ARCHIVUM MATHEMATICUM (BRNO)
Tomus 56 (2020), 171–182

THE REDUCED IDEALS OF A SPECIAL ORDER IN A PURE CUBIC NUMBER FIELD

Abdelmalek Azizi*, Jamal Benamara*, Moulay Chrif Ismaili*, and Mohammed Talbi**

Abstract. Let $K = \mathbb{Q}(\theta)$ be a pure cubic field, with $\theta^3 = D$, where D is a cube-free integer. We will determine the reduced ideals of the order $\mathcal{O} = \mathbb{Z}[\theta]$ of K which coincides with the maximal order of K in the case where D is square-free and $\not\equiv \pm 1 \pmod 9$.

1. Introduction

Reduced ideals of a number field K form a finite and regularly distributed set in the infrastructure of K. They can be used to compute the regulator and the class number of a number field, see [5]–[10]. They can also be used to describe a method for testing an arbitrary (fractional) ideal for principality in algebraic number field of unit rank one, see [4].

In cryptography, J.A. Buchmann and H.C. Williams described a key exchange protocol based on the finite set of reduced principal ideals of a real quadratic order, see [2]. Yet, in [3], the same authors described another key exchange system which makes use of the properties of reduced ideals of an imaginary quadratic field. They use the fact that there exists exactly one reduced ideal in each ideal class.

Most of the work on reduced ideals is realized on quadratic fields, see for example [8]. If K is a quadratic field and $\mathcal{O} = \mathbb{Z}[\theta]$ an order of K, then any rank 2 sub-$\mathbb{Z}$-module M of $\mathcal{O}$ can be uniquely written in the canonical form $M = [a, b + c\theta]$ where a, b and c are integers such that $a > 0$, $c > 0$, and $0 \le b < a$. For such a sub-$\mathbb{Z}$-module to be an ideal of $\mathcal{O}$, the integers a, b and c must satisfy the three following conditions: $c \mid a$, $c \mid b$ and $ac \mid N_{K/\mathbb{Q}}(b + c\theta)$. The ideal $I = [a,\ b + c\theta]$ in canonical form is reduced, if and only if, I is primitive ($c = 1$), and the integers a and b satisfy certain conditions in addition to those mentioned above. The integer a in canonical form of the ideal I, is the smallest positive rational integer in I, and it is shown that if a is smaller than a lower bound depending on the field K then I is reduced, and conversely, if a exceeds an upper bound depending on the field K, then I is not reduced. It is also proved that the order $\mathcal{O}$ can only have finitely many reduced ideals and every class contains a reduced ideal.

2020 *Mathematics Subject Classification*: primary 11R16; secondary 11R29, 11T71.
Key words and phrases: cubic field, reduced ideal.
Received June 15, 2019, revised June 2020. Editor R. Kučera.
DOI: 10.5817/AM2020-3-171

In this paper, we consider a pure cubic number field $K = \mathbb{Q}(\sqrt[3]{D})$ where $D > 1$ is a cube-free integer and the sub-ring $\mathcal{O} = \mathbb{Z}[\sqrt[3]{D}]$. Our goal is to mirror the results realized in quadratic field. First, we give a canonical presentation for ideals of $\mathcal{O}$, called in our paper the HNF-basis. Next, we adopt the general definition of a reduced ideal (see [6, Definition 6.5.1, p. 352]) and identify necessary and sufficient conditions, in terms of that presentation for an ideal to be reduced. We also determine a lower and upper bound as in quadratic field and give a method for determining the set of all reduced ideals of $\mathcal{O}$. We also show that every class contains a reduced ideal. This continues and extends the work begun in [7], where the author considers only the square free integer D such that $D \not\equiv \pm 1 \pmod 9$. We will see in Section 6 that for $D = 7$ we have eight reduced ideals not nine as computed by the python code presented in [7] and for $D = 11$ there are twelve reduced ideals not just eleven. This is because the python code contains errors in the function "isReduced (a, b, c, d, e, m)" which is based on [7, Theorem 2.8]. Therefore, we will replace this theorem with another one (Theorem 5.1); hence, we will give another function "isReduced (a, b, c, d, e, D)" based on our new theorem.

2. Some definitions and properties of a pure cubic field

A pure cubic field is a field of type $K = \mathbb{Q}(\theta)$ with $\theta^3 = D$, where D is a cube-free integer. We can assume that $D > 1$, and we can write D in a unique fashion:

$$D = rs^2, \text{ where } r, s \in \mathbb{N}, \ \gcd(r, s) = 1, \ rs > 1, \quad \text{and } rs \text{ is square-free.}$$

Any such field has one real embedding and a pair of conjugate complex embeddings and, hence, has one fundamental unit and negative discriminant.

The pure cubic number field $K = \mathbb{Q}(\sqrt[3]{D})$ is said to be of type I if $D \not\equiv \pm 1 \pmod 9$ otherwise it is said to be of type II.

Using the previous notation, we have the following theorem:

Theorem 2.1. *Let $K = \mathbb{Q}(\theta)$ be a pure cubic number field.*

(1) *If K is of type* I *then $\left(1, \theta, \frac{\theta^2}{s}\right)$ is an integral basis of K and $\Delta_K = -27r^2s^2$ is the discriminant of K.*

(2) *If K is of type* II *then $\left(1, \theta, \frac{\theta^2 + rs^2\theta + s^2}{3s}\right)$ is an integral basis of K and $\Delta_K = -3r^2s^2$ is the discriminant of K.*

Proof. See [6, Theorem 6.4.13, p. 346]. □

The theorem above gives us an integral basis for both types of a pure cubic number field, a basis that is not always simple. Some pure cubic number fields may have a simple basis if we set some conditions on D.

Definition 2.1. Let K be a number field and $\mathcal{O}_K$ its ring of integers. We say that $\mathcal{O}_K$ is monogenic if there exist $\theta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Corollary 2.1. *Let $K = \mathbb{Q}(\sqrt[3]{D})$ be a pure cubic number field of type* I. *If D is square-free then $\mathcal{O}_K$ is monogenic.*

Proof. If $K = \mathbb{Q}(\sqrt[3]{D})$ is a pure cubic number field of type I and D is a square-free, we must have $s = 1$; therefore, $(1, \theta, \theta^2)$ is an integral basis of K. $\square$

Definition 2.2. Let K be a number field of degree $[K : \mathbb{Q}] = n$ and $\mathcal{O}_K$ its ring of integers. A sub-ring $\mathcal{O} \subset K$ is called an order in K if and only if one of the following equivalent conditions is satisfied :

(1) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module and the quotient field of $\mathcal{O}$ is K.

(2) $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank n.

(3) $\mathcal{O} \subset \mathcal{O}_K$ and $\mathcal{O}$ contains a $\mathbb{Q}$-basis for K.

(4) $\mathcal{O} \subset \mathcal{O}_K$ and $[\mathcal{O}_K : \mathcal{O}] < \infty$.

See [11] for the proof of equivalence of these assertions.

Remark 2.1. Let $K = \mathbb{Q}(\theta)$ be a number field where $\theta \in \mathcal{O}_K$, the ring of integers of K, $F \in \mathbb{Z}[X]$ be the minimal monic polynomial of θ, and Δ_θ the discriminant of F. Then $\mathcal{O} = \mathbb{Z}[\theta]$ is an order of K, because we have $\mathcal{O} \subset \mathcal{O}_K$ and $[\mathcal{O}_K : \mathcal{O}]^2 = \frac{\Delta_\theta}{\Delta_K} < \infty$.

3. Representation of an ideal

Theorem 3.1. *Let K be a number field with degree n over $\mathbb{Q}$ and let $\mathcal{O} = [\theta_1, \ldots, \theta_n]$ be an order in K. Then for any sub-$\mathbb{Z}$-module M of $\mathcal{O}$ of rank n, there exists a unique basis $[\omega_1, \ldots, \omega_n]$ such that if we write $\omega_j = \sum_{i=1}^{n} \omega_{ij}\theta_i$, then the matrix $W = (\omega_{ij})_{1\le i,j\le n}$ satisfies the following conditions:*

(1) *For all i and j, ω_{ij} is an integer.*

(2) *W is an upper triangular matrix.*

(3) *For all i, $\omega_{ii} > 0$.*

(4) *For all $j > i$, $0 \le \omega_{ij} < \omega_{ii}$.*

Furthermore we have $[\mathcal{O} : M] = \det W$.

The corresponding basis $[\omega_1, \ldots, \omega_n]$ will be called the HNF-basis (Hermite Normal Form) of M with respect to $\mathcal{O}$.

Proof. See [6, Theorem 4.7.3, p. 189]. $\square$

Remark 3.1. Let $K = \mathbb{Q}(\theta)$ be a pure cubic number field with $\theta^3 = D$ a cube-free integer, and let $\mathcal{O} = [\theta_1, \theta_2, \theta_3]$ be an order in K. If I is an ideal of $\mathcal{O}$, then I is a sub-$\mathbb{Z}$-module of $\mathcal{O}$, hence by the above theorem, the HNF-basis of I with respect to $\mathcal{O}$ is of the form:

$$I = [a\theta_1,\ b\theta_1 + c\theta_2,\ d\theta_1 + e\theta_2 + f\theta_3]\,,$$

and we have

$$W = \begin{pmatrix} a & b & d \\ & c & e \\ & & f \end{pmatrix}$$

where $a,\ b,\ c,\ d,\ e$ and f are integers such that $0 \le b < a$, $0 \le d < a$, $0 \le e < c$ and $0 < f$. Furthermore, we have $N(I) = acf$ where $N(I) = [\mathcal{O} : I]$ is the norm of I.

The reverse is not always true because a sub-$\mathbb{Z}$-module of $\mathcal{O}$ is not always an ideal of $\mathcal{O}$.

The above information on the integers $a,\ b,\ c,\ d,\ e$ and f come just from the fact that I is considered as a sub-$\mathbb{Z}$-module of $\mathcal{O}$. We will of course get more information if we use the fact that I is a sub-$\mathcal{O}$-module of $\mathcal{O}$.

Theorem 3.2. *Let $K = \mathbb{Q}(\theta)$ be a pure cubic number field with $\theta^3 = D$ where D is a cube-free integer, and let $\mathcal{O} = \mathbb{Z}[\theta]$. Let $I = [a, b + c\theta, d + e\theta + f\theta^2]$ be a sub-$\mathbb{Z}$-module of $\mathcal{O}$ in HNF-basis form. Then I is an ideal of $\mathcal{O}$ if and only if*

1. *f divides the integers $a,\ b,\ c,\ d,\ e$;*
2. *c divides the integers $a,\ b$;*
3. *cf divides the integers $df - e^2$ and $Df^2 - de$;*
4. *acf divides the integers $bce - c^2d - fb^2$, $Dfc^2 + b^2e - bcd$, $Dcf^2 - bdf + be^2 - cde$ and $Dcef - Dbf^2 + bde - cd^2$.*

Proof. Let's suppose that $I = [a, b + c\theta, d + e\theta + f\theta^2]$ is an ideal of $\mathcal{O}$. To prove the divisibility properties, we will use the fact that some elements belong to I.

We have $a\theta \in I$, then there exists $x,\ y$ and $z \in \mathbb{Z}$ such that $a\theta = xa + y(b + c\theta) + z(d + e\theta + f\theta^2)$, therefore

$$\begin{cases} ax + by + dz = 0 \\ cy + ez = a \\ zf = 0 \end{cases} \Longrightarrow \begin{cases} ax + by = 0 \\ cy = a \\ z = 0 \end{cases} \Longrightarrow \begin{cases} cx = -b \\ cy = a \\ z = 0 \end{cases} \Longrightarrow \begin{cases} c \mid a \\ c \mid b\,. \end{cases}$$

Since $a\theta^2 \in I$, then there exists $x,\ y$ and $z \in \mathbb{Z}$ such that $a\theta^2 = xa + y(b + c\theta) + z(d + e\theta + f\theta^2)$, therefore

$$\begin{cases} ax + by + dz = 0 \\ cy + ez = 0 \\ zf = a, \end{cases} \Longrightarrow f \mid a\,.$$

Since $b\theta + c\theta^2 \in I$, hence there exists $x,\ y$ and $z \in \mathbb{Z}$ such that $b\theta + c\theta^2 = xa + y(b + c\theta) + z(d + e\theta + f\theta^2)$, therefore

$$\begin{aligned} \begin{cases} ax + by + dz = 0 \\ cy + ez = b \\ fz = c \end{cases} &\Longrightarrow \begin{cases} acfx = -bf(b - ze) - dc^2 \\ cy = b - ez \\ fz = c \end{cases} \\ &\Longrightarrow \begin{cases} acfx = -b^2f + bce - dc^2 \\ cy = b - ez \\ fz = c \end{cases} \\ &\Longrightarrow \begin{cases} acf \mid bce - b^2f - c^2d \\ f \mid c\,. \end{cases} \end{aligned}$$

In the same way we have:

$$b\theta^2 + cD \in I \Longrightarrow \begin{cases} acf \mid c^2 f D + b^2 e - bcd \\ f \mid b \end{cases}$$

and

$$d\theta + e\theta^2 + Df \in I \Longrightarrow \begin{cases} acf \mid Dcf^2 - bdf + be^2 - cde \\ cf \mid df - e^2 \\ f \mid e \end{cases}$$

and

$$d\theta^2 + eD + Df\theta \in I \Longrightarrow \begin{cases} acf \mid cDef - bDf^2 + bde - cd^2 \\ cf \mid Df^2 - de \\ f \mid d\,. \end{cases}$$

Conversely, let $I = [a, b + c\theta, d + e\theta + f\theta^2]$ be a sub-$\mathbb{Z}$-module of $\mathcal{O}$ satisfying the divisibility condition of the theorem. Let $\alpha \in \mathcal{O}$ and $\beta \in I$, then $\alpha = x + y\theta + z\theta^2$ and $\beta = x'a + y'(b + c\theta) + z'(d + e\theta + f\theta^2)$ with $x,\ y,\ z,\ x',\ y',\ z' \in \mathbb{Z}$. We have:

$$\begin{aligned} \alpha\beta &= x\beta + y\theta\beta + z\theta^2\beta \\ &= x\beta + yx'a\theta + yy'(b\theta + c\theta^2) + yz'(d\theta + e\theta^2 + Df) + zx'(a\theta^2) \\ &\quad + zy'(b\theta^2 + cD) + zz'(d\theta^2 + eD + Df\theta)\,. \end{aligned} \tag{3.1}$$

If we exploit the conditions of divisibility of the theorem, we then get the following results:

$$\begin{cases} a\theta = -\frac{b}{c}a + \frac{a}{c}(b + c\theta) + 0(d + e\theta + f\theta^2) \in I \\ a\theta^2 = a\frac{be-dc}{cf} - \frac{ea}{cf}(b + c\theta) + \frac{a}{f}(d + e\theta + f\theta^2) \in I \\ b\theta + c\theta^2 = a\frac{bce-b^2f-dc^2}{acf} + \frac{bf-ec}{cf}(b + c\theta) + \frac{c}{f}(d + e\theta + f\theta^2) \in I \\ b\theta^2 + cD = a\frac{Dc^2f+b^2e-bdc}{acf} - \frac{be}{cf}(b + c\theta) + \frac{b}{f}(d + e\theta + f\theta^2) \in I \\ d\theta + e\theta^2 + Df = a\frac{Dcf^2-bdf+be^2-cde}{acf} + \frac{df-e^2}{cf}(b + c\theta) + \frac{e}{f}(d + e\theta + f\theta^2) \in I \\ d\theta^2 + eD + Df\theta = \frac{a(Dcef-Dbf^2+bde-cd^2)}{acf} + \frac{(Df^2-de)(b+c\theta)}{cf} + \frac{d(d+e\theta+f\theta^2)}{f} \in I\,. \end{cases}$$

So according to (3.1), we have $\alpha\beta \in I$ which proves that I is an ideal of $\mathcal{O}$. $\square$

It is clear that a is the smallest positive element of $I \cap \mathbb{Z}$, which is called the length of I and denoted by $\ell(I)$.

4. The primitive ideals of the order $\mathcal{O} = \mathbb{Z}[\theta]$

Definition 4.1. Let K be a number field, and $\mathcal{O}$ an order of K. We say that an ideal I of $\mathcal{O}$ is primitive if I is without rational factor. In other words, if there is no prime number p such that $I \subset p\mathcal{O}$.

It is equivalent to say that I is not divisible by any ideal generated by a rational integer except $\mathcal{O}$. Likewise, it is also equivalent to say that the ideal $n^{-1}I$ is not integral ($n^{-1}I \not\subseteq \mathcal{O}$) for any integer $n > 1$.

Proposition 4.1. *Let $K = \mathbb{Q}(\theta)$ be a pure cubic number field with $\theta^3 = D$ where D is a cube-free integer, and let $\mathcal{O} = \mathbb{Z}[\theta]$. Let $I = [a, b + c\theta, d + e\theta + f\theta^2]$ be a sub-$\mathbb{Z}$-module of $\mathcal{O}$ in HNF-basis form. Then I is a primitive ideal of $\mathcal{O}$ if and only if*

(1) $f = 1$;

(2) *c divides the integers a, b, $d - e^2$ and $D - de$;*

(3) *ac divides the integers $bce - c^2d - b^2$, $Dc^2 + b^2e - bcd$, $Dc - bd + be^2 - cde$ and $Dce - Db + bde - cd^2$.*

Proof. If $I = [a, b + c\theta, d + e\theta + f\theta^2]$ is an ideal of $\mathcal{O} = \mathbb{Z}[\theta]$, then according to Theorem 3.2, f is a positive integer which divides a, b, c, d and e. Therefore I is primitive if and only if $f = 1$. The divisibility statements are deduced by Theorem 3.2. $\square$

In the case where $\mathcal{O} = \mathcal{O}_K$ (i.e. D is square free and $\not\equiv \pm 1 \pmod 9$), we have the following result:

Theorem 4.1. *Let $K = \mathbb{Q}(\theta)$ be a pure cubic number field with $\theta^3 = D$ where D is square free and $\not\equiv \pm 1 \pmod 9$. Then, each class in the class group $\mathrm{Cl}(K)$ of K contains a primitive ideal I with $N(I) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$. Moreover, $\mathrm{Cl}(K)$ is generated by the primitive non-inert prime ideals $\mathcal{P}$ with $N(\mathcal{P}) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$.*

Proof. Let $[I]$ be an arbitrary class in $\mathrm{Cl}(K)$, and let $\beta \in \mathcal{O}_K$, $\beta \neq 0$, such that $J = \beta I^{-1} \subset \mathcal{O}_K$. By [9, Lemma 6.2, p. 35], there exists $\alpha \in J$, $\alpha \neq 0$, such that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{2}{\pi}\sqrt{|\Delta_K|}N(J)\,,$$

therefore

$$N(\alpha\mathcal{O}_K)N(J)^{-1} = N(\alpha J^{-1}) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}\,,$$

then, if the ideal $I' = \alpha J^{-1} = \alpha\beta^{-1}I$ is primitive, the proof of the first assertion is finished, if not, there exists an integer $f > 1$ such that $I' = fI''$ with I'' is primitive, and we have $N(I'') \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$ and $I'' = \frac{\alpha}{f\beta}I$. Finally, if the primitive ideal $\mathcal{P} = [a, b + c\theta, d + e\theta + \theta^2]$ is a prime ideal above p, then $N(\mathcal{P}) = ac \neq p^3$ because $a = p$ and $c \mid a$, therefore $\mathcal{P}$ is non-inert. $\square$

5. Reduced ideals of the order $\mathcal{O} = \mathbb{Z}[\theta]$

Definition 5.1. Let K be a number field of degree n over $\mathbb{Q}$, and let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K in $\mathbb{C}$ and let $\mathcal{O}$ be an order of K. We will say that an ideal I of $\mathcal{O}$ is reduced if I is primitive and every element $\alpha \in I$ verifying $\forall i \in \{1, \ldots, n\}$, $|\sigma_i(\alpha)| < \ell(I)$, is zero (where $\ell(I)$ is the length of I).

Theorem 5.1. *Let $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt[3]{D} \in \mathbb{R}$ where $D > 1$ is a cube free integer, and $\mathcal{O} = \mathbb{Z}[\theta]$. Let $I = [a, b + c\theta, d + e\theta + \theta^2]$ be a primitive ideal of $\mathcal{O}$ in HNF-basis form. Then I is reduced if and only if the only triple of integers (x, y, z) satisfying:*

- $c \mid y - ze$,
- $ac \mid cx - by + (be - cd)z$,
- $|x + y\theta + z\theta^2| < \ell(I)$,
- $(x - \frac{y}{2}\theta - \frac{z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(y - z\theta)^2\ell(I)^2$,

is $(0, 0, 0)$.

Proof. For any $\alpha \in K$ let α' and α'' denote the conjugates of α, we have $\theta' = \zeta\theta$ and $\theta'' = \zeta^2\theta$, where $\zeta = e^{2i\pi/3}$ is a primitive cube root of unity and therefore $|\alpha'| = |\alpha''|$.

Let $I = [a, b + c\theta, d + e\theta + \theta^2]$ be a primitive ideal of $\mathcal{O} = \mathbb{Z}[\theta]$. If $\alpha \in I$ then $\alpha = Xa + Y(b + c\theta) + Z(d + e\theta + \theta^2)$ with $X, Y, Z \in \mathbb{Z}$ and we can easily verify that $|\alpha'| = ((aX + bY + dZ - \frac{cY+eZ}{2}\theta - \frac{Z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(cY + eZ - Z\theta)^2)^{\frac{1}{2}}$. Now, the ideal I is reduced, if and only if, for all $\alpha \in I$, we have $|\alpha| < \ell(I)$ and $|\alpha'| < \ell(I)$ implies that $\alpha = 0$. On the other hand, we have

$$\begin{cases} \alpha \in I \\ |\alpha| < \ell(I) \\ |\alpha'| < \ell(I) \end{cases}$$

if and only if

$$\begin{cases} X, Y, Z \in \mathbb{Z} \\ |aX + bY + dZ + (cY + eZ)\theta + Z\theta^2| < \ell(I) \\ (aX + bY + dZ - \frac{cY+eZ}{2}\theta - \frac{Z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(cY + eZ - Z\theta)^2 < \ell(I)^2 . \end{cases}$$

We shall use the substitution $x = aX + bY + dZ$, $y = cY + eZ$, $z = Z$, having the inverse $X = \frac{cx-by+(be-cd)z}{ac}$, $Y = \frac{y-ze}{c}$, $Z = z$. Therefore we see that the ideal I is reduced if and only if $(0, 0, 0)$ is the only solution of

$$\begin{cases} x, y, z \in \mathbb{Z} \\ c \mid y - ze \\ ac \mid cx - by + (be - cd)z \\ |x + y\theta + z\theta^2| < \ell(I) \\ (x - \frac{y}{2}\theta - \frac{z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(y - z\theta)^2 < \ell(I)^2 . \end{cases}$$

The theorem is proved. □

Remark 5.1. According the two inequalities in the above theorem, we can easily show that $|x| < \ell(I)$, $|y| < \frac{2+\sqrt{3}}{3}\frac{\ell(I)}{\theta}$ and $|z| < \frac{2+\sqrt{3}}{3}\frac{\ell(I)}{\theta^2}$.

Let $I = [a, b + c\theta, d + e\theta + \theta^2]$ be a primitive ideal of $\mathcal{O}$ in HNF-basis form. The function "isReduced (a, b, c, d, e, D)" in the python code, computes whether the ideal I is reduced or not. By the above theorem and remark, this function becomes as follows:

```
def isReduced (a,b,c,d,e,D):
  theta=math.exp(math.log(D)/3)
  reduced = 1
  for x in range (-a+1,a):
    for y in range (-int(((2+ math.sqrt(3))*a)/(3*theta)),1+int(((2+
    math.sqrt(3))*a)/(3*theta))):
      for z in range (-int(((2+ math.sqrt(3))*a)/(3*theta**2)),1+int
      (((2+ math.sqrt(3))*a)/(3*theta**2))):
        if not ((x==0) and (y==0) and (z==0)):
          if (y-z*e)%c==0:
            N=a*c
            if (c*x-b*y+(b*e-c*d)*z)%N==0:
              if ((x+y*theta+z*theta**2)<a) and ((x+y*theta+z*theta*
              *2)>-a):
                if (x-((y*theta)/2)-((z*(theta**2))/2))**2+(3/4)*(y*
                theta-z*z*theta**2)**2<a**2:
                  reduced =0
                  return reduced
  return reduced
```

Remark 5.2. In addition to the modification of the function “isReduced (a, b, c, d, e, D)”, we also replace the function “isSquarefree(n)” by a function “isCubefree(n)” for the task to decide whether a given positive integer is cube-free or not, and remove the condition $D \not\equiv \pm 1 \pmod 9$ and conserve the rest of python code presented in [7].

Corollary 5.1. *Let $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt[3]{D} \in \mathbb{R}$ where $D > 1$ is a cube free integer, $\mathcal{O} = \mathbb{Z}[\theta]$ and I be a primitive ideal of $\mathcal{O}$. If $\ell(I) < \theta$, then I is reduced.*

Proof. Let $I = [a, b + c\theta, d + e\theta + \theta^2]$ be a primitive ideal of $\mathcal{O}$ in its HNF-basis form, with $\ell(I) < \theta$.

Let (x, y, z) be a triple of integers such that $c \mid y - ze$ and $ac \mid cx - by + (be - cd)z$ satisfying

$$\begin{cases} |x + y\theta + z\theta^2| < \ell(I) \\ (x - \frac{y}{2}\theta - \frac{z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(y - z\theta)^2 < \ell(I)^2 . \end{cases}$$

According to Remark 5.1, we have $|z| < \frac{2+\sqrt{3}}{3}\frac{\ell(I)}{\theta^2}$ and since $\ell(I) < \theta$ then $z = 0$. On the other hand, we have $|y| < \frac{2+\sqrt{3}}{3}\frac{\ell(I)}{\theta} < \frac{2+\sqrt{3}}{3}$ which means $y \in \{-1, 0, 1\}$. But $y = 1$ means that $0 < x < \theta$ and $-2\theta < x < 0$ together, and $y = -1$ means that $-\theta < x < 0$ and $0 < x < 2\theta$ together. These are impossible, hence $y = 0$. Finally, we have $|x| < \ell(I)$ and $\ell(I) = a \mid x$; therefore, $x = 0$. Hence the triplet (x, y, z) is zero, so I is reduced. □

Theorem 5.2. *Let $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt[3]{D} \in \mathbb{R}$ where $D > 1$ is a cube free integer, $\mathcal{O} = \mathbb{Z}[\theta]$, and let I be an ideal of $\mathcal{O}$. If I is reduced then $\ell(I) \leq \frac{6\sqrt{3}D}{\pi}$.*

Proof. Let $V(S)$ denote the volume of the set

$$S = \{(x,y,z) \in \mathbb{R}^3 \mid |x+y\theta+z\theta^2| < \ell(I);\ (x-\frac{y}{2}\theta-\frac{z}{2}\theta^2)^2+\frac{3}{4}\theta^2(y-z\theta)^2 < \ell(I)^2\}\,.$$

It is clear that S is a convex subset of $\mathbb{R}^3$ and symmetrical about the origin $(0,0,0)$. Let's suppose that I is a reduced ideal of $\mathcal{O}$; then S does not contain any triples (x,y,z) representing a non-zero element of I considered as a lattice of $\mathbb{R}^3$, so according to Minkowski's Lattice Point Theorem, (see [9, p. 27]) we have $\frac{1}{2^3}V(S) \leq N(I)$.

Using the triple integrals we have

$$V(S) = \int\int\int_S \mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z = \frac{4\pi\ell(I)^3}{3D\sqrt{3}}\,,$$

therefore $\frac{1}{8}\frac{4\pi\ell(I)^3}{3D\sqrt{3}} \leq \ell(I)c$, it means that $\frac{\pi\ell(I)^3}{6D\sqrt{3}} \leq \ell(I)c$ and since $c \leq \ell(I)$ then $\frac{\pi\ell(I)^3}{6D\sqrt{3}} \leq \ell(I)^2$, hence $\ell(I) \leq \frac{6D\sqrt{3}}{\pi}$. □

Theorem 5.3. *Let $K = \mathbb{Q}(\theta)$ with $\theta^3 = D$ and D cube-free integer, and $\mathcal{O} = \mathbb{Z}[\theta]$. Then $\mathcal{O}$ contains at least one reduced ideal and at most a finite number of reduced ideals.*

Proof. The existence is assured by $\mathcal{O}$ which is itself a reduced ideal since $\ell(\mathcal{O}) = 1 < \theta$. According to the previous theorem, if I is reduced then $\ell(I) \leq \frac{6D\sqrt{3}}{\pi}$ and since $N(I) = ac = \ell(I)c \leq \ell(I)^2$ then $N(I) < (\frac{6D\sqrt{3}}{\pi})^2 = \frac{108D^2}{\pi^2}$. According to [1, Theorem 12.5.3], there exists a finite number of ideals of a given norm, which completes the proof of the theorem. □

The last result is also true in the quadratic case, and it is proved that each class of ideals contains a reduced ideal (see [8, Remark 1.4.1.]). More than that, in the case of an imaginary quadratic field, it is proved that there are at most two reduced ideals in any class of ideals, and when two distinct such ideals are in the same class, then one is the conjugate of the other (see [8, Theorem 1.4.2.(e)]).
In the general case, we can show that each class of ideals contains a reduced ideal, but no information on the number of reduced ideals in this class can be provided.

Theorem 5.4. *Let K be a number field and let $\mathcal{O}$ be an order in K. Then every class of ideals of $\mathcal{O}$ contains a reduced ideal.*

Proof. Let $[I]$ be an arbitrary class of ideals of $\mathcal{O}$, and let $\eta \neq 0$ be an element of I of minimal nonzero absolute value of norm. Let $d_I = \min\{m \in \mathbb{Z}^+ \mid m\eta^{-1}I \subset \mathcal{O}\}$. We have $1 = \eta\eta^{-1} \in \eta^{-1}I$, therefore $d_I \in d_I\eta^{-1}I$, so the ideal $J = d_I\eta^{-1}I$ is integral and primitive, and we have $\ell(J) \leq d_I$. Let's show now that J is reduced. For that, we will use Definition 5.1, let $\alpha \in J$ satisfy: $\forall i \in \{1,\ldots,n\}$, $|\sigma_i(\alpha)| < \ell(J)$, $(\alpha = d_I\eta^{-1}\beta,\ \beta \in I)$, therefore

$$|N_{K/\mathbb{Q}}(\alpha)| < \ell(J)^n\,,$$

so

$$d_I^n|N_{K/\mathbb{Q}}(\beta)| < \ell(J)^n|N_{K/\mathbb{Q}}(\eta)|\,,$$

hence

$$|N_{K/\mathbb{Q}}(\beta)| < |N_{K/\mathbb{Q}}(\eta)|,$$

but by hypothesis, η is of minimal nonzero absolute value of norm, hence $\beta = 0$ and $\alpha = 0$ and therefore J is reduced. $\square$

6. Numerical examples

Let us suppose we have a pure cubic number field $K = \mathbb{Q}(\theta)$ with $\theta^3 = D$ and $D > 1$ a cube free integer, and $\mathcal{O} = \mathbb{Z}[\theta]$.

To determine the list of all reduced ideals $I = [a, b + c\theta, d + e\theta + \theta^2]$ in $\mathcal{O}$, we determine at first all the primitive ideals of $\mathcal{O}$ whose length is such that $\ell(I) \leq \frac{6\sqrt{3}D}{\pi}$, i.e for any integer a such that $1 \leq \ell(I) = a \leq \frac{6\sqrt{3}D}{\pi}$, we determine the different possible positive values of b, such that $0 \leq b < a$. Next, for each possible pair (a, b), we determine the possible values of the integer c such that $c \mid a$ and $c \mid b$. After that, we determine the possible values of integers d and e such that $0 \leq d < a$ and $0 \leq e < c$ which satisfy also the other conditions of Theorem 3.2.

The primitive ideals whose length is strictly less than $\theta = \sqrt[3]{D}$ are therefore included in the sought list, if $\sqrt[3]{D} \leq \ell(I) \leq \frac{6\sqrt{3}D}{\pi}$ then we apply to it Theorem 5.1.

Example 6.1. Let $D = 7$, so $K = \mathbb{Q}(\sqrt[3]{7})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$, we have the lower bound is $\sqrt[3]{7} \approx 1.91$, and the upper bound is $\frac{6\sqrt{3}D}{\pi} \approx 23.16$, we obtain 8 reduced ideals presented in the following table with their norms.

a	b	c	d	e	f	Reduced ideals	N
1	0	1	0	0	1	$I_1 = \mathcal{O}_K = [1, \sqrt[3]{7}, \sqrt[3]{49}]$	1
2	1	1	1	0	1	$I_2 = [2, 1 + \sqrt[3]{7}, 1 + \sqrt[3]{49}]$	2
2	0	2	1	1	1	$I_3 = [2, 2\sqrt[3]{7}, 1 + \sqrt[3]{7} + \sqrt[3]{49}]$	4
3	0	3	1	1	1	$I_4 = [3, 3\sqrt[3]{7}, 1 + \sqrt[3]{7} + \sqrt[3]{49}]$	9
4	0	4	1	3	1	$I_5 = [4, 4\sqrt[3]{7}, 1 + 3\sqrt[3]{7} + \sqrt[3]{49}]$	16
5	0	5	4	3	1	$I_6 = [5, 5\sqrt[3]{7}, 4 + 3\sqrt[3]{7} + \sqrt[3]{49}]$	25
6	0	6	1	1	1	$I_7 = [6, 6\sqrt[3]{7}, 1 + \sqrt[3]{7} + \sqrt[3]{49}]$	36
12	0	12	1	7	1	$I_8 = [12, 12\sqrt[3]{7}, 1 + 7\sqrt[3]{7} + \sqrt[3]{49}]$	144

We have just 8 reduced ideals, not 9 as given by the code in [7, p. 35]. The ninth ideal displayed by this code is $I = [6, 3 + 3\theta, 4 + \theta + \theta^2]$, which is not reduced, indeed, we have $\alpha = 2 - \theta - \theta^2 \in I$ and α satisfies the two inequalities $|\alpha| < 6$ and $|\sigma(\alpha)| < |\sigma(6)| = 6$, but $\alpha \neq 0$.

Example 6.2. Let $D = 11$, so $K = \mathbb{Q}(\sqrt[3]{11})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{11}]$, we have the lower bound is $\sqrt[3]{11} \approx 2.22$, and the upper bound is $\frac{6\sqrt{3}D}{\pi} \approx 36.39$, we obtain 12 reduced ideals presented in the following table with their norms.

a	b	c	d	e	f	Reduced ideals	N
1	0	1	0	0	1	$I_1 = \mathcal{O}_K = [1, \sqrt[3]{11}, \sqrt[3]{121}]$	1
2	0	2	1	1	1	$I_2 = [2, 2\sqrt[3]{11}, 1 + \sqrt[3]{11} + \sqrt[3]{121}]$	4
2	1	1	1	0	1	$I_3 = [2, 1 + \sqrt[3]{11}, 1 + \sqrt[3]{121}]$	2
3	0	3	1	2	1	$I_4 = [3, 3\sqrt[3]{11}, 1 + 2\sqrt[3]{11} + \sqrt[3]{121}]$	9
3	1	1	2	0	1	$I_5 = [3, 1 + \sqrt[3]{11}, 2 + \sqrt[3]{121}]$	3
4	0	4	1	3	1	$I_6 = [4, 4\sqrt[3]{11}, 1 + 3\sqrt[3]{11} + \sqrt[3]{121}]$	16
5	0	5	1	1	1	$I_7 = [5, 5\sqrt[3]{11}, 1 + \sqrt[3]{11} + \sqrt[3]{121}]$	25
6	0	6	1	5	1	$I_8 = [6, 6\sqrt[3]{11}, 1 + 5\sqrt[3]{11} + \sqrt[3]{121}]$	36
6	2	2	3	1	1	$I_9 = [6, 2 + 2\sqrt[3]{11}, 3 + \sqrt[3]{11} + \sqrt[3]{121}]$	12
6	3	3	1	2	1	$I_{10} = [6, 3 + 3\sqrt[3]{11}, 1 + 2\sqrt[3]{11} + \sqrt[3]{121}]$	18
8	0	8	1	3	1	$I_{11} = [8, 8\sqrt[3]{11}, 1 + 3\sqrt[3]{11} + \sqrt[3]{121}]$	64
19	0	19	6	5	1	$I_{12} = [19, 19\sqrt[3]{11}, 6 + 5\sqrt[3]{11} + \sqrt[3]{121}]$	361

We have 12 reduced ideals, not just 11 as given by the code in [7, p. 35]. The twelfth reduced ideal which is not displayed by the given code is the ideal $I_9 = [6, 2 + 2\sqrt[3]{11}, 3 + 1\sqrt[3]{11} + \sqrt[3]{121}]$, because the only triplet $(x, y, z) \in \mathbb{Z}$ verifying $2 \mid y - z$, $6 \mid x - y - 2z$, $|x + y\sqrt[3]{11} + z\sqrt[3]{121}| < 6$ and $(x - \frac{y}{2}\sqrt[3]{11} - \frac{z}{2}\sqrt[3]{121})^2 + \frac{3}{4}\sqrt[3]{121}(y - z\sqrt[3]{11})^2 < 36$ is $(0, 0, 0)$.

Example 6.3 (K is monogenic of type I)**.**
Let $K = \mathbb{Q}(\sqrt[3]{4})$, then $\mathcal{O} = \mathbb{Z}[\sqrt[3]{4}] \subsetneq \mathcal{O}_K = \left[1, \sqrt[3]{4}, \frac{\sqrt[3]{16}}{2}\right] = \mathbb{Z}[\sqrt[3]{2}]$ and $\frac{6\sqrt{3}D}{\pi} \approx 13.23$, we obtain 4 reduced ideals:

a	b	c	d	e	f	Reduced ideal	N
1	0	1	0	0	1	$[1, \sqrt[3]{4}, \sqrt[3]{16}]$	1
2	0	2	0	0	1	$[2, 2\sqrt[3]{4}, \sqrt[3]{16}]$	4
3	0	3	1	1	1	$[3, 3\sqrt[3]{4}, 1 + \sqrt[3]{4} + \sqrt[3]{16}]$	9
4	0	4	0	2	1	$[4, 4\sqrt[3]{4}, 2\sqrt[3]{4} + \sqrt[3]{16}]$	16

Example 6.4 (K is of type II, (never monogenic))**.**
Let $K = \mathbb{Q}(\sqrt[3]{10})$, then $\mathcal{O} = \mathbb{Z}[\sqrt[3]{10}] \subsetneq \mathcal{O}_K = \left[1, \sqrt[3]{10}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\right]$ and $\frac{6\sqrt{3}D}{\pi} \approx 27.54$, we obtain 6 reduced ideals:

a	b	c	d	e	f	Reduced ideal	N
1	0	1	0	0	1	$[1, \sqrt[3]{10}, \sqrt[3]{100}]$	1
2	0	1	0	0	1	$[2, \sqrt[3]{10}, \sqrt[3]{100}]$	2
2	0	2	0	0	1	$[2, 2\sqrt[3]{10}, \sqrt[3]{100}]$	4
3	0	3	1	1	1	$[3, 3\sqrt[3]{10}, 1 + \sqrt[3]{10} + \sqrt[3]{100}]$	9
6	0	6	4	4	1	$[6, 6\sqrt[3]{10}, 4 + 4\sqrt[3]{10} + \sqrt[3]{100}]$	36
9	0	9	7	4	1	$[9, 9\sqrt[3]{10}, 7 + 4\sqrt[3]{10} + \sqrt[3]{100}]$	81

References

[1] Alaca, S., Williams, K.S., *Introductory algebraic number theory*, Cambridge University Press, Cambridge, UK, 2004.

[2] Buchmann, J.A., Scheidler, R., Williams, H.C., *Implementation of a key exchange protocol using real quadratic fields*, Advances in Cryptography–EUROCRYPT'90. EUROCRYPT 1990. Lecture Notes in Computer Science (Damgård, I.B., ed.), vol. 473, Springer, Berlin, Heidelberg, 1991, pp. 98–109.

[3] Buchmann, J.A., Williams, H.C., *A key-exchange system based on imaginary quadratic fields*, J. Cryptology **1** (1988), 107–118.

[4] Buchmann, J.A., Williams, H.C., *On the infrastructure of the principal ideal class of an algebraic number field of unit rank one*, Math. Comp. **50** (182) (1988), 569–579.

[5] Buchmann, J.A., Williams, H.C., *A sub exponential algorithm for the determination of class groups and regulators of algebraic number fields*, Seminaire de Theorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhauser Boston, Boston, MA, 1990, pp. 27–41.

[6] Cohen, H., *A course in computational algebraic number theory*, Springer–Verlag, 1996.

[7] Jacobs, G.T., *Reduced ideals and periodic sequences in pure cubic fields*, Ph.D. thesis, University of North Texas, 2015, August 2015, `https://digital.library.unt.edu/ark:/67531/metadc804842`.

[8] Mollin, R., *Quadratics*, CRC Press, Inc., Boca Raton, Florida, 1996.

[9] Neukirch, J., *Algebraic Number Theory*, Springer–Verlag Berlin, Heidelberg, 1999.

[10] Payan, J., *Sur le groupe des classes d'un corps quadratique*, Cours de l'institut Fourier **7** (1972), 2–30.

[11] Prabpayak, C., *Orders in pure cubic number fields*, Ph.D. thesis, Univ. Graz. Grazer Math. Ber. 361, 2014.

*Department of Mathematics, Faculty of Sciences,
Mohammed First University,
60000 Oujda, Morocco
E-mail: abdelmalekazizi@yahoo.fr, benamarajamal@hotmail.fr, mcismaili@yahoo.fr

**Regional center of Education and Training,
60000 Oujda, Morocco
E-mail: talbimm@yahoo.fr