Euclidean minima of totally real number fields, algorithmic determination

Jean-Paul Cerri

EUCLIDEAN MINIMA OF TOTALLY REAL NUMBER FIELDS ALGORITHMIC DETERMINATION

JEAN-PAUL CERRI

Abstract. This article deals with determining of the Euclidean minimum $M(K)$ of a totally real number field K of degree $n \geq 2$, using techniques from the geometry of numbers. Our improvements of existing algorithms allow us to compute Euclidean minima for fields of degree 2 to 8 and small discriminants, most of which were unknown. Tables are given at the end of this paper.

1. Introduction

This article is devoted to the determination of Euclidean minima (for the norm form) of totally real number fields of small degree. This constant, and more generally the inhomogeneous minimum of lattices, was first studied because of its relation to classical problems such as the norm-Euclideanity of number fields, or as the famous Minkowski's conjecture, but, essentially, in terms of rough estimates. Recall that when the Euclidean minimum is strictly less than 1, the field is norm-Euclidean, hence its ring of integers has a Euclidean division algorithm and therefore is a PID.

On the one hand, beyond the intrinsic interest of the Euclidean minimum, a lot of work has been done on Euclidean number fields. An indispensable paper on the many ramifications of the subject is F. Lemmermeyer's survey [L]. Another recent publication on Euclidean number fields is the article [Q] of R. Quême, published in 1998, in which he describes an algorithm to test whether a given number field is Euclidean. His paper contains tables of norm-Euclidean number fields of degrees 4, 5 and 6, but even for small values of the discriminant, there are some indeterminate cases; moreover, in the totally real case, the tables are very modest for $n \geq 5$.

On the other hand, the problem of determining the Euclidean minimum of number fields has been intensively studied in the years 1940–1950, in the particular case of quadratic fields. The most important reference for this special case is the work of E.S. Barnes and H.P.F. Swinnerton-Dyer [BSD]. More recently S. Cavallar and F. Lemmermeyer [CL] have studied the Euclidean minimum of cubic fields and have developed an algorithm which allowed them to compute it in a large number of cases. Nevertheless, in the totally real case, finding the exact value of the Euclidean minimum is often difficult, and the algorithm is essentially used to see whether a number field is norm-Euclidean or not. Moreover, the criterium used to compute the inhomogeneous minimum does not work when, for instance, the critical points are not isolated. For degree $n > 3$, as far as we know, nothing has been done, except in a few particular cases (see for instance [Ce1]).

Our approach is also algorithmic, but is more efficient for the following reasons:

Date: March 16, 2006.

1991 *Mathematics Subject Classification.* Primary 11Y40 ; Secondary 11R04, 12J15, 13F07.

- the nature of the discretization that we use allows us to work with an optimal precision at each step of the algorithm, which was not the case before (section 5),
- the architecture of the algorithm itself enables us to determine quickly a minimal set of problematic zones,
- thanks to more general theoretical arguments relative to the unit group action on problematic regions (section 4), it is possible to treat difficult cases, when for instance critical points are not isolated.

Our work has two applications:

- in the quadratic and cubic cases, complete the tables that can be found in [L] and [CL],
- in the case of degree greater than 3, compute the Euclidean minimum of number fields of small discriminant. This will allow us to answer some questions that remained open after R. Quême's work, and to extend his tables.

2. Generalities

In this section we give definitions and elementary properties relative to the notions of Euclidean minimum and inhomogeneous minimum. Most results are stated without proofs, for which we refer to the standard literature, e.g. [Ca] and [BSD] for the quadratic case.

2.1. **Basic notations.** Let n be an integer greater than 1. For $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ we put

$$\mathcal{N}(x) = \Big| \prod_{i=1}^{n} x_i \Big|.$$

Let K be a totally real number field of degree n, $\mathbb{Z}_K$ its ring of integers, and D_K its absolute discriminant.
Denote by σ_i, $1 \leq i \leq n$, the n embeddings of K in $\mathbb{R}$, and let Φ be the canonical embedding of K in $\mathbb{R}^n$ defined by

$$\Phi(\xi) = (\sigma_1(\xi), \dots, \sigma_n(\xi)) \quad \text{for all } \xi \in K.$$

Note that $\Phi(\mathbb{Z}_K)$ is a lattice in $\mathbb{R}^n$, and that $|N_{K/\mathbb{Q}}(\xi)| = \mathcal{N}(\Phi(\xi))$.

Definition 2.1. If $x \in \mathbb{R}^n$ is an element of $\Phi(K)$, we shall say that it is a *rational point*. Otherwise, we shall say that it is an *irrational point*.

Let $\mathcal{F}$ be a fundamental domain for $\Phi(\mathbb{Z}_K)$ defined as the fundamental parallelotope associated to a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

Finally, let E_K be the group of units of K. We know, by Dirichlet's theorem, that E_K can be generated by -1 and $n-1$ fundamental units. From now on, we assume that we have at our disposal a system of fundamental units of K denoted by $(\varepsilon_i)_{1 \leq i \leq n-1}$.

We denote by $\mathcal{L}$ the logarithmic embedding of $K \backslash \{0\}$ in $\mathbb{R}^n$ defined by

$$\mathcal{L}(\xi) = (\ln|\sigma_1(\xi)|, \dots, \ln|\sigma_n(\xi)|)\,.$$

Recall that $\mathcal{L}(E_K)$ is a lattice of the hyperplane of $\mathbb{R}^n$ defined by the equation $\sum_{1 \leq i \leq n} x_i = 0$, which admits $(\mathcal{L}(\varepsilon_i))_{1 \leq i \leq n-1}$ as a $\mathbb{Z}$-basis, and that the kernel of $\mathcal{L}$ is $\{\pm 1\}$.

2.2. **Inhomogeneous minimum of a lattice.** The notion of Euclidean minimum of a number field being closely related to the more geometrical notion of inhomogeneous minimum of a lattice, we recall some definitions and properties about the latter.

Definition 2.2. Let $\mathcal{R}$ be a lattice of $\mathbb{R}^n$ and let x be an element of $\mathbb{R}^n$. The real number

$$m_{\mathcal{R}}(x) = \inf\Big\{\mathcal{N}(x - X);\ X \in \mathcal{R}\Big\}$$

is called the *inhomogeneous minimum of* x (for the product form) relative to $\mathcal{R}$.

Proposition 2.1. *$m_{\mathcal{R}}$ has the following properties:*

i) *$m_{\mathcal{R}}(x) = m_{\mathcal{R}}(x - X)$ for all $x \in \mathbb{R}^n$ and all $X \in \mathcal{R}$; thus $m_{\mathcal{R}}$ induces a map (also denoted by $m_{\mathcal{R}}$) on the compact quotient $\mathbb{R}^n/\mathcal{R}$.*

ii) *Make $\mathbb{R}^n$ into an $\mathbb{R}$-algebra via $(x_i) \cdot (y_j) = (x_i y_i)$; if $z \cdot \mathcal{R} = \mathcal{R}$ for some $z \in \mathbb{R}^n$ then $\mathcal{N}(z) = 1$ and $m_{\mathcal{R}}(x) = m_{\mathcal{R}}(z \cdot x - X)$ for all $x \in \mathbb{R}^n$ and all $X \in \mathcal{R}$.*

iii) *$m_{\mathcal{R}}$ is upper semi-continuous on $\mathbb{R}^n$, and on $\mathbb{R}^n/\mathcal{R}$.*

Proof. For i) and iii) see [Ca]. For ii), let f denote the embedding of $\mathbb{R}^n$ in $\mathbb{R}^n$ defined by $f(x) = (z_1 x_1, \ldots, z_n x_n)$. Since $f(\mathcal{R}) = \mathcal{R}$, we have $\mathcal{N}(z) = |\det(f)| = 1$. Moreover, from the definition of $m_{\mathcal{R}}$ and $z.\mathcal{R} = \mathcal{R}$ we have $m_{\mathcal{R}}(z \cdot x) = \mathcal{N}(z) m_{\mathcal{R}}(x)$, and i) gives the result. □

Property iii) of Proposition 2.1 has interesting consequences.

Corollary 2.2. *If $(u_p) \in (\mathbb{R}^n)^{\mathbb{N}}$ and if $\lim_{p \to +\infty} u_p = x \in \mathbb{R}^n$, we have*

$$\limsup_{p \to +\infty} m_{\mathcal{R}}(u_p) \leq m_{\mathcal{R}}(x).$$

Corollary 2.3. *$m_{\mathcal{R}}$ is bounded and attains its maximum at an $x \in \mathbb{R}^n$ (at least one modulo $\mathcal{R}$).*

Now we need some more definitions.

Definition 2.3. We call *inhomogeneous minimum of* $\mathcal{R}$ and we denote $m(\mathcal{R})$ the real number defined by

$$m(\mathcal{R}) = \sup\{m_{\mathcal{R}}(x);\ x \in \mathbb{R}^n\}.$$

Definition 2.4. If $x \in \mathbb{R}^n$ is such that $m_{\mathcal{R}}(x) = m(\mathcal{R})$ we shall say that x is *critical*.

2.3. **Euclidean minimum of K.** Let us now recall some basic facts about the Euclidean minimum of the number field K.

Definition 2.5. Let $\xi \in K$. The *Euclidean minimum of* ξ (relatively to the norm) is the real number $M_K(\xi)$ defined by

$$M_K(\xi) = \inf\Big\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\Big\}.$$

M_K has the following properties.

Proposition 2.4. *We have*

i) *$M_K(\varepsilon\xi - \Upsilon) = M_K(\xi)$ for all $\xi \in K$, $\Upsilon \in \mathbb{Z}_K$ and $\varepsilon \in E_K$.*

ii) *for all $\xi \in K$ there is an $\Upsilon \in \mathbb{Z}_K$ such that $M_K(\xi) = |N_{K/\mathbb{Q}}(\xi - \Upsilon)|$.*

iii) *for $\xi \in K$ we have $M_K(\xi) \in \mathbb{Q}$ and $M_K(\xi) = 0$ if and only if $\xi \in \mathbb{Z}_K$.*

A fundamental example is the following.

Proposition 2.5. *If $\Upsilon \in \mathbb{Z}_K \backslash \{0\}$ and $\Upsilon \notin E_K$, then for every $\xi \in K$ such that $\xi \equiv 1/\Upsilon \bmod \mathcal{R}$, we have*

$$M_K(\xi) = \frac{1}{|N_{K/\mathbb{Q}}(\Upsilon)|}.$$

Proof. Elementary. □

Since $\Phi(\mathbb{Z}_K)$ is a lattice of $\mathbb{R}^n$, the connection between the notions of inhomogeneous and Euclidean minima is obvious. In fact we have

$$M_K(\xi) = m_{\Phi(\mathbb{Z}_K)}(\Phi(\xi))$$

for all $\xi \in K$. From now on, we shall denote $\Phi(\mathbb{Z}_K)$ by $\mathcal{R}$.

To be in conformity with usual notations we shall write $M(\overline{K})$ instead of $m(\mathcal{R})$.

Remark 1. It follows from Proposition 2.1.ii) that

$$m_{\mathcal{R}}(\Phi(\varepsilon) \cdot x - X) = m_{\mathcal{R}}(x) \quad \text{for all } x \in \mathbb{R}^n,\ \varepsilon \in E_K,\ \text{and } X \in \mathcal{R}.$$

As a consequence of Corollary 2.3, we obtain that M_K is bounded on K, and we can give the following definition.

Definition 2.6. We call *Euclidean minimum of K* (for the norm) and we denote by $M(K)$ the real number defined by

$$M(K) = \sup\{M_K(\xi);\ \xi \in K\}.$$

Proposition 2.6. *The value of $M(K)$ gives the following information:*

- *If $M(K) < 1$, then K is norm-Euclidean.*
- *If $M(K) > 1$, then K is not norm-Euclidean.*
- *If $M(K) = 1$, we cannot conclude a priori except if there is an element $\xi \in K$ such that $M(K) = M_K(\xi)$, in which case K is not norm-Euclidean.*

Remark 2. It is clear from the definitions that $M(K) \leq M(\overline{K})$. In fact we have an equality:

$$M(K) = M(\overline{K}).$$

For $n = 2$, this is due to Barnes and Swinnerton-Dyer [BSD]; for a proof for $n \geq 3$ see [Ce2].

We have seen in Proposition 2.4 that if $\xi \in K$, then $m_{\mathcal{R}}(\Phi(\xi))$ (or $M_K(\xi)$) is attained by an element of $\mathcal{R}$ (or $\mathbb{Z}_K$), but this is not true for arbitrary elements of $\mathbb{R}^n$. Thus the fact that for all $\xi \in K$ there is an $\Upsilon \in \mathbb{Z}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K)$, does not imply that for all $x \in \mathbb{R}^n$ there is an $X \in \mathcal{R}$ such that $\mathcal{N}(x - X) \leq M(\overline{K})$ (see Example 2.1 below).

On the other hand, by Corollary 2.3, $M(\overline{K})$ is attained by an $x \in \mathbb{R}^n$, but the same phenomenon concerning M_K is far from being obvious. It has been conjectured by Barnes and Swinnerton-Dyer in the case $n = 2$ (see [BSD]) that there is an element $\xi \in K$ such that $M(\overline{K}) = M_K(\xi)$. Of course, if it is true, we have $M(K) = M(\overline{K}) \in \mathbb{Q}$. In fact, we have also recently proved that this conjecture is true for totally real fields of degree $n \geq 3$, which only leaves the case $n = 2$ indeterminate. An important consequence of this result, in relation with Proposition 2.6,

is that, if $n \geq 3$ and $M(K) = 1$ then K is not norm-Euclidean. Another important corollary is that the question whether a totally real number field of degree $n \geq 3$ is norm-Euclidean or not, is decidable. For more details see [Ce2] and [Ce3].

Example 2.1. The field $\mathbb{Q}\left(\sqrt{13}\right)$ verifies

$$M(K) = M(\overline{K}) = \frac{1}{3}.$$

Modulo $\mathcal{R}$, there are four elements $x_1, \ldots, x_4 \in \Phi(K)$ with $m_{\mathcal{R}}(x_i) = 1/3$, and four infinite sequences $(x_{i,p})$ (with $1 \leq i \leq 4$) of elements of $\mathbb{R}^2 \backslash \Phi(K)$ converging to x_i, with $m_{\mathcal{R}}(x_{i,p}) = \frac{1}{3}$ for all $p \in \mathbb{N}$ and such that $\mathcal{N}(x_{i,p} - X) > \frac{1}{3}$ for all $x_{i,p}$ and all $X \in \mathcal{R}$.

We shall discuss this case later, to illustrate the efficiency of our algorithm.

3. The Euclidean minimum of rational points

In this section, we interest ourselves in the possibility of computing $M_K(\xi)$ for $\xi \in K$. As we shall see later, this is an indispensable condition to the computation of $M(K)$. Let us begin with a lemma.

Lemma 3.1. *If $c_1, \ldots, c_{n-1}$ are $n-1$ given positive real numbers, then there is a unit ν such that*

$$c_i \leq |\sigma_i(\nu)| \leq c_i \Gamma_i$$

for all $i \in \{1, \ldots, n-1\}$, where

$$\Gamma_i = \prod_{j=1}^{n-1} \max\left\{|\sigma_i(\varepsilon_j)|, \frac{1}{|\sigma_i(\varepsilon_j)|}\right\} \tag{1}$$

for all $i \in \{1, \ldots, n\}$.

Proof. The proof is standard and is an easy generalization of the arguments used in [CL] for the cubic case. It rests on the fact that $\mathcal{L}(E_K)$ is a lattice of the hyperplane of $\mathbb{R}^n$ with equation $\sum x_i = 0$ and that

$$\mathcal{D} = \left\{ \sum_{i=1}^{n-1} \lambda_i \mathcal{L}(\varepsilon_i);\ \lambda_i \in [0,1) \text{ for all } i \right\}$$

is a fundamental domain for $\mathcal{L}(E_K)$. □

Our next result will allow us to compute $M_K(\xi)$ if $\xi \in K$.

Proposition 3.2. *Let $x \in \mathbb{R}^n$ and $k' > 0$. If there is an $X \in \mathcal{R}$ such that $x_i = X_i$ for some $i \in \{1, \ldots, n\}$, then $m_{\mathcal{R}}(x) = 0$. If not, suppose that there is an $X \in \mathcal{R}$ such that $\mathcal{N}(x - X) < k'$.*

Then there exists a unit $\nu \in E_k$ and some $Y \in \mathcal{R}$ such that for $y = \Phi(\nu) \cdot x - Y$ we have $\mathcal{N}(y) < k'$ and

$$|y_i| \leq \left(k' \prod_{j=1}^{n-1} \Gamma_j \right)^{\frac{1}{n}}$$

for all $i \in \{1, \ldots, n\}$, with Γ_j as in (1).

Proof. In the same way, the proof is standard. It is a consequence of Lemma 3.1, with

$$c_i = \frac{\left(k' \prod_{j=1}^{n-1} \Gamma_j\right)^{\frac{1}{n}}}{\Gamma_i \, |x_i - X_i|},$$

for $1 \leq i \leq n-1$. □

Now we study what happens with rational points. Recall that E_K acts on $\mathbb{R}^n/\mathcal{R}$ by $(\varepsilon, \overline{x}) \mapsto \overline{\Phi(\varepsilon) \cdot x}$, where $\overline{y}$ is the class of $y \in \mathbb{R}^n$ in $\mathbb{R}^n/\mathcal{R}$.

Let $\mathrm{Orb}(x)$ be the orbit of $\overline{x}$ under this action. It is known that if $x \in \Phi(K)$, $\mathrm{Orb}(x)$ is finite (see for example [CL]). Identifying $\mathbb{R}^n/\mathcal{R}$ and $\mathcal{F}$, this shows that the lift of $\mathrm{Orb}(x)$ in $\mathcal{F} \subset \mathbb{R}^n$ is finite. We shall also denote it by $\mathrm{Orb}(x)$. Remark 1 shows that for all $x \in \mathbb{R}^n$, if $z \in \mathrm{Orb}(x)$ we have $m_{\mathcal{R}}(z) = m_{\mathcal{R}}(x)$. Proposition 3.2 leads us to the following important result.

Theorem 3.3. *Let $x = \Phi(\xi)$ for $\xi \in K$, and let $k' > 0$ be a given positive real number. Then $\mathrm{Orb}(x)$ is finite and, for a given $z \in \mathrm{Orb}(x)$, there are only finitely many $Z \in \mathcal{R}$ with*

$$|z_i - Z_i| \leq \left(k' \prod_{j=1}^{n-1} \Gamma_j\right)^{\frac{1}{n}} \quad \textit{for } i \in \{1, \ldots, n\}.$$

Let $\mathcal{I}_z$ be the set of such Z, and put

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

Then

$$\mathcal{M}_{k'} \leq k' \;\Rightarrow\; m_{\mathcal{R}}(x) = \mathcal{M}_{k'}.$$

Proof. The finiteness assertions are obvious.
We can exclude the trivial case where $x \in \mathcal{R}$, because in this case $x \in \mathrm{Orb}(x)$, $x \in \mathcal{I}_x$ and $\mathcal{M}_{k'} = 0 = m_{\mathcal{R}}(x)$. Thus we can assume that $x \notin \mathcal{R}$, and by Proposition 2.4.iii) we have $m_{\mathcal{R}}(x) > 0$ so that we can apply Proposition 3.2.
Then, for all $z \in \mathrm{Orb}(x)$ and for all $Z \in \mathcal{R}$, we have

$$m_{\mathcal{R}}(x) = m_{\mathcal{R}}(z) \leq \mathcal{N}(z - Z),$$

and by definition of $\mathcal{M}_{k'}$,

$$m_{\mathcal{R}}(x) \leq \mathcal{M}_{k'}.$$

Assume that $m_{\mathcal{R}}(x) < \mathcal{M}_{k'}$ so that for some $X \in \mathcal{R}$ we have

$$\mathcal{N}(x - X) < \mathcal{M}_{k'} \leq k'.$$

By Proposition 3.2, there exists a unit ν and some $Y \in \mathcal{R}$ such that, if $y = \Phi(\nu) \cdot x - Y$, which is of the form $z - Z$ for $(z, Z) \in \mathrm{Orb}(x) \times \mathcal{R}$, we have $\mathcal{N}(y) < \mathcal{M}_{k'}$ and

$$|y_i| \leq \left(\mathcal{M}_{k'} \prod_{j=1}^{n-1} \Gamma_j\right)^{\frac{1}{n}} \leq \left(k' \prod_{j=1}^{n-1} \Gamma_j\right)^{\frac{1}{n}}$$

for all $i \in \{1, \ldots, n\}$. This contradicts the definition of $\mathcal{M}_{k'}$, so that $m_{\mathcal{R}}(x) = \mathcal{M}_{k'}$. □

Thus in order to compute $M_K(\xi) = m_{\mathcal{R}}(x)$ (with $x = \Phi(\xi)$) we just need to determine $\mathrm{Orb}(x)$. Then we compute $k' = \mathcal{M}_k$ for some $k > 0$. If $k' \leq k$ we have $m_{\mathcal{R}}(x) = k'$, otherwise $k'' = \mathcal{M}_{k'} \leq \mathcal{M}_k = k'$, so that $m_{\mathcal{R}}(x) = k''$.

Remark 3. Obviously, it is not necessary to proceed in this way if x is of the form $X + \Phi(1/\Upsilon)$ with $X \in \mathcal{R}$ and $\Upsilon \notin E_K$, because Proposition 2.5 gives us directly $m_{\mathcal{R}}(x) = 1/|N_{K/\mathbb{Q}}(\Upsilon)|$. In practice, this situation is quite common.

4. Theoretical aspect

4.1. **Overview of the strategy.** Now that we know how to compute $M_K(\xi)$ for any ξ in K, it is time to set out the ideas which are behind the algorithm used to compute $M(K) = M(\overline{K})$.

To simplify things we assume that we have an idea of the exact value of $M(K)$. We shall see in the subsection 5.9 how one can find a good candidate for $M(\overline{K})$ or $M(K)$. From now on, we denote by k our guess of $M(K)$.

In fact, instead of proving the equality $M(K) = k$, in view of Remark 2, we shall establish the stronger and more precise result:

$$M(\overline{K}) \leq k \text{ and there exists a } \xi \in K \text{ such that } M_K(\xi) = k.$$

It will clearly follow that $M(K) = M(\overline{K}) = k$. Moreover, we shall try to find all the critical rational points.

Since $m_{\mathcal{R}}$ is defined modulo $\mathcal{R}$, it is sufficient to work on $\mathcal{F}$, i.e. to prove that for all $x \in \mathcal{F}$, $m_{\mathcal{R}}(x) \leq k$, and to find all the $\xi \in K$ such that $\Phi(\xi) \in \mathcal{F}$ and $M_K(\xi) = k$ (every solution to $M_K(\xi) = k$ will be of this form modulo $\mathbb{Z}_K$).

Let k' be a positive number smaller than k. In practice one takes $k' = k - \epsilon$ where ϵ is a small positive number. Let us consider a finite family of elements of $\mathcal{R}$, say $\mathcal{X}$, and the regions centered in the X of $\mathcal{X}$ and defined by the inequalities $\mathcal{N}(x - X) \leq k'$. Every element x of the subset of $\mathcal{F}$, covered by these regions verifies $m_{\mathcal{R}}(x) \leq k' < k$, and since k' is supposed smaller than $M(\overline{K})$, "holes" appear in the covering of $\mathcal{F}$ by these regions. These holes contain the potentially critical points of $\mathcal{F}$.

Figure 1 illustrates what is happening for $K = \mathbb{Q}(\sqrt{2})$. Here we have taken $k' = 0.35$, we have chosen $\mathcal{F}$ as the parallelogramm whose four vertices are $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(\sqrt{2})$ and $D = \Phi(\sqrt{2} - 1)$, and $\mathcal{X}$ as the set of these four points. We see that the four regions nearly cover $\mathcal{F}$. In fact, a single hole T is uncovered.

The main idea is then to analyze the action of the unit group on uncovered subsets of $\mathcal{F}$, in the following way. Let T be a hole of $\mathcal{F}$, and ε a non-torsion unit of K ($\varepsilon \neq \pm 1$). We look at the possible intersections of $\Phi(\varepsilon) \cdot T$ with holes of $\mathcal{F}$ modulo $\mathcal{R}$. If $\Phi(\varepsilon) \cdot T$ does not intersect any hole of $\mathcal{F}$ modulo $\mathcal{R}$, we know by Remark 1 that for every x of T, we have $m_{\mathcal{R}}(x) \leq k'$, so that T can be eliminated as a subset of $\mathcal{F}$ potentially containing a critical point. The interesting case is when the intersection is nonempty.

Figure 2, which corresponds to Figure 1, displays the action of $\varepsilon = 1 + \sqrt{2}$ on the hole T. Here, we have $T' = \Phi(\varepsilon) \cdot T$, $T'' = \Phi(\varepsilon) \cdot T - \Phi(1)$. Putting $\Upsilon = 1$, we can write

$$(\Phi(\varepsilon) \cdot T - \Phi(\Upsilon)) \setminus \mathcal{H} \subset T,$$

where $\mathcal{H}$ is the subset of $\mathbb{R}^n$ whose elements x verify $m_{\mathcal{R}}(x) \leq k' < k$. This inclusion corresponds to the simplest case that can occur. What can be said in this case will be the object of our next theorem.

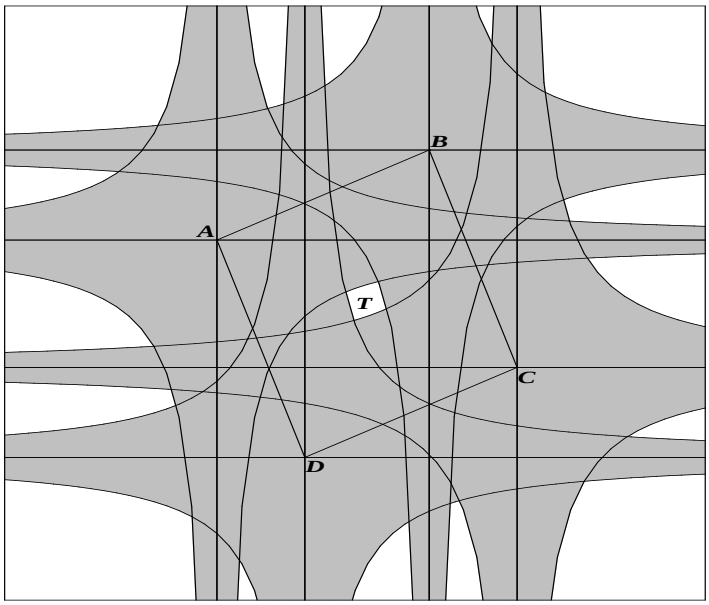

Figure 1. Covering of $\mathcal{F}$ by hyperbolic regions

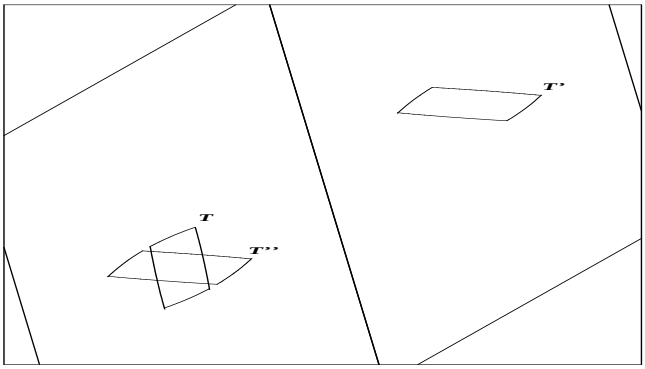

Figure 2. $T'' = \Phi(1+\sqrt{2}) \cdot T - \Phi(1)$ meets T

Remark 4. Here we have expressed things in terms of holes. In what follows, we consider "easy" regions larger than holes. For instance, in the algorithm, holes are replaced by regions composed of small parallelotopes. All what we need is to have a partition of $\mathcal{F}$ in a covered region and in regions potentially containing critical points. Then we check that these regions have an exploitable behaviour under the action of E_K.

4.2. **Theoretical argumentation.** As in the previous subsection, we consider $k' > 0$ and the subset $\mathcal{H}$ of $\mathbb{R}^n$ defined by

$$\mathcal{H} = \{x \in \mathbb{R}^n \text{ such that } m_{\mathcal{R}}(x) \leq k'\}.$$

We consider also a unit $\varepsilon \neq \pm 1$.

4.2.1. *First results.* The cyclic situation studied in the following theorem is a generalization of the situation of Figure 2.

Theorem 4.1. *Let $\mathcal{T}_0,\dots,\mathcal{T}_{j-1}$ be bounded subsets of $\mathbb{R}^n$ ($j\geq 1$). Assume that for all l there is an $\Upsilon_l\in\mathbb{Z}_K$ such that*

$$(\Phi(\varepsilon)\cdot\mathcal{T}_l-\Phi(\Upsilon_l))\setminus\mathcal{H}\subset\mathcal{T}_{l+1}, \tag{2}$$

where the indices in $\mathcal{T}_r$ are to be read modulo j. Assume also that there is an x in $\mathcal{T}_0$ which verifies $m_{\mathcal{R}}(x)>k'$ and define $\Omega\in\mathbb{Z}_K$ by

$$\Omega=\varepsilon^{j-1}\Upsilon_0+\varepsilon^{j-2}\Upsilon_1+\ldots.+\varepsilon\Upsilon_{j-2}+\Upsilon_{j-1}.$$

Consider the sequence defined by $y_0=x$ and $y_{p+1}=\Phi(\varepsilon^j)\cdot y_p-\Phi(\Omega)$ for all $p\geq 0$. Then, if we put

$$\xi=\frac{\Omega}{\varepsilon^j-1}\quad\text{and}\quad t=\Phi(\xi),$$

we have

i) *For all $i\in\{1,\dots,n\}$ such that $|\sigma_i(\varepsilon)|>1$ and for all $p\geq 0$, $(y_p)_i=t_i$.*
ii) *The sequence $(y_p)_{p\geq 0}$ converges to t.*
iii) *$k'<m_{\mathcal{R}}(x)\leq m_{\mathcal{R}}(t)$.*
iv) *If $x\in\Phi(K)$ then $x=t$.*

Proof. First of all, let us prove that

$$\big(\Phi(\varepsilon^j)\cdot\mathcal{T}_0-\Phi(\Omega)\big)\setminus\mathcal{H}\subset\mathcal{T}_0. \tag{3}$$

Put $z=\Phi(\varepsilon^j)\cdot z_0-\Phi(\Omega)$ where $z_0\in\mathcal{T}_0$ and suppose $z\notin\mathcal{H}$. Let us define z_1, $z_2,\dots,z_j$ by the induction formula $z_{p+1}=\Phi(\varepsilon)\cdot z_p-\Phi(\Upsilon_p)$ for $0\leq p<j$.
It is easy to see that we have $z_j=z$. By Remark 1 we can write

$$m_{\mathcal{R}}(z)=m_{\mathcal{R}}(z_j)=m_{\mathcal{R}}(z_{j-1})=\ldots=m_{\mathcal{R}}(z_0)>k'.$$

Thus for all $p\in\{0,\dots,j\}$ we have $z_p\notin\mathcal{H}$, and by successive applications of (2) we get $z_p\in\mathcal{T}_p$ for all $p\in\{0,\dots,j-1\}$, and finally $z=z_j\in\mathcal{T}_0$, so that we have (3).

Now, consider the sequence $(y_p)_{p\geq 0}$. By Remark 1 we see by induction that for all $p\geq 0$

$$m_{\mathcal{R}}(y_p)=m_{\mathcal{R}}(x)>k' \tag{4}$$

so that for all $p\geq 0$, $y_p\notin\mathcal{H}$. Then, as $y_0=x\in\mathcal{T}_0$, using (3) we easily establish by induction that $y_p\in\mathcal{T}_0$ for all $p\geq 0$. Thus, as $\mathcal{T}_0$ was assumed to be bounded, the sequence $(y_p-t)_{p\geq 0}$ is bounded.

But, by the definition of t and the induction formula which defines $(y_p)_{p\geq 0}$, we have $y_p-t=\Phi(\varepsilon)^p\cdot(x-t)$ for all $p\geq 0$, so that

$$|(y_p)_i-t_i|=|\sigma_i(\varepsilon)|^p\,|x_i-t_i|\text{ for all }i\in\{1,\dots,n\}\text{ and for all }p\geq 0. \tag{5}$$

If $|\sigma_i(\varepsilon)|>1$, since the sequence $(|(y_p)_i-t_i|)_{p\geq 0}$ is bounded, we must have $x_i-t_i=0$, and then by (5) we obtain

$$(y_p)_i=t_i\text{ for all }p\geq 0. \tag{6}$$

This is i).

Moreover if $|\sigma_i(\varepsilon)|<1$, then (5) shows that

$$\lim_{p\to+\infty}(y_p)_i=t_i. \tag{7}$$

Since $|\sigma_i(\varepsilon)| \neq 1$ (otherwise $\varepsilon = \pm 1$, which is excluded by hypothesis), (6) and (7) yield

$$\lim_{p\to+\infty} y_p = t.$$

This is ii). Finally by Corollary 2.2 and (4), we obtain:

$$k' < m_{\mathcal{R}}(x) = \limsup_{p\to+\infty} m_{\mathcal{R}}(y_p) \leq m_{\mathcal{R}}(t),$$

which gives iii).

Now, assume that $x \in \Phi(K)$. Since we cannot have $|\sigma_i(\varepsilon)| \leq 1$ for every i, there exists an $i \in \{1, \ldots, n\}$ such that $|\sigma_i(\varepsilon)| > 1$, and by i) (with $p = 0$) we have $x_i = t_i$. But x and t are both in $\Phi(K)$, and by injectivity of σ_i, this leads to $x = t$. □

Remark 5. Obviously the same property holds for $\mathcal{T}_1$, $\mathcal{T}_2$,... the only thing changed being the formula for Ω, in which indices must be trivially permuted. More precisely, for $r \in \{0, \ldots, j-1\}$, if we put $t_r = \Phi(\xi_r)$ with

$$\xi_r = \frac{\Omega_r}{\varepsilon^j - 1},$$

and

$$\Omega_r = \varepsilon^{j-1}\Upsilon_r + \varepsilon^{j-2}\Upsilon_{r+1} + \ldots + \Upsilon_{j-1+r},$$

where the indices are still to be read modulo j, we have the same property as in Theorem 4.1 for $\mathcal{T}_r$ (with t_r instead of t). Moreover $t_0 = t$ and we have the cyclic law:

$$t_{r+1} = \Phi(\varepsilon) \cdot t_r - \Phi(\Upsilon_r)$$

for all $r \in \{0, \ldots, j-1\}$. In particular, all the t_r are in $\mathrm{Orb}(t)$ modulo $\mathcal{R}$.

Example 4.1. In the case of $K = \mathbb{Q}(\sqrt{2})$ seen above (Figures 1 and 2) with $\varepsilon = 1 + \sqrt{2}$, we have $j = 1$, and $\Upsilon_0 = 1$. Theorem 4.1 shows that for every point x of T which verifies $m_{\mathcal{R}}(x) > 0.35$, we necessarily have $m_{\mathcal{R}}(x) \leq M_K(\xi)$ where $\xi = \sqrt{2}/2$. Since $M_K(\xi)$ is equal to $1/2$ this leads to the well known equality $M(K) = M(\overline{K}) = 1/2$.

Theorem 4.1 admits the following corollary, which can be useful for proving that the critical points are isolated and for computing the second inhomogeneous minimum of $\mathcal{R}$.

Corollary 4.2. *Assume the hypotheses of Theorem* 4.1 *and that* ε^{-1} *acts on the* $\mathcal{T}_l$ *in the following way: for all* l *there is some* $\Upsilon'_l \in \mathbb{Z}_K$ *such that*

$$\left(\Phi(\varepsilon^{-1}) \cdot \mathcal{T}_l - \Phi(\Upsilon'_l)\right) \setminus \mathcal{H} \subset \mathcal{T}_{l-1},$$

with the same convention on the indices as in (2). *Assume also that* $\mathcal{T}_0$ *is sufficiently "small" to have*

$$(z_1, z_2) \in \mathcal{T}_0^2 \text{ and } z_1 - z_2 \in \mathcal{R} \Rightarrow z_1 = z_2. \tag{10}$$

Then we have the stronger conclusion $x = t$.

Proof. Let us define y'_1 by

$$y'_1 = \Phi(\varepsilon^{-j}) \cdot x - \Phi(\Omega'), \tag{11}$$

with $\Omega' = \varepsilon^{1-j}\Upsilon'_0 + \varepsilon^{2-j}\Upsilon'_1 + \ldots. + \varepsilon^{-1}\Upsilon'_{j-2} + \Upsilon'_{j-1}$. Starting again as in the precedent demonstration (with the inverse order on the $\mathcal{T}_l$) we see that $y'_1 \in \mathcal{T}_0 \backslash \mathcal{H}$. But again by (3),

$$\Phi(\varepsilon^j) \cdot y'_1 - \Phi(\Omega) \in \mathcal{T}_0 \backslash \mathcal{H}.$$

Then (11) gives

$$x - \Phi(\varepsilon^j \Omega' + \Omega) \in \mathcal{T}_0 \backslash \mathcal{H}.$$

But we see that x and $x - \Phi(\varepsilon^j\Omega' + \Omega)$ are both in $\mathcal{T}_0$ and that their difference is in $\mathcal{R}$. By (10) this implies that they are equal. Thus we have

$$\varepsilon^j \Omega' + \Omega = 0. \tag{12}$$

By Theorem 4.1 (applied with ε^{-1} and $p = 0$) and (12) we find that

$$x_i = \left(\frac{\Omega'}{\varepsilon^{-j} - 1}\right)_i = \left(\frac{\Omega}{\varepsilon^j - 1}\right)_i = t_i. \tag{13}$$

for all i such that $|\sigma_i(\varepsilon^{-1})| > 1$.

But we also know by Theorem 4.1 that

$$\text{for all } i \text{ such that } |\sigma_i(\varepsilon)| > 1,\ x_i = t_i. \tag{14}$$

Since for all i, $|\sigma_i(\varepsilon)| \neq 1$, (13) and (14) yield $x = t$. □

4.2.2. *Generalization.* Even if Theorem 4.1 allows one to treat a lot of situations, it is not sufficient, in the form seen above, to cover all the cases that one meets in practice. A generalization of the previous situation is the following one.

Let $\mathcal{T}_i$ $(0 \leq i \leq s-1)$ be distinct bounded sets of $\mathbb{R}^n$, and $T = \{\mathcal{T}_0, \ldots, \mathcal{T}_{s-1}\}$. Assume that for all $\mathcal{T}_i$ in T there exists an $X_i \in \mathcal{R}$ and s_i integers $n_{i,1}, \ldots, n_{i,s_i}$ $(s_i > 0)$ such that

$$(\Phi(\varepsilon) \cdot \mathcal{T}_i - X_i) \setminus \mathcal{H} \subset \bigcup_{1 \leq k \leq s_i} \mathcal{T}_{n_{i,k}}. \tag{15}$$

To simplify notations we shall consider the $\mathcal{T}_i$ as the vertices of a directed graph (from now on digraph) G and represent (15) by s_i directed edges (from now on arcs) whose tail is $\mathcal{T}_i$ and whose respective heads are the $\mathcal{T}_{n_{i,k}}$ $(1 \leq k \leq s_i)$. Of course, such an arc can be a loop.
We shall write $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$ (X_i) or $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$, if it is not necessary to precise X_i.

Example 4.2. Theorem 4.1 corresponds to the digraph

$$G_1 : \mathcal{T}_0 \to \mathcal{T}_1\ (\Phi(\Upsilon_0)), \ldots, \mathcal{T}_{j-1} \to \mathcal{T}_0\ (\Phi(\Upsilon_{j-1})).$$

To describe paths of G we shall use the notation $\mathcal{T}'_1 \to \mathcal{T}'_2 \to \ldots \to \mathcal{T}'_k$.

The digraph G has the following properties: if $\mathcal{T}$ and $\mathcal{T}'$ are vertices of G, there is at most one arc whose tail is $\mathcal{T}$ and whose head is $\mathcal{T}'$, and every vertex of G has a positive outvalency. Obviously the last property implies that G contains circular paths (or circuits). Consequently, the set of simple circuits of G (paths of the form $\mathcal{T}'_0 \to \ldots \to \mathcal{T}'_k \to \mathcal{T}'_0$, where $k \geq 0$ and all the $\mathcal{T}'_i$ are distinct) is *nonempty* (take a circuit of minimal length) and is *finite* (their length cannot exceed s). Let us denote the latter by $\mathcal{C}$. Each element c of $\mathcal{C}$ of length j is of the form of the circular path met in Theorem 4.1 (and seen above in G_1), $\mathcal{T}'_0 \to \mathcal{T}'_1(X'_0) \ldots \to \mathcal{T}'_{j-1}(X'_{j-2}) \to \mathcal{T}'_0(X'_{j-1})$ with $X'_i = \Phi(\Upsilon_i)$. It defines, in a unique way, j rational points $t_0, \ldots, t_{j-1}$ by the formulae of Remark 5.

Definition 4.1. In this context, we say that $t_0, \ldots, t_{j-1}$ are *associated* to c (implicitly t_i corresponds to $\mathcal{T}_i'$).

The t_i are in the same orbit modulo $\mathcal{R}$ and verify $m_{\mathcal{R}}(t_0) = \ldots = m_{\mathcal{R}}(t_{j-1})$. Let us denote this rational number by $m(c)$ and put

$$m(G) = \max_{c \in \mathcal{C}} m(c).$$

Moreover, let us denote by $\mathcal{E}$ the set of all rational points associated to the elements of $\mathcal{C}$. The set $\mathcal{E}$ is *finite* and we also have

$$m(G) = \max_{t \in \mathcal{E}} m_{\mathcal{R}}(t).$$

Finally let us put

$$\mathcal{E}' = \{t \in \mathcal{E} \text{ such that } m_{\mathcal{R}}(t) = m(G)\}.$$

Definition 4.2. An *infinite path* of G is an infinite sequence of arcs of G, $(A_i)_{i \geq 0}$ such that the head of A_i is the tail of A_{i+1}. If A_i is defined by $\mathcal{T}_i' \to \mathcal{T}_{i+1}'$, we shall denote the path by $(\mathcal{T}_i')_{i \geq 0}$.

Such a path is not simple, but can have a periodicity property.

Definition 4.3. An infinite path $(\mathcal{T}_i')$ is said to be *ultimately periodic* if there exist integers $r \geq 0$ and $p \geq 1$ such that

$$\text{for all } i \geq r,\ \mathcal{T}_{i+p}' = \mathcal{T}_i'. \tag{16}$$

Let $(\mathcal{T}_i')_{i \geq 0}$ be an ultimately periodic infinite path. Let $\mathcal{P}$ be the set of $p \geq 1$ such that there exists an r with (16) true. Then $\mathcal{P}$ is nonempty and we can define

$$\rho = \min \mathcal{P} \geq 1. \tag{17}$$

Then

$$\text{there exists an } r_\rho \text{ such that for all} i \geq r_\rho,\ \mathcal{T}_{i+\rho}' = \mathcal{T}_i'. \tag{18}$$

Definition 4.4. ρ will be called the period length of $(\mathcal{T}_i')_{i \geq 0}$ and every circuit $\mathcal{T}_i' \to \ldots \to \mathcal{T}_{i+\rho}'$, where $i \geq r_\rho$, will be called a period of $(\mathcal{T}_i')_{i \geq 0}$

Definition 4.5. We shall say that G is *convenient* if every infinite path of G is ultimately periodic.

Example 4.3. G_1 is convenient. Figure 3 gives examples of convenient and not convenient digraphs.

Proposition 4.3. *Assume that G is convenient. Then every circuit is a power of a simple circuit.*

Proof. Let c be a circuit of G. Denote it by $\mathcal{T} \to \ldots \to \mathcal{T}$. Decompose c as $c_1 c_2 \ldots c_d$ ($d \geq 1$) where the c_i are circuits of the form $\mathcal{T} \to \ldots \to \mathcal{T}$ "simple in $\mathcal{T}$". Suppose that there exists $i > 1$ with $c_i \neq c_1$. Then we can exhibit an infinite path which is not ultimately periodic, namely $c_1 c_i c_1 c_1 c_i c_1 c_1 c_1 c_i \ldots$, which is impossible since G is convenient. Thus $c = c_1^d$.
Now, let us prove that c_1 is simple. If it is not, since it is "simple in $\mathcal{T}$", it is of the form $\mathcal{T} \to \ldots \to \mathcal{T}' \to \ldots \to \mathcal{T}' \to \ldots \to \mathcal{T}$ with $\mathcal{T}' \neq \mathcal{T}$ and where $\mathcal{T}$ is not a vertex of $\mathcal{T}' \to \ldots \to \mathcal{T}'$. If we decompose c_1 in the product of paths $P_1 P_2 P_3$ where P_2 is $\mathcal{T}' \to \ldots \to \mathcal{T}'$, we see that $P_1 P_3 = P$ and P_2 are two circuits having a

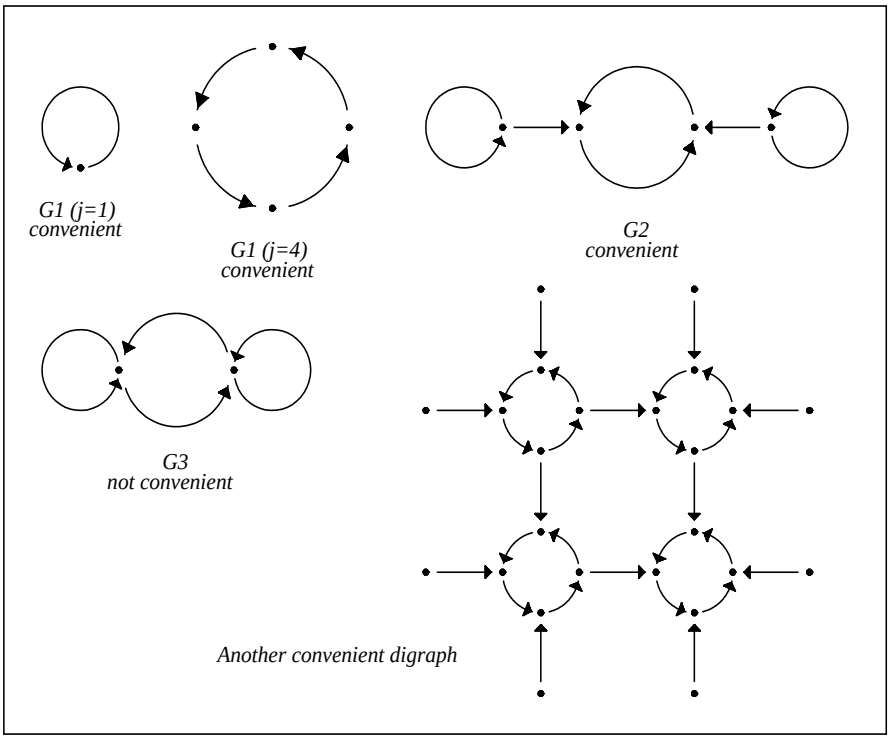

Figure 3. Some digraphs

common vertex $\mathcal{T}'$. Thus we can define the infinite path $PP_2PP_2P_2PP_2P_2P_2P\ldots$ which is not ultimately periodic since $\mathcal{T}$ is not a vertex of P_2. Once again this contradicts the fact that G is convenient. □

Remark 6. It can be shown that the above condition implies that G is convenient. Another characterisation of convenient digraphs could be the following one: two distinct simple circuits have no common vertex.

Corollary 4.4. *Assume that G is convenient and let $P = (\mathcal{T}'_i)_{i\geq 0}$ be an infinite path of G. Then, P is ultimately periodic and every period of P is a simple circuit.*

Proof. Since G is convenient P is ultimately periodic. Consider a period c of length ρ. By Proposition 4.3, c is the power of a simple circuit: $c = c_1^d$ with $d \geq 1$. But if $d > 1$, it is clear that c_1 has a length $p = \rho/d$ smaller than ρ. From $c = c_1^d$ and (18) we see that $p \in \mathcal{P}$, but this contradicts (17). Thus $d = 1$ and c is simple. □

Now, we can establish the theorem which will allow us to treat all the situations.

Theorem 4.5. *Assume that G is convenient and that there exists a $\mathcal{T} \in T$ and an $x \in \mathcal{T}$ such that $m_{\mathcal{R}}(x) > k'$. Then*

i) $k' < m_{\mathcal{R}}(x) \leq m(G)$.
ii) *If $x \in \Phi(K)$, there exists a $t \in \mathcal{E}$ such that $x \equiv t \bmod \mathcal{R}$.*
iii) *If $x \in \Phi(K)$ is critical, there exists a $t \in \mathcal{E}'$ such that $x \equiv t \bmod \mathcal{R}$.*

Proof. Put $x_0 = x$ and $\mathcal{T}'_0 = \mathcal{T}$. By (15) we know that there exists $X'_0 \in \mathcal{R}$ and s'_0 elements of T, denoted by $\mathcal{T}_{n'_{0,k}}$ $(1 \leq k \leq s'_0)$ such that

$$(\Phi(\varepsilon) \cdot \mathcal{T}'_0 - X'_0) \setminus \mathcal{H} \subset \bigcup_{1 \leq k \leq s'_0} \mathcal{T}_{n'_{0,k}}.$$

Set $x_1 = \Phi(\varepsilon) \cdot x_0 - X'_0$. Since $m_{\mathcal{R}}(x_1) = m_{\mathcal{R}}(x_0) > k'$, we have

$$x_1 \in (\Phi(\varepsilon) \cdot \mathcal{T}'_0 - X'_0) \setminus \mathcal{H},$$

and necessarily, there is an $i \in \{1, \ldots, s'_0\}$ such that $x_1 \in \mathcal{T}_{n'_{0,i}}$. We put $\mathcal{T}'_1 = \mathcal{T}'_{n'_{0,i}}$, and we continue with $x_2 = \Phi(\varepsilon) \cdot x_1 - X'_1$ where X'_1 is the element of $\mathcal{R}$ associated to $\mathcal{T}'_1$ by (15). We see that we can construct by induction a sequence $(x_i)_{i \geq 0}$ and an infinite path $(\mathcal{T}'_i)_{i \geq 0}$ which verify: $x_0 = x$, for all $i \geq 0$, $x_{i+1} = \Phi(\varepsilon) \cdot x_i - X'_i$ where $X'_i \in \mathcal{R}$ and

$$\text{for all } i \geq 0,\ x_i \in \mathcal{T}'_i. \tag{19}$$

Moreover, by Remark 1, we have $m_{\mathcal{R}}(x_i) = m_{\mathcal{R}}(x) > k'$ for all i.
G being convenient, the infinite path $(\mathcal{T}'_i)_{i \geq 0}$ is ultimately periodic. We denote its period length ρ and we consider one of its periods c, described by $\mathcal{T}'_r \to \ldots \to \mathcal{T}'_{r+\rho} = \mathcal{T}'_r$, which is a simple circuit by Corollary 4.4.
Define $\mathcal{T}''_s = \{x_{r+s+i\rho};\ i \in \mathbb{N}\}$, for $0 \leq s \leq \rho - 1$.
By (19), for every $s \in \{0, \ldots, \rho - 1\}$, we have $\mathcal{T}''_s \subset \mathcal{T}'_{r+s}$. This implies that the $\mathcal{T}''_s$ are bounded. Moreover, by construction, for all s there exists $\Upsilon_s \in \mathbb{Z}_K$ (in fact $\Phi^{-1}(X'_{r+s})$) such that

$$\Phi(\varepsilon) \cdot \mathcal{T}''_s - \Phi(\Upsilon_s) \setminus \mathcal{H} = \Phi(\varepsilon) \cdot \mathcal{T}''_s - \Phi(\Upsilon_s) \subset \mathcal{T}''_{s+1},$$

where the indices are to be read modulo ρ. Putting $y = x_r \in \mathcal{T}''_0$ which verifies $m_{\mathcal{R}}(y) > k'$, we see that we are exactly under the hypotheses of Theorem 4.1 (with y instead of x, $\mathcal{T}''_i$ instead of $\mathcal{T}_i$ and ρ instead of j). This theorem defines ρ rational points t_i associated to the simple circuit c.
By definition of $m(c)$, and by Theorem 4.1.iii), we obtain

$$k' < m_{\mathcal{R}}(x) = m_{\mathcal{R}}(x_r) \leq m(c),$$

and by definition of $m(G)$ we have i).

Assume now that $x \in \Phi(K)$ so that, by induction, $x_r \in \Phi(K)$. By Theorem 4.1.iv) we have $x_r = t_0$, and thus $x_r - t_0 \in \mathcal{R}$. By the induction formula of the definition of (x_i) and the formulae of Remark 5, we see that

$$\text{for all } k \in \{0, \ldots, r\},\ \Phi(\varepsilon) \cdot (x_{r-k} - t_{-k}) \in \mathcal{R},$$

where the index in t_{-k} is taken modulo ρ. Finally, $x = x_0 \equiv t_{-r} \bmod \mathcal{R}$, which is an element of $\mathcal{E}$ by definition of $\mathcal{E}$. This proves ii).

Assume now that x is critical so that we have $m_{\mathcal{R}}(x) = M(\overline{K})$. From the definitions, we can write $m_{\mathcal{R}}(x) \geq m(G)$ and by i) we obtain $m_{\mathcal{R}}(x) = m(G)$ so that $m_{\mathcal{R}}(t_{-r}) = m(G)$. Since $t_{-r} \in \mathcal{E}$, we find $t_{-r} \in \mathcal{E}'$. This proves iii). □

Remark 7. Note that in (15) (as in the hypotheses of Theorem 4.1), we can have for some i, $(\Phi(\varepsilon) \cdot \mathcal{T}_i - X_i) \setminus \mathcal{H} = \emptyset$. This does not affect the argument.

5. The algorithm: theoretical aspects

From now on, we fix a $\mathbb{Z}$-basis $(e_i)_{1\leq i\leq n}$ of $\mathbb{Z}_K$. Thus, K can be identified with $\mathbb{Q}^n$ via the map $\Psi : \mathbb{Q}^n \to K$ defined by $\Psi(r) = \sum_{i=1}^n r_i e_i$ for $r \in \mathbb{Q}^n$.

The map $\Phi \circ \Psi : \mathbb{Q}^n \to \mathbb{R}^n$ can be extended by continuity to a map $\overline{\Phi} : \mathbb{R}^n \to \mathbb{R}^n$ via

$$\overline{\Phi}(x) = \left(\sum_{i=1}^n x_i \sigma_1(e_i), \ldots, \sum_{i=1}^n x_i \sigma_n(e_i) \right) \quad \text{for all} \quad x \in \mathbb{R}^n.$$

$\overline{\Phi}$ is an $\mathbb{R}$-linear automorphism of $\mathbb{R}^n$. Its invertible matrix (with respect to the canonical basis) is denoted $M = (m_{i,j})_{1\leq i,j\leq n}$. We have $|\det(M)| = \sqrt{D_K}$ and

$$M = (\sigma_i(e_j))_{1\leq i,j\leq n}\,.$$

The inverse matrix M^{-1} of M will be denoted $M' = \left(m'_{i,j}\right)_{1\leq i,j\leq n}$.

Let $\mathcal{F}$ be the fundamental parallelotope of volume $\sqrt{D_K}$ defined by

$$\mathcal{F} = \overline{\Phi}\left([0,1)^{\,n}\right) = \Big\{ \sum_{i=1}^n x_i \Phi(e_i);\ 0 \leq x_i < 1 \Big\}.$$

5.1. **Overview of the algorithm.** Assume as previously that we have an idea of $M(K)$ denoted k. Suppose that we have at our disposal a set $\mathcal{X}$ of elements of $\mathcal{R}$, and let us take a small $\epsilon > 0$.

Definition 5.1. A subset of $\mathbb{R}^n$ will be said to be *absorbed* by $X \in \mathcal{X}$, if it is contained in the region defined by the inequality $\mathcal{N}(x - X) \leq k - \epsilon$.

The computations are organized in the following way.

1. The first step of the algorithm consists in covering $\mathcal{F}$ with small parallelotopes. The shape of these parallelotopes will be explained later.

2. Following the philosophy stated in the previous section, the second step consists in eliminating all the parallelotopes which are absorbed by integers of $\mathcal{X}$. Every parallelotope which cannot be eliminated is stored in a list of so-called *problematic parallelotopes*. Let $\mathcal{P}_i$, $i = 1 \ldots N$ be this list at the end of this step. Every x in the union $\mathcal{G}$ of the parallelotopes which have been eliminated, verifies $m_{\mathcal{R}}(x) \leq k - \epsilon$. We shall call this step the *absorption test*.

3. Then we use the action of the unit group. We choose a unit $\varepsilon \neq \pm 1$, in practice one of the fundamental units. First, we eliminate every $\mathcal{P}_i$ such that $\Phi(\varepsilon) \cdot \mathcal{P}_i \subset \mathcal{G} + \mathcal{R}$, and enlarge $\mathcal{G}$ gradually. Then we repeat this elimination loop until the number N of remaining parallelotopes stabilizes. Of course we can use successively several units. This step will be called the *units test*.

4. The next idea is to cut every remaining parallelotope into 2^n smaller parallelotopes, and to restart the whole process while the number of remaining parallelotopes decreases. Finally, we analyze the smallest collection of problematic parallelotopes that we have obtained, thanks to Theorem 4.5. This theorem, if it can be used, allows us to obtain a finite set $\mathcal{E}$ of potentially critical rational points t_i. We can compute $m_{\mathcal{R}}(t_i)$ for $t_i \in \mathcal{E}$ by Theorem 3.3. If the value k is the Euclidean minimum we shall get:

$$\text{for all } i,\ m_{\mathcal{R}}(t_i) \leq k \text{ and there exists an } i \text{ such that } m_{\mathcal{R}}(t_i) = k,$$

which proves $M(K) = M(\overline{K}) = k$. Moreover, under these conditions, Theorem 4.5 proves that the t_i of $\mathcal{E}'$ are the only rational critical points modulo $\mathcal{R}$.

Remark 8. Using the fact that $m_{\mathcal{R}}(x) = m_{\mathcal{R}}(-x)$, we see that we can restrict our calculation to one half of $\mathcal{F}$ that we shall denote by $\mathcal{F}'$. The choice of $\mathcal{F}'$ will be explained later.

5.2. **The choice of integers.** We need to choose a collection $\mathcal{X}$ of elements of $\mathcal{R}$ susceptible to absorb most of our parallelotopes. A naive approach is to take all the $X = \overline{\Phi}(t)$ where $t \in \mathbb{Z}^n \cap [-B, B]^n$ and $B > 0$. One might expect a small value of B to be sufficient, but this is not always the case: the problem comes from the necessity of resorting to distant integers if we want to be efficient. It is thus often advisable to take B rather large, and to keep only the X that could eventually be useful. This is done as follows.

For every $i \in \{1, \dots, n\}$ we put

$$a_i = \sum_{\substack{i=1 \\ m_{i,j} \leq 0}}^{n} m_{i,j} \text{ and } b_i = \sum_{\substack{i=1 \\ m_{i,j} > 0}}^{n} m_{i,j}.$$

Since $\mathcal{F} = \overline{\Phi}([0,1)^n)$, it is easy to see that

$$\mathcal{F} \subset [a_1, b_1] \times \dots . \times [a_n, b_n],$$

and that if $X \in \mathcal{R}$ verifies

$$\mathcal{F} \cap \Big\{ x \in \mathbb{R}^n \text{ such that } \mathcal{N}(x - X) \leq k \Big\} \neq \emptyset,$$

then, for some $i \in \{1, \dots, n\}$ we have $X_i \in [a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}]$.

Thus we choose $B > 0$ sufficiently large and consider the set of $X \in \mathcal{R}$ which verify $X_i \in [a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}]$ for some i.

5.3. **Cutting and covering $\mathcal{F}$ and $\mathcal{F}'$.** The main idea is to cover $\mathcal{F}$ with small parallelotopes of the form $\{x \in \mathbb{R}^n;\ \alpha_i \leq x_i \leq \beta_i\}$, i.e. whose faces are orthogonal to the canonical axes of $\mathbb{R}^n$. We are using the same covering as in [Ce1]; it is better suited for the computations of the absorption and units tests than the perhaps more natural covering used e.g. in [CL] or [CD].

Recall that $\mathcal{F} \subset [a_1, b_1] \times \dots . \times [a_n, b_n]$. Let us now cut $[a_1, b_1] \times \dots . \times [a_n, b_n]$ in the following way. We choose n even positive integers $r_1, \dots, r_n$, and put

$$\text{for all } i \in \{1, \dots, n\},\ h_i = \frac{b_i - a_i}{2r_i},$$

$$\text{for all } i \in \{1, \dots, n\} \text{ and for all } j \in \{0, \dots, r_i\},\ y_{j,i} = a_i + 2jh_i,$$

$$\text{for all } i \in \{1, \dots, n\} \text{ and for all } j \in \{0, \dots, r_i - 1\},\ c_{j,i} = a_i + (2j+1)h_i.$$

See Figure 4 for an illustration with $n = 2$, $r_1 = 10$ and $r_2 = 8$. Set

$$L = \{(l_1, \dots, l_n) \text{ such that for all } i \in \{1, \dots, n\},\ 0 \leq l_i \leq r_i - 1\}.$$

If $l = (l_1, \dots, l_n) \in L$, the parallelotope defined by

$$\mathcal{B}_l = \{x \in \mathbb{R}^n \text{ such that for all } i \in \{1, \dots, n\},\ y_{l_i,i} \leq x_i \leq y_{l_i+1,i}\},$$

is centered in C_l where $(C_l)_i = c_{l_i,i}$.

Of course $\mathcal{F}$ is covered by the $\mathcal{B}_l$, but this covering is uncouth (many $\mathcal{B}_l$ are useless) and we must reduce it to a more reasonable one. It is done as follows.

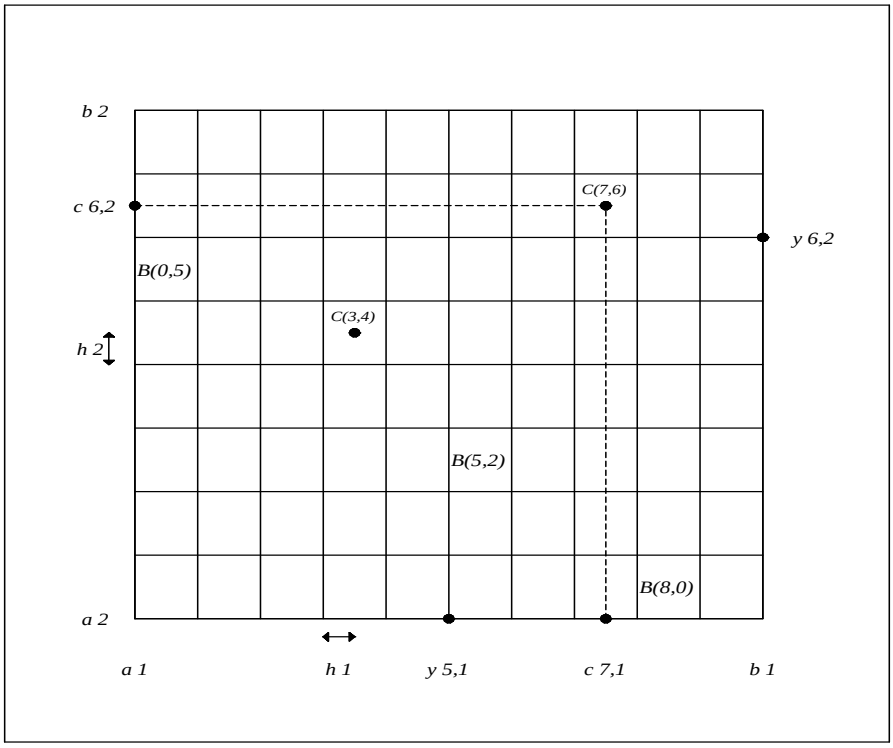

Figure 4. Notations

Let $(l_1, \ldots, l_{n-1}) \in \{0, \ldots, r_1 - 1\} \times \ldots \times \{0, \ldots, r_{n-1} - 1\}$. The question is: for what values of l_n do we have $\mathcal{B}_l \cap \mathcal{F} \neq \emptyset$? It is easy to see that, since $\overline{\Phi}$ is one-to-one, this is equivalent to $\overline{\Phi}^{-1}(\mathcal{B}_l) \cap [0,1)^n \neq \emptyset$.

For i and j in $\{1, \ldots, n\}$, set $u_{i,j} = y_{l_j+1,j}$ or $y_{l_j,j}$ according to whether $m'_{i,j} > 0$ or not, and $v_{i,j} = y_{l_j,j}$ or $y_{l_j+1,j}$ according to whether $m'_{i,j} > 0$ or not.

Let $t = (t_i)_{1 \leq i \leq n} \in \overline{\Phi}^{-1}(\mathcal{B}_l)$. For all $i \in \{1, \ldots, n\}$ the largest value of t_i and the smallest value of t_i are respectively given by

$$\mu_i = \sum_{j=1}^{n} m'_{i,j} u_{i,j} \quad \text{and} \quad \lambda_i = \sum_{j=1}^{n} m'_{i,j} v_{i,j}.$$

We can exclude the values of l_n for which there exists an i such that $\mu_i < 0$ or $\lambda_i > 1$, since in these cases, for all $t \in \overline{\Phi}^{-1}(\mathcal{B}_l)$, $t_i < 0$ or for all $t \in \overline{\Phi}^{-1}(\mathcal{B}_l)$, $t_i > 1$, which implies $\overline{\Phi}^{-1}(\mathcal{B}_l) \cap [0,1)^n = \emptyset$. Thus, for all $i \in \{1, \ldots, n\}$ we must have $\mu_i \geq 0$ and $\lambda_i \leq 1$. Replacing $y_{l_n,n}$ and $y_{l_n+1,n}$ by $a_n + 2l_n h_n$ and $a_n + 2(l_n + 1)h_n$ we find inequalities that must be verified by l_n, in function of $l_1, \ldots, l_{n-1}$. The formulae are rather heavy and will easily be established by the reader if necessary.

Remark 9. In many cases, the interval such defined for the values of l_n is empty. In dimension greater than 4, it is useful to determine in the same way an interval for l_{n-1} when $(l_1, \ldots, l_{n-2})$ is given. To obtain such an interval we write, with the

same notations as above

$$\mu_i \leq \begin{cases} \sum_{j=1}^{n-2} m'_{i,j}u_{i,j} + m'_{i,n-1}y_{l_{n-1}+1,n-1} + m'_{i,n}\alpha_i & \text{if } m'_{i,n-1} > 0 \\ \sum_{j=1}^{n-2} m'_{i,j}u_{i,j} + m'_{i,n-1}y_{l_{n-1},n-1} + m'_{i,n}\alpha_i & \text{if } m'_{i,n-1} \leq 0 \end{cases}$$

and

$$\lambda_i \geq \begin{cases} \sum_{j=1}^{n-2} m'_{i,j}v_{i,j} + m'_{i,n-1}y_{l_{n-1},n-1} + m'_{i,n}\beta_i & \text{if } m'_{i,n-1} > 0 \\ \sum_{j=1}^{n-2} m'_{i,j}v_{i,j} + m'_{i,n-1}y_{l_{n-1}+1,n-1} + m'_{i,n}\beta_i & \text{if } m'_{i,n-1} \leq 0, \end{cases}$$

where $\alpha_i = b_n$ or a_n according to whether $m'_{i,n} > 0$ or not, and $\beta_i = a_n$ or b_n according to whether $m'_{i,n} > 0$ or not.

As we must have $\mu_i \geq 0$ and $\lambda_i \leq 1$ for all i, these inequalities lead us to the desired interval for l_{n-1}.
In the same way, for higher dimensions (say when $n \geq 6$) it can be interesting to define intervals for l_{n-2} when $(l_1, \ldots, l_{n-3})$ is given, or again intervals for l_{n-3} when $(l_1, \ldots, l_{n-4})$ is given, etc. This process allows us to accelerate the computations in a sensible way.

Remark 10. Let s be the reflection of center $\frac{1}{2}\Phi(\sum e_i)$. By Remark 8, we have $m_{\mathcal{R}}(s(x)) = m_{\mathcal{R}}(x)$ for all $x \in \mathbb{R}^n$. It is easy to see that we have $\left(\frac{1}{2}\Phi\left(\sum_{i=1}^n e_i\right)\right)_1 = \frac{b_1+a_1}{2}$. Thus, if we want to reduce the study to half a fundamental domain $\mathcal{F}'$, the nature of the covering of $\mathcal{F}$ by small parallelotopes that we have defined leads us to choose

$$\mathcal{F}' = \Big\{x \in \mathcal{F} \text{ such that } x_1 \in [a_1, \frac{b_1 + a_1}{2}]\Big\},$$

and to work with the $\mathcal{B}_l$ which verify $0 \leq l_1 \leq \frac{r_1}{2} - 1$.
Clearly they cover $\mathcal{F}'$. Moreover, $l = (l_1, \ldots, l_n)$ being given, we have $s(\mathcal{B}_l) = \mathcal{B}_{l'}$ where $l' = (r_1 - 1 - l_1, \ldots, r_n - 1 - l_n)$, and $\mathcal{F}$ is covered by the $\mathcal{B}_l$ which verify $0 \leq l_1 \leq \frac{r_1}{2} - 1$ and their images by s.

In Figure 5, we see the covering of $\mathcal{F} = \{a + b\,\Phi(\sqrt{2});\ (a,b) \in [0,1)^2\}$ for $K = \mathbb{Q}(\sqrt{2})$. $\mathcal{F}$ is the parallelogramm whose vertices are $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(1+\sqrt{2})$, $D = \Phi(\sqrt{2})$. Here $r_1 = r_2 = 10$. $\mathcal{F}'$ is the part of $\mathcal{F}$ which is at the left of the central vertical line and the covering of $\mathcal{F}'$ is composed of the white rectangles which are at the left of this line.

5.4. **The absorption test.** We first scan the $\mathcal{B}_l$ which cover $\mathcal{F}$ (or $\mathcal{F}'$ as defined in Remark 10) and eliminate all those which are absorbed by an element X of $\mathcal{X}$.

Let us consider one of these $\mathcal{B}_l$ that we shall denote by $\mathcal{P}$. To simplify notations we denote by C its center so that

$$\mathcal{P} = [C_1 - h_1, C_1 + h_1] \times \ldots \times [C_n - h_n, C_n + h_n].$$

Recall that we have chosen a small $\epsilon > 0$ and that we want to eliminate $\mathcal{P}$ if we have

(21) there exists an $X \in \mathcal{X}$ such that for all $x \in \mathcal{P}$, $\mathcal{N}(x - X) \leq k - \epsilon$.

The test is defined in the following way.

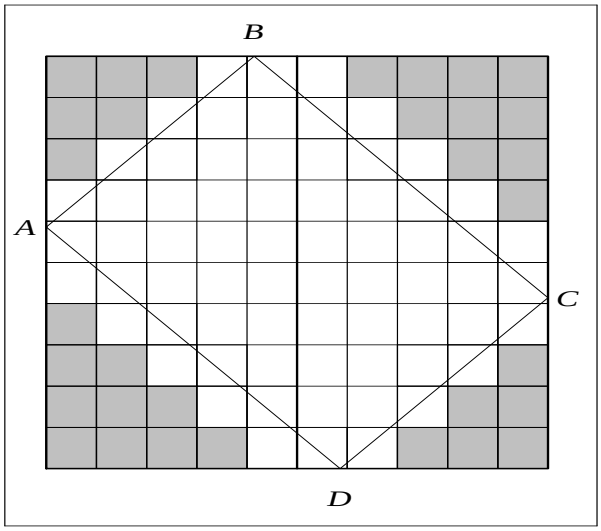

Figure 5. A covering of $\mathcal{F}$ and $\mathcal{F}'$

Proposition 5.1. *The following assertion is equivalent to* (21)*:*

$$\text{there exists an } X \in \mathcal{X} \text{ such that } \prod_{i=1}^{n} \Big(|C_i - X_i| + h_i \Big) \leq k - \epsilon. \tag{22}$$

Proof. Let $x \in \mathcal{P}$. The triangle inequality gives

$$\text{for all } i \in \{1, \dots, n\},\ |x_i - X_i| \leq |x_i - C_i| + |C_i - X_i|. \tag{23}$$

But since $x_i \in [C_i - h_i, C_i + h_i]$, we have $|x_i - C_i| \leq h_i$, so that

$$\text{for all } i \in \{1, \dots, n\},\ |x_i - X_i| \leq h_i + |C_i - X_i|. \tag{24}$$

Taking the product on i, we see that

$$\mathcal{N}(x - X) \leq \prod_{i=1}^{n} \Big(|C_i - X_i| + h_i \Big),$$

so that (22) implies (21).
Moreover the inequalities (23) and (24) are equalities for

$$x_i = \begin{cases} C_i - h_i & \text{if } C_i \text{ is beetween } C_i - h_i \text{ and } X_i, \\ C_i + h_i & \text{if } C_i \text{ is beetween } C_i + h_i \text{ and } X_i, \end{cases}$$

and it is easy to see that we are necessarily in a case or in the other one. This shows that (22) is in fact an equality for a vertex of $\mathcal{P}$ and that the majorization used is optimal. Thus (22) is equivalent to (21). □

Remark 11. The last proposition exhibits one of the advantages of our cutting-covering. The inequality used is the best possible, contrary to what one can obtain with the same cutting-covering as in [CL].

Let us resume. We scan all the $\mathcal{B}_l$ covering $\mathcal{F}'$ (see Remark 10) with the help of the inequalities obtained as above, and we submit them to the test of Proposition 5.1. If (22) holds for a $\mathcal{B}_l$, it can be eliminated and we know that, by Remark 8,

$s(\mathcal{B}_l)$ can also be eliminated from the covering of $\mathcal{F}$. If (22) does not hold for $\mathcal{B}_l$, we store $\mathcal{B}_l$ and $s(\mathcal{B}_l)$ in our list of problematic parallelotopes.

Remark 12. At each step of the algorithm, we shall work with only half of the parallelotopes, but shall not forget to store and take into account their images by s. To do that, at each step (absorption test, units test, successive cuttings of the parallelotopes), we give to each parallelotope corresponding to $\mathcal{F}'$ an odd index $i = 2p-1$ ($p \geq 1$) and the index $i = 2p$ to its image by s.

5.5. **The units test.** Let $\varepsilon \neq \pm 1$ be the unit used for this test. We shall denote by $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$ the list of problematic parallelotopes found at the previous step, and by D_p the center of every $\mathcal{P}_p$. Assume that $\mathcal{P}$ is one of these problematic parallelotopes. Let C be its center so that

$$\mathcal{P} = [C_1 - h_1, C_1 + h_1] \times \ldots \times [C_n - h_n, C_n + h_n].$$

We have

$$\Phi(\varepsilon) \cdot \mathcal{P} = [w_1, z_1] \times \ldots \times [w_n, z_n],$$

where for all i, $w_i = \sigma_i(\varepsilon)C_i - |\sigma_i(\varepsilon)|h_i$ and $z_i = \sigma_i(\varepsilon)C_i + |\sigma_i(\varepsilon)|h_i$.

This is a parallelotope whose faces are orthogonal to the canonical axes of $\mathbb{R}^n$ (like the $\mathcal{P}_p$), centered in

$$C'' = (\sigma_i(\varepsilon)C_i)_{1 \leq i \leq n}.$$

The determination of the $X \in \mathcal{R}$ such that $\Phi(\varepsilon) \cdot \mathcal{P} - X$ meets $\mathcal{F}$, is the first problem that we have to solve.

First consider $T = (T_1, \ldots, T_n) = \overline{\Phi}^{-1}(C'')$. Let $X_0 = \overline{\Phi}((\lfloor T_1 \rfloor, \ldots, \lfloor T_n \rfloor)) \in \mathcal{R}$. Since $T - \overline{\Phi}^{-1}(X_0) \in [0,1)^n$, it is clear that $C'' - X_0 \in \mathcal{F}$, and then

$$(\Phi(\varepsilon) \cdot \mathcal{P} - X_0) \cap \mathcal{F} \neq \emptyset.$$

As already mentioned, X_0 is not necessarily the only translation vector of $\mathcal{R}$ that we can use to take back $\Phi(\varepsilon) \cdot \mathcal{P}$ to $\mathcal{F}$. Some others can be used if $\Phi(\varepsilon) \cdot \mathcal{P} - X_0$ has elements outside of $\mathcal{F}$ but the different possibilities are easy to compute.

Put $\mathcal{P}' = \Phi(\varepsilon) \cdot \mathcal{P} - X_0$. It is a parallelotope centered in $C' = C'' - X_0$ and we have $\mathcal{P}' = [C'_1 - h'_1, C'_1 + h'_1] \times \ldots \times [C'_n - h'_n, C'_n + h'_n]$, where

$$\text{for all } i \in \{1, \ldots, n\},\ h'_i = h_i\ |\sigma_i(\varepsilon)|.$$

For all $i \in \{1, \ldots, n\}$ the smallest and the largest values for $(\overline{\Phi}^{-1}(x))_i$ where $x \in \mathcal{P}'$ are respectively

$$\alpha_i = \sum_{j=1}^{n} m'_{i,j}(C'_j - \delta_{i,j}h'_j) \text{ and } \beta_i = \sum_{j=1}^{n} m'_{i,j}(C'_j + \delta_{i,j}h'_j),$$

where $\delta_{i,j} = 1$ or -1 according to whether $m'_{i,j} > 0$ or not.

These formulae give us easily the only possible desired translation vectors of $\mathcal{R}$.

Proposition 5.2. *With above notations, if $X \in \mathcal{R}$ is such that $\Phi(\varepsilon) \cdot \mathcal{P} - X$ meets $\mathcal{F}$, then X is of the form $X = X_0 + \overline{\Phi}(\nu_1, \ldots, \nu_n)$, where*

$$\textit{for all } i \in \{1, \ldots, n\},\ \nu_i \in \mathbb{Z} \textit{ and } \lfloor \alpha_i \rfloor \leq \nu_i \leq \lfloor \beta_i \rfloor.$$

Note that all the X defined that way are not useful in the sense that we shall not always have $(\Phi(\varepsilon) \cdot \mathcal{P} - X) \cap \mathcal{F} \neq \emptyset$, but that we are sure to have all the translation vectors of $\mathcal{R}$ which can send a part of $\Phi(\varepsilon) \cdot \mathcal{P}$ into $\mathcal{F}$.

Remark 13. When for some i, $|\sigma_i(\varepsilon)|h_i$, and consequently the number of possible translation vectors, are too large, we go directly to the next step (refining the cutting) which is described in subsection 5.6.

Let us now denote these translation vectors by X_0, X_1, ..., X_g ($g \geq 0$).

Proposition 5.3. *With the above notations, if for all j (with $0 \leq j \leq g$) we have*

$$\begin{cases} \text{for all } p \in \{1,\dots,2q\}, \text{ there exists an } i_p \in \{1,\dots,n\} \text{ such that} \\ |(C'' - X_j - D_p)_{i_p}| > \left(1 + |\sigma_{i_p}(\varepsilon)|\right) h_{i_p}, \end{cases} \tag{25}$$

then $\mathcal{P}$ and $s(\mathcal{P})$ can be eliminated from the list of problematic parallelotopes.

Proof. Let $x \in \mathcal{P}$. By construction of the X_j we know that there exists j in $\{0,\dots,g\}$ such that $y = \Phi(\varepsilon)\cdot x - X_j \in \mathcal{F}$. But $\Phi(\varepsilon)\cdot\mathcal{P} - X_j$ is a parallelotope centered in $C'' - X_j$ isometric to $\mathcal{P}'$ and we have

$$\text{for all } i \in \{1,\dots,n\},\ |y_i - C''_i + (X_j)_i| \leq h'_i. \tag{26}$$

Let now $p \in \{1,\dots,2q\}$. By (25), (26) and the triangle inequality, there exists $i_p \in \{1,\dots,n\}$ such that $|y_{i_p} - (D_p)_{i_p}| > \left(1 + |\sigma_{i_p}(\varepsilon)|\right) h_{i_p} - h'_{i_p}$, or equivalently $|y_{i_p} - (D_p)_{i_p}| > h_{i_p}$.

This last inequality implies: $y \in \mathcal{F}$ and for all $p \in \{1,\dots,2q\}$ $y \notin \mathcal{P}_p$. Thus, $m_{\mathcal{R}}(y) \leq k - \epsilon$, and by Remark 1 we finally get $m_{\mathcal{R}}(x) \leq k - \epsilon$.

This shows that $\mathcal{P}$ can be eliminated. □

Remark 14. Here again, it is thanks to the nature of our cutting of $\mathcal{F}$ that we have an elementary criterion to see whether $\Phi(\varepsilon)\cdot\mathcal{P}$ intersects or not some $\mathcal{P}_p$ modulo $\mathcal{R}$. Moreover it is easy to see that the inequality of (25) is the best possible.

The procedure is now simple. Consider our set of problematic parallelotopes $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$. By reflection, we need only to test the $\mathcal{P}_{2p-1}$, for $1 \leq p \leq q$. If $\mathcal{P}_{2p-1}$ verifies (25), we eliminate $\mathcal{P}_{2p-1}$ and $\mathcal{P}_{2p} = s(\mathcal{P}_{2p-1})$ from our list. At the end of this loop, we scan again in the same way our new list, and start again while the list decreases.

Note that the final list still verifies

$$\text{for all } p,\ s(\mathcal{P}_{2p-1}) = \mathcal{P}_{2p}. \tag{27}$$

5.6. **The next step: refining the partition.** Let $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$ be our new reduced list of problematic parallelotopes. As we have seen above, the next step consists in cutting again each remaining parallelotope $\mathcal{P}_{2p-1}$ centered in C into the 2^n smaller parallelotopes $[C_1 - \eta_1 h_1, C_1 + (1-\eta_1)h_1] \times \ldots \times [C_n - \eta_n h_n, C_n + (1-\eta_n)h_n]$, where $\eta_i \in \{0,1\}$, and test each of them thanks to Proposition 5.1. If the test is negative, we store the small parallelotope in a new list in an odd position, and its reflection by s in the next position. At the end we have a new set of small problematic parallelotopes $\mathcal{P}'_i$ (where $1 \leq i \leq 2q'$) with the property (27).

As previously, we can again use units to eliminate most of $\mathcal{P}'_i$ by Proposition 5.3 and the sub-algorithm described above. If the final list is still denoted by $\mathcal{P}'_i$ (where $1 \leq i \leq 2q'$), we compare q and q'.

If $q' \leq q$ we replace the old list by the new one and restart. If $q' > q$, we stop and analyze the $\mathcal{P}_i$ ($1 \leq i \leq 2q$).

5.7. **What to do with the remaining parallelotopes.**

5.7.1. *General strategy.* At this point we are left with $2q$ problematic parallelotopes $\mathcal{P}_1, \ldots, \mathcal{P}_{2q}$ which verify (27), and we know, by the previous considerations, that

$$\mathcal{F} \setminus \bigcup_{1 \leq i \leq 2q} \mathcal{P}_i \subset \mathcal{H},$$

where, with the same notation as in section 4,

$$\mathcal{H} = \{x \in \mathbb{R}^n \text{ such that } m_{\mathcal{R}}(x) \leq k - \epsilon\}.$$

We take again a unit $\varepsilon \neq \pm 1$, which is, for instance, the unit (or one of the units) previously used and we consider the problematic parallelotopes $\mathcal{P}_i$ (with $1 \leq i \leq 2q$), trying to collect them into sets $\mathcal{T}$ which verify (15) and are the vertices of a convenient digraph G, as already seen in subsection 4.2.

By the way the $\mathcal{P}_i$ have been selected, we have partially (15), the only point to which we must pay attention is the treatment of the problematic parallelotopes that can be translated back to $\mathcal{F}$ after multiplication by $\Phi(\varepsilon)$ in several ways. For this problem, see subsection 5.7.2 below.

To define the $\mathcal{T}_i$ we can first exclude the $\mathcal{P}_i$ which are not intersected by any $\Phi(\varepsilon) \cdot \mathcal{T}_j - X_j$, try to collect the others in coherent sets (same translation vector, same intersections...), with the help of a geometrical proximity criterium, and only at the end, add the remaining $\mathcal{T}_i$ (which is not anyway necessary).
If we obtain a convenient digraph, it remains to compute the $m_{\mathcal{R}}(t_i)$ for $t_i \in \mathcal{E}$ and to apply Theorem 4.5, which must give, if everything goes off smoothly, $m(G) = k$.

5.7.2. *The peripheral parallelotopes.* In Figures 6 and 7, we give an illustration with $K = \mathbb{Q}(\sqrt{2})$, $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(1+\sqrt{2})$ and $D = \Phi(\sqrt{2})$ as vertices of $\mathcal{F}$. In Figure 6 we see that we have two problematic regions (each of them composed of four parallelotopes). The problem comes from the fact that each of them can be sent on itself or on the other one via the unit action, and that we are not exactly under the hypotheses of section 4.2.2. To get over the obstacle, we consider in Figure 7 a new fundamental domain, here $\mathcal{F} - \Phi(0.4)$, with vertices A', B', C', D'. Then we translate by $\Phi(-1)$ some of the covering parallelotopes, including those of the upper problematic region, so that we obtain a covering of this new fundamental domain. In this case we check that we have a single problematic region sent over itself under the unit action, and the digraph associated to the situation is G_1 (with $j = 1$) which is convenient.

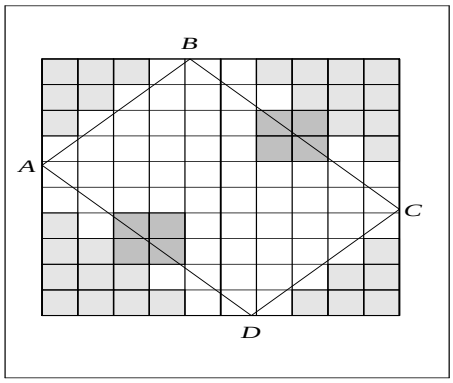

Figure 6.

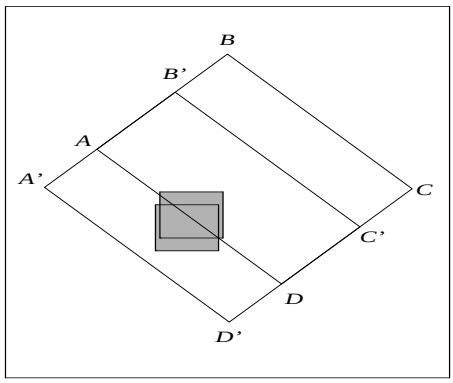

Figure 7.

In fact, the problem when we have several possibilities for the translation vector associated to a problematic parallelotope $\mathcal{P}$, is that, if we fix one, say X, $\Phi(\varepsilon)\cdot\mathcal{P}-X$ can intersect a zone $\mathcal{T}'$ equivalent modulo $\mathcal{R}$ to one of the $\mathcal{T}$ that we have defined, but which is out of $\mathcal{F}$ and then not listed. In this case, the $\mathcal{P}$ in question are very small and near the boundary of $\mathcal{F}$, so that we can, as previously, consider another fundamental domain whose covering is obtained by translation of some of the initial $\mathcal{B}_l$. It is then sufficient to check that results of section 4 are compatible with this new covering.

5.8. **Computation of the inhomogeneous minimum.** We still have to show how we compute $m_{\mathcal{R}}(t_i)$ for $t_i \in \mathcal{E}$, or more generally, $m_{\mathcal{R}}(t)$ for $t \in \Phi(K)$. This is done thanks to Theorem 3.3.

5.8.1. *Determination of the orbits.* Let $\xi \in K$ and $t = \Phi(\xi)$. In order to compute $\mathrm{Orb}(t)$, or equivalently $\{\varepsilon\xi \bmod \mathbb{Z}_K;\ \varepsilon \in E_K\}$, we first compute for each $i \in \{1,\dots,n-1\}$ the smallest positive integer p_i such that

$$\varepsilon_i^{p_i}\xi \equiv \xi \bmod \mathbb{Z}_K.$$

Then, using euclidean divisions by the p_i, it is easy to see that for all $\varepsilon \in E_K$, there exists $(m_1,\dots,m_{n-1}) \in \{0,\dots,p_1-1\}\times\ldots\times\{0,\dots,p_{n-1}-1\}$ such that

$$\varepsilon\xi \equiv \pm\varepsilon_1^{m_1}\dots\varepsilon_{n-1}^{m_{n-1}}\xi \bmod \mathbb{Z}_K.$$

Thus, we just need to compute successively $2p_1\dots p_{n-1}$ values, and to store each new one, as one goes along.

5.8.2. *Selection of the good integers.* Let z be an element of $\mathrm{Orb}(t)$. How do we scan the $Z \in \mathcal{R}$ such that $|z_i - Z_i| \le (k\prod_{l=1}^{n-1}\Gamma_l)^{1/n}$ for all i?
Let us denote $z = \Phi(\xi)$ with $\xi = \sum \xi_i e_i \in K$ and $Z = \Phi(\Upsilon)$ with $\Upsilon = \sum \Upsilon_i e_i \in \mathbb{Z}_K$. One establishes easily that Υ must verify

$$\text{for all } i \in \{1,\dots,n-1\},\ |\Upsilon_i - \xi_i| \le \left(\sum_{i=1}^{n}|m'_{i,j}|\right)\left(k\prod_{l=1}^{n-1}\Gamma_l\right)^{\frac{1}{n}}, \tag{28}$$

and $(\Upsilon_1,\dots,\Upsilon_{n-1})$ being given with (28), the n following conditions:

$$\text{for all } i \in \{1,\dots,n\},\ m_{i,n}\Upsilon_n \in \left[\alpha_i - \left(k\prod_{l=1}^{n-1}\Gamma_l\right)^{\frac{1}{n}}, \alpha_i + \left(k\prod_{l=1}^{n-1}\Gamma_l\right)^{\frac{1}{n}}\right], \tag{29}$$

where

$$\alpha_i = m_{i,n}\xi_n + \sum_{j=1}^{n-1} m_{i,j}(\xi_j - \Upsilon_j).$$

5.9. **How do we guess k?** In all the previous subsections, we have supposed that, in fact, we had a guess for $k = M(\overline{K})$, and that we just wanted to prove that it was exact.

As in general such a value is not a priori known, we must describe a heuristic which works quite well. First we try the algorithm with a reasonable value k', e.g. $k' = 0.999$. If the first part (cutting and eliminating) returns no problem then we try a smaller value (always denoted k'), until we find a reasonable number of problematic parallelotopes: if there are too many such parallelotopes, we try a larger value for k'. At this point we apply Theorem 4.5, if it is possible. In this

case, we have a convenient digraph G, and we compute $m(G)$. We can do it thanks to Theorem 3.3 and the procedure described at the end of section 3 (beginning with k'). If $m(G) < k'$ we have $M(\overline{K}) < k'$ and we start again with a smaller k'. If $m(G) \geq k'$ then Theorem 4.5 gives $M(K) = M(\overline{K}) = m(G)$ and the rational critical points correspond to $\mathcal{E}'$.

Usually, this procedure quickly converges.

If we only want to prove that K is norm-Euclidean we try $k = 0.999$. If we have problematic parallelotopes which give us points t to evaluate, it is not necessary to compute $m_{\mathcal{R}}(t)$ but rather to find, for each t, an $X \in \mathcal{R}$ such that $\mathcal{N}(t - X) < 1$.

5.10. **The example $\mathbb{Q}(\sqrt{13})$.** As we have already said, one of the advantages of Theorem 4.5 is that it allows us to treat "pathological" fields such as $\mathbb{Q}(\sqrt{13})$.

Let us give the results obtained for this last field. It will also illustrate what we have said about peripheral problematic parallelotopes.

Let $K = \mathbb{Q}(\sqrt{13})$ and let $(e_1, e_2) = (1, -\frac{1+\sqrt{13}}{2})$ and $\varepsilon_1 = \frac{3-\sqrt{13}}{2}$, be the $\mathbb{Z}$-basis and the fundamental unit returned by PARI. Using $r_1 = r_2 = 50$, $k = 1/3$, $\epsilon = 0.01$, and applying the elimination procedure with both ε_1 and ε_1^{-1} we find 16 problematic parallelotopes (see Figure 8 in which $A = \Phi(0)$, $B = \Phi(e_1)$, $C = \Phi(e_2)$ and $D = \Phi(e_1 + e_2)$).

First we can see that $\mathcal{P}_1$ is in the neighborhood of $\overline{\Phi}(0, 2/3)$ and is isolated, while $\mathcal{P}_i$ for $i \in \{8, 10, 12\}$, are in the neighborhood of $\overline{\Phi}(1, 2/3)$. So, instead of $\mathcal{P}_1$, we can consider $\mathcal{P}_1 + \overline{\Phi}(1, 0)$ which has the same behaviour as $\mathcal{P}_8$ under the action of ε_1 and ε_1^{-1}, and which will still be denoted by $\mathcal{P}_1$. We have the same phenomenon with $\mathcal{P}_2$ (the reflection of $\mathcal{P}_1$) that we translate on the $\mathcal{P}_i$ with $i \in \{7, 9, 11\}$. This amounts to consider a slightly different fundamental domain (see Figure 8). With this new approach, all the $\mathcal{P}_i$ are inside the fundamental domain and are sent back to it after multiplication by ε_1 or ε_1^{-1}, by a single translation vector of $\mathcal{R}$.

If we take $\varepsilon = \varepsilon_1$ we can collect the $\mathcal{P}_i$ in the following way: $\mathcal{T}_1 = \mathcal{P}_3 \cup \mathcal{P}_5$, $\mathcal{T}_2 = \mathcal{P}_4 \cup \mathcal{P}_6$, $\mathcal{T}_3 = \mathcal{P}_1 \cup \mathcal{P}_8 \cup \mathcal{P}_{10} \cup \mathcal{P}_{12} \cup \mathcal{P}_{14} \cup \mathcal{P}_{16}$ and $\mathcal{T}_4 = \mathcal{P}_2 \cup \mathcal{P}_7 \cup \mathcal{P}_9 \cup \mathcal{P}_{11} \cup \mathcal{P}_{13} \cup \mathcal{P}_{15}$.

We obtain the digraph G: $\mathcal{T}_1 \to \mathcal{T}_2(\Phi(3, 1))$, $\mathcal{T}_2 \to \mathcal{T}_1(\Phi(1, 0))$, $\mathcal{T}_3 \to \mathcal{T}_3(\Phi(3, 1))$, $\mathcal{T}_3 \to \mathcal{T}_1(\Phi(3, 1))$, $\mathcal{T}_4 \to \mathcal{T}_4(\Phi(1, 0))$, $\mathcal{T}_4 \to \mathcal{T}_2(\Phi(1, 0))$.

It is a convenient digraph (previously seen in Figure 3 as G_2), and we can apply Theorem 4.5. We find four rational points t_i which can give us $M(\overline{K})$. These points are in fact $\overline{\Phi}(1/3, 1/3)$, $\overline{\Phi}(2/3, 2/3)$, $\overline{\Phi}(1, 2/3)$ and $\overline{\Phi}(0, 1/3)$, which are of the form $\Phi(\xi)$ as in Proposition 2.5, with $|N_{K/\mathbb{Q}}(\Upsilon)| = 3$. Thus we have $m_{\mathcal{R}}(t_i) = 1/3$ for all i and

$$M(K) = M(\overline{K}) = \frac{1}{3},$$

with exactly four critical rational points in $\mathcal{F}$.

5.11. **Computation of the second Euclidean minimum.** Assume that we apply the algorithm with k and that we find, thanks to Theorem 4.5, p rational points ($p \geq 2$) $t_0, \ldots, t_{p-1}$, defined by p bounded sets $\mathcal{T}_i$ ($0 \leq i \leq p-1$) as usual and which verify

$$m_{\mathcal{R}}(t_0) = \ldots = m_{\mathcal{R}}(t_{r-1}) = k' \text{ and } m_{\mathcal{R}}(t_r) = \ldots = m_{\mathcal{R}}(t_{p-1}) = k,$$

where $1 \leq r \leq p-2$ and $k < k'$. Then, we have $M(K) = M(\overline{K}) = k'$.

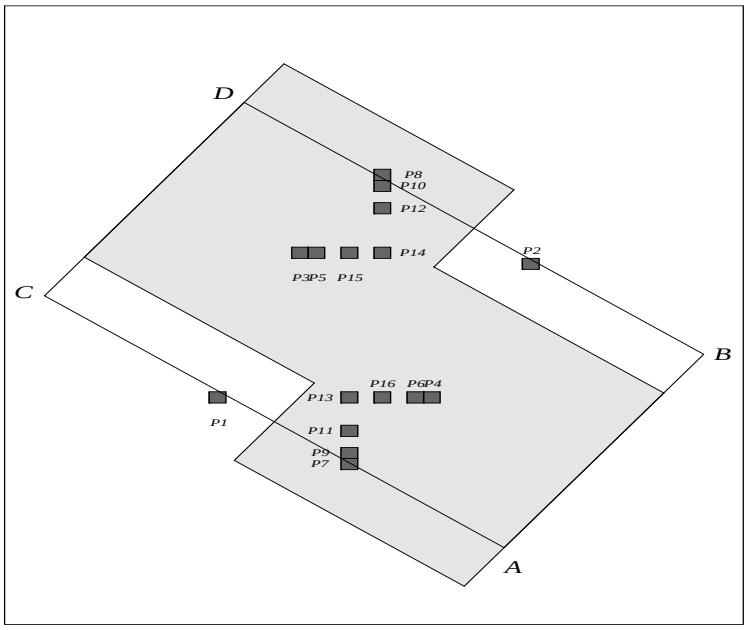

Figure 8. The case $K = \mathbb{Q}(\sqrt{13})$

Now, let $x \in \Phi(K)$ such that $k < m_{\mathcal{R}}(x) < k'$. By Theorem 4.5, if $x \in \mathcal{T}_i$ where $i \leq r-1$, then $x = t_i$ and $m_{\mathcal{R}}(x) = k'$ which is excluded. Thus, $x \in \mathcal{T}_i$ with $i \geq r$ and $m_{\mathcal{R}}(x) \leq m_{\mathcal{R}}(t_i) = k$, which is impossible.

This allows us to write $M_2(K) = k$, where

$$M_2(K) = \sup_{\substack{\xi \in K \\ M_K(\xi) < M(K)}} \left(\inf_{\Upsilon \in \mathbb{Z}_K} \left(\left| N_{K/\mathbb{Q}}(\xi - \Upsilon) \right| \right) \right).$$

Moreover, if $\mathcal{T}_1, \ldots, \mathcal{T}_r$ verify the hypotheses of Corollary 4.2, we can do the same thing with $x \in \mathbb{R}^n$ (instead of $\Phi(K)$) and we obtain also $M_2(\overline{K}) = k$, where

$$M_2(\overline{K}) = \sup_{\substack{x \in \mathbb{R}^n \\ m_{\mathcal{R}}(x) < M(\overline{K})}} \left(\inf_{X \in \mathcal{R}} \left(\mathcal{N}(x - X) \right) \right).$$

We have easily established this way the following result which had been conjectured in [CD].

Theorem 5.4. *If* $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$, *we have*

$$M(K) = M(\overline{K}) = \frac{1}{2} \text{ and } M_2(K) = M_2(\overline{K}) = \frac{1}{4}.$$

Our main object of study being $M(K)$, we shall not go further in that direction, even if incidently we have computed $M_2(K)$ for some fields. For the problems relative to these notions, see [L] and [Ce2] in which we prove that for $n \geq 3$, we have $M_2(K) \in \mathbb{Q}$ and $M_2(K) = M_2(\overline{K}) < M(K) = M(\overline{K})$ among other things. For further developments we refer also to our thesis [Ce3].

6. Practical aspects.

6.1. **Generalities.** The program has been written in C and the computations have been done on a Pentium II 300Mhz. Sometimes, for $n = 2$, when the value found for $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$ was too large (see below), we have used MAPLE for the last part of the computations. For $n > 2$ it has never been the case. In general, the time of computation for "easy fields" varies from less than 2 seconds for $n = 4$ to half an hour for $n = 7$.

For the number fields, we have used the tables available from [A2X] and computed the $\mathbb{Z}$-basis (e_i), M and the ε_i $(1 \leq i \leq n-1)$ thanks to PARI (see [P]). We have always used a LLL-reduced basis, which gives relatively short vectors and a "good" geometrical configuration.

6.2. **Cutting, covering and absorption test.** In the first part of the algorithm (cutting and covering) when the bounds found for l_n (or l_{n-1}, etc) are close to an integer (and less than this integer for the upper bound, or greater for lower bound) we took into account this one for the possible values of l_n (or l_{n-1}, etc). Thus we are sure to cover $\mathcal{F}$ and even a little more.
For the absorption test, in general we use $\epsilon = 10^{-3}$ (for $n = 2$, sometimes, we need to use a smaller ϵ, but for small degrees, we can do it), and different values for B in function of n and of K (for some of them a small value is sufficient). We also use a particular set of integers $\mathcal{I} \subset \mathcal{X}$ which is defined in the following way. $\mathcal{I}$ is initialized at $\emptyset$. When we test a $\mathcal{B}_l$ we first observe whether $\mathcal{B}_l$ is absorbed by some element of $\mathcal{I}$, beginning by its last element. If it is not the case, we search in $\mathcal{X}$ a convenient integer. If we find one, we put it in $\mathcal{I}$ in last position, and test the next $\mathcal{B}_l$. If we cannot, the $\mathcal{B}_l$ studied is temporarily problematic.

6.3. **The units test.** For the next step, we just strengthen (25) (see Proposition 5.3) and take $(1 + |\sigma_{i_p}(\varepsilon)|)h_{i_p} + \epsilon$ instead of $(1 + |\sigma_{i_p}(\varepsilon)|)h_{i_p}$ to be absolutely sure that intersection with others $\mathcal{P}$ is reduced to $\emptyset$. So it is possible that we select a $\mathcal{P}$ which should have been eliminated. This is without consequence (see Remark 7). In general we use two units (most of the time ε_1 and ε_2) for this test.

6.4. **Determination of the critical rational points.** For the computations of the t_i given by Theorem 4.5 and of the $m_{\mathcal{R}}(t_i)$, we must precise the way we proceed. The problem is that all our computations use floating point, but that we want exact rational values.

First, a circuit $\mathcal{T}_0(X_0) \to \ldots \to \mathcal{T}_0(X_{j-1})$ being given, how can we compute $\xi = \sum u_i e_i$ where $\Phi(\xi) = t$ and t corresponds to $\mathcal{T}_0$? We know that

$$\xi = \frac{\Omega}{\varepsilon^j - 1}$$

where

$$\Omega = \varepsilon^{j-1}\Upsilon_0 + \varepsilon^{j-2}\Upsilon_1 + \ldots. + \varepsilon\Upsilon_{j-2} + \Upsilon_{j-1}.$$

Then we must have

$$\text{for all } i,\ u_i \in \frac{1}{|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|}\mathbb{Z}.$$

The first thing to do is to obtain an exact value for $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$. We compute for that $|\prod_{i=1}^{n}(\sigma_i(\varepsilon^j) - 1)|$, check that the number obtained is sufficiently close to

an integer N and identify $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$ to N. Then we compute t which is given by:

$$\text{for all } i,\ t_i = \frac{\sum_{l=0}^{j-1} \sigma_i(\varepsilon)^l \sigma_i(\Upsilon_{j-1-l})}{\sigma_i(\varepsilon)^j - 1}.$$

Finally we compute $u = \overline{\Phi}^{-1}(t)$ with the help of M'. We check that all the u_i obtained are near integers a_i when multiplied by N, and we identify u_i to a_i/N, thus having the exact value of u. It is frequent that, by simplification, we can replace in the a_i/N, N by a smaller integer d. Anyway, we obtain $u_i \in 1/d\,\mathbb{Z}$ where d is a divisor of N, and we set $N' = \min(N, d^n)$ so that $\mathcal{N}(x - X) \in 1/N'\,\mathbb{Z}$ for all $(x, X) \in \mathrm{Orb}(t) \times \mathcal{R}$. It is then possible, but not necessary, to re-compute $t = \overline{\Phi}(u)$.

In relation with Proposition 2.5, if the tested k is of the form $1/p$, we can search for integers Υ of norm $\pm p$, compute the "inverse" of $\Phi(\Upsilon)$ in $\mathbb{R}^n$ which when multiplied by M' must give an element of $1/p\ \mathbb{Z}^n$, identified by approximation. It remains to see whether or not we find (modulo $\mathbb{Z}$) the exact coordinates of ξ determined earlier on. If it is the case, we have $m_K(\xi) = 1/p$ without computation.

6.5. **Determination of the orbits.** In the general case, we must determine $\mathrm{Orb}(t)$, where $t = \Phi(\xi)$. We first check that t has not already been met in a precedent orbit. The following step consists in the determination of p_i $(1 \le i \le n-1)$ as defined in subsection 5.8.1.

We compute successively $\xi_1 = \varepsilon_i \xi - X_1$ with $X_1 \in \mathbb{Z}_K$ such that $\Phi(\xi_1) \in \mathcal{F}$, $\xi_2 = \varepsilon_i \xi_1 - X_2$ with $X_2 \in \mathbb{Z}_K$ such that $\Phi(\xi_2) \in \mathcal{F}$ (note that $\xi_2 \equiv \varepsilon_i \xi_1 \bmod \mathbb{Z}_K$), and so on, until we find $\xi_{p_i} = \xi$. At each step we identify $\xi_{j+1} = \Phi^{-1}(\Phi(\varepsilon_i).\Phi(\xi_j)) \bmod \mathbb{Z}_K$ with the nearest element of $1/d\,\mathbb{Z}_K$ if it is sufficiently close, and re-compute $\Phi(\xi_{j+1})$.

The last step is the determination of $\mathrm{Orb}(t)$. We make a loop in which we compute successively all the $\xi' = \pm\xi \prod \varepsilon_i^{k_i}$ where for all i, $0 \le k_i \le p_i - 1$. For that, at each step, we compute $\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K$ and $\Phi(\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K)$ from the precedent value of this power, by a multiplication by $\Phi(\varepsilon_i)$ or by giving the value $\Phi(1)$, if it is necessary (change of k_i). Then we apply M', we check whether we are close to an element of $\mathbb{Z}_K$ whose coordinates are reduced modulo d, and take for $\Phi(\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K)$ its image by Φ.

Thus, we are sure to have "good" and small values for the successive powers of units: we work modulo $d\,\mathbb{Z}_K$ because if we multiply $\xi \in 1/d\,\mathbb{Z}_K$ by ε^{k_i} or by $\varepsilon^{k_i} \bmod d\,\mathbb{Z}_K$ the result is the same modulo $\mathbb{Z}_K$. Then, for the computation of $\xi' = \pm\xi \prod \varepsilon_i^{k_i} \in 1/d\,\mathbb{Z}_K$, at each step of the product we identify the partial product to the nearest element of $1/d\,\mathbb{Z}_K$ if it is sufficiently close. Thus we know the exact values of the elements of $\mathrm{Orb}(t)$.

6.6. **Computation of $m_{\mathcal{R}}(t)$.** We still have to determine $m_{\mathcal{R}}(t)$ as explained in section 3. To be sure that we have all needed integers we take $k' = k + \epsilon$ in Theorem 3.3. Since for all $x \in \mathrm{Orb}(t)$ and all $X \in \mathcal{R}$, we have $\mathcal{N}(x - X) \in 1/N'\,\mathbb{Z}$, we check whether the successive norms computed are close to $1/N'\,\mathbb{Z}$ and we identify them to the nearest values of $1/N'\,\mathbb{Z}$ found.

7. Tables

Tables of our results are available from [Ce4].

For $n = 2$ we have completed the tables that can be found in F. Lemmermeyer's survey ([L]) and that give the Euclidean minima of $\mathbb{Q}(\sqrt{m})$ for $2 \leq m \leq 102$, where m is a squarefree integer. Apparently, before our work, there was no known minimum beyond the limit $m = 102$, except for particular sequences of fields studied by Barnes and Swinnerton-Dyer (see [BSD]). We have computed $M(K)$ for $K = \mathbb{Q}(\sqrt{m})$, m squarefree and $103 \leq m \leq 400$, except when the size of the fundamental unit ($|\varepsilon| > 10^7$) was too large (28 exceptions). Of course, this can be done in multi-precision.

For $n = 3$, we have completed the results obtained by S. Cavallar and F. Lemmermeyer: we have treated all the number fields with discriminant less than 15000 (291 new results).

For $n = 4$ we have computed Euclidean minima of the 286 number fields of discriminant less than 40000. The Euclidean nature of a large number of them had already been found by R. Quême [Q] but he had left some fields indeterminate. In fact, some of these last ones are not norm-Euclidean although they have class number one (for $D_K = 18432$, 34816 and 35152).

For $n = 5$ there were just 25 number fields known to be norm-Euclidean (see [Q]). We have computed the Euclidean minima of the 156 number fields of discriminant less than 511000. With one exception, the field K of discriminant 390625 which has class number one but verifies $M(K) = 7/5$, they are all norm-Euclidean.

For $n \geq 6$ as far as we know, very little was known on the fields of degree greater than 5. We have treated the 156 first number fields for $n = 6$ and the 132 first number fields for $n = 7$. They are all norm-Euclidean.

Until now, we have not used the algorithm in a systematic way for degree 8. Nevertheless we have computed the Euclidean minimum of the 18 first fields given in J. Klüners's tables [K], which are all norm-Euclidean.

Recall that we had already treated the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{32})$, $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$, whose Euclidean minimum is $1/2$ [Ce1]. We have also found with the algorithm of the present paper, that, if $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{3}}}\right)$, we have $M(K) = M(\overline{K}) = 1/2$.

8. Concluding remark

By Proposition 2.5, if we put

$$\mu(K) = \frac{1}{\inf\left\{|N_{K/\mathbb{Q}}(\Upsilon)|;\ \Upsilon \in \mathbb{Z}_K \setminus (E_k \cup \{0\})\right\}},$$

we can write

$$\mu(K) \leq M(K).$$

It is remarkable to observe that there is in fact an equality for small values of D_K, the number of cases in which this phenomenon occurs growing with n. For instance, for $n = 6$, among the 156 first discriminants ($300125 \leq D_K \leq 5279033$), the only ones for which $\mu(K) < M(K)$ are 4148928 and 4305125. In the cases

$n = 7$ and 8, all the fields K for which we have computed $M(K)$ verify the equality $\mu(K) = M(K)$.
This remark does not contradict the feeling that we have already had about the fields $\mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})$ (where $n \geq 0$ and $\zeta_{2^{n+2}}$ is a primitive 2^{n+2}th root of unity) whose Euclidean minimum, which is $1/2$ for $n \leq 3$, can be conjectured to be $1/2$ also for $n = 4$ and perhaps for n greater than 4 (see [Ce1]).

9. Acknowledgements

I owe a particular debt of gratitude to Guillaume Hanrot for his precious help. Likewise, I warmly thank Christine Bachoc, Eva Bayer-Fluckiger, Harvey Cohn and Franz Lemmermeyer for the interest that they manifested. Finally, I am grateful to the anonymous referee for the many suggestions that he made, and which enabled me to improve the presentation of the paper.

References

[A2X] The A2X laboratory, Number field tables available from `ftp://megrez.math.u-bordeaux.fr/pub/numberfields`.

[BSD] E.S. Barnes and H.P.F Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms, I, *Acta Mathematica* **87** (1952), 259–323. II, ibid. **88** (1952), 279–316.

[Ca] J.W.S. Cassels, *Introduction to the geometry of numbers* Classics in Mathematics, Springer-Verlag, 1971.

[Ce1] J-P. Cerri, De l'euclidianité de $\mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$ et $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ pour la norme, *J. Th. Nombres Bordeaux* **12** (2000), 103–126.

[Ce2] J-P. Cerri, Euclidean and inhomogeneous spectra of number fields with unit rank greater than 1, (to appear in *Journal für die Reine und Angewandte Mathematik*).

[Ce3] J-P. Cerri, Spectres euclidiens et inhomogènes des corps de nombres, *Thèse de Doctorat, Université Henri Poincaré, Nancy* (2005) available from `http://tel.ccsd.cnrs.fr/tel-00011151`.

[Ce4] J-P. Cerri, Tables of Euclidean minima of totally real number fields, available from `ftp://megrez.math.u-bordeaux.fr/pub/cerri`

[CL] S. Cavallar and F. Lemmermeyer, The Euclidean algorithm in cubic number fields, in Győry, Pethő, Sos eds., Proceedings Number Theory Eger 1996, de Gruyter, 1998, 123–146.

[CD] H. Cohn and J. Deutsch, Use of a computer scan to prove $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ and $\mathbb{Q}\left(\sqrt{3+\sqrt{2}}\right)$ are euclidean, *Mathematics of computation* **46** (1986), 295–299.

[K] J. Klüners, Tables available at `http://www.mathematik.uni-kassel.de/~klueners`

[L] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Expositiones Mathematicae* **13** (1995), 385–416.

[P] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, The Pari/GP system, `http://pari.math.u-bordeaux.fr`

[Q] R. Quême, A computer algorithm for finding new Euclidean number fields, *J. Th. Nombres Bordeaux* **10** (1998), 33–48.

[T] W.T. Tutte *Graph Theory*, Encyclopedia of Mathematics and its Applications, vol. 21, Addison-Wesley 1984.

Jean-Paul Cerri, 2, route de Saint-Dié, F-88600 Aydoilles France, e-mail: Jean-Paul.CERRI@wanadoo.fr