Examples of norm-Euclidean ideal classes

Pierre Lezowski

January 24, 2012

Keywords: Euclidean ideal classes; Euclidean minimum; pure cubic fields.

Mathematics Subject Classification 2010: 11A05, 11R04, 11R16, 13F07.

Abstract

In [11], Lenstra defined the notion of Euclidean ideal class. Using a slight modification of an algorithm described in [12], we give new examples of number fields with norm-Euclidean ideal classes. Extending the results of Cioffari ([5]), we also establish the complete list of pure cubic number fields which admit a norm-Euclidean ideal class.

1 Introduction

The classical notion of norm-Euclidean number field has been deeply studied, in particular from the second half of the 19th century. Let us recall that a number field K, whose ring of integers is denoted by $\mathbf{Z}_K$ and norm by $\mathbf{N}_{K/\mathbf{Q}}$ is said to be norm-Euclidean if and only if

$$\forall (a,b) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\},\ \exists (q,r) \in \mathbf{Z}_K^2,\ a = bq + r \text{ and } \left|\mathbf{N}_{K/\mathbf{Q}}(r)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|,$$

or equivalently,

$$\forall x \in K,\ \exists u \in \mathbf{Z}_K,\ \left|\mathbf{N}_{K/\mathbf{Q}}(x-u)\right| < 1. \tag{1}$$

In the 1970s, Hendrik W. Lenstra generalized this notion while studying ideals $0 \subsetneq I \subseteq \mathbf{Z}_K$ verifying

$$\forall (a,b) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\},\ \exists (q,r) \in I \times \mathbf{Z}_K,\ a = bq + r \text{ and } \left|\mathbf{N}_{K/\mathbf{Q}}(r)\right| < \mathbf{N}I \cdot \left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|,$$

or equivalently,

$$\forall x \in K,\ \exists u \in I,\ \left|\mathbf{N}_{K/\mathbf{Q}}(x-u)\right| < \mathbf{N}I, \tag{2}$$

where $\mathbf{N}$ is the norm of ideals:

$$\mathbf{N}I = \left|\frac{\mathbf{Z}_K}{I}\right|,$$

Obviously, if K is principal, condition (2) holds if and only if for every integral ideal $I \neq \{0\}$, condition (1) holds. However, there exist some non-principal number fields K admitting integral ideals I such that (1) holds. Nevertheless, such examples are quite scarce in the literature, and our main purpose will be to present new ones.

IMB, Université Bordeaux 1
351 Cours de la Libération 33405 Talence France,
e-mail: pierre.lezowski@math.u-bordeaux1.fr

First, we will recall the definitions and main properties of norm-Euclidean ideal classes. Then, by analogy with the principal case, we will introduce a notion of Euclidean minimum, whose properties will allow us to write an algorithm (Algorithm 3.7) to prove the existence of a norm-Euclidean ideal class. Afterwards, we will list present examples of imaginary cubic fields with a norm-Euclidean ideal class and study the family of pure cubic number fields to obtain the following result.

Theorem 4.1. *A pure cubic field $K = \mathbf{Q}(\sqrt[3]{n})$ admits a norm-Euclidean class if and only if $n \in \{2, 3, 10\}$. In particular, there exists no pure cubic number field with a non-principal norm-Euclidean ideal class.*

Then, we will deal with examples in other signatures and using Algorithm 3.7, we will obtain the following examples.

Theorem 5.1. *We can list quintic and sextic number fields admitting a non-principal norm-Euclidean class. Besides, there exists a (quartic) number field whose class number is equal to 4 and which admits a norm-Euclidean ideal class.*

On the other hand, we will show that the number field presented by Graves in [9] admits no norm-Euclidean ideal class.

Theorem 5.3. *$K = \mathbf{Q}\left(\sqrt{2}, \sqrt{35}\right)$ admits an ideal class*[a] *but no norm-Euclidean ideal class.*

2 Definitions

We consider an algebraic number field K, we denote by $\mathbf{Z}_K$ its ring of integers, r_1 its number of real places, $2r_2$ its number of imaginary places, $n = r_1 + 2r_2$ its degree (over $\mathbf{Q}$), $r = r_1 + r_2 - 1$ the rank of the units $\mathbf{Z}_K^\times$ of $\mathbf{Z}_K$ and $\mathbf{N}_{K/\mathbf{Q}}$ the usual norm. We denote by $\mathbf{N}$ the norm of ideals, extended by multiplicativity to the fractional ideals. Given an ideal $I \subseteq \mathbf{Z}_K$, we denote by $[I]$ its class in the class group. We write h_K the class number of K.

2.1 Basic presentation

Definition 2.1. *Let I be a fractional ideal of $\mathbf{Z}_K$. We say that I is a* norm-Euclidean ideal *if for any $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, there exists $\gamma \in I$ such that*

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \beta\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right| \cdot \mathbf{N}I.$$

Remark 2.2.

- *Lenstra introduced this notion in a more general setting ([11]), but this generality will be useless for us.*
- *With this definition, $\mathbf{Z}_K$ is norm-Euclidean if and only if it is norm-Euclidean as an ideal.*
- *Thanks to the multiplicativity of the norm, I is norm-Euclidean if and only if any ideal of the class $[I]$ is norm-Euclidean. Consequently, we rather speak of* norm-Euclidean ideal classes. *So, if K admits a norm-Euclidean ideal, we also say that K admits a norm-Euclidean ideal class.*
- *Using again the multiplicativity of the norm, we see that I is a norm-Euclidean ideal if and only if for any $x \in K$, there exists some $z \in I$ such that $\left|\mathbf{N}_{K/\mathbf{Q}}(x - z)\right| < \mathbf{N}I$.*

[a] This notion will be defined in section 5.3.

As the notion of norm-Euclidean ideal depends only on the ideal class, it is particularly interesting in the case where K is not principal.

Definition 2.3. *We say that an ideal* $\{0\} \subsetneq I \subsetneq \mathbf{Z}_K$ *is of* minimal norm *if for any ideal* J *such that* $\{0\} \subsetneq J \subsetneq \mathbf{Z}_K$, $\mathbf{N}I \leqslant \mathbf{N}J$.

An ideal of minimal norm always exists, we denote its norm by $\Lambda(K)$. The results of the following proposition were proved by Lenstra ([11]).

Proposition 2.4. 1. *If* K *admits an norm-Euclidean ideal* I*, then for every integral ideal* J *of* $\mathbf{Z}_K$*, there exists an integer* $0 \leqslant n < \mathbf{N}J$ *such that* $[J] = [I]^n$*. In particular, the class group of* K *is cyclic and generated by* $[I]$.

2. K *admits at most one norm-Euclidean ideal class. If* K *admits a norm-Euclidean ideal class* $\mathcal{C}$ *and* I *is an integral ideal of minimal norm, then* $\mathcal{C} = [I]$.

Note that if K admits a norm-Euclidean ideal class, it is the class of *any* ideal of minimal norm. By contraposition, if two ideals of minimal norm are not in the same class, then K has no norm-Euclidean class.

Example 2.5. *Take* $K = \mathbf{Q}\left(\sqrt{229}\right)$*, we have* $\mathrm{h}_K = 3$ *and* $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}-1}{2}$*. Then* $\Lambda(K) = 3$*, we have the two following ideals of norm* 3*:*

$$I_1 = 3\mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}-1}{2} \qquad \textit{and} \qquad I_2 = 3\mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}+1}{2}.$$

These ideals are not principal, $I_1 + I_2 = \mathbf{Z}_K$*, so* $I_1 I_2 = I_1 \cap I_2 = 3\mathbf{Z}_K$*, therefore* $[I_1] \neq [I_2]$*. Consequently,* K *has no norm-Euclidean ideal class.*

Example 2.6. *We can consider the other example* $K = \mathbf{Q}(x)$ *where* $x^4 - x^3 - 32x^2 + 23x + 229 = 0$*. Then* $\mathrm{h}_K = 3$*,* $\mathrm{disc}_K = 97025$ *and* $\Lambda(K) = 4$*. Besides,* $\mathbf{Z}_K$ *admits the following two ideals of norm* 4*:*

$$\begin{aligned} I_1 =& 2\mathbf{Z} + \mathbf{Z}\frac{x^3+2x^2-18x-39}{4} + \mathbf{Z}(x-1) + \mathbf{Z}\frac{x^3+6x^2-18x-99}{4} \\ \textit{and } I_2 =& 2\mathbf{Z} + \mathbf{Z}\frac{x^3+2x^2-18x-39}{4} + \mathbf{Z}\frac{-x^3-2x^2+26x+39}{8} \\ &+ \mathbf{Z}\frac{3x^3+14x^2-54x-237}{8}. \end{aligned}$$

We can prove that $I_1 I_2 = 2\mathbf{Z}_K$*, whereas* I_1 *and* I_2 *are not principal, therefore,* $[I_1] \neq [I_2]$*. Consequently,* K *cannot admit a norm-Euclidean ideal class.*

From now on, we will denote by I an ideal of minimal norm.

2.2 Euclidean minimum

As in the classical case, given an ideal $0 \subsetneq J \subseteq \mathbf{Z}_K$, we define a *local Euclidean minimum* by

$$m_{K,J}(x) := \inf_{z \in J} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right|}{\mathbf{N}J}.$$

We immediately notice that this minimum is reached, that is to say that there exists $z_0 \in J$ such that $m_{K,J}(x) = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z_0)\right|}{\mathbf{N}J}$. Therefore, K admits a norm-Euclidean ideal J if and only if for any $x \in K$,

$$m_{K,J}(x) < 1.$$

This leads to the following natural definition.

Definition 2.7. *We call* Euclidean minimum *with respect to J the nonnegative real number*

$$M(K,J) := \sup_{x\in K} m_{K,J}(x).$$

Let $k \in K^{\times}$, for any $x \in K$, $m_{K,J}(k^{-1}x) = m_{K,kJ}(x)$. As a result, $M(K,J)$ only depends on the class $[J]$, and we can write $M(K,[J]) = M(K,J)$.

Taking into account 2.4, 2 we will be particularly interested in $M(K,[I])$, for any integral ideal I of minimal norm, given the following observation. If $M\left(K,[I]\right) < 1$, then K admits the norm-Euclidean ideal class $[I]$, if $M\left(K,[I]\right) > 1$, then K admits no norm-Euclidean ideal class.

As we choose *any* ideal I of minimal norm, we may wonder about the dependence of $M\left(K,[I]\right)$ on this choice.

Proposition 2.8. *Let I be an ideal of minimal norm. If $M\left(K,[I]\right) < 1$, then K admits a norm-Euclidean ideal class and the value $M\left(K,[I]\right)$ does not depend on the choice of such an ideal I. If $M\left(K,[I]\right) > 1$, then K has no norm-Euclidean ideal norm. The value $M\left(K,[I]\right)$ may depend on the choice of I, but for any ideal J of minimal norm, $M\left(K,[J]\right) \geqslant 1$.*

Proof. This is a simple consequence of the fact that K admits at most one norm-Euclidean ideal class, and that this class may only be the class of *any* ideal of minimal norm. □

Example 2.9. *As in the classical Euclidean case, we can easily compute the Euclidean minimum in the imaginary quadratic case. Let K stand for $\mathbf{Q}(\sqrt{-m})$ where m is a positive squarefree integer.*

Proposition 2.10. *According to the value of m, there exists an ideal of minimal norm I such that we have the following formulæ.*

- *If $m \equiv 1 \pmod 4$, then $M(K,[I]) = \frac{(m+1)^2}{8m}$ for $I = 2\mathbf{Z} + \mathbf{Z}\left(1+\sqrt{-m}\right)$ of norm 2.*
- *If $m = 2$, then $M(K,[I]) = \frac{3}{4}$ for $I = 2\mathbf{Z} + \mathbf{Z}\sqrt{-m}$ of norm 2.*
- *If $m = 3$, then $M(K,[I]) = \frac{1}{3}$ for $I = 3\mathbf{Z} + \mathbf{Z}\frac{3+\sqrt{-3}}{2}$ of norm 3.*
- *If $m \equiv 7 \pmod 8$, then $M(K,[I]) = \frac{m^2+10m+9}{32m}$ for $I = 2\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-m}}{2}$ of norm 2.*
- *If $m \equiv 11 \pmod{24}$, then $M(K,[I]) = \frac{m^2+26m+25}{48m}$ for $I = 3\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-m}}{2}$ of norm 3.*
- *If $m \equiv 19 \pmod{24}$, then $M(K,[I]) = \frac{(m+1)^2}{16m}$ for $I = 2\mathbf{Z}_K$ of norm 4.*
- *If $m \equiv 3 \pmod{24}$ and $m \neq 3$, then $M(K,[I]) = \frac{(m+9)^2}{48m}$ for $I = 3\mathbf{Z} + \mathbf{Z}\frac{3+\sqrt{-m}}{2}$ of norm 3.*

In particular, K has a norm-Euclidean class if and only if $m \in \{1,2,3,5,7,11,15\}$. This result was already stated in [11]. An extension to a more general case was provided by [10].

2.3 Inhomogeneous minimum

As in the classical case, we will study $M\left(K,[I]\right)$ in a geometric setting.

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

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

We define $\Phi : \left\{ \begin{array}{ccc} K & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & \Phi(x) \end{array} \right.$, where

$$\Phi(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_2}(x)) .$$

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

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

We introduce $H = K \otimes_{\mathbf{Q}} \mathbf{R}$, which we identify with $\mathbf{R}^n$ equipped with the product previously defined. We can extend the norm to H by setting

$$\mathcal{N} : \left\{ \begin{array}{ccc} H & \longrightarrow & \mathbf{R}_{\geqslant 0} \\ x = (x_i)_{1\leqslant i\leqslant n} & \longmapsto & \prod_{i=1}^{r_1} x_i \prod_{i=r_1+1}^{r_1+r_2} (x_i^2 + x_{i+r_2}^2) \end{array} \right. .$$

We see that for any $x, y \in H$, $\mathcal{N}(x \cdot y) = \mathcal{N}(x)\mathcal{N}(y)$ and that for any $\xi \in K$, $\mathbf{N}_{K/\mathbf{Q}}(\xi) = \mathcal{N}(\Phi(\xi))$.

With these notations, we write for any $x \in H$, $m_{\overline{K},I}(x) := \inf_{Z\in\Phi(I)} \frac{|\mathcal{N}(x-Z)|}{\mathbf{N}I}$ and we set

$$M\left(\overline{K}, I\right) := \sup_{x\in H} m_{\overline{K},I}(x).$$

As previously, this real number depends only on the class $[I]$, so we can write $M\left(\overline{K}, [I]\right) = M\left(\overline{K}, I\right)$.

The units $\mathbf{Z}_K^\times$ act on H, for any $x \in H$, we define the orbit of x modulo $\Phi(I)$ by $\operatorname{Orb}(x) := \left\{\Phi(\nu) \cdot x \text{ modulo } \Phi(I),\, \nu \in \mathbf{Z}_K^\times\right\}$.

2.4 Computation of the local Euclidean minimum

Given $x \in K$, there exists $z \in I$ such that $m_{K,I}(x) = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right|}{\mathbf{N}I}$ but this property is not enough to compute $m_{K,I}(x)$ in practice. However, we may compute it exactly as in the classical Euclidean case (see [4]) and we may compute a function $k \longmapsto \Gamma(k)$ which depends on the number field K such that we have the following statement.

Lemma 2.11. *Let $x \in \Phi(K) \setminus \Phi(I)$ and $k > 0$. If there exists $X \in I$ such that $0 < \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-X)\right|}{\mathbf{N}I} < k$, then there exists $\nu \in \Phi(\mathbf{Z}_K^\times)$ and $Y \in \Phi(I)$ such that*

$$\frac{\left|\mathbf{N}_{K/\mathbf{Q}}(\nu \cdot x - Y)\right|}{\mathbf{N}I} < k \quad \text{and} \quad |Y_i| \leqslant \Gamma(k) \text{ for all } 1 \leqslant i \leqslant n.$$

With this result, we can compute the local Euclidean minimum, for any given $z \in \Phi(K)$. Let us set $\mathcal{I}_z := \{Z \in I,\, |z_i - Z_i| \leqslant \Gamma(k) \text{ for all } 1 \leqslant i \leqslant n\}$.

Proposition 2.12. *Let $x \in \Phi(K)$ and $k > 0$. Then $\operatorname{Orb}(x)$ is finite and for any $z \in \operatorname{Orb}(x)$, $\mathcal{I}_z$ is finite. Let us write $\mathcal{M}_k := \min\limits_{z\in\operatorname{Orb}(x)} \min\limits_{Z\in\mathcal{I}_z} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(z-Z)\right|}{\mathbf{N}I}$. Then $\mathcal{M}_k \leqslant k$ implies $m_{\overline{K},I}(x) = \mathcal{M}_k$.*

As the function $k \longmapsto \mathcal{M}_k$ is nonincreasing, if $k' := \mathcal{M}_k > k$, then $m_{\overline{K},I}(x) = \mathcal{M}_{k'}$ and this provides a procedure to compute $m_{K,I}$.

3 Properties

3.1 Link between Euclidean and inhomogeneous minima

As for the classical Euclidean minimum, we have the following result, which is a direct generalisation of [3].

Theorem 3.1. *Let K be a number field such that $r > 1$ and J be an ideal. Then there exists $\xi \in K$ such that $M\left(\overline{K}, [J]\right) = m_{K,J}(\xi)$. In particular, $M\left(\overline{K}, [J]\right) = M\left(K, [J]\right)$.*

Corollary 3.2. *Let K be a number field such that $r > 1$ and I an ideal of minimal norm of K. Then K admits a norm-Euclidean ideal class if and only if*

$$M\left(K, [I]\right) = M\left(\overline{K}, [I]\right) < 1.$$

With this result, we can write a slight extension of Proposition 2.8.

Proposition 3.3. *Let K be a number field such that $r > 1$ and I be an ideal of minimal norm of $\mathbf{Z}_K$. If $M\left(K, [I]\right) < 1$, then K admits a norm-Euclidean ideal class and the value $M\left(K, [I]\right)$ does not depend on the choice of such an ideal I. If $M\left(K, [I]\right) \geqslant 1$, then K has no norm-Euclidean ideal norm. The value $M\left(K, [I]\right)$ may depend on the choice of I, but for any ideal J of minimal norm, $M\left(K, [J]\right) \geqslant 1$.*

Proof. The proof is the similar to the one of Proposition 2.8, except we can now use Corollary 3.2 to conclude when $M\left(K, [I]\right) = 1$. □

3.2 Lower bound for the Euclidean minimum

Lemma 3.4. *For any ideal J, $\frac{\max\{M(K),1\}}{\mathbf{N}J} \leqslant M\left(K, [J]\right)$.*

Even though this easy bound seems quite bad, it may be used in some cases to conclude quickly that a number field admits no norm-Euclidean ideal class.

Example 3.5. *The totally real cubic field K of discriminant 2597 admits no norm-Euclidean ideal class since $M(K) = \frac{5}{2}$ and $\Lambda(K) = 2$.*

3.3 Upper bounds

We know upper bounds for $M(K)$ expressed with the discriminant of K in the cases $r_1 = 2$, $r_2 = 0$ (the best one is given by [8]) and $r_1 = r_2 = 1$ ([2]) and $r_1 = 0$, $r_2 = 2$ ([2], corrected by [13]).

Such bounds are proved with quadratic and cubic forms and still hold for norm-Euclidean ideal classes (this was already noted by [13]).

Theorem 3.6 (Ennola, Cassels, van der Linden)**.** *Let K be a number field with an norm-Euclidean ideal class such that $r = 1$.*

- *if $r_1 = 2$, $r_2 = 0$, then $\mathrm{disc}_K \leqslant 945$,*
- *if $r_1 = r_2 = 1$, then $|\mathrm{disc}_K| \leqslant 170520$,*
- *if $r_1 = 0$, $r_2 = 2$, then $\mathrm{disc}_K \leqslant 230202117$.*

disc_K	h_K	$M\left(K,[I]\right)$
− 283	2	$\frac{3}{4}$
− 331	2	$\frac{3}{4}$
− 643	2	$\frac{121}{144}$
− 648	3	$\frac{3}{4}$
− 676	3	$\frac{7}{8}$

Table 1: Non-principal complex cubic number fields with a norm-Euclidean ideal class up to discriminant -3299.

3.4 Algorithm

We can modify the algorithm described in [12] to compute the minimum $M\left(K,[I]\right)$ of a given number field. Generally speaking, we replace $\mathbf{Z}_K$ with any ideal I of minimal norm. In practice, we know a $\mathbf{Z}$-basis of the ideal I denoted by $(z_i)_{1\leqslant i\leqslant n}$ and, instead of $\mathcal{M}$, we use the matrix $\mathcal{M}' = \left(m'_{i,j}\right)_{1\leqslant i,j\leqslant n}$ where for any $1 \leqslant i,j \leqslant n$,

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

Algorithm 3.7. *Given a number field K, there exists a procedure which returns* failure *or an ideal I of minimal norm, $M(K,[I])$ and all points $x \in K$ modulo I such that $M(K,[I]) = m_{K,I}(x)$.*

In practice, this algorithm is almost always successful, its execution may even be shorter if we only want to know if $M(K,[I]) < 1$.

3.5 Already known examples

In degrees $n \geqslant 3$, few examples of number fields with a norm-Euclidean ideal class were known if $\mathrm{h}_K > 1$. An example in signature $(1,1)$ was found by van der Linden ([13], it is the number field of discriminant -283 in Table 1), an example in signature $(0,2)$ was originally given by Lenstra ([11], number field of discriminant 1521 in Table 5). Lemmermeyer gave another example in signature $(1,1)$ (number field of discriminant -331 in Table 1).

4 Complex cubic number fields and pure cubic number fields

We consider an ideal I of minimal norm and compute $M\left(K,[I]\right)$ with the algorithm described in section 3.4. We present in Table 1 the examples found of non-principal Euclidean number fields which admit an ideal class. These are the only ones such that $|\mathrm{disc}_K| < 3299$.

We know that these number fields have a class number $\mathrm{h}_K \leqslant 4$ (see [11] or [13] for details), however, no example with class number equal to 4 was found.

We can use several criteria given in [13] to restrict the possibilities of Euclidean ideal classes. However, as in the case of the (classical) norm-Euclideanity, we cannot prove yet that these examples are the only ones.

In the remainder or this section, we will restrict ourselves to pure cubic number fields.

4.1 Notations and result

Let $n > 1$ be an integer, which we may assume cubefree. We consider $K = \mathbf{Q}(\sqrt[3]{n})$. Cioffari ([5]) listed all norm-Euclidean pure cubic number fields, in a similar fashion, we may investigate the pure cubic number fields which admit an Euclidean ideal class.

Theorem 4.1. *$K = \mathbf{Q}(\sqrt[3]{n})$ admits a norm-Euclidean class if and only if $n \in \{2, 3, 10\}$. In particular, there exists no pure cubic number field with a non-principal norm-Euclidean ideal class.*

We suppose that K is such a field, then $1 \leqslant \mathrm{h}_K \leqslant 4$. As the case $\mathrm{h}_K = 1$ was solved in [5], let us suppose that $2 \leqslant \mathrm{h}_K \leqslant 4$. The remainder of this section will be devoted to the proof of Theorem 4.1.

4.2 General properties of a pure cubic number field

We will describe several properties of a pure cubic number fields, our purpose is to restrict as much as possible the list of possible values of n such that $\mathbf{Q}\left(\sqrt[3]{n}\right)$ admits a norm-Euclidean ideal class.

4.2.1 Ring of integers, ramification and ideals of minimal norm

As we assume that n is cubefree, we can write $n = ab^2$, where a and b are two coprime integers such that ab is squarefree. For $\mathbf{Q}\left(\sqrt[3]{ab^2}\right) = \mathbf{Q}\left(\sqrt[3]{a^2b}\right)$, we may suppose that $b < a$. We will write $\alpha = \sqrt[3]{n}$.

The following statement provides information on the integers and some ideals of K. These result are well-known, pure cubic number fields were studied by Dedekind.

Lemma 4.2. *With the previous notations, we can describe the ring of integers of K:*

- *if $a^2 \not\equiv b^2 \pmod 9$, then $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\frac{\alpha^2}{b}$ and $\mathrm{disc}_K = -27a^2b^2$,*
- *if $a^2 \equiv b^2 \pmod 9$, then $\mathbf{Z}_K = \mathbf{Z}\alpha + \mathbf{Z}\frac{\alpha^2}{b} + \mathbf{Z}\frac{1+a\alpha+\alpha^2}{3}$ and $\mathrm{disc}_K = -3a^2b^2$.*

Besides, the primes are ramified in K as follows.

- *Let p be a prime factor of n, $p \neq 3$, then p is totally ramified in K.*
- *If $a^2 \not\equiv b^2 \pmod 9$, then 3 is totally ramified in K. If $a^2 \equiv b^2 \pmod 9$ and $9|n$, then 3 is totally ramified in K.*
- *If $2 \not| n$, then 2 splits into two distinct factors.*

Consequently, in any case, there exists an ideal of norm 2 in K and $\Lambda(K) = 2$.

Proof. All these statements are proved in section 6.4 of [6], where the author gives the explicit expression of ideals of norm 2. □

4.2.2 Class number

Firstly, genus theory gives us the following property.

Lemma 4.3 ([1], Theorem 4.1)**.** *Let t be the number of totally ramified primes in K. If $t \geqslant 2$, then 3^{t-2} divides h_K.*

The fact that K admits a norm-Euclidean ideal class provides the class number number with another condition.

Proposition 4.4. *If $K = \mathbf{Q}(\sqrt[3]{n})$ admits a norm-Euclidean ideal class, then $\mathrm{h}_K \leqslant 4$. Besides, if $2|n$ and K admits a non-principal norm-Euclidean ideal class, then $\mathrm{h}_K = 3$.*

Proof. Thanks to Lemma 4.2, we know that 2 is either totally ramified in K, or splits into two distinct factors.

If 2 is totally ramified in K (that happens exactly when 2 divides n), then $2\mathbf{Z}_K = I^3$ for some ideal I of minimal norm. Then $[I]^3 = \mathbf{Z}_K$ and as $[I]$ is a generator of the class group of K, h_K divides 3.

If $2\mathbf{Z}_K = IJ$, where I is an ideal of minimal norm 2 and $\mathbf{N}J = 4$, then, thanks to Proposition 2.4, 1, there exists $0 \leqslant n < 4$ such that $[J] = [I]^n$. Therefore, $[I]^{n+1} = [\mathbf{Z}_K]$ and $\mathrm{h}_K \leqslant n + 1 \leqslant 4$. □

Remark 4.5. *Any cubic number field equipped with a norm-Euclidean ideal class satisfies $\mathrm{h}_K \leqslant 4$, to see this, the other cases when 2 splits into three factors or is inert are proved similarly.*

Corollary 4.6. *If $K = \mathbf{Q}(\sqrt[3]{n})$ admits a norm-Euclidean ideal class, then n has at most 3 prime factors.*

Proof. Thanks to Lemma 4.3, we know that n admits at most 4 prime factors and may admit 4 prime factors if and only if 3 is one of them. Let us assume that n has exactly four prime factors (including 3). As $3|n = ab^2$, we have $a^2 \not\equiv b^2 \pmod 9$, therefore $\mathrm{disc}_K = -27a^2b^2$. Consequently, $-\mathrm{disc}_K \geqslant 27 \cdot (2 \cdot 3 \cdot 5 \cdot 7)^2 = 1190700 \geqslant 170520$, and K admits no norm-Euclidean ideal class. □

4.2.3 List of candidates

The purpose of this paragraph is to establish a finite list of candidates for pure cubic number fields with a non-principal norm-Euclidean class.

Proposition 4.7. *If pure cubic field K admits a non-principal norm-Euclidean ideal class, then $K = \mathbf{Q}(\sqrt[3]{n})$ where n is one of the 65 following values:*

$$7, 11, 13, 14, 15, 19, 20, 21, 22, 26, 28, 30, 31, 34, 35, 37, 38, 42, 47, 51, 52, 60, 62,$$
$$68, 73, 74, 77, 78, 84, 89, 90, 92, 109, 117, 118, 127, 132, 134, 143, 150, 154, 156,$$
$$161, 163, 170, 172, 175, 181, 190, 206, 233, 244, 260, 275, 325, 350, 388, 396, 460,$$
$$476, 539, 550, 1666, 1700, 1900.$$

Proof. Thanks to Cassels's bound (3.6), we know that $-\mathrm{disc}_K < 170520$. Using the expression of disc_K and Corollary 4.6, we can establish a finite list of candidates.

For instance, if n is prime, then $n < \sqrt{\frac{170520}{3}}$, so $n \leqslant 233$. In fact, we have a better bound if $n^2 \not\equiv 1 \pmod 9$, then $n < \sqrt{\frac{170520}{27}}$, so $n \leqslant 79$. With PARI ([14]), we list all primes n satisfying these conditions such that $2 \leqslant h_K \leqslant 4$, we obtain the following fifteen primes:

$$7, 11, 13, 19, 31, 37, 47, 73, 89, 109, 127, 163, 181, 233.$$

If n admits exactly two prime factors $\alpha < \beta$, then $\alpha < \sqrt[4]{\frac{170520}{3}}$, so $\alpha \leqslant 13$.

- If $\alpha = 13$, then $\beta \leqslant 17$, so $\beta = 17$. But $13 \equiv 4 \pmod 9$ and $17 \equiv -1 \pmod 9$, consequently we cannot have $a^2 \equiv b^2 \pmod 9$, thus $-\mathrm{disc}_K = 27 \cdot 13^2 \cdot 17^2 > 170520$.
- If $\alpha = 11$, then $\beta \leqslant 19$. As in the previous subcase, we can exclude $\beta = 17$ and $\beta = 19$ with congruences modulo 9. Besides, $11 \equiv 2 \pmod 9$ and $13 \equiv 4 \pmod 9$, so we can only have a norm-Euclidean ideal class if $n = 11 \cdot 13 = 143$.
- If $\alpha = 7$, then $\beta \leqslant 31$. There are three possible values $77, 539$ and 161.
- If $\alpha = 5$, then $\beta \leqslant 47$, there are four possible values: $35, 175, 275$ and 325.
- If $\alpha = 3$, then $a^2 \not\equiv b^2 \pmod 9$, so $\beta < \sqrt{\frac{170520}{27 \cdot 3^2}}$ and $5 \leqslant \beta \leqslant 23$. Keeping only values for which $2 \leqslant h_K \leqslant 4$, we find four possible values $15, 21, 117$ and 51.
- If $\alpha = 2$, then $\beta \leqslant 113$. There are eighteen possibilities:

$$20, 14, 28, 22, 26, 52, 34, 68, 38, 92, 62, 74, 172, 118, 244, 134, 388 \text{ and } 206.$$

If n admits three prime factors $\alpha < \beta < \gamma$, then $\alpha < \sqrt[6]{\frac{170520}{3}}$ and $\alpha \leqslant 5$.

- If $\alpha = 5$, then we can easily obtain that $5 = \alpha < \beta < \sqrt[4]{\frac{170520}{3 \cdot 5^2}}$ and there is no such prime.
- If $\alpha = 3$, then $a^2 \not\equiv b^2 \pmod 9$, therefore $\mathrm{disc}_K = -27a^2b^2$, and $3 = \alpha < \beta < \sqrt[4]{\frac{170520}{27 \cdot 3^2}}$, consequently, $\beta = 5$. Then $5 = \beta < \gamma < \sqrt{\frac{170520}{27 \cdot 3^2 \cdot 5^2}}$, there is no such integer.
- If $\alpha = 2$, then we find similarly $\beta \leqslant 7$.
  - If $\beta = 7$, then $\gamma \leqslant 17$ and there are three possibilities $154, 1666$ and 476.
  - If $\beta = 5$, then $\gamma \leqslant 23$ and eight values are possible for n: $350, 550, 260, 170, 1700, 190, 1900$ and 460.
  - If $\beta = 3$, then $\gamma \leqslant 13$ (taking into account $a^2 \not\equiv b^2 \pmod 9$) and there are nine possibilities:

$$30, 90, 60, 42, 84, 132, 396, 78 \text{ and } 156.$$

This completes the proof. □

Consequently, to establish Theorem 4.1, we will prove that none of these fields admits a norm-Euclidean ideal class.

4.2.4 Crucial tool

In the remainder of the proof, we will use the following tool.

Proposition 4.8. *Given a number field k and $a \in \mathbf{Z}_{\geqslant 0}$, we can effectively determine if there exists $z \in \mathbf{Z}_k$ such that $\left|\mathbf{N}_{k/\mathbf{Q}}(z)\right| = a$.*

Proof. See [15], section 6.4. □

n	7	11	13	14	15	19	20	21	22	26	28	30	35	37	38	42	52	73	84	90	117	150	325	350	539
$M(K,[I])$	$\frac{19}{10}$	$\frac{9}{4}$	$\frac{479}{147}$	$\frac{140}{23}$	$\frac{13857}{4052}$	$\frac{9}{8}$	$\frac{36}{19}$	$\frac{24749}{4976}$	$\frac{335}{66}$	$\frac{24}{19}$	$\frac{5}{4}$	$\frac{6859}{1215}$	$\frac{181}{75}$	$\frac{883}{332}$	$\frac{770729}{86762}$	$\frac{682075}{63512}$	$\frac{61}{8}$	$\frac{629127}{150124}$	$\frac{2972191}{250051}$	$\frac{1033977}{174968}$	$\frac{960584}{96905}$	$\frac{491159}{73620}$	$\frac{33403}{6864}$	$\frac{301431}{66158}$	$\frac{6669477}{970472}$

Table 2: Computations of some values of the Euclidean minimum of pure cubic fields.

4.3 First remarks and computations

4.3.1 Principal ideals of norm 2

First, we can discard the number fields for which an ideal of minimal norm 2 is principal, this occurs for $n \in \{31, 34, 60, 62, 68, 109, 118, 127, 172\}$. Indeed, if they admitted an Euclidean ideal class, then the class of this ideal would generate the class group (thanks to Proposition 2.4). This is impossible, since the class group is not trivial.

4.3.2 Application of Algorithm 3.7

We may then compute some of the values of $M(K, [I])$. In practice, this is only possible when the fundamental unit of K is "not too big".

Proposition 4.9. *All the values computed in Table 2 are greater than* 1*, consequently, we can discard all these values of* n*.*

4.4 Consequences of total ramification

The fact that the prime factors of n (except sometimes for 3) are totally ramified in K has some very interesting consequences. We will distinguish the properties according to the principality of the ideals above the product of primes chosen.

4.4.1 Principal case

Lemma 4.10. *Let f be a product of different prime numbers totally ramified in K, we write $\mathfrak{f}$ the ideal of $\mathbf{Z}_K$ such that $f\mathbf{Z}_K = \mathfrak{f}^3$. If $\alpha, \beta \in \mathbf{Z}_K$ are such that $\alpha \equiv \beta \pmod{\mathfrak{f}}$, then*

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{f}.$$

A very similar property is stated by Egami in [7], he attributes this argument to Lenstra.

Proof. Let L be the Galois closure of $K/\mathbf{Q}$. Let us write $\mathfrak{F} = \mathfrak{f}\mathbf{Z}_L$. Then $f\mathbf{Z}_L = f\mathbf{Z}_K\mathbf{Z}_L = \mathfrak{f}^3\mathbf{Z}_L = \mathfrak{F}^3$.

Consequently, if $\varphi : K \longrightarrow L$ is an embedding of K, then $f\mathbf{Z}_L = \varphi(f\mathbf{Z}_L) = \varphi(\mathfrak{F})^n$, so $\varphi(\mathfrak{F}) = \mathfrak{F}$. As $\alpha \equiv \beta \pmod{\mathfrak{F}}$, we have $\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{\mathfrak{F}}$. But $\mathbf{N}_{K/\mathbf{Q}}(\alpha) - \mathbf{N}_{K/\mathbf{Q}}(\beta) \in \mathbf{Z}$, and $\mathfrak{F} \cap \mathbf{Z} = f\mathbf{Z}$, so

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{f}.$$

□

In practice, we know that some elements are norms, we will use this fact.

Lemma 4.11. *Let p be a prime such that $p \not\equiv 1 \pmod 3$, then for any $x \in \mathbf{Z}/p\mathbf{Z}$, there exists $\alpha \in \mathbf{Z}/p\mathbf{Z}$ such that $x = \alpha^3$.*

Proof. For $p = 3$, we can take $\alpha = x$, for other values of p, let us write $p = 3k + 2$, for some integer k, then we can take $\alpha = x^{2k+1}$. □

Lemma 4.12. *Let $f = \prod_{i=1}^{l} p_i$ where $p_i \not\equiv 1 \pmod 3$ are different totally ramified primes of K. Let us write $f\mathbf{Z}_K = \mathfrak{f}^3$. We assume that $\mathfrak{f}$ is principal. If $0 < e < f$ is an integer such that neither $e - 2f$, nor $e - f$, nor e, nor $e + f$ are norms of elements of $\mathbf{Z}_K$, then $M(K) > 2$, therefore $M(K, [I]) > 1$ for any ideal I of minimal norm 2.*

Proof. Thanks to Lemma 4.11 and Chinese Remainder Theorem, we know that there exists some integer α such that $e \equiv \alpha^3 \pmod f$. Consequently, $e \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \pmod f$. Let us write $\mathfrak{f} = \gamma\mathbf{Z}_K$, where $\gamma \in \mathbf{Z}_K \setminus \{0\}$. Then there exists some $\delta \in \mathbf{Z}_K$ such that

$$\begin{aligned} m_K\left(\frac{\alpha}{\gamma}\right) &= \left|\mathbf{N}_{K/\mathbf{Q}}\left(\frac{\alpha}{\gamma} - \delta\right)\right| \\ &= \frac{1}{\mathbf{N}\mathfrak{f}}\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \delta\gamma)\right|. \end{aligned}$$

But $\alpha - \delta\gamma \equiv \alpha \pmod{\mathfrak{f}}$, so, thanks to Lemma 4.10,

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha - \delta\gamma) \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv e \pmod f.$$

Therefore, $m_K\left(\dfrac{\alpha}{\gamma}\right) \geqslant \dfrac{\min\{3f - e, e + 2f\}}{f} > 2.$ □

Remark 4.13. *The hypothesis "$p_i \not\equiv 1 \pmod 3$" is only used to find an element $\alpha \in \mathbf{Z}_K$ such that $\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv e \mod f$, this hypothesis may be dropped if we provide such an element α.*

Proposition 4.14. *The fields corresponding to the values 47, 51, 74, 89, 154, 170, 175, 190, 206, 233, 460, 476, 550, 1666, 1700 admit no norm-Euclidean ideal class.*

Proof. Apply Lemma 4.12 with values given in Table 3, (a). This proves Proposition 4.14 except in the cases 74, 190 and 206. For these values, let us write x a root of $X^3 - n$ in K.

For 74, we can take $f = 74 = 2 \cdot 37$. We have $37 \equiv 1 \pmod 3$, but we can take into account Remark 4.13 with $e = 31$ to conclude that $M(K, [I]) > 1$, because $179 = \mathbf{N}_{K/\mathbf{Q}}(2x^2 - x - 31) \equiv e \mod f$.

For 190, similarly, take $f = 190 = 2\cdot5\cdot19$, and $e = 152$, we can conclude that $M(K, [I]) > 1$, given that $532 = \mathbf{N}_{K/\mathbf{Q}}\left(3393x^2 + 19506x + 112138\right) \equiv e \pmod f$.

For 206, we can proceed likewise with $f = 206 = 2\cdot103$ and $e = 31$ because we know that $443 = \mathbf{N}_{K/\mathbf{Q}}(x^2 - 3x - 17) \equiv e \pmod f$. □

The previous result only applies when the ideal above a product of totally ramified primes is principal. We can establish a similar result in another case.

(a) Principal case.

n	f	e
47	$3 \cdot 47$	29
51	17	2
89	89	5
154	$2 \cdot 11$	4
170	$2 \cdot 5 \cdot 17$	5
175	$3 \cdot 5$	4
233	233	5
460	23	2
476	$2 \cdot 17$	3
550	$2 \cdot 11$	2
1666	$2 \cdot 17$	3
1700	17	2

(b) Other case.

n	f	e
77	$3 \cdot 11$	7
92	23	5
132	11	5
143	11	2
161	23	2
260	$2 \cdot 5$	3
275	11	4
350	5	2
396	11	4
1900	5	2

Table 3: These fields admit no norm-Euclidean ideal class.

4.4.2 Other case

Lemma 4.15. *Let $f = \prod_{i=1}^{l} p_i$ where $p_i \not\equiv 1 \pmod 3$ are different totally ramified primes of K. Let us write $f\mathbf{Z}_K = \mathfrak{f}^3$. We assume that $[\mathfrak{f}] = [I]$, where I is an ideal of minimal norm 2. If $0 < e < f$ is an integer such that neither $e - f$, nor e are norms of elements of $\mathbf{Z}_K$ then $M\left(K, [I]\right) > 1$.*

Proof. Once again, we can apply Lemma 4.11 and Chinese Remainder Theorem to find an integer α such that $e \equiv \alpha^3 \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \pmod f$. Then there exists $\gamma \in \mathfrak{f}$ such that $m_{K,\mathfrak{f}}(\alpha) = \frac{1}{\mathbf{N}\mathfrak{f}} \left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \gamma)\right|$. But $\alpha - \gamma \equiv \alpha \pmod{\mathfrak{f}}$, and Lemma 4.10 implies

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha - \gamma) \equiv e \pmod f.$$

Consequently, $m_{K,\mathfrak{f}}(\alpha) \geqslant \frac{\max\{2f-e, e+f\}}{f} > 1$. Therefore, $M(K,[I]) = M(K,[\mathfrak{f}]) > 1$, and K admits no norm-Euclidean ideal class. □

Proposition 4.16. *The fields corresponding to the values* 77*,* 92*,* 132*,* 143*,* 161*,* 260*,* 275*,* 350*,* 396*,* 1900 *admit no norm-Euclidean ideal class.*

Proof. Apply Lemma 4.15 with values given in Table 3, (b). For each value of n in the table, $\mathrm{h}_K = 3$. Besides, the corresponding values of f are not norms of elements of $\mathbf{Z}_K$. Therefore, $[\mathfrak{f}] = [I]$ or $[\mathfrak{f}] = [I]^2$. In the latter case, $\mathfrak{f}I$ is a principal ideal, thus $2f$ is a norm of an element of $\mathbf{Z}_K$. We easily check that this is false, so $[\mathfrak{f}] = [I]$, and $M\left(K, [\mathfrak{f}]\right) = M\left(K, [I]\right)$. □

4.5 Remaining values

As for the seven remaining values, even though the lemmas previously described do not exactly apply, the ideas remain basically identical: we exhibit a point $t = \frac{a}{b} \in K$ (where $a, b \in \mathbf{Z}_K \setminus \{0\}$), then by computing

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu)$$

n	a	b	l	e	N
78	x	3	54	24	78
134	67	x	134	67	1139
156	x	3	54	50	104
163	32	x	326	168	484
181	60	x	382	248	476
244	x	2	8	4	20
388	97	x	194	97	873

Table 4: Remaining cases, $x = \sqrt[3]{n}$.

for any element u of the ideal I of minimal norm 2 (in these cases, there is a unique ideal of norm 2 and we know a $\mathbf{Z}$-basis of I), we remark that there exist $l \in \mathbf{Z}_{>0}$ and $e \in \{0, 1, \ldots, l-1\}$ such that

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu) \equiv e \pmod{l}.$$

Therefore, $\mathbf{N}_{K/\mathbf{Q}}(a - bu) \in e + l\mathbf{Z}$. We exclude some of these possibilities because they are not norms of integers of K and denote by N the smallest (in absolute value) such possible norm. Consequently,

$$m_{K,I}(t) \geqslant \frac{|N|}{\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right| \cdot \mathbf{N}I} = \frac{|N|}{2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|}$$

If $|N| \geqslant 2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|$, this proves that K admits no norm-Euclidean ideal class.

For instance, for $n = 78$, we write $x = \sqrt[3]{n}$. Then, let us consider $a = x$ and $b = 3$. We know that $I = 2\mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2$ is the ideal of norm 2 of $\mathbf{Z}_K$. For any $\alpha, \beta, \gamma \in \mathbf{Z}$, we can compute

$$\begin{aligned}&\mathbf{N}_{K/\mathbf{Q}}\left(a + 3\left(2\alpha + \beta x + \gamma x^2\right)\right)\\ =&54 \cdot \left(4\alpha^3 - 234\alpha\beta\gamma - 78\alpha\gamma + 39\beta^3 + 39\beta^2 + 13\beta + 3042\gamma^3 + 1\right) + 24.\end{aligned}$$

Consequently, for any $u \in I$,

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu) \equiv 24 \pmod{54},$$

or with the previous notations, $l = 54$ and $e = 24$. Neither 24, nor -30 are norms of elements of $\mathbf{Z}_K$, therefore $N = 78 \geqslant 54 = 2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|$.

We list corresponding elements a, b, l, e and N in Table 4.

5 Other examples

5.1 Totally complex quartic number fields

With Algorithm 3.7, we can list 26 examples of non-principal number fields with a norm-Euclidean ideal class in Table 5. The first one, of discriminant 1521, was already given by Lenstra in [11]. The best bound known for a quartic number field with a norm-Euclidean ideal class is $\mathrm{h}_K \leqslant 6$, but all the examples listed here are such that $\mathrm{h}_K = 2$.

disc_K	h_K	$M\left(K,[I]\right)$	3025	2	$\frac{11}{16}$	4400	2	$\frac{19}{25}$
1521	2	$\frac{4}{9}$	3528	2	$\frac{11}{18}$	4725	2	$\frac{7}{9}$
1872	2	$\frac{4}{9}$	3600[a]	2	$\frac{3}{4}$	4752	2	$\frac{8}{9}$
2304	2	$\frac{3}{4}$	3600[b]	2	$\frac{7}{9}$	5076	2	$\frac{7}{8}$
2457[c]	2	$\frac{7}{13}$	3625	2	$\frac{19}{25}$	5225	2	$\frac{19}{25}$
2457[d]	2	$\frac{4}{7}$	3700	2	$\frac{3}{4}$	5328	2	$\frac{109}{148}$
2889	2	$\frac{5}{6}$	4329[e]	2	$\frac{19}{28}$	5616	2	$\frac{49}{52}$
2925	2	$\frac{7}{9}$	4329[f]	2	$\frac{301}{481}$	6669[g]	2	< 1
3024	2	$\frac{19}{28}$	4352	2	$\frac{33}{34}$	6669[h]	2	< 1

Table 5: Examples of non-principal totally imaginary quartic number fields with a norm-Euclidean ideal class. I is an ideal of minimal norm. If there is an ambiguity, a minimal polynomial is given below. The table is certainly incomplete.

[a] $x^4 - x^3 + 9x^2 - 4x + 16$
[b] $x^4 - x^3 - 6x^2 - x + 19$
[c] $x^4 + x^2 + 4$
[d] $x^4 - 5x^2 + 25$
[e] $x^4 - x^3 + 11x^2 - 2x + 28$
[f] $x^4 - x^3 - 10x^2 + 7x + 31$
[g] $x^4 - 2x^3 - 12x^2 + 13x + 43$
[h] $x^4 - x^3 - 12x^2 + 2x + 49$

5.2 Other signatures

With Algorithm 3.7, we can find many new examples of number fields with a non-principal norm-Euclidean ideal class. In particular, we found examples with the following properties.

Theorem 5.1. *We can list examples of quintic and sextic number fields admitting a non-principal norm-Euclidean class. The number field of signature* $(2,1)$ *and discriminant* -54764 *has a class number equal to* 4 *and a norm-Euclidean ideal class.*

In Table 6, we list some of them, according to their signature and class number.

For a given signature, the non-principal number field of smallest discriminant may have no norm-Euclidean ideal class. For instance, the number field of discriminant 1957 and of signature $(3,0)$ admits no norm-Euclidean ideal class. In fact, we have $M\left(K,[I]\right) = 1$, where I is the ideal of norm 2 of $\mathbf{Z}_K$.

5.3 Graves's example

Lenstra introduced Euclidean ideal classes without restricting himself to the norm.

Definition 5.2. *Let* R *be a Dedekind domain,* $\mathfrak{I}$ *the set of its invertible integral ideals and* $I \in \mathfrak{I}$ *. We say that* I *is Euclidean if there exists a map* $\psi : \mathfrak{I} \to \mathbf{Z}_{>0}$ *such that for all* $J \in \mathfrak{I}$ *and all* $x \in J^{-1}I \setminus I$*, there exists some* $y \in I$ *such that*

$$\psi\left((x-y)JI^{-1}\right) < \psi(J).$$

Obviously, if R is the ring of integers of a number field K and ψ is the norm of ideals, this is equivalent to Definition 2.1.

n	(r_1, r_2)	h_K	a minimal polynomial such that $K = \mathbf{Q}(x)$	disc_K	$M(K, [I])$
3	$(3,0)$	2	$x^3 - x^2 - 14x + 23$	2777	$\frac{5}{9}$
		3	$x^3 - x^2 - 30x + 64$	8281	$\frac{27}{28}$
4	$(4,0)$	2	$x^4 - 17x^2 + 36$	21025	$\frac{5}{16}$
	$(2,1)$	2	$x^4 - 2x^3 + 5x^2 - 2x - 1$	-6848	$\frac{4}{9}$
		3	$x^4 - x^3 - 3x^2 + 12x - 8$	-27620	$\frac{7}{8}$
		4	$x^4 - x^3 - 2x^2 + 4x - 24$	-54764	$\frac{7}{8}$
5	$(5,0)$	2	$x^5 - 11x^3 - 9x^2 + 14x + 9$	4010276	$\frac{3}{4}$
	$(3,1)$	2	$x^5 - 2x^4 + 2x^3 - 12x^2 + 21x - 9$	-243219	$\frac{4}{9}$
	$(1,2)$	2	$x^5 - x^4 - 2x^2 + 4x - 1$	41381	$\frac{4}{9}$
		3	$x^5 - 2x^4 + 4x^3 - 6x^2 + 3x + 1$	130925	$\frac{3}{4}$
6	$(2,2)$	2	$x^6 - 2x^5 - x^4 + 7x^3 - 6x^2 + 3x - 1$	1387029	< 1
	$(0,3)$	2	$x^6 - 3x^5 + 3x^4 - x^3 + 3x^2 - 3x + 1$	-273375	< 1

Table 6: Some new examples of non-principal number fields with a norm-Euclidean ideal class, I is an ideal of minimal norm of K.

Graves ([9]) presented the example $K = \mathbf{Q}\left(\sqrt{2}, \sqrt{35}\right)$, which admits an Euclidean ideal class for some ψ, but did not know about the existence of a norm-Euclidean ideal class. Using Algorithm 3.7, we can prove the following statement.

Theorem 5.3. *$K = \mathbf{Q}\left(\sqrt{2}, \sqrt{35}\right)$ has no norm-Euclidean ideal class.*

Proof. If we write $K = \mathbf{Q}(x)$ where $x^4 - 36x^2 + 289 = 0$, we can consider the following ideal of minimal norm 2,

$$I = 2\mathbf{Z} + \frac{x^3 - 19x}{17}\mathbf{Z} + \frac{-1x^3 + 36x + 17}{17}\mathbf{Z} + (x^2 - 17)\mathbf{Z}.$$

Then $M(K, [I]) = m_{K,I}\left(\frac{x^3+17x^2-19x+17}{34}\right) = m_{K,I}\left(\frac{x^3+17x^2-19x+51}{34}\right) = \frac{7}{4}$. Therefore, K admits no norm-Euclidean ideal class. □

In the case of imaginary quadratic number fields, Graves and Ramsey ([10]) proved that all number fields with an Euclidean ideal class admit in fact a norm-Euclidean ideal class, however, this provides a number field of signature $(4, 0)$ with an Euclidean ideal class, which admits no norm-Euclidean ideal class.

References

[1] P. Barrucand and H. Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*, Journal of Number Theory, 2 (1970), pp. 7–21.

[2] J. W. S. Cassels, *The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic form*, Proceedings of the Cambridge Philosophical Society, 48 (1952), pp. 72–86.

[3] J.-P. Cerri, *Euclidean and inhomogeneous spectra of number fields with unit rank strictly greater than 1*, Journal für die reine und angewandte Mathematik, 592 (2006), pp. 49–62.

[4] ——, *Euclidean minima of totally real number fields. Algorithmic determination*, Mathematics of Computation, 76 (2007), pp. 1547–1575.

[5] V. G. Cioffari, *The Euclidean condition in pure cubic and complex quartic fields*, Mathematics of Computation, 33 (1979), pp. 389–398.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, vol. 138 of Graduate Texts in Mathematics, Springer, 1996.

[7] S. Egami, *On Finiteness of the Numbers of Euclidean Fields in Some Classes of Number Fields*, Tokyo Journal of Mathematics, 7 (1984), pp. 183–198.

[8] V. Ennola, *On the First Inhomogeneous Minimum of Indefinite Binary Quadratic Forms and Euclid's Algorithm in Real Quadratic Fields*, PhD thesis, University of Turku, 1958.

[9] H. Graves, $\mathbf{Q}\left(\sqrt{2},\sqrt{35}\right)$ *has a non-principal Euclidean ideal*, International Journal of Number Theory, 7 (2011), pp. 2269–2271.

[10] H. Graves and N. Ramsey, *Euclidean ideals in quadratic imaginary fields*, Journal of the Ramanujan Mathematical Society, 26 (2011), pp. 85–97.

[11] H. W. Lenstra, Jr., *Euclidean ideal classes*, I.H.É.S., (1978). 32 pages.

[12] P. Lezowski, *Computation of the Euclidean minimum of algebraic number fields.* submitted, available from `http://hal.archives-ouvertes.fr/hal-00632997/en/`, 2011.

[13] F. J. van der Linden, *Euclidean rings with two infinite primes*, PhD thesis, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.

[14] The PARI Group, *PARI/GP, version* `2.4.3`, Bordeaux, 2008. available from `http://pari.math.u-bordeaux.fr/`.

[15] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1989.