Journal de Théorie des Nombres
de Bordeaux **10** (1998), 33–48

A computer algorithm for finding new euclidean number fields

par Roland QUÊME

Résumé. Cet article donne la description d'un algorithme informatique fournissant une condition suffisante pour qu'un corps de nombres soit euclidien pour la norme, ou plus brièvement euclidien. Dans le recensement des corps euclidiens et des méthodes de recherche de ceux-ci, Franz Lemmermeyer a mentionné, [3] p 405, que 743 corps de nombres euclidiens étaient connus (mars 1994), (le premier d'entre eux, $\mathbb{Q}$, découvert par Euclide, trois siècles avant J.-C.!). Durant les premiers mois de 1997, nous avons trouvé plus de 1200 nouveaux corps de nombres euclidiens de degré 4, 5 et 6. Ces résultats ont été obtenus grâce à un algorithme informatique mettant en oeuvre les propriétés classiques des réseaux, plongements de l'anneau des entiers d'un corps de nombres $\mathbf{K}$ de degré n dans $\mathbb{R}^n$, ainsi que la structure du groupe des unités de $\mathbf{K}$. La fin de cet article est une généralisation à la recherche des anneaux euclidiens de S-entiers des corps de nombres $\mathbf{K}$ et à l'étude du minimum inhomogène de la forme Norme. Les résultats obtenus sont cohérents avec ceux de la bibliographie.

Abstract. This article describes a computer algorithm which exhibits a sufficient condition for a number field to be euclidean for the norm. In the survey [3] p 405, Franz Lemmermeyer pointed out that 743 number fields where known (march 1994) to be euclidean (the first one, $\mathbb{Q}$, discovered by Euclid, three centuries B.C.!). In the first months of 1997, we found more than 1200 new euclidean number fields of degree 4, 5 and 6 with a computer algorithm involving classical lattice properties of the embedding of the degree n field $\mathbf{K}$ into $\mathbb{R}^n$ and the structure of the unit group of $\mathbf{K}$. This articles ends with a generalization of the method for the determination of rings of S-integers of number fields euclidean for the norm and for the study of the inhomogeneous minimum of the norm form. Our results are in accordance with known results.

Manuscrit reçu le 10 juin 1997.

1. Some generalities

1.1. **Definitions on number fields.** In this section, we define the principal mathematical objects used in the proofs and in the C++ program. Let $\mathbb{R}$ be the field of real numbers. Let $\mathbb{C}$ be the field of complex numbers. Let $\mathbf{K}$ be a number field of degree n defined by a monic polynomial $P(X)$ with integral coefficients, thus $\mathbf{K} = \mathbb{Q}(x)$ with $P(x) = 0$.

$$\begin{aligned} &P(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \\ &a_1, \ldots, a_n \in \mathbb{Z} \end{aligned} \tag{1}$$

Let us define the signature (r_1, r_2) of the number field $\mathbf{K}$, where r_1 is the number of real roots of $P(X) = 0$ in $\mathbb{C}$ and $2r_2$ is the number of complex roots of $P(X) = 0$ in $\mathbb{C}$. Let $x_i, \quad i = 1, \ldots, n$ be the roots of $P(X) = 0$ in $\mathbb{C}$. In the sequel, these roots will be ordered in this way : $x_i, \quad i = 1, \ldots, r_1$ are the real roots of $P(X) = 0$ and $x_{r_1+2i-1}, x_{r_1+2i}, \quad i = 1, \ldots, r_2$ are the complex roots of $P(X) = 0$, where $x_{r_1+2i} = \overline{x_{r_1+2i-1}}, \quad i = 1, \ldots, r_2$. The discriminant of the number field $\mathbf{K}$ is noted D.

We define the embedding $\mathbf{K} \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, by the relation

$$\begin{aligned} &\mathbf{K} = \mathbb{Q}(x), \\ &\sigma(x) = (x_1, \ldots, x_{r_1}, x_{r_1+1}, x_{r_1+3}, \ldots, x_{r_1+2r_2-1}). \end{aligned} \tag{2}$$

and, concurrently, we note also the n conjugates of x by the relations

$$\sigma_i(x) = x_i, \quad i = 1, \ldots, n. \tag{3}$$

Then, the bijective map $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\tau_1} \mathbb{R}^n$ is defined by

$$\begin{aligned} &b = (b_1, \ldots, b_{r_1}, b_{r_1+1}, \ldots, b_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \\ &\tau_1(b) = (b_1, \ldots, b_{r_1}, \Re(b_{r_1+1}), \Im(b_{r_1+1}), \ldots, \Re(b_{r_1+r_2}), \Im(b_{r_1+r_2})). \end{aligned} \tag{4}$$

Finally, the third map τ is defined as the composition map of the previous ones:

$$\mathbf{K} \xrightarrow{\tau} \mathbb{R}^n \quad \tau = \tau_1 \circ \sigma. \tag{5}$$

Note that, if the field $\mathbf{K}$ is totally real, then τ_1 is the identity map and $\sigma = \tau$. In this article, we note $\mathbf{A}$ the ring of integers of the number field $\mathbf{K} = \mathbb{Q}(x)$. The set $\{1, x, \ldots, x^n\}$ is a basis of $\mathbf{K}$. We define an integral basis $\{y_1, y_2, \ldots, y_n\}$ of $\mathbf{A}$ in function of the basis $\{1, x, \ldots, x^n\}$ of $\mathbf{K}$ by the relations :

$$
\begin{aligned}
&y_1 = \nu_{01} + \nu_{11}x + \cdots + \nu_{i1}x^i + \cdots + \nu_{n1}x^n,\\
&\vdots\\
&y_j = \nu_{0j} + \nu_{1j}x + \cdots + \nu_{ij}x^i + \cdots + \nu_{nj}x^n,\\
&\vdots\\
&y_n = \nu_{0n} + \nu_{1n}x + \cdots + \nu_{in}x^i + \cdots + \nu_{nn}x^n,\\
&\text{where } \nu_{ij} \in \mathbb{Q}, \quad 0 \le i \le (n-1), \quad 1 \le j \le n.
\end{aligned} \tag{6}
$$

1.2. **Classical geometric properties of number fields.** This paragraph states some basic geometric results and notations used in the sequel. We use the notation $\rho = (\rho_1, \ldots, \rho_n)$ for the points of $\mathbb{R}^n$. The map τ defined in the relation (5) allows us to give a geometric description of the ring of integers $\mathbf{A}$. The set $\tau_A = \tau(\mathbf{A}) = \{\tau(a) \mid a \in \mathbf{A}\}$ is a lattice of $\mathbb{R}^n$. A basis of the lattice is the set of n points

$$
\begin{aligned}
b_1 &= \tau(y_1),\\
&\vdots\\
b_n &= \tau(y_n).
\end{aligned} \tag{7}
$$

The fundamental domain F of the lattice τ_A is the set of points $\rho \in \mathbb{R}^n$ which verify the relations $\rho = r_1 b_1 + \cdots + r_i b_i + \cdots + r_n b_n$, where $r_i \in \mathbb{R}$ verify the inequalities $0 \le r_i \le 1, \quad 1 \le i \le n$.

1.3. **Geometric definition of the norm form.** Let c be an algebraic number, $c \in \mathbf{K}$. The norm of c is defined by the formula

$$N(c) = \prod_{i=1}^{n} \sigma_i(c) = \prod_{i=1}^{r_1} \sigma_i(c) \prod_{i=1}^{r_2} \sigma_{r_1+2i-1}(c)\overline{\sigma_{r_1+2i-1}(c)}. \tag{8}$$

From the previous relation, we deduce immediately that :

$$N(c) = \prod_{i=1}^{r_1} \sigma_i(c) \prod_{i=1}^{r_2} (\Re(\sigma_{r_1+2i-1}(c))^2 + \Im(\sigma_{r_1+2i-1}(c))^2). \tag{9}$$

The norm form, or shortly, the norm of a point ρ of $\mathbb{R}^n$ is the form given by the formula :

$$\mathcal{N}(\rho) = |\prod_{i=1}^{r_1} \rho_i| \prod_{i=1}^{r_2} (\rho_{r_1+2i-1}^2 + \rho_{r_1+2i}^2). \tag{10}$$

From the two relations (9) and (10), we deduce that, for $c \in \mathbf{K}$, we have the identity connecting the algebraic and geometric point of view :

$$\mathcal{N}(\tau(c)) = |N(c)|. \tag{11}$$

1.4. **Definition of fundamental units.** The set of units of $\mathbf{A}$, noted $\mathbf{A}^*$, is a group of $\mathbb{Z}$-rank $r = r_1 + r_2 - 1$. Any unit $\varepsilon \in \mathbf{A}^*$ can be written :

$$\varepsilon = \eta_0^{m_0} \eta_1^{m_1} \ldots\ldots\cdots \eta_r^{m_r}, \quad m_1 \in \mathbb{Z}, \ldots, m_r \in \mathbb{Z}, \tag{12}$$

where η_0 generates the group of roots of unity in $\mathbf{K}$ and $\eta_1, \ldots, \eta_r$ is a set of r fundamental units.

1.5. **Definition of euclidean number fields.** The number field $\mathbf{K}$ is said to be euclidean if, for all $c \in \mathbf{K}$, there exists $q \in \mathbf{A}$ such that $|N(c-q)| < 1 \Leftrightarrow \mathcal{N}(\tau(c-q)) < 1 \Leftrightarrow \mathcal{N}(\tau(c) - \tau(q)) < 1$. For $\mathbf{K}$ to be euclidean, a sufficient geometric condition is that, for all $\rho \in \mathbb{R}^n$, there exists $q \in \mathbf{A}$ such as

$$\mathcal{N}(\rho - \tau(q)) < 1 \tag{13}$$

We shall use that sufficient geometric condition in the sequel :

- we say that a point $\rho \in \mathbb{R}^n$ is euclidean if there exists $q \in \mathbf{A}$ such that $\mathcal{N}(\rho - \tau(q)) < 1$.
- we say that a subset G of $\mathbb{R}^n$ is euclidean if for all $\rho \in G$, there exists $q \in \mathbf{A}$ such that $\mathcal{N}(\rho - \tau(q)) < 1$.
- Note that, if the fundamental domain F of $\mathbf{K}$ is euclidean, then $\mathbb{R}^n$ is euclidean and the number field $\mathbf{K}$ is also euclidean.

2. Principles of the algorithm

The fundamental domain F is covered by a set of *small* cubes of $\mathbb{R}^n$ and the algorithm checks over the euclideanity of each of them by different angles of attack. If the fundamental domain F is covered by a set of cubes all euclidean, the number field $\mathbf{K}$ is euclidean. Note that the algorithm exhibits sufficient condition for a number field to be euclidean, but not at all a necessary and sufficient condition. Stage 1 of the algorithm searches for euclidean cubes only by geometric considerations. Stage 2 of the algorithm searches for euclidean cubes, among those left indeterminate in stage 1, using the geometric properties of the embedding τ of the units of the ring of integers $\mathbf{A}$ in $\mathbb{R}^n$.

3. Stage 1

3.1. **Some definitions.** Here, are some specific definitions and notations of this part of the algorithm :

- Let $\rho \in \mathbb{R}^n$ and $a \in \mathbb{R}$. Let $C(\rho, a)$ denote the cube of $\mathbb{R}^n$, of center ρ, of edge length a, of which the n pairs of faces are perpendicular to the n axes $\mathbb{R}^{(i)}, i = 1, \ldots, n$ of $\mathbb{R}^n$.

- Let $\rho_1, \rho_2 \in \mathbb{R}^n$. Let $d(\rho_1, \rho_2)$ denote the distance between ρ_1 and ρ_2 given classically by the formula :

$$d(\rho_1, \rho_2) = \sqrt{(\rho_{11} - \rho_{21})^2 + \cdots + (\rho_{1n} - \rho_{2n})^2}. \tag{14}$$

- Let O be the origin of $\mathbb{R}^n$. Let F be a fundamental domain of $\tau(\mathbf{A})$ of which the origin O is a vertex. F is a parallelotope. Let $b_1, \ldots, b_n$ be the basis of the lattice τ_A defined by (7). Let s be the symmetry center of the parallelotope F. Let $P_i(F)$ be the face of F defined by the set of n points $\{O, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n\}$. Let $P_{n+i}(F)$ be the second face of F parallel to $P_i(F)$. Let $P_i(H)$ be the plane of R^n, parallel to $P_i(F)$, at a distance $\delta = \sqrt{n} \times \frac{a}{2}$ of $P_i(F)$ and not in the same side of $P_i(F)$ than s. Let $P_{n+i}(H)$ be the plane of $\mathbb{R}^n$, parallel to $P_{n+i}(F)$, at a distance $\delta = \sqrt{n} \times \frac{a}{2}$ of $P_{n+i}(F)$ and not in the same side of $P_{n+i}(F)$ than s. Let H be the parallelotope of $\mathbb{R}^n$, of which faces are the $2n$ planes $P_i(H), P_{n+i}(H), \quad i = 1, \ldots, n$.

3.2. **Some theoretic propositions.** This section contains some theoretic propositions used in the programming of stage 1 of the algorithm.

Proposition 1. *The fundamental domain F is symmetric with respect to the point $\tau(b_s) = \tau(\frac{b_1+\cdots+b_n}{2})$. If the point ρ is euclidean (respectively not euclidean), then the point $\tau(2b_s) - \rho$ is euclidean (respectively not euclidean).*

Proof. The fundamental domain F is a parallelotope built on the origin O and the basis $\{b_1, \ldots, b_n\}$ of the lattice τ_A. Classically, this parallelotope is symmetric with respect to the point $\tau(b_s) = \tau(\frac{b_1+\cdots+b_n}{2})$. If ρ is euclidean, then there exists $q \in \mathbf{A}$ such that $\mathcal{N}(\rho - \tau(q)) < 1 \Rightarrow \mathcal{N}((\tau(2b_s) - \rho) - (\tau(2b_s) - \tau(q))) < 1 \Rightarrow \mathcal{N}((\tau(2b_s) - \rho) - (\tau(2b_s - q))) < 1$ where $\tau(2b_s - q) \in \tau_A \Rightarrow \tau(2b_s) - \rho$ is an euclidean point symmetric to the euclidean point ρ. The proof is similar for non euclidean points. □

Therefore, in the algorithm, by symmetry, we shall limit the determination of euclideanity of the fundamental domain F to half a part of this domain and thus reduce the CPU time by 2.

Proposition 2. *Let $C(0, a)$ be a cube of $\mathbb{R}^n$, hence of center 0 and of edge length a. Let ρ be a point of $\mathbb{R}^n$; Then, for all points $u \in C(0, a)$, we have*

$$\mathcal{N}(\rho + u) \leq B(\rho, a) \tag{15}$$

where

$$B(\rho, a) = \prod_{i=1}^{r_1}(|\rho_i| + \frac{a}{2}) \prod_{i=1}^{r_2}(((|\rho_{r_1+2i-1} + \frac{a}{2})^2 + (|\rho_{r_1+2i}| + \frac{a}{2})^2). \tag{16}$$

This inequality is the best possible in the sense that, for a vertex of $C(0, a)$, the inequality becomes an equality.

Proof. Let $u \in C(0,a)$. We have the inequalities :

$$|\rho_i + u_i| \leq |\rho_i| + \frac{a}{2}, \quad i = 1, \dots, n \tag{17}$$

which leads to relation (15). The equality is effectively obtained when, for $i = 1, \dots, n$, we have $|u_i| = \frac{a}{2}$ and $sign(u_i) = sign(\rho_i)$, therefore the result is the best possible. □

Proposition 3. *Let $L_a = \{i_1 a, \dots, i_n a \mid i_1 \in \mathbb{Z}, \dots, i_n \in \mathbb{Z}\}$ be the lattice of $\mathbb{R}^n$ defined from a, edge length of the cube $C(0,a)$. Let I be the (finite) set of points of $L_a \cap H$, where the parallelotope H is defined in the section (3.1). Then, the set J of cubes $\{C(\rho_i, a) \mid \rho_i \in I\}$ covers the fundamental domain F.*

Proof. If $C(\rho_i, a) \cap F \neq \emptyset$, then there exists a point $\gamma \in F$ such that $d(\rho_i, \gamma) \leq a\frac{\sqrt{n}}{2}$ because the euclidean distance δ of any point of the cube $C(0,a)$ to the center of this cube is smaller than $a\frac{\sqrt{n}}{2}$. Then, from the definitions of the parallelotopes F and H, we deduce that $\rho_i \in H$. Therefore, the set J of all the cubes whose center belongs to $L_a \cap H$ cover the fundamental domain F. □

3.3. **Stage 1 of the algorithm.** In this section, we describe the first stage of the algorithm. Let $\mathbf{K}$ be a number field, with the fundamental domain F of the lattice τ_A. To prove that $\mathbf{K}$ is an euclidean number field, it is sufficient to prove that all the cubes of the set J (defined above) are euclidean. Let a cube $C(\rho, a) \in J$. To prove that the cube $C(\rho, a)$ is euclidean, it is sufficient, using the proposition 2, that there exists $q \in \mathbf{A}$ verifying the relation

$$B((\rho - \tau(q)), a) < 1. \tag{18}$$

Determination of euclidean cubes $C(\rho, a)$**.** Recall that $C(\rho, a)$ denotes the cube of $\mathbb{R}^n$ of center $\rho \in L_a \cap H$ and of edge length a. The candidates for $\tau(q)$ are taken from the set of lattice points with $d(\tau(q), 0) < m\sqrt{n}$, verifying relation(18), with $m \to +\infty$. The computer algorithm takes the greatest values m possible which are reasonably compatible with the CPU speed of the computer.

A trick of the algorithm is, when we fail to find q with euclidean cube $C((\rho, a)$, consists in trying again locally for this cube, with a partition of $C(\rho, a)$ in smaller cubes of edge length $\frac{a}{2}$, or $\frac{a}{3}, \dots$

Then, at the end of the stage 1 of the algorithm, the alternative is :

- All the cubes of J are euclidean, and the number field $\mathbf{K}$ is euclidean.
- For m cubes $\{C(\rho_j, a) \subset J, \quad j = 1, \dots, m\}$, the algorithm stage 1 does not allows us to conclude if they are euclidean : then, we say that these m cubes are *indeterminate*.

4. Stage 2 of the algorithm

In this section, we describe the part of the algorithm involving the units of the number field $\mathbf{K}$, to reduce, and, if possible to annihilate, the number of indeterminate cubes. The method is similar to the one explained by Stefania Cavallar and Franz Lemmermeyer in [1] for cubic fields.

4.1. **Definitions.** Recall that the map σ, τ_1 and τ are respectively defined by the relations (2), (4) and (5). We fix some notations and definitions for this part of the algorithm:

- Let $C_j = C(\rho_j, a), \quad j = 1, \ldots, m$ be the remaining indeterminate cubes at the end of stage 1 of the algorithm.
- Let $\varepsilon \in \mathbf{A}^*$ be a unit of the ring $\mathbf{A}$.
- Let $d = \{d_1, \ldots, d_n\}$ be a point of $\mathbb{R}^n$. From the relation (4), we have

$$\tau_1^{-1}(d) = (d_1, \ldots, d_{r_1}, (d_{r_1+1} + \mathbf{i}\ d_{r_1+2}), \ldots, (d_{r_1+2r_2-1} + \mathbf{i}\ d_{r_1+2r_2})), \tag{19}$$

  where $\mathbf{i}$ is the complex number, $\mathbf{i}^2 + 1 = 0$.
- Let $c \in K$. If $|N(c-q)| < 1$ with $q \in A$, then $|N(c\varepsilon - q\varepsilon)| < 1$. In the same way, if $|N(c-q)| \geq 1$ for all $q \in A$, then $|N(c\varepsilon - q)| \geq 1$ for all $q \in A$. The multiplication by a unit ε of A^* lefts invariant the set of non euclidean points of $\tau(K)$. This remark leads us to define a map $\tau(K) \xrightarrow{\gamma_\varepsilon} \tau(K)$ by $\gamma_\varepsilon(\tau(b)) = \tau(b\varepsilon)$.

  Let $d \in \mathbb{R}^n$. The map γ_ε can be extended to the map $\mathbb{R}^n \xrightarrow{\gamma_\varepsilon} \mathbb{R}^n$ by the relation

$$\begin{aligned} &\gamma_\varepsilon(d) = \tau_1((d_1\sigma_1(\varepsilon), \ldots, d_{r_1}\sigma_{r_1}(\varepsilon), \\ &(d_{r_1+1} + \mathbf{i}d_{r_1+2})\sigma_{r_1+1}(\varepsilon), \ldots, (d_{r_1+2r_2-1} + \mathbf{i}d_{r_1+2r_2})\sigma_{r_1+2r_2-1}(\varepsilon)). \end{aligned} \tag{20}$$

  From $\mathcal{N}(\tau(\varepsilon)) = 1$, it can be seen that the transformation γ_ε keeps the volumes of $\mathbb{R}^n$.
- We note, in the sequel, $\Gamma_j(\varepsilon)$ the compact of $\mathbb{R}^n$ defined by :

$$\Gamma_j(\varepsilon) = \{\gamma_\varepsilon(d) |\ \forall d \in C_j\}. \tag{21}$$

  Note that the volume in $\mathbb{R}^n$ of $\Gamma_j(\varepsilon)$ is equal to the volume in $\mathbb{R}^n$ of C_j because the map γ_ε keeps the volumes.

  Call *size* of a compact $\mathbf{C} \subset \mathbb{R}^n$, the real s defined by $s = sup(d(x, y))$ for all $x, y \in C$. The size of the compact $\Gamma_j(\varepsilon)$ is generally much larger than the size of the cube C_j and even of the fundamental domain F of $\tau(A)$ because $sup(|\sigma_i(\varepsilon)|, \quad i = 1, \ldots, r_1 + r_2)$ is, generally, much larger than 1.

4.2. **Some theoretic results.** The cubes $C_j, \quad j=1,\dots,m$ are left indeterminate by stage 1. Generally, some of them are in fact euclidean, sometimes all. The stage 2 of the algorithm aims to reduce, or to annihilate, the number of cubes left indeterminate in stage 1. Stage 2 rests on the three next propositions using the geometric properties of the fundamental units.

The compact $\Gamma_l(\varepsilon), \quad l=1,\dots,m$ is said euclidean if all its points are euclidean. $\Gamma_l(\varepsilon)$ is euclidean if and only if the cube C_l is euclidean because γ_ε lefts invariants the units of A^*. The subset $\bigcup_{j=1,\forall\alpha\in A}^{m}(C_j-\tau(\alpha))$ of $\mathbb{R}^n$ contains all the non euclidean points of $\mathbb{R}^n$. In the same way, the subset $\bigcup_{l=1,\forall\alpha\in A}^{m}(\Gamma_l(\varepsilon)-\tau(\alpha))$ of $\mathbb{R}^n$ contains all the non euclidean points of $\mathbb{R}^n$. Therefore, if a cube C_j has a non euclidean point, there exists at least one $l, \quad 1\le l\le m$ and one $\alpha\in A$ such that $C_j\cap(\Gamma_l(\varepsilon)-\tau(\alpha))\neq\emptyset$. On the other hand, if $C_j\bigcap\left(\cup_{l=1,\forall\alpha\in A}^{m}(\Gamma_l(\varepsilon)-\tau(\alpha))\right)=\emptyset$, we conclude that C_j is euclidean, which leads to the next proposition:

Proposition 4. *If we have the relation*

$$\{\cup_{l=1,\forall\alpha\in A}^{m}(\Gamma_l(\varepsilon)-\tau(\alpha))\}\bigcap C_j=\emptyset \tag{22}$$

then the cube C_j is euclidean.

The two next propositions aim to find cubes Cj verifying the relation (22) to eliminate them qua euclidean cubes.

Proposition 5. *Let m be the number of indeterminate cubes $C_j=C(\rho_j,a)$ at the end of stage 1 of the algorithm. Let the cube C_j and the compact $\Gamma_l(\varepsilon)$. A necessary condition on $\alpha\in A$ for $C_j\cap\left(\Gamma_l(\varepsilon)-\tau(\alpha)\right)\neq\emptyset$ is that $\tau(\alpha)=(\alpha_1,\dots,\alpha_{r_1},\alpha_{r_1+1},\alpha_{r_1+2},\dots,\alpha_{r_1+2r_2-1},\alpha_{r_1+2r_2}) \quad \in\mathbb{R}^n$ verify the relations :*

$$\begin{aligned}
&\alpha_i\le\sigma_i(\varepsilon)\rho_{li}-\rho_{ji}+a\frac{(1+|\sigma_i(\varepsilon)|)}{2}, \quad i=1,\dots,r_1\\
&\alpha_i\ge\sigma_i(\varepsilon)\rho_{li}-\rho_{ji}-a\frac{(1+|\sigma_i(\varepsilon)|)}{2}, \quad i=1,\dots,r_1
\end{aligned} \tag{23}$$

$$\begin{aligned}
&\alpha_{r_1+2i-1} \ \le\\
&\Re(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i-1}-\Im(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i}-\rho_{j,r_1+2i-1}\\
&+a\frac{(1+|\Re(\sigma_{r_1+2i-1}(\varepsilon))|+|\Im(\sigma_{r_1+2i-1}(\varepsilon))|)}{2}, \quad i=1,\dots,r_2
\end{aligned} \tag{24}$$

$$\begin{aligned}\alpha_{r_1+2i-1} \;&\geq \\ \Re(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i-1} &- \Im(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i} - \rho_{j,r_1+2i-1} \\ &- a\frac{(1+|\Re(\sigma_{r_1+2i-1}(\varepsilon))|+|\Im(\sigma_{r_1+2i-1}(\varepsilon))|)}{2}, \quad i=1,\ldots,r_2\end{aligned} \tag{25}$$

$$\begin{aligned}\alpha_{r_1+2i} \;&\leq \\ \Im(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i-1} &+ \Re(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i} - \rho_{j,r_1+2i} \\ &+ a\frac{(1+|\Re(\sigma_{r_1+2i-1}(\varepsilon))|+|\Im(\sigma_{r_1+2i-1}(\varepsilon))|)}{2}, \quad i=1,\ldots,r_2\end{aligned} \tag{26}$$

$$\begin{aligned}\alpha_{r_1+2i} \;&\geq \\ \Im(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i-1} &+ \Re(\sigma_{r_1+2i-1}(\varepsilon))\rho_{l,r_1+2i} - \rho_{j,r_1+2i} \\ &- a\frac{(1+|\Re(\sigma_{r_1+2i-1}(\varepsilon))|+|\Im(\sigma_{r_1+2i-1}(\varepsilon))|)}{2}, \quad i=1,\ldots,r_2\end{aligned} \tag{27}$$

Proof. To have the relation $(\Gamma_l(\varepsilon) - \tau(\alpha)) \bigcap C_j \neq \emptyset$, it is necessary that there exists $u \in C(0,a), v \in C(0,a)$ and $\alpha \in \mathbf{A}$ which verify the relation

$$\gamma_\varepsilon(\rho_l + u) - \tau(\alpha) = \rho_j + v. \tag{28}$$

- For $i = 1, \ldots, r_1$: we deduce

$$(\rho_{li} + u_i)\sigma_i(\varepsilon) - \alpha_i = \rho_{ji} + v_i. \tag{29}$$

  From this relation and from the inequalities $|u_i| \leq \frac{a}{2}$ and $|v_i| \leq \frac{a}{2}$, we can deduce the relation (23).
- For $i = 1, \ldots, r_2$: From the relation (28), we have

$$\tau_1^{-1}(\gamma_\varepsilon(\rho_l + u)) - \tau_1^{-1}(\alpha) = \tau_1^{-1}(\rho_j + v). \tag{30}$$

  Then, we obtain from the relation (20) and the previous relation (30) the relation in $\mathbb{C}$,

(31)
$$\begin{aligned}&(\rho_{l,r_1+2i-1} + u_{r_1+2i-1} + \mathbf{i}(\rho_{l,r_1+2i} + u_{r_1+2i}))\sigma_{r_1+2i-1}(\varepsilon) - \sigma_{r_1+2i-1}(\alpha) = \\ &\quad (\rho_{j,r_1+2i-1} + v_{r_1+2i-1} + \mathbf{i}(\rho_{j,r_1+2i} + v_{r_1+2i})).\end{aligned}$$

  From this relation and of the inequalities $|u_{r_1+2i-1}| \leq \frac{a}{2}$, $|u_{r_1+2i}| \leq \frac{a}{2}$, $|v_{r_1+2i-1}| \leq \frac{a}{2}$ and $|v_{r_1+2i}| \leq \frac{a}{2}$, we can deduce the relations (24), (25),(26) and (27).

□

4.3. **Remark.** If the edge length a of $C(\rho_j, a)$ is *small* compared to the fundamental domain F, there exists at most one $\alpha \in \mathbf{A}$ verifying the proposition (5).

4.4. **Remark.** The proposition (5) shows that the integers α of $\mathbf{A}$ verifying (23),(24),(25),(26) and (27) if any, are contained in a parallelotope T whose faces are perpendicular to axes $\mathbb{R}^{(i)}$ of $\mathbb{R}^n$ and of which the relations (23),(24),(25),(26) and (27) gives the vertex coordinate on $\mathbb{R}^n$. In the computer algorithm, the determination of the integers $\alpha \in \mathbf{A}$ such that $\tau(\alpha)$ belongs to this parallelotope is obtained in this way: We compute, for $k = 1, \dots, 2^n$ the coordinates $t_k(i), \quad i = 1, \dots, n$ of the vertex of T on the integral basis $Y = \{\tau(y_1), \dots, \tau(y_n)\}$, and then, for each $i, \quad 1 \leq i \leq n$, the minimum $m_i = \min(t_k(i)), \quad k = 1, \dots, 2^n$ and maximum $M_i = \max(t_k(i)),\ k = 1, \dots, 2^n$.

Let, for $\alpha \in \mathbf{A}$, the expression of $\tau(\alpha)$ on the integral basis Y:

$\tau(\alpha) = a_1\tau(y_1) + a_2\tau_2(y_2) + \dots + a_n\tau_n(y_n)$

$a_1, a_2, \dots, a_n \in \mathbb{Z}$. The possible values a_i are bounded by the relations

$$m_i \leq a_i \leq M_i, \quad i = 1, \dots, n \tag{32}$$

where the number of candidate α is finite because $a_i \in \mathbb{Z}$.

Let the cube C_j and the compact $\Gamma_l(\varepsilon)$ for j, l given. Then, let $\alpha \in A$ verifying the necessary condition of proposition (5). The next proposition gives a criterium, easily implemented on a computer, to determine if

$C_j \cap (\Gamma_l(\varepsilon) - \tau(\alpha)) = \emptyset$. In fact, we define a discrete set of points $M_l(\varepsilon) \subset \Gamma_l(\varepsilon)$ such that $M_l(\varepsilon) \cap C_j = \emptyset \Rightarrow \Gamma_l(\varepsilon) \cap C_j = \emptyset$.

Proposition 6. *Let the cube C_j and the compact $\Gamma_l(\varepsilon)$ given. Let $\alpha \in \mathbf{A}$ verifying the relations (23),(24),(25),(26) and(27) of the proposition (5). Let $p_i \in \mathbb{R}, \quad i = 1, \dots, n$ be elements defined by the relations:*

$$\begin{aligned} p_i &= \frac{a}{2}, \quad \text{if } |\sigma_i(\varepsilon)| \leq 1, \\ p_i &= \frac{a}{2|\sigma_i(\varepsilon)|}, \quad \text{if } |\sigma_i(\varepsilon)| > 1. \end{aligned} \tag{33}$$

Let M_l be the finite discrete set of points μ of $\mathbb{R}^n$ defined by the relations

$$\begin{aligned} &\mu_i = \rho_i + m_i \times p_i, \quad m_i \in \mathbb{Z}, \quad i = 1, \dots, n, \\ &\mu \in C(\rho_l, 2a). \end{aligned} \tag{34}$$

Let $M_l(\varepsilon)$ be the set of points $\gamma_\varepsilon(\mu) - \tau(\alpha)$ for $\mu \in M_l$. If $(M_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) = \emptyset$, we have $(\Gamma_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) = \emptyset$.

Proof. We examine successively the case of real and complex embeddings:

- At first, consider the real embeddings $i = 1, \dots, r_1$: the minimal distance δ_i on the i^{th} coordinate $\mathbb{R}^{(i)}$ of $\mathbb{R}^n$ between two points of $M_l(\varepsilon)$ is given by the relation $\delta_i = p_i|\sigma_i(\varepsilon)|$. Therefore, from the relation (33),

$$\delta_i \leq \frac{a}{2}. \tag{35}$$

- Then, consider the complex embeddings $(r_1+2i-1, r_1+2i), i = 1, \ldots, r_2$: Note that the square of edge length a of $\mathbb{R}^{(r_1+2i-1)} \times \mathbb{R}^{(r_1+2i)} \cong \mathbb{C} \cong \mathbb{R}^2$, whose the vertex coordinate are $(0,0),(a,0),(0,a),(a,a)$ is transformed by the multiplication
  $\sigma_{r_1+2i-1}(\varepsilon) = \Re(\sigma_{r_1+2i-1}(\varepsilon)) + \mathbf{i}\Im(\sigma_{r_1+2i-1}(\varepsilon))$
  on a square of edge length $a|\sigma_{r_1+2i-1}(\varepsilon)| \Rightarrow$ the minimal distance δ_{r_1+2i-1} between two points of $M_l(\varepsilon)$ on the coordinate $\mathbb{R}^{(r_1+2i-1)} \times \mathbb{R}^{(r_1+2i)} \cong \mathbb{R}^2$ is given by the relation $\delta_{r_1+2i-1} = |\sigma_{r_1+2i-1}(\varepsilon)| \times p_{r_1+2i-1}$, which leads, from the definition of p_{r_1+2i-1}, as for the real embeddings to

$$\delta_{r_1+2i-1} \leq \frac{a}{2}. \tag{36}$$

Therefore, the minimal distance $\delta_i, \quad i = 1, \ldots, r_1$ between two points of a real embedding on $\mathbb{R}^{(i)}$, or the minimal distance $\delta_{r_1+2i-1}, \quad i = 1, \ldots, r_2$ between two points of a complex embedding on $\mathbb{R}^{(r_1+2i-1)} \times \mathbb{R}^{r_1+2i)} \cong \mathbb{R}^2$ is always $\leq \frac{a}{2}$. Then, from the definition of $M_l(\varepsilon)$ and from the relations (35) and (36), we deduce that if $(\Gamma_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) \neq \emptyset$, there is at least one point of $(M_l(\varepsilon) - \tau(\alpha)) \in C(\rho_j, a) \Rightarrow (M_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) \neq \emptyset$, which leads to the result :

If $(M_l(\varepsilon) - \tau(\alpha))$ has no points in the cube $C(\rho_j, a)$, then $(\Gamma_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) = \emptyset$. □

4.5. **Description of stage 2 of the algorithm.** At the end of the stage 1 of the algorithm, the alternative is : all the cubes $C(\rho, a)$ covering F are euclidean and the number field $\mathbf{K}$ is euclidean, or there are m cubes $C(\rho_j, a), \quad , j = 1, \ldots, m$ which are left indeterminate: stage 1 did not allow us to conclude that these cubes are euclidean. Stage 2 of the algorithm aims to find some euclidean cubes among them. Let the indeterminate cubes $\{C(\rho_j, a) \mid j = 1, \ldots, m\}$. The algorithm examines each of them, for $j = 1, \ldots, m$. Suppose j and l are given. If there are not any $\alpha \in \mathbf{A}$ which verify the relations (23), (24), (25),(26) and (27) of proposition (5), then, for all $\alpha \in \mathbf{A}, \quad (\Gamma_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) = \emptyset \Rightarrow$ the pair (j, l) can be eliminated. If not, we can then find α such that the relations (23),(24),(25),(26) and (27) are verified. Notice that, if we suppose that the edge length a of the cubes C is sufficiently small, α is unique. Then, we apply the proposition (6) : if we have $(M_l(\varepsilon) - \tau(\alpha)) \bigcap C(\rho_j, a) = \emptyset$, we can eliminate the pair (j, l). If, for j given, we can eliminate all the pairs $(j, l), \quad l = 1, \ldots, m$, then the cube $C(\rho_j, a)$ is euclidean from the proposition (4).

We have made no assumption on the unit ε, thus this algorithm can be used with all units $\varepsilon \in \mathbf{A}^*$. It is CPU time consuming if the unit is of *large* size, more precisely if $|\max(\sigma_i(\varepsilon))|,\ i = 1,\dots,n$ is a large real number, for instance greater than 10^6. Therefore, we limit the algorithm to a set of fundamental units of *small* size and their inverse $\{\eta_i, \quad \eta_i^{-1} \mid \quad, i = 1,\dots,r_1+r_2-1\}$. If there are no cubes $C(\rho_j, a)$ left indeterminate by stage 2 of the algorithm, the number field $\mathbf{K}$ is euclidean.

5. Computer Results

This section gives the results obtained in the first semester of 1997 for the number fields of degree $n, \quad 4 \le n \le 6$ with the C++ program described in this article. The number field $\mathbf{K}$, generated by a root x of the polynomial $P(X)$, of discriminant D, of integral basis $\{y_1,\dots,y_n\}$ expressed in function of the basis $\{1, x, \dots, x^n\}$ of $\mathbf{K}$, with the set of fundamental units $\{\varepsilon_1,\dots,\varepsilon_{r_1+r_2-1}\}$ expressed in function of the integral basis $\{y_1,\dots,y_n\}$, are found in the files of the Server

`megrez.math.u-bordeaux.fr/numberfields/`

of the Bordeaux University.

When, in the following results, the discriminants are noted $D_1, D_2, \dots$, that means that in the given degree and signature, there are several fields $\mathbf{K}$ with the same discriminant D.

5.1. Number fields $n = 4, r_1 = 0, r_2 = 2$. 114 fields $\mathbf{K}$ whose discriminant D are listed below are norm-euclidean: $D =$ 117, 125, 144, 189, 225, 229, 256, 257, 272, 320, 333, 392, 400, 432, 441, 512, 513, 549, 576_1, 576_2, 592, 605, 656, 657, 697, 761,784,788, 832, 837, 873, 892, 981, 985, 1008_1, 1008_2, 1016, 1025, 1040_1, 1040_2, 1076, 1088_1, 1088_2, 1089, 1129, 1161, 1168, 1197_1, 1197_2, 1225, 1229, 1257, 1264, 1372, 1384, 1396, 1413, 1421, 1424, 1489, 1492, 1509, 1525, 1552, 1556, 1568, 1593, 1600, 1616, 1629, 1728, 1737, 1765, 1808, 1809, 1813, 1825, 1856, 1929, 1937, 1940, 1953_1, 1953_2, 2021 ,2048_1, 2057, 2061, 2112_1, 2156_2, 2169, 2197, 2256, 2272, 2292, 2296, 2312, 2320_1, 2368, 2429, 2597_2, 2601, 2673, 2725, 2736, 2781, 2836, 3024_1, 3033, 3141, 3173, 3221,3316, 3368, 3757.

Among them, 65 are new, compared with the list given by Franz Lemmermeyer in [3].

5.2. Number fields $n = 4, r_1 = 2, r_2 = 1$. Among the fields with $|D| \le$ 15000, the fields whose $|D| =$ 6848, 7975_1, 7975_2, 8375, 10475_1, 10800_1, 10975_1, 11200_2, 11500, 11600_1, 11600_2, 12375, 12675, 12844, 12875, 13100, 13175, 13575, 13775_1, 13775_2, 14000, 14336 are not principal, therefore not euclidean. The fields with $|D| =$ 4564, 5488, 5732, 6883_3, 7087, 8123, 8183, 8492, 8667, 9127, 9163, 9216, 9248, 9364, 9972, 10079, 10091, 10187, 10531, 10688, 10859, 11280, 11568, 11627, 11907, 11975, 11979, 12047, 12103, 12203, 12344, 12539, 12547, 12763_1, 12763_3, 12811, 13231, 13248, 13327, 13448, 13456, 13723, 13924, 14003, 14035, 14087, 14227, 14272, 14336_2, 14400, 14515,14591, 14703, 14843, 14896, 14975 are left indeterminate [1] in the computer test we made [2]. The other 681 fields are norm-euclidean. Among them, 664 are new, compared with the list given in [3].

5.3. **Number fields** $n = 4, r_1 = 4, r_2 = 0$. Among the 283 fields with $0 < |D| \leq 37532$, the field with $D = 21025$ is not principal therefore not euclidean, the 26 fields with discriminant $D =$ 13725, 15125, 16400, 17725, 18432, 22000, 23525, 24336, 26225, 27725, 28400, 30125, 30400, 32225, 32625, 33625, 33725, 34816, 35152, 35225, 37525, 37952, 38000, 38225, 38725, 38864. are indeterminate. The 256 other fields are euclidean. Among them, 239 are new, compared with [3].

5.4. **Number fields** $n = 5, r_1 = 3, r_2 = 1$. The two fields with $D = -18463, -24671$ are indeterminate for a trivial reason! the Bairstow method of resolution of P(x)=0 for the polynomial $P(X)$ has failed in the test).

All the other 92 fields with discriminant $D, \quad 0 < |D| \leq 37532$ are norm-euclidean. Among them, at least 82 are new, compared with [3].

5.5. **Number fields** $n = 5, r_1 = 1, r_2 = 2$. The field with $D = 16129$ is indeterminate for the same reason. the Bairstow method of resolution of P(x)=0 for the polynomial $P(X)$ fails in the test) All the other 146 fields with $0 < D \leq 17232$ are euclidean. Among them, at least 132 are new, compared with [3].

5.6. **Number fields** $n = 5, r_1 = 5, r_2 = 0$. The 25 fields with $0 < D \leq 161121$ are euclidean. Among them, 22 are new, compared with [3].

5.7. **Number fields** $n = 6, r_1 = 0, r_2 = 3$. The 5 fields with $9747 \leq |D| \leq 11691$ are euclidean.

5.8. **Number fields** $n = 6, r_1 = 2, r_2 = 2$. The 11 fields with $28037 \leq |D| \leq 35557$ are euclidean.

5.9. **Synthesis.** There are at least 1204 new fields, compared with [3], where the number of euclidean fields known in 1994 was 743, with degree $n, \quad 1 \leq n \leq 12$.

---

[1] The meaning of this word is given previously in the article

[2] with the initial parameters chosen, especially the value of the edge a of the cubes $C(\rho_j, a)$ covering the fundamental domain F : it is possible, that for different initial parameters , some of them would be found norm-euclidean

6. Some generalizations

We give here two generalizations of the algorithm:

- the study of euclidean rings of S-integers $\mathbf{A}_S$ of number fields $\mathbf{K}$, with $\mathbf{A} \subset \mathbf{A}_S,\ \mathbf{A} \neq \mathbf{A}_S,\ \mathbf{A}_S \subset \mathbf{K}$.
- the study of the inhomogeneous minimum of the norm form $\mathcal{N}(\rho - \tau(q))$ for $\rho \in \mathbb{R}^n$ and $q \in \mathbf{A}$.

6.1. **Rings of S-integers $\mathbf{A}_S$ of number fields $\mathbf{K}$.** Let $v_{p_1}, \ldots, v_{p_t}$ be a set of t non archimedean valuations of $\mathbf{K}$. Let $\mathbf{A}_S$ be the ring of S-integers of the number field $\mathbf{K}$ corresponding to this set of valuations, therefore such that for all $v_p \notin \{v_{p_1}, \ldots, v_{p_t}\}$ and for all $a \in \mathbf{A}_S$, we have $v_p(a) \geq 0$. O'Meara's theorem asserts that, for all rings A_S defined by a valuation set $\mathcal{S} = \{v_{p_1}, \ldots, v_{p_t}\}$, it is always possible to find a finite set of valuations $\mathcal{S}' = \{v_{p_1}, \ldots, v_{p_{t'}}\}$ with $\mathcal{S} \subseteq \mathcal{S}'$ such that the ring $\mathbf{A}_{S'}$ is euclidean for the norm, see for instance O.T. O'Meara in [5]. The Minkowski Bound of a number field K is the constant B given by the formula

$$B = (\frac{4}{\pi})^{r_2} \times \frac{n!}{n^n} \times \sqrt{D} \tag{37}$$

The quantitative form of O'Meara's theorem asserts that, if there exists $m \geq B$ with $s_1, \ldots, s_m \in \mathbf{A}_S, \quad s_k \neq s_{k'}$ for $k \neq k', \quad (s_k - s_{k'}) \in A_S^*$, group of units of $\mathbf{A}_S$, then the ring $\mathbf{A}_S$ is euclidean for the norm, see for instance H.W. Lenstra in [4]. The next proposition aims to enlarge the algorithm we have explained to the rings $\mathbf{A}_S$ of $\mathbf{K}$.

Proposition 7. *Let $C(\rho_j, a), \quad j = 1, \ldots, t$ be a set of cubes covering the fundamental domain F of the lattice τ_A. Let $M \in \mathbb{N}$. Let $\mathcal{S}$ be the set of valuations corresponding to all the primes ideals of $\mathbf{A}$ above a prime p of $\mathbb{N}$ verifying $1 \leq p \leq M$. Let $\mathbf{A}_S$ be the ring of $\mathbf{K}$ corresponding to the set of valuations $\mathcal{S}$. Then, for $\mathbf{A}_S$ to be euclidean, it is sufficient that, for all $j, \quad 1 \leq j \leq t$, there exists one value $k_j \in \mathbb{N}, \quad 1 \leq k_j \leq M$ such that the cube $C(k_j\rho, k_j a)$ is euclidean.*

Proof. Let $k_j \in \mathbb{N}$ verify the hypothesis. We deduce that, $\forall u \in C(0, k_j a)$ there exists $q \in \mathbf{A}$ such that $\mathcal{N}(k_j\rho_j + u - \tau(q)) < 1 \Rightarrow \forall u_1 \in C(0, a)$, there exists $q \in \mathbf{A}$ such that $\mathcal{N}(k_j(\rho_j + u_1) - \tau(q)) < 1$. But, if $1 \leq k_j \leq M$, it results from the definition of the ring $\mathbf{A}_S$, that $k_j \in (\mathbf{A}_S)^*$. Therefore, for all $c \in \mathbf{K}$, it is possible to find $\varepsilon \in (\mathbf{A}_S)^*$ and $q \in \mathbf{A} \subseteq \mathbf{A}_S$ verifying the relation $\mathcal{N}(\tau(c\varepsilon) - \tau(q)) < 1$, which is a sufficient condition, for $\mathbf{A}_S$ to be norm-euclidean. □

6.2. **Remark.** Note that this proposition is effectively more general than the sufficient condition that we considered for the ring of integers $\mathbf{A}$ to be euclidean : it is possible that, for j, ρ_j given, the algorithm fails to find the euclideanity of one cube $C(\rho_j, a)$, but succeeds in finding the euclideanity of the cube $C(k_j\rho_j, k_j a)$ for **one** value $k_j, 1 \leq k_j \leq M$. Then, it is possible that, for some M, the algorithm conclude that $\mathbf{A}_S$ is euclidean though it leaves $\mathbf{A}$ indeterminate, which is confirmed by the tests of the computer program.

6.3. **Example of results.** Let us consider the example of the complex cubic fields $\mathbf{K}$, $n = 3, r_1 = 1, r_2 = 1$. Among the fields with $D, 0 < |D| < 492$, the fields with $|D| = 199$, 283, 307, 327, 331, 335, 339, 351, 364, 367, 436, 439, 459, 491 are not euclidean, see for instance [3]. The computer program result shows that, for all these discriminants $D, 0 < |D| < 492$, then the fraction ring $A_{S(2)}$ is norm-euclidean, where the set of non archimedean valuations $\mathcal{S}$ corresponds to the set of all primes above the prime ideal $2\mathbb{Z}$ of $\mathbb{Z}$. The Minkowski bound, for this set of number fields is bounded by $M_B < 6,276$. Therefore, with the quantitative version of O'Meara Theorem, the ring $A_{S'(6)}$ is norm-euclidean, where the set of non archimedean valuations $\mathcal{S}'(6)$ corresponds to the set of all primes above the prime ideals $2\mathbb{Z}$, $3\mathbb{Z}$ and $5\mathbb{Z}$ of $\mathbb{Z}$, which, clearly, is less precise than the previous result.

6.4. **Inhomogeneous minimum of the norm form.** To study the inhomogeneous minimum of the norm form with the computer algorithm, we have only to replace in the program the condition $\mathcal{N}(\rho - \tau(q)) < 1$ by $\mathcal{N}(\rho - \tau(q)) < \mathbf{M}$, where $\mathbf{M} > 0$ is given. To do that, we have only to change one instruction of the C++ program!

6.5. **Example of results.** Let K be a number field of degree n, of signature (r_1, r_2) and of discriminant D. H. Davenport has shown in [2], that for all number fields K, we have the inequality

$$\mathcal{N}(\rho - \tau(q)) < \gamma D^{\frac{n}{2n-2r_2}} \tag{38}$$

where γ is a positive constant depending on n only.

Consider, as an example, the fields K with :

1. $n = 3, r_1 = 1, r_2 = 1, \quad 0 < |D| < 4000$
2. $n = 4, r_1 = 0, r_2 = 2, \quad 0 < |D| < 4000$
3. $n = 4, r_1 = 2, r_2 = 1, \quad 0 < |D| < 4000$
4. $n = 5, r_1 = 1, r_2 = 2, \quad 0 < |D| < 4000$
5. $n = 5, r_1 = 3, r_2 = 1, \quad 0 < |D| < 10000$

Some of them are left indeterminate for euclideanity in the section of computer results. We have verified that, for all of them we have the relation

$$\mathcal{N}(\rho - \tau(q)) < B, \tag{39}$$

where B is the Minkowski Bound of the field $\mathbf{K}$. For these fields, this result is better than the result of Davenport: in that case, our result is on $\sqrt{D}$ instead of $D^{\frac{n}{2n-2r_2}}$.

Perhaps, it would be possible, to formulate a generalization of the Minkowski conjecture for totally real fields ($\mathcal{N}(\rho - \tau(q)) < 2^{-n}\sqrt{D}$) : for all number fields K with $(r_1, r_2) \neq (0, 1)$, we should have

$$\mathcal{N}(\rho - \tau(q)) < B. \tag{40}$$

Acknowledgements It is our pleasure to express our gratitude to Prof. Jacques Martinet and Henri Cohen for helpful advice on this work and to Franz Lemmermeyer for many suggestions during all the period of conception and of testing of the C++ algorithm. The consistency of the results of Stefania Cavallar and Franz Lemmermeyer in [1] for cubic fields and of Franz Lemmermeyer for the quartic fields with our results was largely used for the validation of the algorithm and of the C++ program.

References

[1] S. Cavallar and F. Lemmermeyer, *The euclidean algorithm in cubic number fields*, draft (August 1996).
[2] H. Davenport, *Linear forms associated with an algebraic number field*, Quarterly J. Math., (2) 3, (1952), pp. 32–41.
[3] F. Lemmermeyer, *The euclidean algorithm in algebraic number fields*, Expo. Mat., no 13 (1995), pp. 385–416.
[4] H.W. Lenstra, *Euclidean number fields of large degree*, Invent. Math., n0 38, (1977), pp. 237–254.
[5] O.T. O'Meara, *On the finite generation of linear groups over Hasse domains*, J. Reine Angew. Math. n0 217 (1965), pp. 79–108.
[6] P. Samuel, *Théorie algébrique des nombres*, Hermann, (1967).

Roland Quême
13, avenue du château d'eau
31490 Brax
France
E-mail : 106104.1447@compuserve.com