MATHEMATICA, 63 (86), N° 1, 2021, pp. 13–22

CYCLES OF REDUCED IDEALS AND CLASS NUMBER OF PURE CUBIC NUMBER FIELD

ABDELMALEK AZIZI, JAMAL BENAMARA, MOULAY CHRIF ISMAILI, and MOHAMMED TALBI

Abstract. For some pure cubic field K, we compute the class number of K based on the notion of reduced ideals and the notion of the minimum of an ideal.

MSC 2010. Primary 11R16, 11R29; Secondary 11T71.

Key words. Cubic field, minimum of ideal, reduced ideal, cycle of reduced ideal.

1. INTRODUCTION

The calculation of the class number of a number field has always been an interesting problem. Several methods are known in this subject, namely the method using analytic formulas, the method using modular forms and others. The reduced ideals, too, play a very important role in some methods of calculating the class number of quadratic fields and this has prompted us to think of exploiting them again on the pure cubic fields whose purpose, in the first place, is to provide a method of calculating the class number of an order of a pure cubic field. On the imaginary quadratic field it is proved that there are at most two reduced ideals in any class and, when two distinct such ideals are in a class, they are conjugated. Thus, eliminating the conjugates in question, the number of classes is exactly the number of reduced ideals. In the case of a real quadratic field, examples show that one class can contain several reduced ideals which are connected by a specific equivalence relation and form a cycle, therefore, the idea is to represent each class of ideals by such a cycle. In the quadratic case, different methods describe the construction steps of these cycles: the method using the notion of continued fractions (see [5]), the method using the notion of the root of an ideal (see [7]) and the method using the quadratic forms (see [3]). In addition to these notions used on quadratic fields, another very important notion is that of the convergent of an ideal (see [1]) or its equivalent term which is the minimum of an ideal (see [2]).

Let K be a number field of degree n over $\mathbb{Q}$ and $\mathcal{O}_K$ its ring of integers. Let $\sigma_1, \ldots, \sigma_n$ be the n embedding of K in $\mathbb{C}$. For all units u of $\mathcal{O}_K$ we have the following property: $\mathcal{O}_K$ does not contain any non-zero element α such that $\forall i \in \{1, \ldots, n\}$, $|\sigma_i(\alpha)| < |\sigma_i(u)|$, because $|N_{K/\mathbb{Q}}(u)| = 1$ and $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

DOI: 10.24193/mathcluj.2021.1.02

On the other hand, if I is an ideal of $\mathcal{O}_K$, then for every element $\mu \in I$ of minimal nonzero norm, there is no non-zero element $\alpha \in I$ such that $\forall i \in \{1, \dots, n\}$, $|\sigma_i(\alpha)| < |\sigma_i(\mu)|$. In general, this property does not characterize only the units of $\mathcal{O}_K$ and the elements of minimal nonzero norm of I, but there are many more elements of $\mathcal{O}_K$ checking this property, these elements are called the minimums of an ideal. The connection between the notion of reduced ideal and that of the minimum of an ideal is based on the fact that an ideal I of $\mathcal{O}_K$ is reduced if and only if the smallest positive integer belonging to I is a minimum of I, this link can be better used, first, to show that each class contains at least one reduced ideal and to identify the reduced ideals in each class, which makes it possible to form a cycle of reduced ideals in each class. Second, to prove that the set of reduced ideals of $\mathcal{O}_K$ is finite and therefore the class number of $\mathcal{O}_K$ is equal to the number of cycles of reduced ideals.

In this paper we consider the pure cubic fields $K = \mathbb{Q}(\sqrt[3]{D})$, where D is square-free integer and $\not\equiv \pm 1 \pmod 9$, in this case we have $\mathcal{O}_K = \mathbb{Z}(\sqrt[3]{D})$. As in [4], we can determine all the reduced ideals of $\mathcal{O}_K$ and we use the cycle of minimums of an ideal, but not as it is considered in [2], to build a cycles of reduced ideals of $\mathcal{O}_K$; the number of this cycles is exactly the class number of K. Note that the procedure and the calculations are the same for the general case of a pure cubic field.

2. MINIMUM OF AN IDEAL

Let $K = \mathbb{Q}(\sqrt[3]{D})$ be a pure cubic number field, where D is square-free integer and $\not\equiv \pm 1 \pmod 9$, if we put $\theta = \sqrt[3]{D}$, then we know that $\mathcal{O}_K = \mathbb{Z}[\theta] = [1, \theta, \theta^2]$ is the ring of integers of K and $\Delta_K = -27D^2$ its discriminant. The embedding of K in $\mathbb{C}$ are the identity and the pairs of complex $\mathbb{Q}$-isomorphisms $(\sigma, \overline{\sigma})$, with $\sigma(\theta) = \zeta\theta$ and $\overline{\sigma}(\theta) = \zeta^2\theta$, where $\zeta = \mathrm{e}^{2i\pi/3}$.

Definition 2.1. Let I be a fractional ideal of $\mathcal{O}_K$. We say that a non-zero element $\mu \in I$ is a minimum of I, if I does not contain any non-zero element α verifying $|\alpha| < |\mu|$ and $|\sigma(\alpha)| < |\sigma(\mu)|$.

If μ is a minimum of I, then for all $\alpha \in I$ we have

$$|\alpha| < |\mu| \text{ and } |\sigma(\alpha)| < |\sigma(\mu)| \Longrightarrow \alpha = 0.$$

Every element in I of minimal nonzero norm is a minimum of I.

Proposition 2.2. *If μ is a minimum of I then $\alpha\mu$ is a minimum of αI for all $\alpha \in K^*$. In particular, if u is a unit of $\mathcal{O}_K$, then $u\mu$ is a minimum of I.*

Proof. Let $\beta \in \alpha I$ ($\beta = \alpha\lambda$ with $\lambda \in I$) such that $|\beta| < |\alpha\mu|$ and $|\sigma(\beta)| < |\sigma(\alpha\mu)|$, hence $|\alpha\lambda)| < |\alpha\mu|$ and $|\sigma(\alpha)\sigma(\lambda)| < |\sigma(\alpha)\sigma(\mu)|$, and, since $\alpha \neq 0$, it follow that $|\lambda| < |\mu|$ and $|\sigma(\lambda)| < |\sigma(\mu)|$, consequently $\lambda = 0$, therefore $\beta = 0$. $\square$

Let us denote by M_I the set of minimums of I and by C_I the set of minimums of I not associated two by two and we call the latter a cycle of minimums of I.

PROPOSITION 2.3. *Let I be an ideal of $\mathcal{O}_K$. Then C_I is finite.*

Proof. If μ is a minimum of the ideal I, then, by [6, Theorem 5.3, p. 32], we have $|\mu||\sigma(\mu)||\overline{\sigma}(\mu)| \leq \frac{2}{\pi}\sqrt{|\Delta_K|}N(I)$ hence $|N(\mu)| \leq \frac{2}{\pi}\sqrt{|\Delta_K|}N(I)$, up to multiplication by units there are only finitely many elements in I whose absolute norm is increased by the constant $\frac{2}{\pi}\sqrt{|\Delta_K|}N(I)$, hence the result. □

If $C_I = \{\mu_1, \ldots, \mu_m\}$, then we can find another set of minimums of I not associated two by two, for example $C'_I = \{u\mu_1, \ldots, u\mu_m\}$, where u is in U_K, the unit group of $\mathcal{O}_K$.

THEOREM 2.4. *Let I and J be two ideals of $\mathcal{O}_K$. Let μ be a minimum of I and η be a minimum of J. Then the following conditions are equivalent:*

(1) *I and J are equivalent;*
(2) *there is a unique μ' in C_I such that $\mu'^{-1}I = \eta^{-1}J$;*
(3) *there is a unique η' in C_J such that $\mu^{-1}I = \eta'^{-1}J$.*

Proof. We have (2) $\Longrightarrow$ (1) is clear. Conversely, if I and J are equivalent, then there is $\gamma \in K$ such that $I = \gamma J$ and, since η is a minimum of J, $\gamma\eta$ is a minimum of I, hence there is $\mu' \in C_I$ such that $\gamma\eta = \mu' u$ with $u \in U_K$, therefor we have $(\mu' u)^{-1}I = (\gamma\eta)^{-1}I$, hence $\mu'^{-1}I = \eta^{-1}J$. If there is another minimum $\mu'' \in C_I$ such that $\mu''^{-1}I = \eta^{-1}J$, then $\mu''^{-1}I = \mu'^{-1}I$, so μ' and μ'' are associated, hence the uniqueness of μ' in C_I holds and finally we have (1) $\Longrightarrow$ (2). We show that (1) $\Longleftrightarrow$ (3) in the same way. □

COROLLARY 2.5. *Let I and J be two ideals of $\mathcal{O}_K$. If I and J are equivalent, then C_I and C_J have the same cardinal.*

3. REDUCED IDEALS AND MINIMUM

DEFINITION 3.1. We say that an ideal I of $\mathcal{O}_K$ is primitive, if I is without rational factor. Otherwise, if there is no prime number p such that $I \subset p\mathcal{O}$.

DEFINITION 3.2. We will say that an ideal I of $\mathcal{O}_K$ is reduced, if I is primitive and $\ell(I)$ is a minimum of I, where $\ell(I)$ is the smallest positive non-zero element in $I \cap \mathbb{Z}$, and called the length of I.

A fractional ideal I of $\mathcal{O}_K$ is reduced if 1 is a minimum of I.

PROPOSITION 3.3. *Let I be an ideal of $\mathcal{O}_K$. If μ is a minimum of I, then $\mu^{-1}I$ is reduced.*

Proof. If μ is a minimum of I then, by Proposition 2.2, we have $1 = \mu^{-1}\mu$ is a minimum of $\mu^{-1}I$, hence $\mu^{-1}I$ is reduced. □

Theorem 3.4. *The number of reduced ideals of $\mathcal{O}_K$ is finite. We note it by r_K.*

Proof. See [4]. □

Theorem 3.5. *Let I be an ideal of $\mathcal{O}_K$ and let $\mu \in M_I$. Then there is a non-zero positive integer d such that $d\mu^{-1}I$ is a reduced ideal of $\mathcal{O}_K$.*

Proof. The ideal $\mu^{-1}I$ is fractional, so there is an integer d such that $d\mu^{-1}I \subset \mathcal{O}_K$. The smallest positive d such that $d\mu^{-1}I \subset \mathcal{O}_K$ is called the denominator of $\mu^{-1}I$ with respect to $\mathcal{O}_K$. since $\mu \in M_I$ then $1 = \mu\mu^{-1}$ is a minimum of $\mu^{-1}I$ and therefor d is a minimum of $d\mu^{-1}I$ which is primitive, in addition we have $d = \ell(d\mu^{-1}I)$ hence $d\mu^{-1}I$ is a reduced ideal of $\mathcal{O}_K$. □

The last proposition proves that every class of ideals contains a reduced ideal and the last theorem proves that the number of reduced ideals in $\mathcal{O}_K$ is finite, and therefore we have $h_K \leqslant r_K$, where we have the idea of exploiting reduced ideals which comes from the determination of the class number of K, as already done on quadratic fields.

Remark 3.6. Let I be an ideal of $\mathcal{O}_K$. The number of reduced integral ideals in the class of I is exactly the cardinal of C_I.

Now, as in [4], we can find all the reduced ideals of $\mathcal{O}_K$. First of all, a reduced ideal of $\mathcal{O}_K$ is a sub-$\mathbb{Z}$-module of $\mathcal{O}_K$, and hence it is of the form

$$I = [a,\ b + c\theta,\ d + e\theta + f\theta^2],$$

where $a,\ b,\ c,\ d,\ e$ and f are integers such that $0 \leq b,\ d < a,\ 0 \leq e < c,\ 0 < f$. The norm of I is $N(I) = [\mathcal{O}_K : I] = acf$, and $\ell(I) = a$. A sub-$\mathbb{Z}$-module $I = [a,\ b + c\theta,\ d + e\theta + f\theta^2]$ of $\mathcal{O}_K$ is not always an ideal of $\mathcal{O}_K$, for it to be, it is necessary and sufficient that we have the following conditions:

(1) f divides the integers $a,\ b,\ c,\ d$ and e;
(2) c divides the integers a and b;
(3) cf divides the integers $df - \mathrm{e}^2$ and $Df^2 - de$;
(4) acf divides the integers $bce - b^2f - c^2d$, $Dc^2f + b^2e - bcd$, $Dcf^2 - bdf + b\mathrm{e}^2 - cde$ and $Dcef - Dbf^2 + bde - cd^2$.

The ideal $I = [a,\ b + c\theta,\ d + e\theta + f\theta^2]$ is primitive if and only if $f = 1$.

To determine the list of all reduced ideals $I = [a, b + c\theta, d + e\theta + \theta^2]$ in $\mathcal{O}_K$ we determine at first all the primitive ideals of $\mathcal{O}_K$ 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 $c \mid b$ and after we determine the possible values of integers d and e such that $0 \leq d < a$ and $0 \leq e < c$ and according to the divisibility conditions above after the substitution of f by 1 .

The Primitive ideals whose length is strictly less than $\theta = \sqrt[3]{D}$ are therefore included in the sought list, and those whose length is such that $\sqrt[3]{D} \leq \ell(I) \leq$

$\frac{6\sqrt{3}D}{\pi}$, we apply to it the following theorem which is the equivalent of [4, Theorem 2.8].

THEOREM 3.7. *Let $K = \mathbb{Q}(\theta)$ with $\theta^3 = D$ where D 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 $\mathcal{O}$. Then I is reduced if and only if the only triple of integers (x, y, z) satisfying :*

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

is $(0, 0, 0)$.

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

Let's suppose that ideal $I = [a, b+c\theta, d+e\theta+\theta^2]$ is reduced. Let (x, y, z) be a triple of integers such that $c \mid y - ze$ and $ac \mid cx - by + (be - cd)z$ satisfying:

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

Put $X = \frac{cx-by+(be-cd)z}{ac}$, $Y = \frac{y-ze}{c}$ and $Z = z$, then we have $x = aX + bY + dZ$ and $y = cY + eZ$, therefore

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

still

$$\begin{cases} |aX + Y(b + c\theta) + Z(d + e\theta + \theta^2)| < \ell(I) \\ |(aX + bY + dZ - \frac{cY+eZ}{2}\theta - \frac{Z}{2}\theta^2) + i\frac{\sqrt{3}}{2}\theta(cY + eZ - Z\theta)| < \ell(I), \end{cases}$$

therefore

$$\begin{cases} |aX + Y(b + c\theta) + Z(d + e\theta + \theta^2)| < \ell(I) \\ |(aX + Y(b - \frac{c\theta}{2} + i\frac{\sqrt{3}c\theta}{2}) + Z(d - \frac{e\theta}{2} + i\frac{\sqrt{3}e\theta}{2} - \frac{1+i\sqrt{3}}{2}\theta^2)| < \ell(I), \end{cases}$$

hence

$$\begin{cases} |aX + Y(b + c\theta) + Z(d + e\theta + \theta^2)| < \ell(I) \\ |(aX + Y(b + c\zeta\theta) + Z(d + e\zeta\theta + \zeta^2\theta^2)| < \ell(I). \end{cases}$$

Let $\alpha = Xa+Y(b+c\theta)+Z(d+e\theta+\theta^2)$, then $\alpha \in I$, $|\alpha| < \ell(I)$ and $|\alpha'| < \ell(I)$. Since I is reduced, then $\alpha = Xa + Y(b + c\theta) + Z(d + e\theta + \theta^2)$ must be zero, then $X = Y = Z = 0$, therefore $x = y = z = 0$.

Conversely, let $I = [a, b + c\theta, d + e\theta + \theta^2]$ be a primitive ideal of $\mathcal{O}$, and let's suppose that for any triples of integers (x, y, z) such that $c \mid y - ze$ and

$ac \mid cx - by + (be - cd)z$ satisfying

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

is zero.

Given that $\alpha = Xa + Y(b + c\theta) + Z(d + e\theta + \theta^2) \in I$ such that $|\alpha| < \ell(I)$ and $|\alpha'| < \ell(I)$, then

$$\begin{cases} |Xa + Y(b + c\theta) + Z(d + e\theta + \theta^2)| < \ell(I) \\ |Xa + Y(b + c\zeta\theta) + Z(d + e\zeta\theta + \zeta^2\theta^2)| < \ell(I), \end{cases}$$

still

$$\begin{cases} |aX + Y(b + c\theta) + Z(d + e\theta + \theta^2)| < \ell(I) \\ (aX + Y(b - \frac{c\theta}{2}) + Z(d - \frac{e\theta}{2} - \frac{\theta^2}{2}))^2 + \frac{3}{4}\theta^2(cY + eZ - Z\theta)^2 < \ell(I)^2, \end{cases}$$

hence

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

Put $x = aX + bY + dZ$, $y = cY + eZ$ and $z = Z$, then $c \mid y - ze$, $ac \mid cx - by + (be - cd)z$, and we will have

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

By hypothesis we have $x = y = z = 0$, so $X = Y = Z = 0$, hence $\alpha = 0$. $\square$

This theorem can be represented in the python code as in the following:

```
def isReduced (a,b,c,d,e,m):
  alpha=math.exp(math.log(m)/3)
  reduced = 1
  for x in range (-a+1,a):
    for y in range (-int(a/alpha),1+int(a/alpha)):
      for z in range (-int(a/alpha**2),1+int(a/alpha**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*alpha+z*alpha**2)<a) and \
                 ((x+y*alpha+z*alpha**2)>-a):
                if (x-((y*alpha)/2)-((z*(alpha**2))/2))**2 \
                    +(3/4)*(y*alpha-z*alpha**2)**2<a**2:
                  reduced =0
                  return reduced
  return reduced
```

4. THE CYCLES OF REDUCED IDEALS OF $\mathcal{O}_K$

Let I be an ideal of $\mathcal{O}_K$ and let $C_I = \{\mu_1, \mu_2, \ldots, \mu_m\}$ be a cycle of minimums of I. By Theorem 3.5, for all $i \in \{1, \ldots, m\}$, we obtain a reduced ideal $I_i = d_i\mu_i^{-1}I$ where $d_i = \ell(d_i\mu_i^{-1}I) = \ell(I_i)$. For $i \neq j$ we can't have $I_i = I_j$, if not, we will have $\mu_i = u\mu_j$, with $u \in U_K$, which is not possible, hence, by $C_I = \{\mu_1, \mu_2, \ldots, \mu_m\}$, we can build a set of reduced ideals $\{I_1, \ldots, I_m\}$ in the class of I - this set is called a cycle of reduced ideals in the class of I and we denote it by $C_r(I)$.

THEOREM 4.1. *Let J and J' be two reduced ideals of $\mathcal{O}_K$. The following two assertions are equivalent:*

(1) *The ideals J and J' are equivalent.*
(2) *The ideals J and J' belong to the same cycle.*

Proof. If the ideals J and J' belong to the same cycle then there is μ and $\mu' \in C_I$ for some ideal I of $\mathcal{O}_K$ such that $J = d\mu^{-1}I$ and $J' = d'\mu'^{-1}I$ hence $d\mu^{-1}J' = d'\mu'^{-1}J$, so J and J' are equivalent. Conversely, if the ideals J and J' are equivalent so they are in the same class of an ideal I, since J and J' are reduced then $\ell(J)$ is a minimum of J and then $\ell(J')$ is a minimum of J' and by Theorem 2.4 there is a unique μ_k in C_I such that $\mu_k^{-1}I = \ell(J)^{-1}J$, so $d_k\mu_k^{-1}I = d_k\ell(J)^{-1}J$, and since $d_k = \ell(J)$ then we have $J = d_k\mu_k^{-1}I$. Likewise, for J', there is a unique μ_t in C_I such that $\mu_t^{-1}I = \ell(J')^{-1}J'$, so $d_t\mu_t^{-1}I = d_t\ell(J')^{-1}J'$, and, since $d_t = \ell(J')$, we have $J' = d_k\mu_k^{-1}I$, therefore J and J' belong to the same cycle formed by C_I. □

COROLLARY 4.2. *The set of reduced ideals of $\mathcal{O}_K$ is partitioned into a cycle of reduced ideals, the number of these cycles is equal to the class number of K.*

Proof. Each class $[I]$ corresponds to one and only one cycle $C_r(I)$. □

Remember that the unit group of $\mathcal{O}_K$ is of the form $U_K = \{\pm\varepsilon_0^k \mid k \in \mathbb{Z}\}$, where ε_0 is the fundamental unit of $\mathcal{O}_K$ and we have the following result.

THEOREM 4.3. *Let I be a reduced ideal of $\mathcal{O}_K$. Then there is one and only one of the cycles of minimums of I in the interval $[\ell(I), \ell(I)\varepsilon_0[$. It is called the fundamental cycle of minimums of I. In particular, the fundamental cycle of minimums of $\mathcal{O}_K$ is in the interval $[1, \varepsilon_0[$.*

Proof. Let $\eta \in M_I$ with $\eta > 0$. If $\eta \geq \ell(I)\varepsilon_0$, let k the largest positive integer such that $\eta \geq \ell(I)\varepsilon_0^k$, (it is clear that $k \geq 1$), therefore $\eta < \ell(I)\varepsilon_0^{k+1}$, and so we have $\ell(I)\varepsilon_0^k \leq \eta < \ell(I)\varepsilon_0^{k+1} \Rightarrow \ell(I) \leq \eta\varepsilon_0^{-k} < \ell(I)\varepsilon_0$, and then we impose $\mu = \eta\varepsilon_0^{-k}$.

If $\eta < \ell(I)$, let k be the smallest positive integer such that $\ell(I)\varepsilon_0^{-k} \leq \eta$, therefore $\eta < \ell(I)\varepsilon_0^{-(k-1)}$. Then we have $\ell(I) \leq \eta\varepsilon_0^k < \ell(I)\varepsilon_0$, and we impose $\mu = \eta\varepsilon_0^k$. Consequently, each $\eta \in M_I$ is associated with a minimum μ of I belonging to $[\ell(I), \ell(I)\varepsilon_0[$, therefore, if $C_I' = \{\eta_1, \ldots, \eta_m\}$ is a cycle of minimums of I, then, for all $i \in \{1,\ldots,m\}$, there is $\mu_i \in [\ell(I), \ell(I)\varepsilon_0[$ and $u_i \in U_K$ such that $\mu_i = u_i\eta_i$, hence the searched cycle is $C_I = \{\mu_1,\ldots,\mu_m\}$.

Suppose that there is an other cycle $C'_I = \{\nu_1,\ldots,\nu_m\}$ of I in $[\ell(I), \ell(I)\varepsilon_0[$, then $\nu_j = \mu_i\varepsilon_0^k$, and, if $\nu_j < \mu_i$, then we will have $\ell(I) < \mu_i\varepsilon_0^k < \mu_i < \ell(I)\varepsilon_0$, so by $\mu_i\varepsilon_0^k < \mu_i$ we have $k < 0$, and, by $\ell(I)\varepsilon_0^{-k} < \mu_i < \ell(I)\varepsilon_0$, we have $-1 < k$, contradiction. The same reasoning works if $\nu_j > \mu_i$. □

Corollary 4.4. *Let I be a reduced ideal of $\mathcal{O}_K$. If $\mu \in M_I$ and $\mu \in [\ell(I), \ell(I)\varepsilon_0[$, then $\mu \in C_I$.*

Remark 4.5.
(1) The fundamental cycle of minimums of a reduced ideal I is of the form $C_I = \{\mu_1 = \ell(I), \mu_2, \ldots, \mu_m\}$ and every minimum μ of I is of the form $\mu = \pm\mu_i\varepsilon_0^k$ with $1 \le i \le m$ and $k \in \mathbb{Z}$.
(2) If $\mu \in C_I$ and $\mu \neq \ell(I)$, then we have $\ell(I) < \mu < \ell(I)\varepsilon_0$ and therefore $|\sigma(\mu)| \le \ell(I)$, if we represent μ by the point $(x,y,z) \in \mathbb{Z}^3$, then we can search the elements of C_I in the set $S = \{(x,y,z) \in \mathbb{Z}^3 \mid \ell(I) < x + y\theta + z\theta^2 < \ell(I)\varepsilon_0;\ (x - \frac{y}{2}\theta - \frac{z}{2}\theta^2)^2 + \frac{3}{4}\theta^2(y - z\theta)^2 < \ell(I)^2\}$.

Theorem 4.6. *The ring of integers $\mathcal{O}_K$ is principal if and only if for every reduced ideal I of $\mathcal{O}_K$ there is $\mu \in C_{\mathcal{O}_K}$ such that $I = (\ell(I)\mu^{-1})$.*

Proof. Let I be any fractional ideal of $\mathcal{O}_K$. If η is a minimum of I, then $\eta^{-1}I$ is reduced, therefore $J = d\eta^{-1}I$ is a reduced ideal of $\mathcal{O}_K$, where d is as in the proof of Theorem 3.5, and, by hypothesis, there is $\mu \in C_{\mathcal{O}_K}$ such that $J = (\ell(J)\mu^{-1})$, it follow that $d\eta^{-1}I = (\ell(J)\mu^{-1})$, hence I is principal.

Conversely, suppose that $\mathcal{O}_K$ is principal. Let I be a reduced ideal of $\mathcal{O}_K$, therefore $\ell(I)$ is a minimum of I, and, since I is principal, then it is equivalent to $\mathcal{O}_K$ and it follows, by Theorem 2.4, that there is $\mu \in C_{\mathcal{O}_K}$ such that $I = (\ell(I)\mu^{-1})$. □

We can interpret this as follows. The ring of integers $\mathcal{O}_K$ is principal if and only if every reduced ideal is principal if and only if the cardinal of $C_{\mathcal{O}_K}$ is equal to r_K.

5. NUMERICAL EXAMPLES

Example 5.1. Let $D = 5$, $K = \mathbb{Q}(\sqrt[3]{5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$, $\varepsilon_0 = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{25}$ and $\frac{6\sqrt{3}D}{\pi} \approx 16.539866862653763$.

We have five reduced ideals ($r_K = 5$) listed in the following table with their norms.

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

The ideal $I_1 = \mathcal{O}_K$ have five minimum listed in the following table, and hence we have one cycle of reduced ideals in the second column.

$C_{I_1} = C_{\mathcal{O}_K}$	$N(\mu_i)$	1 Cycle: $C_r(I_1) = \{I_1, I_2, I_3, I_4, I_5\}$
$\mu_1 = 1$	1	$\mathcal{O}_K$
$\mu_2 = 3 + 2\sqrt[3]{5} + \sqrt[3]{25}$	2	$\frac{1}{3+2\sqrt[3]{5}+\sqrt[3]{25}} I_1 = \frac{1}{2} I_3$
$\mu_3 = 9 + 5\sqrt[3]{5} + 3\sqrt[3]{25}$	4	$\frac{1}{9+5\sqrt[3]{5}+3\sqrt[3]{25}} I_1 = \frac{1}{2} I_2$
$\mu_4 = 12 + 7\sqrt[3]{5} + 4\sqrt[3]{25}$	3	$\frac{1}{12+7\sqrt[3]{5}+4\sqrt[3]{25}} I_1 = \frac{1}{3} I_4$
$\mu_5 = 29 + 17\sqrt[3]{5} + 10\sqrt[3]{25}$	4	$\frac{1}{29+17\sqrt[3]{5}+10\sqrt[3]{25}} I_1 = \frac{1}{4} I_5$

We find again $h_K = 1$.

EXAMPLE 5.2. Let $D = 7,\ K = \mathbb{Q}(\sqrt[3]{7}),\ \mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}],\ \varepsilon_0 = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$ and $\frac{6\sqrt{3}D}{\pi} \approx 23.155813607715267$.

We obtain eight reduced ideals ($r_K = 8$) listed 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

The ideal I_1 has two minimums, I_2 has three minimums and I_3 has three minimums as in the following table:

	minimums	norm of minimum
C_{I_1}	$\mu_1 = 1$	1
	$\mu_2 = 3 + 2\sqrt[3]{7} + \sqrt[3]{49}$	6
C_{I_2}	$\eta_1 = 2$	8
	$\eta_2 = 1 + \sqrt[3]{7}$	8
	$\eta_3 = 3 + 2\sqrt[3]{7} + \sqrt[3]{49}$	6
C_{I_3}	$\nu_1 = 2$	8
	$\nu_2 = 3 + \sqrt[3]{7} + \sqrt[3]{49}$	20
	$\nu_3 = 6 + 4\sqrt[3]{7} + 2\sqrt[3]{49}$	48

hence we obtain three cycles of reduced ideals as in the following table:

3 cycle of reduced ideals		
$\{I_1 = \mathcal{O}_K, I_7\}$	$\{I_2, I_5, I_4\}$	$\{I_3, I_6, I_8\}$
$\frac{1}{\mu_2} I_1 = \frac{1}{6} I_7$	$\frac{1}{\eta_2} I_2 = \frac{1}{4} I_5$	$\frac{1}{\nu_2} I_3 = \frac{1}{5} I_6$
	$\frac{1}{\eta_3} I_2 = \frac{1}{3} I_4$	$\frac{1}{\nu_3} I_3 = \frac{1}{12} I_8$

We find again $h_K = 3$.

REFERENCES

[1] H. Appelgate and H. Onishi, *Periodic expansions of modules and its relation to units*, J. Number Theory, **15** (1982), 283–294.

[2] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J. Number Theory, **26** (1987), 8–30.

[3] H. Cohen, *A course in computational algebraic number theory*, 3rd ed., Springer-Verlag, 1996.

[4] G.T. Jacobs, *Reduced ideals in pure cubic fields*, arXiv:1905.00242v3.

[5] R.A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996.

[6] J. Neukirch, *Algebraic number theory*, Springer-Verlag, New York, 1999.

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

Received June 20, 2019
Accepted May 22, 2020

Mohammed First University
Faculty of Sciences
Department of Mathematics
60000, Oujda, Morocco
E-mail: abdelmalekazizi@yahoo.fr
https://orcid.org/0000-0002-0634-1995
E-mail: benamarajamal@hotmail.fr
https://orcid.org/0000-0003-0303-0355
E-mail: mcismaili@yahoo.fr

Regional center of Education and Training
60000, Oujda, Morocco
E-mail: talbimm@yahoo.fr
https://orcid.org/0000-0001-5430-3144