Some Generalized Euclidean and 2-stage Euclidean number fields that are not norm-Euclidean

Jean-Paul Cerri

To cite this version:
Jean-Paul Cerri. Some Generalized Euclidean and 2-stage Euclidean number fields that are not norm-Euclidean. Mathematics of Computation, American Mathematical Society, 2011, 80 (276), pp.2289-2298. hal-00505142v2
SOME GENERALIZED EUCLIDEAN AND 2-STAGE EUCLIDEAN NUMBER FIELDS THAT ARE NOT NORM-EUCLIDEAN

JEAN-PAUL CERRI

Abstract. We give examples of Generalized Euclidean but not norm-Euclidean number fields of degree strictly greater than 2. In the same way we give examples of 2-stage Euclidean but not norm-Euclidean number fields of degree strictly greater than 2. In both cases, no such examples were known.

1. Introduction

In 1985, Johnson, Queen and Sevilla [9] introduced a generalization of the classical notion of Euclidean number field.

Definition 1.1. A number field $K$ is said to be Generalized Euclidean or simply G.E. if for every $(\alpha, \beta) \in \mathbb{Z}_K \times \mathbb{Z}_K \setminus \{0\}$ such that the ideal $(\alpha, \beta)$ is principal, there exists $\Upsilon \in \mathbb{Z}_K$ such that $|N_{K/Q}(\alpha - \Upsilon \beta)| < |N_{K/Q}(\beta)|$.

If $(\alpha, \beta)$ is principal, we thus have at our disposal the Euclidean algorithm to compute a gcd of $\alpha$ and $\beta$ because it is easy to see that $(\beta, \alpha - \Upsilon \beta)$ is principal again, and so on. Note that if $K$ is norm-Euclidean then $K$ is G.E. and that if $K$ has class number 1, then $K$ is G.E. if and only if $K$ is norm-Euclidean. If we want to illustrate the difference between “G.E.” and “norm-Euclidean”, the interesting case is when $K$ is not principal, G.E. but not norm-Euclidean. The following result was established by Johnson, Queen and Sevilla in [9].

Theorem 1.1. The quadratic number field $\mathbb{Q}(\sqrt{d})$ is G.E. but not norm-Euclidean for $d = 10$ and $d = 65$. The quadratic number field $\mathbb{Q}(\sqrt{d})$ is not G.E. for $d = 15, 26, 30, 35, 39, 51, 78, 87, 102, 115, 195$ and 230.

Furthermore, Johnson, Queen and Sevilla conjectured that $K = \mathbb{Q}(\sqrt{d})$ (with $d > 1$ squarefree) is G.E. if and only if $K$ is norm-Euclidean or $d = 10$ or 65.

Another variation on norm-Euclidean number fields has been introduced by Cooke [7].

Definition 1.2. Let $m$ be a rational integer $\geq 1$. The number field $K$ is $m$-stage Euclidean if and only if for every $\alpha \in \mathbb{Z}_K$ and every $\beta \in \mathbb{Z}_K \setminus \{0\}$ there exists a positive rational integer $k \leq m$ and $k$ pairs $(q_i, r_i)$ ($1 \leq i \leq k$) of elements of $\mathbb{Z}_K$.
such that
\[ \alpha = \beta q_1 + r_1, \]
\[ \beta = r_1 q_2 + r_2, \]
\[ \vdots \]
\[ r_{k-2} = r_{k-1} q_k + r_k, \]
and \(|N_{K/Q}(r_k)| < |N_{K/Q}(\beta)|\).

When it is well defined, let us put
\[ [q_1, q_2, \ldots, q_k] = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_k}}}, \]
where \(a_k\) and \(b_k\) are given by
\[ a_1 = q_1, \quad b_1 = 1, \]
\[ a_2 = a_1 q_2 + 1, \quad b_2 = q_2, \]
and recursively by
\[ a_k = a_{k-1} q_k + a_{k-2}, \quad b_k = q_k b_{k-1} + b_{k-2}. \]

Since
\[ \frac{\alpha}{\beta} = \frac{a_k}{b_k} + (-1)^{k+1} \frac{r_k}{b_k \beta}, \]
this definition is equivalent to the following.

**Definition 1.3.** The number field \(K\) is \(m\)-stage Euclidean if and only if for every \(\xi \in K\), there exists a positive rational integer \(k \leq m\), and \(k\) elements \(q_1, q_2, \ldots, q_k \in \mathbb{Z}_K\) such that
\[ |N_{K/Q}(\xi - [q_1, q_2, \ldots, q_k])| < \frac{1}{|N_{K/Q}(b_k)|}. \]

As in the previous case, norm-Euclidean implies \(m\)-stage Euclidean, but contrary to what happens with the G.E. condition, we have the following result [7].

**Theorem 1.2.** A number field \(K\) with unit rank \(r \geq 1\) is principal if and only if \(K\) is \(m\)-stage Euclidean for some \(m\).

As a consequence, if we want to study the difference between \(m\)-stage Euclidean and norm-Euclidean, we have to look at number fields with class number 1 and find some example where \(K\) is principal, \(m\)-stage Euclidean but not norm-Euclidean. The following result was established by Cooke [7].

**Theorem 1.3.** For \(d = 14, 22, 23, 31, 38, 43, 46, 53, 61, 69, 89, 93, 97, \mathbb{Q}(\sqrt{d})\) is 2-stage euclidean but not norm-Euclidean.

Furthermore, Cooke and Weinberger [8] proved that, under GRH, every principal number field \(K\) with unit rank \(r \geq 1\) is 4-stage Euclidean, and even 2-stage Euclidean if \(K\) has at least one real place.
For both notions (G.E. and m-stage Euclidean), no examples of number fields of degree strictly greater than 2 were known. Our main results are the following.

**Theorem 1.4.** None of the totally real number fields enumerated in Table 1 are principal. They all are G.E. except for the second cubic number field of discriminant 3969, defined by \( x^3 - 21x - 35 \), which is neither principal nor G.E.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( D_K )</th>
<th>( P(x) )</th>
<th>( h )</th>
<th>( M(K) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1957</td>
<td>( x^3 - x^2 - 9x + 10 )</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2597</td>
<td>( x^3 - x^2 - 9x + 8 )</td>
<td>3</td>
<td>5/2</td>
</tr>
<tr>
<td>3</td>
<td>2777</td>
<td>( x^3 - 3x^2 - 14x + 23 )</td>
<td>2</td>
<td>5/3</td>
</tr>
<tr>
<td>3</td>
<td>3969</td>
<td>( x^3 - 21x - 28 )</td>
<td>3</td>
<td>4/3</td>
</tr>
<tr>
<td>3</td>
<td>3969</td>
<td>( x^3 - 21x - 35 )</td>
<td>3</td>
<td>7/3</td>
</tr>
<tr>
<td>3</td>
<td>3981</td>
<td>( x^3 - x^2 - 11x + 12 )</td>
<td>2</td>
<td>3/2</td>
</tr>
<tr>
<td>3</td>
<td>4212</td>
<td>( x^3 - 12x - 10 )</td>
<td>3</td>
<td>7/2</td>
</tr>
<tr>
<td>3</td>
<td>4312</td>
<td>( x^3 - x^2 - 16x + 8 )</td>
<td>3</td>
<td>11/4</td>
</tr>
<tr>
<td>3</td>
<td>5684</td>
<td>( x^3 - 14x - 14 )</td>
<td>3</td>
<td>9/2</td>
</tr>
<tr>
<td>4</td>
<td>21025</td>
<td>( x^3 - 17x^2 + 36 )</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>32625</td>
<td>( x^3 - x^2 - 19x^2 + 4x + 76 )</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>46400</td>
<td>( x^3 - 22x^2 + 116 )</td>
<td>2</td>
<td>5/4</td>
</tr>
<tr>
<td>4</td>
<td>51200</td>
<td>( x^3 - 20x^2 + 50 )</td>
<td>2</td>
<td>7/2</td>
</tr>
</tbody>
</table>

**Table 1.** Here, \( n \) is the degree of the field \( K \), \( D_K \) its discriminant, \( P(x) \) its equation, \( h \) its class number and \( M(K) \) its Euclidean minimum.

**Theorem 1.5.** The totally real number fields of degree 3 and of discriminants < 15000 which are principal but not norm-Euclidean (82 cases) are 2-stage norm-Euclidean. The same is true for degree 4 and discriminants 18432, 34816, 35152 and for degree 5 and discriminant 390625. In all these cases, the number field is principal, not norm-Euclidean, but 2-stage norm-Euclidean.

Details on the number fields appearing in Theorem 1.5 are available from [6]. In Section 2, we recall other definitions and general results. In Section 3 and 4, we study the case of Generalized Euclidean number fields and the case of 2-stage Euclidean number fields, respectively.

### 2. The Algorithm, Generalities

Let \( K \) be a number field of degree \( n \). We have designed an algorithm which allows us to compute the Euclidean minimum of \( K \), in particular when \( K \) is totally real [5], but also in the general case [3]. According to theoretical results [4], this algorithm can also give the upper part of the Euclidean spectrum of \( K \) and this yields new examples of number fields with interesting properties.

From now on, we suppose that \( K \) is totally real and that \( n > 2 \). We denote by \( \mathbb{Z}_K \) the ring of its integers and by \( N_{K/Q} \) its absolute norm. The **Euclidean minimum**

\(^1\)In [2] and [10] the Euclidean minimum of this number field is falsely announced to be 1.
of an element \( \xi \in K \) is
\[
m_K(\xi) = \inf_{\mathcal{U} \in \mathbb{Z}_K} |N_K/\mathbb{Q}(\xi - \mathcal{U})|
\]
and the Euclidean minimum of \( K \) is
\[
M(K) = \sup_{\xi \in K} m_K(\xi).
\]
The set of values taken by \( m_K \) is called the Euclidean spectrum of \( K \). We know the following important result [4].

**Theorem 2.1.** The Euclidean spectrum of \( K \) is the union of \( \{0\} \) and of a strictly decreasing sequence of rationals \((r_i)_{i \geq 0}\) with limit 0. For each \( k \), the set of \( \xi \in K \) such that \( m_K(\xi) = r_i \) is finite modulo \( \mathbb{Z}_K \).

In fact, we have a stronger result, which can be formulated in terms of the inhomogeneous spectrum but we shall not need this in what follows.

**Corollary 2.2.** The set of \( \xi \in K \) such that \( m_K(\xi) \geq 1 \) is finite modulo \( \mathbb{Z}_K \).

Recall now that we have at our disposal an algorithm which can give us all the \( \xi \in K \) with this property. Without going into details – these can be found in [5] – let us give nevertheless the theorem which justifies the algorithm and the main ideas that are behind it. Let us choose a constant \( k > 0 \) and a let us embed \( K \) into \( K \otimes \mathbb{Q} \mathbb{R} \), which we can identify with \( \mathbb{R}^n \), in which \( \mathbb{Z}_K \) is a lattice. Under this identification an element \( \xi \) of \( K \) is viewed as \((\sigma_i(\xi))_{1 \leq i \leq n})\), where the \( \sigma_i \) are the embeddings of \( K \) into \( \mathbb{R} \). The map \( m_K \) extends to a map \( m_\mathcal{F} \) from \( \mathbb{R}^n \) to \( \mathbb{R}^+ \) in a natural way:
\[
m_\mathcal{F}(x) = \inf_{\mathcal{U} \in \mathbb{Z}_K} \left| \prod_{i=1}^n (x_i - \sigma_i(\mathcal{U})) \right|.
\]
Moreover, the product of two elements of \( K \) is extended to the product coordinate by coordinate in \( \mathbb{R}^n \). This new product of two elements \( x, y \in \mathbb{R}^n \) will be denoted by \( x \cdot y \). Let finally \( \varepsilon \) be a non-torsion unit of \( \mathbb{Z}_K \).

The main idea is to find in a fundamental domain \( \mathcal{F} \) associated to \( \mathbb{Z}_K \) in \( \mathbb{R}^n \), \( s \) distinct bounded sets \( \mathcal{T}_i \) \((1 \leq i \leq s)\) with the property that for each such \( \mathcal{T}_i \) there exists an \( X_i \in \mathbb{Z}_K \) and \( s_i \) integers \( n_i, 1, \ldots, n_i, s_i \) \((s_i > 0)\) such that
\[
(\varepsilon \cdot \mathcal{T}_i - X_i) \mathcal{H} \subseteq \bigcup_{1 \leq i \leq s_i} \mathcal{T}_{n_i, i} \quad (i = 1, \ldots, s),
\]
where
\[
\mathcal{H} = \{ x \in \mathbb{R}^n \text{ such that } m_\mathcal{F}(x) \leq k \}.
\]
We consider the \( \mathcal{T}_i \) as the vertices of a directed graph \( G \) and represent (1) by \( s_i \) directed edges whose tail is \( \mathcal{T}_i \) and whose respective heads are the \( \mathcal{T}_{n_i, i} \) \((1 \leq l \leq s_i)\). To describe such an edge of \( G \) we shall use the notation \( \mathcal{T}_i \to \mathcal{T}_{n_i, i}(X_i) \). The set \( \mathcal{C} \) of simple cycles of \( G \) is nonempty and finite. Each element \( c \) of \( \mathcal{C} \) of length \( j \) is in the form of the circular path, \( \mathcal{T}_0 \to \mathcal{T}_1(X_0) \to \mathcal{T}_2(X_1) \to \cdots \to \mathcal{T}_{j-1}(X_{j-2}) \to \mathcal{T}_j(X_{j-1}) \), for some subset \( \{\mathcal{T}_1, \ldots, \mathcal{T}_{j-1}\} \subseteq \{\mathcal{T}_1, \ldots, \mathcal{T}_s\} \), where \( X_j \) denotes the element \( X \in \mathbb{Z}_K \) associated to \( \mathcal{T}_i \). This defines, in a unique way, \( j \) elements of \( K \), \( \xi_0, \ldots, \xi_{j-1} \) by the formulae:
\[
\xi_r = \frac{\varepsilon^{j-r}X_r + \varepsilon^{j-2}X_{r+1} + \cdots + \varepsilon^{j-1}X_{j-1} + X_j}{\varepsilon^{j-1}},
\]
the indices being read modulo \( j \). In this context, we say that \( \xi_0, \ldots, \xi_{j-1} \) are associated to the cycle \( c \).

We denote by \( E \) the finite set of all elements of \( K \) associated to the elements of \( C \). The \( \xi_i \) associated to a cycle \( c \) are in the same orbit modulo \( Z \) under the action of \( Z_K^* \) (in fact \( \xi_{r+1} = \varepsilon \cdot \xi_r - X'_r \)) and satisfy

\[
m_{\overline{K}}(\xi_0) = \ldots = m_{\overline{K}}(\xi_{j-1}) =: m(c),
\]
which is a rational number. Finally, define

\[
m(G) = \max_{c \in C} m(c) = \max_{\xi \in E} m_{\overline{K}}(\xi).
\]

Let us say that \( G \) is convenient if every infinite path of \( G \) is ultimately periodic. The essential result is the following.

**Theorem 2.3.** Assume that \( G \) is convenient and that there exists \( T \in \{T_1, \ldots, T_s\} \) and \( x \) such that \( m_{T}(x) > k \). Then

i) \( m_{\overline{K}}(x) \leq m(G) \).

ii) If \( x \in K \), there exists \( \xi \in E \) such that \( x \equiv \xi \mod Z \).

In this situation we know all the potential \( \xi \in K \) such that \( m_K(\xi) > k \), and since computing \( m_K(\xi) \) is possible (again see [5] for more details), we know in fact all the \( \xi \in K \) such that \( m_K(\xi) > k \). To identify the elements \( \xi \in K \) such that \( m_K(\xi) \geq 1 \), it is sufficient to run the algorithm with \( k = 0.999 \), for instance.

3. **Generalized Euclidean number fields**

3.1. **Generalities.** From the definition of G.E. number fields and the definition of the map \( m_K \), we have the following result.

**Proposition 3.1.** The field \( K \) is G.E. if and only if for every \( (\alpha, \beta) \in \mathbb{Z}_K \times \mathbb{Z}_K \setminus \{0\} \) such that \( m_K(\alpha/\beta) \geq 1 \), the ideal \( (\alpha, \beta) \) is not principal.

**Remark 1.** Suppose that we have at our disposal the finite set \( S \) of all \( \xi \in K \) (modulo \( Z_K \)) such that \( m_K(\xi) \geq 1 \), and that for each such \( \xi \) we have a representative \( u/v \) where \( (u, v) \in \mathbb{Z}_K \times \mathbb{Z}_K \setminus \{0\} \). Let \( (\alpha, \beta) \in \mathbb{Z}_K \times \mathbb{Z}_K \setminus \{0\} \) such that \( m_K(\alpha/\beta) \geq 1 \). Then there exists \( \xi \equiv u/v \) in \( S \) such that \( \alpha/\beta = u/v + \gamma \) with \( \gamma \in Z_K \). Since

\[
(\alpha, \beta) = (\beta u/v + \gamma \beta, \beta) = (\beta u/v, \beta) = \beta(u/v, u/v),
\]

it is sufficient, for proving that \( K \) is G.E., to check that for every \( \xi \equiv u/v \in S \), \( (u, v) \) is not principal.

3.2. **A first example.** The purpose of this subsection is to study in detail a particular case. Other results, obtained in another way, will be given in the next subsection. Let \( K \) be the normal quartic field generated by any one of the roots of

\[
P(X) = X^4 - 20X^2 + 50.
\]

The field \( K \) is totally real, its discriminant is 51200, its class number is 2, and a \( \mathbb{Z} \)-basis of \( Z_K \) is \((e_1, e_2, e_3, e_4)\) with

\[
e_1 = 1, \quad e_2 = \sqrt{2}, \quad e_3 = \sqrt{10 + 5\sqrt{2}}, \quad e_4 = \sqrt{10 - 5\sqrt{2}}.
\]

Our algorithm shows that

\[
M(K) = \frac{7}{2},
\]
and that there is a unique $\xi \in K$ (modulo $\mathbb{Z}_K$) such that $m_K(\xi) \geq 1$. More precisely

$$\xi \equiv \frac{1}{2}(e_3 + e_4).$$

According to Remark 1, if we want to establish that $K$ is G.E., we have just to prove that the ideal $(2, e_3 + e_4)$ is not principal.

**Theorem 3.2.** The field $K$ is not norm-Euclidean but it is G.E.

**Proof.** First of all, we note that $e_3 + e_4 = e_2 \cdot e_3$ so that we are reduced to proving that the ideal $(e_2, e_3)$ is not principal. Suppose on the contrary that it is principal so that we have

$$e_2 \mathbb{Z}_K + e_3 \mathbb{Z}_K = \nu \mathbb{Z}_K,$$

with $\nu \in \mathbb{Z}_K$. Since $N_{K/Q}(e_2) = 4$ and $N_{K/Q}(e_3) = 50$, we have

$$N_{K/Q}(\nu) \mid 2 = \gcd(4, 50),$$

so that we have two possibilities: either $\nu \in \mathbb{Z}_K^*$ or $N_{K/Q}(\nu) = \pm 2$.

**First case :** $\nu$ is a unit and we have in fact $e_2 \mathbb{Z}_K + e_3 \mathbb{Z}_K = \mathbb{Z}_K$.

In this case, there exist $u, v \in \mathbb{Z}_K$ such that

$$1 = e_2 \cdot u + e_3 \cdot v. \quad (2)$$

Let us write

$$\begin{cases} u = a + be_2 + ce_3 + de_4 \\ v = a' + b'e_2 + c'e_3 + d'e_4, \end{cases} \quad (3)$$

where $a, b, c, d, a', b', c', d' \in \mathbb{Z}$.

Since $e_2 \cdot e_3 = e_3 + e_4$, $e_2 \cdot e_4 = e_3 - e_4$ and $e_3 \cdot e_4 = 5e_2$, if we substitute (3) into (2) we obtain, by identification of the coefficients in our $\mathbb{Z}$-basis, that $2b + 10c' = 1$, which is clearly impossible.

**Second case :** $\nu$ has norm $\pm 2$.

Let us prove that this is impossible. If

$$\nu = a + be_2 + ce_3 + de_4$$

where $a, b, c, d \in \mathbb{Z}$, an easy computation leads to

$$\pm 2 = N_{K/Q}(\nu)$$

$$= a^4 + 4b^4 + 50c^4 + 50d^4 - 4a^2b^2 - 20a^2c^2 - 20a^2d^2 - 40b^2c^2$$

$$- 400b^2d^2 + 100c^2d^2 + 40abc^2 - 40abd^2 + 200cd^3 - 200dc^3 + 80abcd.$$

This implies that

$$\pm 2 \equiv (a^2 - 2b^2)^2 \quad (\text{mod} 5),$$

which is impossible as neither of $\pm 2$ are quadratic residues (mod 5). \qed
3.3. Dedekind-Hasse criterion. In this subsection, we study the link between G.E. and a Euclidean-type map that we shall deduce from the Dedekind-Hasse criterion. This will lead us to define an easy test which allows to find new examples, without requiring detailed calculations as above. First of all, recall the Dedekind-Hasse criterion (see for instance [11]).

Theorem 3.3. A number field \( K \) has class number 1 if and only if for every \( \alpha, \beta \in \mathbb{Z}_K \setminus \{0\} \) such that \( \beta \nmid \alpha \), there exist \( \gamma, \delta \in \mathbb{Z}_K \) such that

\[
0 < |N_{K/Q}(\alpha\gamma - \beta\delta)| < |N_{K/Q}(\beta)|.
\]

This leads to the following natural definition.

Definition 3.1. For every \( \xi \in K \setminus \mathbb{Z}_K \) we shall denote by \( h_K(\xi) \) the real number defined by

\[
h_K(\xi) = \inf\{m_K(\Upsilon\xi); \Upsilon \in \mathbb{Z}_K \text{ and } \Upsilon\xi \not\in \mathbb{Z}_K\}.
\]

This map has the following elementary properties, which we give here without proof.

Proposition 3.4. For every \( \xi \in K \setminus \mathbb{Z}_K \) we have

1. \( 0 < h_K(\xi) \leq m_K(\xi) \);
2. For every \( \alpha \in \mathbb{Z}_K \), \( h_K(\xi + \alpha) = h_K(\xi) \);
3. For every \( \varepsilon \in \mathbb{Z}_K^* \), \( h_K(\varepsilon\xi) = h_K(\xi) \).

We can now reformulate Dedekind-Hasse criterion as follows.

Theorem 3.5. A number field \( K \) has class number 1 if and only if for every \( \xi \in K \setminus \mathbb{Z}_K \) we have \( h_K(\xi) < 1 \).

Proof. The norm being multiplicative, (4) can be reformulated: for every \( \xi \in K \setminus \mathbb{Z}_K \) there exist \( \gamma, \delta \in \mathbb{Z}_K \) such that

\[
0 < |N_{K/Q}(\gamma\xi - \delta)| < 1,
\]

which leads to \( m_K(\gamma\xi) < 1 \). Since (5) cannot be true if \( \gamma\xi \in \mathbb{Z}_K \), we have \( h_K(\xi) < 1 \). Conversely, since \( |N_{K/Q}(\gamma\xi - \delta)| = 0 \) implies \( \gamma\xi \in \mathbb{Z}_K \) which is excluded in the definition of \( h_K \), we see that if \( h_K(\xi) < 1 \) then (5) is true. \( \Box \)

Now consider a number field \( K \) and put

\[
S = \{\xi \in K; m_K(\xi) \geq 1\}.
\]

Suppose that \( K \) is not norm-euclidean so that \( S \neq \emptyset \). We have the following result.

Theorem 3.6. One of the following three possibilities holds:

1. For every \( \xi \in S \), \( h_K(\xi) < 1 \). Then \( K \) has class number 1 and is not G.E.
2. For every \( \xi \in S \), \( h_K(\xi) \geq 1 \). Then \( K \) is G.E. (and not principal).
3. There exist \( \xi, \mu \in S \) such that \( h_K(\xi) < 1 \) and \( h_K(\mu) \geq 1 \). Then \( K \) is not principal. If in addition, there exists \( \xi = \alpha/\beta \in S \) (with \( \alpha, \beta \in \mathbb{Z}_K \)) with \( h_K(\xi) < 1 \) and such that \( (\alpha, \beta) \) is principal, then \( K \) is not G.E. Otherwise it is G.E.

Proof. Clearly we have the three cases.

Case 1. The result is a consequence of Theorem 3.5 and of the fact that when the field is principal norm-Euclidean and G.E. are synonymous.
Case 2. Theorem 3.5 indicates that $K$ is not principal. By Proposition 3.1 it is sufficient to prove that for every $\xi = \alpha/\beta \in S$ where $\alpha, \beta \in \mathbb{Z}_K$, the ideal $(\alpha, \beta)$ is not principal. Otherwise, we have $(\alpha, \beta) = \nu \mathbb{Z}_K$ with $\nu \in \mathbb{Z}_K$. By hypothesis $h_K(\xi) \geq 1$ so that for every $X, Y \in \mathbb{Z}_K$ with $X\xi \notin \mathbb{Z}_K$ we have

$$|N_{K/Q}(X\alpha - Y\beta)| \geq |N_{K/Q}(\beta)|.$$

Now $\nu$ can be written $\nu = X\alpha - Y\beta$ with $X, Y \in \mathbb{Z}_K$ and $X\xi \notin \mathbb{Z}_K$. Otherwise $\nu \in \beta \mathbb{Z}_K$ so that $\beta \mid \nu$. But this implies that $\nu$ and $\beta$ are associates and we have $(\alpha, \beta) = \beta \mathbb{Z}_K$ which implies $\beta \mid \alpha$ and $\xi \in \mathbb{Z}_K$, which is impossible. We deduce from this that $|N_{K/Q}(\nu)| \geq |N_{K/Q}(\beta)|$. Since $N_{K/Q}(\nu) \mid N_{K/Q}(\beta)$ we have $|N_{K/Q}(\nu)| = |N_{K/Q}(\beta)|$, and since $\nu \mid \beta$, $\nu$ and $\beta$ are associates, which is impossible by the previous argument.

Case 3. Theorem 3.5 indicates that $K$ is not principal. The second assertion is a consequence of Proposition 3.1. Indeed, as previously, if $h_K(\xi) \geq 1$ and $\xi = \alpha/\beta$ then $(\alpha, \beta)$ is not principal and this case is not an obstruction for $K$ to be G.E. Finally, the only possibilities for contradicting G.E. come from the $\xi = \alpha/\beta \in S$ such that $h_K(\xi) < 1$ and $(\alpha, \beta)$ is principal.

Corollary 3.7. Suppose that $K$ is not norm-Euclidean and that, with the above notation, $S$ modulo $\mathbb{Z}_K$ is composed of a single orbit under the (multiplicative) action of $\mathbb{Z}_K^*$ modulo $\mathbb{Z}_K$, i.e. that if $\xi, \mu \in S$ there exists an $\varepsilon \in \mathbb{Z}_K^*$ and an $\alpha \in \mathbb{Z}_K$ such that $\mu = \varepsilon \xi + \alpha$. Then either $K$ is principal and not G.E. or $K$ is not principal but is G.E.

Proof. If $K$ is principal, we are in case 1. Otherwise, since all the elements of $S$, which are in the same orbit, have the same image by $h_K$ (Proposition 3.4), we cannot be in case 3 of Theorem 3.6. Finally, we are in case 2 and $K$ is G.E. □

Remark 2. To simplify notation and vocabulary, we shall often, by abuse of language, speak indifferently of $\xi \in K$ or $\xi \in K \mod \mathbb{Z}_K$. For instance we shall speak of orbits in $S$ under the action of $\mathbb{Z}_K^*$; in this context $S$ and these orbits should be understood modulo $\mathbb{Z}_K$.

Corollary 3.8. The totally real number fields of degree 3 and discriminants 1957, 2777, 3981 are G.E. The totally real number fields of degree 4 and discriminants 46400 and 51200 are G.E.

Proof. In fact, in all these cases, our algorithm establish that we are under the previous hypotheses. For discriminant 1957, we have $M(K) = 2$ and one orbit with one element in $S$. For discriminant 2777, we have $M(K) = 5/3$ and one orbit with 2 elements in $S$. For discriminant 3981, we have $M(K) = 3/2$ and one orbit with one element in $S$. For discriminant 46400, we have $M(K) = 5/4$ and one orbit with 3 elements in $S$. For discriminant 51200, we have $M(K) = 7/2$ and one orbit with one element in $S$. □

And now, if there are several orbits in $S$, and we want to use Theorem 3.6, we have to see whether, for one element $\xi$ by orbit, and for every orbit, we have $h_K(\xi) \geq 1$, in which case necessarily $K$ is G.E. The problem is now: how can we compute $h_K(\xi)$? Our algorithm gives us every such $\xi$ by its coordinates in a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. These coordinates are of the form $(a_1/d, a_2/d, \ldots, a_n/d)$ where $a_i \in \mathbb{Z}$ for every $i$ and $d \in \mathbb{Z}_{>0}$. Furthermore we can compute $m_K(\mu)$ for every $\mu \in K$. Hence,
it is easy to see that, to compute \( h_K(\xi) \), it is sufficient to compute \( m_K(\Upsilon\xi) \) for every \( \Upsilon \) with coordinates in \( \{0,1,\ldots,d-1\} \) for our basis, such that \( \Upsilon\xi \notin \mathbb{Z}_K \). This is easy to check. By definition, the value of \( h_K(\xi) \) will be the minimum of these \( m_K(\Upsilon\xi) \). Of course if for every \( \xi \) and every such \( \Upsilon \) we have \( \Upsilon\xi \in S \mod \mathbb{Z}_K \), then \( K \) is G.E. Using this last approach we have established the following result.

**Theorem 3.9.** The following totally real number fields of degree \( n \) are G.E. but not norm-Euclidean:

- when \( n = 3 \), the fields with discriminants 2597, 4212, 4312, 5684;
- when \( n = 4 \), the fields with discriminants 21025, 32625.

**Proof.** We just give a typical example. For \( n = 3 \) and discriminant 2597, we have two orbits in \( S \), the first one \( O_1 \) with 2 elements \( \{\pm(e_1 + 2e_2 + 2e_3)/3 \} \) with \( (e_1) \) is the \( \mathbb{Z} \)-basis of \( \mathbb{Z}_K \) returned by PARI [1] and the second one \( O_2 \) with 1 element \( (e_1 + e_2 + e_3)/2 \) modulo \( \mathbb{Z}_K \). Then we can easily check that \( \mathbb{Z}_K \cdot O_1 = O_1 \cup \{0\} \) and that \( \mathbb{Z}_K \cdot O_2 = O_2 \cup \{0\} \). The same thing happens in other cases with sometimes more complicated equalities but always with \( \mathbb{Z}_K \cdot O \subseteq S \cup \{0\} \). \( \square \)

**Remark 3.** If we want to treat all the non principal number fields of degree 3 and discriminant \(< 6000 \), it remains to study the two number fields with discriminant 3969. In these cases, our previous method does not work because we have some \( \xi = \alpha/\beta \in S \) such that \( h_K(\xi) < 1 \). The first one, \( K_1 \), is defined by \( x^3 - 21x - 28 \).

For this field, \( S \) is composed of five orbits \( O_i, 1 \leq i \leq 5 \). For 4 of them, say for \( 1 \leq i \leq 4 \), we have \( \mathbb{Z}_K \cdot O_i \subseteq S \cup \{0\} \) but for the last one \( O_5 \) this is not true. Take an element \( \alpha/\beta \) of \( O_5 \); here we can take \( \alpha = 3e_1 + 2e_2 + 2e_3 \) and \( \beta = 6 \) where \( (e_1, e_2, e_3) \) is the \( \mathbb{Z} \)-basis returned by PARI [1]. We can then prove directly as in Section 3.2 that the ideal \( (\alpha, \beta) \) is not principal. We conclude that \( K_1 \) is G.E.

For the second field, \( K_2 \), defined by \( x^3 - 21x - 35 \) the situation is different. Here \( S \) is composed of seven orbits \( O_i, 1 \leq i \leq 7 \) and four of them, say \( O_i \), with \( 1 \leq i \leq 4 \), are such that \( \mathbb{Z}_K \cdot O_i \subseteq S \cup \{0\} \). Now if we look at the three others, we find that two of them contain an \( \alpha/\beta \) for which \( (\alpha, \beta) \) is principal. For completeness these \( (\alpha, \beta) \) are \( \{7e_1 + 12e_2 + 4e_3, 21\} \) and \( \{7e_1 + 5e_2 + 11e_3, 21\} \) with the usual notation. Consequently \( K_2 \) is not G.E. All the computations, which are long and complicated - in particular for \( K_2 \) - have been done by hand and checked using PARI [1]. We do not give them here for lack of space and because they are not especially enlightening.

Finally, we put all these results together to give us Theorem 1.4.

4. The 2-stage Euclidean number fields

Let us begin with an example. Let \( K \) be the totally real cubic number field with discriminant 3988. Using our algorithm we see that the upper part of the Euclidean spectrum of \( K \) has five elements, more precisely

\[
\text{sp}(K) \cap [1, \infty) = \{19/8, 11/8, 5/4, 19/16, 133/128\}.
\]

The set \( S \) is composed of five orbits, respectively the orbits of \( ae_1 + be_2 + ce_3 \) with \( (a, b, c) = (0, 1/2, 1/2), (1/2, 1/2, 0), (1/2, 1/2, 1/2), (0, 3/4, 1/2) \) and \( (0, 3/8, 1/2) \), where \( (e_1, e_2, e_3) \) is the \( \mathbb{Z} \)-basis of \( \mathbb{Z}_K \) returned by PARI [1]. These orbits have
respectively 1, 1, 1, 2 and 4 elements. For one element $\xi$ by orbit, we try to find $q_1, q_2 \in \mathbb{Z}_K$ such that
\begin{equation}
\left| N_{K/Q}(\xi - q_1 - \frac{1}{q_2}) \right| < \frac{1}{|N_{K/Q}(q_2)|},
\end{equation}
by testing “small” $q_1 \in \mathbb{Z}_K$ and “small” $q_2 \in \mathbb{Z}_K \setminus \{0\}$. In each case this is possible, so that for every $\xi \in S$, (6) is true. Finally this implies that $K$ is 2-stage norm-Euclidean. Using exactly the same approach we have established the results of Theorem 1.5.

Remark 4. Obviously these fields, which are principal and not norm-Euclidean, are not G.E.

References