 2 to 14) requires at most $n\cdot\#\mathcal{T}_0$ tests of condition 2.d for each translation vector of each problematic parallelotope. Therefore, each step requires $O\left(n\cdot(\#\mathcal{T}_0)^2\cdot\left(\left\|\mathcal{M}^{-1}\right\|_\infty\left(\|\mathcal{M}\|_\infty\left(1+2\|\nu\|_\infty\right)\right)+1\right)^n\right)$ operations (this is an easy consequence of Lemma 2.14). In the "worst" case (in which we actually succeed in discarding all the parallelotopes), we may need to repeat the loop $\#\mathcal{T}$ times, hence the result. □

Corollary 5.8. *Algorithm 2.5 requires*

$$O\left(n^{\frac{n+2}{2}}\cdot(\#\mathcal{T})^3\cdot\left(2^{\frac{n(n-1)}{4}}\cdot\left(n\left(\frac{2^{\frac{n+2}{4}}}{\sqrt{n}}\right)^{n-1}\frac{\sqrt{|d(K)|}}{2r_2}(1+2\|\nu\|_\infty)\right)+1\right)^n\right)$$

floating-point operations.

Proof. This is a direct consequence of Proposition 5.7 and Lemma 5.1. □

5.2. **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.

5.2.1. *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 $\Gamma(k)$. Let us recall that $\Gamma(k)$ is used to bound each coordinate of vectors of $\Phi(\mathbf{Z}_K)$ required to compute a local Euclidean minimum, therefore, it is enough to find $\Gamma'(k) \geqslant \Gamma(k)$ regardless of errors of computation. As $\Gamma(k)$ is a product of elements $(\Gamma_i)_{1\leqslant i\leqslant n}$, we simply set $(\Gamma'_i)_{1\leqslant i\leqslant n}$ such that for any $1 \leqslant i \leqslant n$,

$$\Gamma_i \leqslant \Gamma'_i.$$

But for any $1 \leqslant i \leqslant n$, $\Gamma_i = \prod_{j=1}^{r} \max\left\{\left|\sigma_i(\varepsilon_j)\right|, \left|\sigma_i(\varepsilon_j^{-1})\right|\right\}$, and if we can compute approximations denoted by $\alpha_{i,j}$ and $\beta_{i,j}$ of $|\sigma_i(\varepsilon_j)|$ and $\left|\sigma_i(\varepsilon_j^{-1})\right|$ up to ϵ, we take $\Gamma'_i = \prod_{j=1}^{r} \max\{\alpha_{i,j}+\epsilon, \beta_{i,j}+\epsilon\}$ and $\Gamma'(k) = \prod_{j=1}^{r} \Gamma'_i \geqslant \Gamma(k)$.

However, the precision is not the actual problem here. In fact, if $\Gamma(k)$ is too big (which happens when the absolute value of a coordinate of the conjugate vectors of the unit ε used is too big or too small), then the computation of the local Euclidean minimum may require too many estimations of norms.

To all practical purposes, we can use the PARI library [19], which features a built-in function to compute the norm of elements of number fields.

5.2.2. *Covering and cutting of the fundamental domain.* All the computations are performed using the matrix $\mathcal{M}$. However, 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 $1 \leqslant i,j \leqslant n$, $|\widetilde{m}_{i,j} - m_{i,j}| < \epsilon$.

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^{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.

5.2.3. *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 $\widetilde{P}$ for the value $k > 0$, which occurs (Lemma 2.8) when $\mathcal{L} < k$, where

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

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 $\mathcal{L}$, we will compute

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

The purpose is to find a real number $\widetilde{k} > 0$ such that the condition $\widetilde{\mathcal{L}} < k'$ implies $\mathcal{L} < k$.

We write $D := \|\widetilde{\mathcal{M}}\|_\infty = \max_{1\leqslant i\leqslant n} \sum_{j=1}^n |\widetilde{m}_{i,j}|$.

Let us recall that the absorption test uses a list $\mathcal{L}$ of integers, we suppose that $\mathcal{L} \subseteq \mathcal{M}[-B, B]^n$. Then the element $\widetilde{Z}$ will be such that, for any $1 \leqslant i \leqslant n$,

$$\left|\widetilde{Z}_i - Z_i\right| < n\epsilon B.$$

We will need to know the following easy estimations on the terms of the products defining $\mathcal{L}$ and $\widetilde{\mathcal{L}}$.

Remark 5.9. For any $1 \leqslant i \leqslant n$,

- $\left|\left|\widetilde{c}_i - \widetilde{Z}_i\right| - |\widetilde{c}_i - Z_i|\right| < nB\epsilon$,
- $\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i < D(B+1) + n\epsilon$.

With these notations, we can estimate the error of computation.

Lemma 5.10.

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

Before proving it, let us start with some easy Lemma.

Lemma 5.11. *We have the following properties.*

(1) Let a, b, c, d be four complex numbers, 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. The first one is obvious. As for the second one, we simply compute

$$\begin{aligned}\left|\prod_{i=1}^{l} b_i - \prod_{i=1}^{l} a_i\right| &= \left|\sum_{i=1}^{l}\left\{\sum_{1\leqslant j_1<\cdots<j_i\leqslant l}\left(\prod_{k=1}^{i}(b_{j_k}-a_{j_k})\right)\left(\prod_{\substack{j=1\\ j\notin\{j_1,\ldots,j_i\}}}^{l} a_j\right)\right\}\right| \\ &< \sum_{i=1}^{l}\binom{l}{i}\rho^i A^{l-i}, \text{ thanks to the triangle inequality,} \\ &= (A+\rho)^l - A^l.\end{aligned}$$

□

Now, we go back to the proof of Lemma 5.10.

Proof of Lemma 5.10. Let us define the n-tuples $a = (a_i)_{1\leqslant i\leqslant n}$ and $b = (b_i)_{1\leqslant i\leqslant n}$ by

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

and

$$b_i = \begin{cases} |\widetilde{c}_i - Z_i| + \widetilde{h}_i & \text{if } 1 \leqslant i \leqslant r_1, \\ |\widetilde{c}_i - Z_i| + \widetilde{h}_i + \mathcal{I}\left(|\widetilde{c}_{i+r_2} - Z_{i+r_2}| + \widetilde{h}_{i+r_2}\right) & \text{if } r_1 < i \leqslant r_1+r_2, \\ |\widetilde{c}_{i-r_2} - Z_{i-r_2}| + \widetilde{h}_{i-r_2} - \mathcal{I}\left(|\widetilde{c}_i - Z_i| + \widetilde{h}_i\right) & \text{if } r_1+r_2 < i \leqslant n. \end{cases}$$

We write $\widetilde{\mathcal{L}}^{(1)} := \prod_{i=1}^{r_1} a_i$, $\widetilde{\mathcal{L}}^{(2)} := \prod_{i=r_1+1}^{n} a_i$, $\mathcal{L}^{(1)} := \prod_{i=1}^{r_1} b_i$ and $\mathcal{L}^{(2)} := \prod_{i=r_1+1}^{n} b_i$, so that

$$\begin{aligned}\left|\widetilde{\mathcal{L}} - \mathcal{L}\right| &= \left|\widetilde{\mathcal{L}}^{(1)}\widetilde{\mathcal{L}}^{(2)} - \mathcal{L}^{(1)}\mathcal{L}^{(2)}\right|, \\ &\leqslant \frac{1}{2}\left(\left|\widetilde{\mathcal{L}}^{(1)} - \mathcal{L}^{(1)}\right|\cdot\left|\widetilde{\mathcal{L}}^{(2)} + \mathcal{L}^{(2)}\right| + \left|\widetilde{\mathcal{L}}^{(1)} + \mathcal{L}^{(1)}\right|\cdot\left|\widetilde{\mathcal{L}}^{(2)} - \mathcal{L}^{(2)}\right|\right) \\ &\quad \text{(thanks to Lemma 5.11, 1),} \\ &\leqslant \frac{1}{2}\left(\left|\widetilde{\mathcal{L}}^{(1)} - \mathcal{L}^{(1)}\right|\cdot\left(2\left|\widetilde{\mathcal{L}}^{(2)}\right| + \left|\widetilde{\mathcal{L}}^{(2)} - \mathcal{L}^{(2)}\right|\right)\right) \\ &\quad + \frac{1}{2}\left(\left(2\left|\widetilde{\mathcal{L}}^{(1)}\right| + \left|\widetilde{\mathcal{L}}^{(1)} - \mathcal{L}^{(1)}\right|\right)\cdot\left|\widetilde{\mathcal{L}}^{(2)} - \mathcal{L}^{(2)}\right|\right).\end{aligned}$$

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

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

We use Lemma 5.11, 2 with $A = D(B+1)+n\epsilon$, $\rho = nB\epsilon$ to obtain

$$\left|\widetilde{\mathcal{L}}^{(1)} - \mathcal{L}^{(1)}\right| < (D(B+1)+n\epsilon)^{r_1}\left[(1+\mu)^{r_1} - 1\right].$$

We apply Lemma 5.11, 2 again with $A = \sqrt{2}\,(D(B+1)+n\epsilon)$, $\rho = nB\epsilon\sqrt{2}$ and we get

$$\left|\widetilde{\mathcal{L}}^{(2)} - \mathcal{L}^{(2)}\right| < 2^{r_2}\,(D(B+1)+n\epsilon)^{r_2}\left[(1+\mu)^{2r_2} - 1\right].$$

Therefore, we obtain

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

from which we easily deduce the result. □

Remark 5.12. The aim of this lemma is to justify the precision of the algorithm. For all practical purposes, the matrix $\widetilde{\mathcal{M}}$ will have a norm smaller than 10, we will use doubles, the minimum will be roughly 1, so $\epsilon \simeq 10^{-15}$ and we will choose B decreasing with the degree n. The table below provides some examples of the precision in the worst case of computation of extended norms.

$n=[K:\mathbf{Q}]$	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	$4\cdot 10^{-2}$

For practical purposes, when we try to absorp parallelotopes by integers for some value $k>0$, we replace k by $k':=k-\eta$, where η is the precision on the norms.

Obviously, the precision is described in the table is computed in the worst case for $D=10$, in practice, we often have a smaller value of D and so a better precision.

5.2.4. *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 embedding of the unit, $\mathcal{M}$ 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 Φ 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 ν 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 $\widetilde{h'}=\left(\widetilde{h'}_i\right)_{1\leqslant i\leqslant n}$.

Lemma 5.13.
- *If* $1\leqslant i\leqslant r_1$, *then* $\left|\widetilde{h'}_i-h'_i\right|<h_i\cdot\epsilon$,
- *if* $r_1<i\leqslant r_1+r_2$, *then* $\left|\widetilde{h'}_i-h'_i\right|<\epsilon\sqrt{h_i^2+h_{i+r_2}^2}$.

Proof. The first case is straightforward, so let us consider $r_1<i\leqslant r_1+r_2$. By definition,

$$h'_i=\left|\nu_i h_i+\mathcal{I}\nu_{i+r_2}h_{i+r_2}\right| \qquad\text{and}\qquad \widetilde{h'}_i=\left|\widetilde{\nu}_i h_i+\mathcal{I}\widetilde{\nu}_{i+r_2}h_{i+r_2}\right|.$$

Consequently, we can apply the triangle inequality to obtain

$$\begin{aligned}\left|\widetilde{h'}_i-h'_i\right| &\leqslant \left|\nu_i h_i+\mathcal{I}\nu_{i+r_2}h_{i+r_2}-(\widetilde{\nu}_i h_i+\mathcal{I}\widetilde{\nu}_{i+r_2}h_{i+r_2})\right| \\ &\leqslant \sqrt{\left(\nu_i-\widetilde{\nu}_i\right)^2 h_i^2+\left(\nu_{i+r_2}-\widetilde{\nu}_{i+r_2}\right)^2 h_{i+r_2}^2} \\ &< \epsilon\sqrt{h_i^2+h_{i+r_2}^2}.\end{aligned}$$

□

Remarks 5.14.
- We have the same estimation 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 ν. Therefore, we compute $\widetilde{c'} = \widetilde{\nu} \cdot c$ and in the same way as for Lemma 5.13, we find

Lemma 5.15.
- *If* $1 \leqslant i \leqslant r_1$, *then* $\left|\widetilde{c'}_i - c'_i\right| < |c_i| \cdot \epsilon$,
- *if* $r_1 < i \leqslant r_1 + r_2$, *then* $\left|\widetilde{c'}_i - c'_i\right| < (|c_i| + |c_{i+r_2}|) \cdot \epsilon$,
- *if* $r_1 + r_2 < i \leqslant n$, *then* $\left|\widetilde{c'}_i - c'_i\right| < (|c_{i-r_2}| + |c_i|) \cdot \epsilon$.

Remark 5.16. Each of these errors is at most $2D\epsilon$, so they are very small. Once again, 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 5.17. *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.

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 Lukas 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, *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.
6. ———, *Euclidean minima of totally real number fields. Algorithmic determination*, Mathematics of Computation **76** (2007), 1547–1575.
7. Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1996.

8. 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.
9. ———, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. II.*, Journal für die reine und angewandte Mathematik **283-284** (1976), 71–85.
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. Keith Matthews, *The Diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers*, Expositiones Mathematicae **18** (2000), 323–331.
17. Richard Mollin, *Simple continued fraction solutions for Diophantine equations*, Expositiones Mathematicae **19** (2001), 55–73.
18. Robert E. Tarjan, *Depth-first search and linear graph algorithms*, SIAM Journal on Computing **1** (1972), 146–160.
19. The PARI Group, Bordeaux, *PARI/GP, version* `2.4.3`, 2008, available from `http://pari.math.u-bordeaux.fr/`.
20. Franciscus Jozef van der Linden, *Euclidean rings with two infinite primes*, Ph.D. thesis, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.

Université de Bordeaux 1, 351 cours de la Libération, 33405 TALENCE - FRANCE
E-mail address: `pierre.lezowski@math.u-bordeaux1.fr`