Revista de la Unión Matemática Argentina — Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

PRINCIPALITY BY REDUCED IDEALS IN PURE CUBIC NUMBER FIELD

JAMAL BENAMARA AND MOHAMMED TALBI

Abstract. This paper describes a method for determining the list of reduced ideals of any pure cubic number field, which we can use for testing the principality of these fields and give a generator for a principal ideal.

1. Introduction

The notion of a reduced ideal can be used to compute the regulator and the class number of a number field, see [3, 11]. Besides, it can be used in cryptography as in [4, 5] where the authors sketched the first Diffie-Hellman protocol which does not require a group structure, namely on the set of reduced principal ideals of a real quadratic field. Most of the work on reduced ideals is realized on quadratic fields, see for example [9]. In [8] (respectively [2]), the authors describe a method for finding all reduced ideals of the ring of integers of a monogenic pure cubic field (respectively of a special order of any pure cubic field). In this paper, we give a complete overview on the reduced ideals in any pure cubic number field and we provide a method which allows us to determine the set of reduced ideals. In addition, we develop the notion of a minimum of an ideal and its relation with the reduced ideal to study the principality of the ring of integers. Then, we give a procedure to find a generator of a principal ideal. Finally we illustrate the results by two examples to improve the readability and the flow paper.

Throughout this paper, we consider a pure cubic number field $K = \mathbb{Q}(\sqrt[3]{D})$, where $D > 1$ is a cube-free integer. We may assume with no loss of generality that $D = rs^2$ where r and s are square-free, and $(r, s) = 1$. It is well known (see for example [1, 7]) that if $D \not\equiv \pm 1 \pmod 9$, then the ring of integers $\mathcal{O}_K$ has a basis $\left[1, \theta, \delta = \theta^2/s\right]$ where $\theta = \sqrt[3]{D}$ and the discriminant of K is $\Delta_K = -27r^2s^2$. In this case, K is called a pure cubic field of the first kind. If $D \equiv \pm 1 \pmod 9$, then $\mathcal{O}_K = \left[1, \theta, \delta = (1 + r\theta + \theta^2)/3\right]$, $\Delta_K = -3r^2s^2$ and K is called a pure cubic field of the second kind. When there exists $\vartheta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\vartheta]$, we say that K is monogenic (for example, when D is square-free ($s = 1$) and $D \not\equiv \pm 1 \pmod 9$, $\mathcal{O}_K = \mathbb{Z}[\theta]$), in this case, we find the results as in [8].

We also recall that an order $\mathcal{O}$ of K is a sub-ring of K which as a $\mathbb{Z}$-module is finitely generated and of maximal rank $[K : \mathbb{Q}] = 3$, see [12]. This equivalent to

2020 *Mathematics Subject Classification.* 11Y40, 13F10, 11H06, 11R16, 13A15.

Key words and phrases. Cubic field; Reduced ideal; Minimum of ideal; Principality.

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

say that $\mathcal{O} \subset \mathcal{O}_K$ and $[\mathcal{O}_K : \mathcal{O}] < \infty$ (for example $\mathcal{O} = \mathbb{Z}[\theta]$), in this case, we find the results as in [2].

In general, we denote by λ' and λ'' the conjugate roots of any $\lambda \in K$. Therefore the norm of λ is $\mathcal{N}(\lambda) = \lambda\lambda'\lambda''$ and we know that $\theta' = \theta\zeta$ and $\theta'' = \theta\zeta^2$ where $\zeta = exp(2i\pi/3)$. Note: in a field $\mathbb{Q}(\sqrt[3]{D})$,

$$\mathcal{N}(x + y\sqrt[3]{D} + z\sqrt[3]{D^2}) = x^3 + y^3D + z^3D^2 - 3xyzD.$$

And by the Dirichlet theorem, we know that the units group $\mathcal{U}_K$ of K is of rank one and we note by ε_0 the fundamental unit of K.

2. Arithmetic of ideals in pure cubic fields

We will be treating ideals as special kinds of $\mathbb{Z}$-modules. We recall that I is an ideal of $\mathcal{O}_K$ if $I \subset \mathcal{O}_K$ and for all $\alpha, \beta \in I$ and $\lambda \in \mathcal{O}_K$ we have $\alpha + \beta \in I$ and $\lambda\alpha \in I$.

Proposition 2.1. *Let K be a pure cubic number field and $\mathcal{O} = [1, \phi, \psi]$ be an order of K. Then every non-zero ideal I of $\mathcal{O}$ has a representation*

$$I = [a, b + c\phi, d + e\phi + f\psi]$$

where $a, b, c, d, e, f \in \mathbb{Z}$, $0 \le b < a$, $0 \le d < a$, $0 \le e < c$ and $0 < f$. This basis will be called the HNF-basis (Hermite Normal Form) of I. In addition, the integer a is the smallest positive element of $I \cap \mathbb{Z}$ and the norm of I is $N(I) = acf$. The integer a is called the length of I and we denote it $\ell(I)$.

Proof. Every ideal of $\mathcal{O}$ is a sub-$\mathbb{Z}$-module of $\mathcal{O}$, the rest follows by [6, theorem 4.7.3] and [6, proposition 4.7.4]. □

Theorem 2.2 (Uniqueness of the coefficients)**.** *Let $\mathcal{O} = [1, \phi, \psi]$ be an order of K. Let I_1 and I_2 be two ideals of $\mathcal{O}$ with HNF-basis $[a_1, b_1 + c_1\phi, d_1 + e_1\phi + f_1\psi]$ and $[a_2, b_2 + c_2\phi, d_2 + e_2\phi + f_2\psi]$ successively. Then $I = J$ if and only if $a_1 = a_2$, $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, $e_1 = e_2$ and $f_1 = f_2$.*

Proof. If $I_1 = I_2$, then $I_1 \subseteq I_2$, hence a_1, $b_1 + c_1\phi$ and $d_1 + e_1\phi + f_1\psi \in I_2$, which means that $a_2|a_1$, $c_2|c_1$, $f_2|f_1$, $b_1c_2 \equiv b_2c_1 \pmod{a_2c_2}$, $e_1f_2 \equiv e_2f_1 \pmod{c_2f_2}$ and $d_1c_2f_2 + b_2f_1e_2 \equiv b_2e_1f_2 + c_2d_2f_1 \pmod{a_2c_2f_2}$. On the other hand, we have $I_2 \subseteq I_1$, then a_2, $b_2 + c_2\phi$ and $d_2 + e_2\phi + f_2\psi \in I_1$, which means that $a_1|a_2$, $c_1|c_2$, $f_1|f_2$, $b_2c_1 \equiv b_1c_2 \pmod{a_1c_1}$, $e_2f_1 \equiv e_1f_2 \pmod{c_1f_1}$ and $d_2c_1f_1 + b_1f_2e_1 \equiv b_1e_2f_1 + c_1d_1f_2 \pmod{a_1c_1f_1}$. Directly, we get $a_1 = a_2$, $c_1 = c_2$ and $f_1 = f_2$, therefore $b_1 \equiv b_2 \pmod{a_1}$, and since $0 \le b_1 < a_1$ and $0 \le b_2 < a_1$, we get $b_1 = b_2$. by the same way we get $e_1 = e_2$ and $d_1 = d_2$. □

Sometimes we write $I = [a, \alpha, \beta]$ with $\alpha = b + c\phi$ and $\beta = d + e\phi + f\psi$.

Definition 2.3. Let $\mathcal{O} = [1, \phi, \psi]$ be an order of K. We will say that an ideal I of $\mathcal{O}$ is primitive if there is no integer $n > 1$ such that $I \subset n\mathcal{O}$.

The ideal $I = [a, b + c\phi, d + e\phi + f\psi]$ is primitive if $gcd(a, b, c, d, e, f) = 1$.

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

Theorem 2.4 (Criterion for ideal equality)**.** *If $I = [a, \alpha, \beta]$ is a primitive ideal of $\mathcal{O}_K$, then*
$I = [a, ma \pm \alpha, na + p\alpha \pm \beta]$ for any $m, n, p \in \mathbb{Z}$.

Proof. We have

$$\begin{pmatrix} a \\ ma \pm \alpha \\ na + p\alpha \pm \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ m & \pm 1 & 0 \\ n & p & \pm 1 \end{pmatrix} \begin{pmatrix} a \\ \alpha \\ \beta \end{pmatrix}$$

and $M = \begin{pmatrix} 1 & 0 & 0 \\ m & \pm 1 & 0 \\ n & p & \pm 1 \end{pmatrix} \in GL_3(\mathbb{Z})$, the group of all 3×3 matrices with coefficient integers and determinants equal ± 1. □

Note that the converse of the proposition 2.1 is false. Indeed, if we consider $\mathcal{O} = \mathbb{Z}[\theta] = \left[1, \theta, \theta^2\right]$, the sub-$\mathbb{Z}$-module $I = \left[6, 5 + 3\theta, 4 + 2\theta + 5\theta^2\right]$ is not an ideal of $\mathcal{O}$ because $6\theta \notin I$. For the reverse to be true, we need more conditions on the coefficients a, b, c, d, e and f.

Theorem 2.5. *Let K be a pure cubic field of the first kind. Then, a sub-$\mathbb{Z}$-module I of $\mathcal{O}_K$ with HNF-basis $[a, b + c\theta, d + e\theta + f\delta]$ is an ideal of $\mathcal{O}_K$ if and only if the following conditions are satisfied.*

1. $a \equiv b \equiv cs \equiv d \equiv es \equiv 0 \pmod f$
2. $a \equiv b \equiv 0 \pmod c$
3. $ea \equiv eb \equiv df - e^2 s \equiv f^2 r - de \equiv 0 \pmod{cf}$
4. $bces - b^2 f - c^2 ds \equiv c^2 frs + b^2 e - bcd \equiv cf^2 rs - bdf + be^2 s - cdes \equiv cefrs - bf^2 r + bde - cd^2 \equiv 0 \pmod{acf}$

Proof. Let $I = \left[a, b + c\theta, d + e\theta + f\dfrac{\theta^2}{s}\right]$ be a sub-$\mathbb{Z}$-module of $\mathcal{O}_K$. We know that I is an ideal of $\mathcal{O}_K$ if and only if for all $\alpha \in I$ and $\beta \in \mathcal{O}_K$ we have $\alpha\beta \in I$. For this, let $\alpha \in \mathcal{O}_K$ and $\beta \in I$, then $\alpha = x + y\theta + z\dfrac{\theta^2}{s}$ and $\beta = x'a + y'(b + c\theta) + z'(d + e\theta + f\dfrac{\theta^2}{s})$ with $x,\ y,\ z,\ x',\ y',\ z' \in \mathbb{Z}$, therefore

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

hence $\alpha\beta \in I$ if and only if the elements $a\theta$, $b\theta + c\theta^2$, $d\theta + e\theta^2 + \dfrac{Df}{s}$, $a\dfrac{\theta^2}{s}$, $b\dfrac{\theta^2}{s} + cD/s$ and $d\dfrac{\theta^2}{s} + eD/s + Df\dfrac{\theta}{s^2}$ belong to I.

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

But we have $a\theta \in I \iff a\theta = x''a + y''(b + c\theta) + z''(d + e\theta + f\frac{\theta^2}{s})$ with $x'', y'', z'' \in \mathbb{Z}$

$$\Leftrightarrow \begin{cases} ax'' + by'' + dz'' = 0 \\ cy'' + ez'' = a \\ z''f = 0 \end{cases} \Leftrightarrow \begin{cases} ax'' + by'' = 0 \\ cy'' = a \\ z'' = 0 \end{cases} \Leftrightarrow \begin{cases} cx'' = -b \\ cy'' = a \\ z'' = 0 \end{cases} \Leftrightarrow \begin{cases} c \mid a \\ c \mid b. \end{cases}$$

It is easy to verify with the same way that we also have the following equivalences:

$$a\frac{\theta^2}{s} \in I \iff \begin{cases} cf \mid be - dc \\ cf \mid ea \\ f \mid a \end{cases}$$

$$b\theta + c\theta^2 \in I \iff \begin{cases} acf \mid bces - b^2f - c^2ds \\ cf \mid bf - ces \\ f \mid cs \end{cases}$$

$$b\frac{\theta^2}{s} + \frac{D}{s} \in I \iff \begin{cases} acf \mid c^2frs + b^2e - bcd \\ cf \mid eb \\ f \mid b \end{cases}$$

$$d\theta + e\theta^2 + \frac{Df}{s} \in I \iff \begin{cases} acf \mid cf^2rs - be^2s + bdf - cdes \\ cf \mid df - e^2s \\ f \mid es \end{cases}$$

and

$$d\frac{\theta^2}{s} + \frac{eD}{s} + Df\frac{\theta^2}{s} \in I \iff \begin{cases} acf \mid cefrs - bf^2r + bde - cd^2 \\ cf \mid f^2r - de \\ f \mid d. \end{cases}$$

□

Theorem 2.6. *Let K be a pure cubic field of the second kind. Then, a sub-$\mathbb{Z}$-module I of $\mathcal{O}_K$ with HNF-basis $[a, b + c\theta, d + e\theta + f\delta]$ is an ideal of $\mathcal{O}_K$ if and only if the following conditions are satisfied.*

(1) *c divides a and b*
(2) *f divides a, $3c$, $3e$, $b + cr$ and $d + er$*
(3) *cf divides ea, $be-cd$, $eb+cer$, $f^2\frac{1-r^2}{3}+df-3e^2-2efr$ and $f^2r\frac{s^2-r^2}{3}-3de-3e^2r-ef-2efr^2$*
(4) *acf divides $bcfr+3bce-c^2f-b^2f-3dc^2$, $c^2fr\frac{s^2-1}{3}+bcf\frac{r^2-1}{3}+(be-cd)(b+cr)$, $cf^2r\frac{s^2-1}{3}+bf^2\frac{r^2-1}{3}+(be-cd)(3e+fr)+befr-bdf-cef$ and*

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

$(be-cd)(d+er)+cefr\dfrac{s^2-1}{3}+bef\dfrac{2r^2+1}{3}-cdf\dfrac{r^2+2}{3}+cf^2\dfrac{2rD-r^2-1}{9}+$
$bf^2r\dfrac{r^2-s^2}{9}$.

Proof. The proof is similar to that of the first kind with $\delta = \dfrac{1+r\theta+\theta^2}{3}$, except here we must also show that $\dfrac{r^2-1}{3}$, $\dfrac{s^2-1}{3}$, $\dfrac{2r^2+1}{3}$, $\dfrac{r^2+2}{3}$, $\dfrac{r^2-s^2}{9}$ and $\dfrac{2rD-r^2-1}{9}$ are integers. Indeed, we have $D = rs^2 \equiv \pm 1 \pmod 9$ which is equivalent to say that $r^2 \equiv s^2 \pmod 9$, and this means that $r^3 \equiv \pm 1 \pmod 9$, therefore $r \equiv \pm 1 \pmod 3$, it follows that $r^2 \equiv 1 \pmod 3$ (which also means that $2r^2+1 \equiv 0 \pmod 3$ and $r^2+2 \equiv 0 \pmod 3$) we get also $s^2 \equiv 1 \pmod 3$. Finally, we have $(r \pm 1)^2 \equiv 0 \pmod 9$, it follows that $r^2+1 \equiv \pm 2r \pmod 9$, and since $2rD \equiv \pm 2r \pmod 9$, then we get $2rD - r^2 - 1 \equiv 0 \pmod 9$. ☐

Corollary 2.7. *The number of ideals of $\mathcal{O}_K$ with a given length is finite.*

Proof. Let $I = [a, b+c\theta, d+e\theta+f\delta]$ be an ideal of $\mathcal{O}_K$. Given that $\ell(I) = a$, we will only have a finite number of integers b, c, d, e, and f according to the conditions of the two theorems 2.5 and 2.6. ☐

Proposition 2.8. *Let I be an ideal of $\mathcal{O}_K$ with HNF-basis $[a, b+c\theta, d+e\theta+f\delta]$. Then, I is primitive if and only if $gcd(c,e,f) = 1$.*

Proof. Let $t = gcd(c,e,f)$. If K is of the first kind, then by 1) theorem 2.5 t divides the integers a, b and d. If K is of the second kind, then by 1) theorem 2.6 $t \mid a$ and $t|b$ and by 2) theorem 2.6 $t \mid d$. In both cases we have $t|gcd(a,b,c,d,e,f)$ and $I \subset t\mathcal{O}_K$, hence, if $t > 1$, then I is not primitive.

Conversely, suppose that $gcd(c,e,f) = 1$. Let $m \in \mathbb{N}$ such that $I \subset m\mathcal{O}_K$, we have $d+e\theta+f\delta \in m\mathcal{O}_K$, therefore $m \mid f$ and $m \mid e$, and we have $b+c\theta \in m\mathcal{O}_K$, then $m \mid c$, it follows that m is a common divisor of c, e and f, hence $m = 1$. ☐

An important case is when we consider the special order $\mathcal{O} = \mathbb{Z}[\theta] = \left[1, \theta, \theta^2\right]$ of K which coincides with the ring of integers $\mathcal{O}_K$ in the case where K is of the first kind with $s = 1$.

Corollary 2.9. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ and let I be a sub-$\mathbb{Z}$-module of $\mathcal{O}$ with HNF-basis $\left[a, b+c\theta, d+e\theta+f\theta^2\right]$. Then I is a primitive ideal of $\mathcal{O}$ if and only if the following conditions are satisfied.*

(1) $f = 1$
(2) $a \equiv b \equiv d - e^2 \equiv D - de \equiv 0 \pmod c$
(3) $bce - b^2 - c^2 d \equiv c^2 D + b^2 e - bcd \equiv cD - bd + be^2 - cde \equiv ceD - bD + bde - cd^2 \equiv 0 \pmod{ac}$

Proof. We get these conditions by theorem 2.5 with $s = 1$ and $r = D$. ☐

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

3. Reduced ideals

Let L be an algebraic number field of degree n, and $\mathcal{O}_L$ its ring of integers and $\sigma_i, 1 \leq i \leq n$ the real and complex $\mathbb{Q}$-isomorphisms of K into $\mathbb{C}$. We say that an ideal I of $\mathcal{O}_L$ is reduced if I is primitive and if there is no element $\omega \neq 0$ in I such that $\mid \sigma_i(\omega) \mid < \ell(I)$, $\forall i \in \{1, 2, ..., n\}$ see [6]. In the case of pure cubic number fields we have $|\omega'| = |\omega''|$, hence we can writ:

Definition 3.1. We say that an ideal I of $\mathcal{O}_K$ is reduced if it is primitive and if there is no element $\omega \neq 0$ in I such that $\mid \omega \mid < \ell(I)$ and $\mid \omega' \mid < \ell(I)$.

Lemma 3.2. *Let K of the first kind and let $\omega = x + y\theta + z\delta \in \mathcal{O}_K$ $(x, y, z \in \mathbb{Z})$. If $\mid \omega \mid < \lambda_1$ and $\mid \omega' \mid < \lambda_2$ $(\lambda_1, \lambda_1 \in \mathbb{R}^+)$, then $\mid x \mid < \dfrac{\lambda_1 + 2\lambda_2}{3}$, $\mid y \mid < \dfrac{\lambda_1 + 2\lambda_2}{3\theta}$ and $\mid z \mid < \dfrac{s(\lambda_1 + 2\lambda_2)}{3\theta^2}$.*

Proof. We have $\omega = x + y\theta + z\dfrac{\theta^2}{s}$, therefore $\omega' = x + y\theta\zeta + z\dfrac{\theta^2}{s}\zeta^2$ and $\omega'' = x + y\theta\zeta^2 + z\dfrac{\theta^2}{s}\zeta$, hence $\omega + \omega' + \omega'' = 3x$, which means that $\mid 3x \mid = \mid \omega + \omega' + \omega'' \mid < \mid \omega \mid + \mid \omega' \mid + \mid \omega' \mid < \lambda_1 + 2\lambda_2$, hence $\mid x \mid < \dfrac{\lambda_1 + 2\lambda_2}{3}$. For y, we have $\omega + \omega'\zeta^2 + \omega''\zeta = 3y\theta$, therefore $\mid 3y\theta \mid < \mid \omega \mid + \mid \omega'\zeta^2 \mid + \mid \omega'\zeta \mid < \lambda_1 + 2\lambda_2$, hence $\mid y \mid < \dfrac{\lambda_1 + 2\lambda_2}{3\theta}$. For z we use the fact that $\omega + \omega'\zeta + \omega''\zeta^2 = 3z\dfrac{\theta^2}{s}$. □

This lemma shows that the number of elements $\omega \in \mathcal{O}_K$ such that $\mid \omega \mid < \lambda_1$ and $\mid \omega' \mid < \lambda_2$, is finite.

Theorem 3.3. *Let K of the first kind and let I be a primitive ideal of $\mathcal{O}_K$ given in term of HNF-basis $[a, b + c\theta, d + e\theta + f\dfrac{\theta^2}{s}]$. Then I is reduced if and only if the only triple (x, y, z) of integers which satisfies the following conditions:*

- $f \mid z$,
- $cf \mid fy - ze$,
- $acf \mid cfx - bfy + (be - cd)z$,
- $\mid x + y\theta + z\dfrac{\theta^2}{s} \mid < \ell(I)$,
- $(x - \dfrac{y}{2}\theta - \dfrac{z}{2}\dfrac{\theta^2}{s})^2 + \dfrac{3}{4}\theta^2(y - z\dfrac{\theta}{s})^2 < \ell(I)^2$,

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 $\mid \alpha' \mid = \mid \alpha'' \mid$.

Let $I = [a, b + c\theta, d + e\theta + f\dfrac{\theta^2}{s}]$ be a primitive ideal of $\mathcal{O}_K$. If $\alpha \in I$, then $\alpha = Xa + Y(b + c\theta) + Z(d + e\theta + f\dfrac{\theta^2}{s})$ with $X, Y, Z \in \mathbb{Z}$ and we can easily verify

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

that $\mid \alpha' \mid^2 = (aX+bY+dZ-\frac{cY+eZ}{2}\theta-\frac{fZ}{2}\frac{\theta^2}{s})^2+\frac{3}{4}\theta^2(cY+eZ-fZ\frac{\theta}{s})^2$. The ideal I is reduced if and only if, for all $\alpha\in I$, we have $\mid\alpha\mid<\ell(I)$ and $\mid\alpha'\mid<\ell(I)$ implies that $\alpha=0$. Now we have

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

if and only if

$$\begin{cases}X,Y,Z\in\mathbb{Z}\\ \mid aX+bY+dZ+(cY+eZ)\theta+fZ\frac{\theta^2}{s}\mid<\ell(I)\\ \mid\alpha'\mid^2=(aX+bY+dZ-\frac{cY+eZ}{2}\theta-\frac{fZ}{2}\frac{\theta^2}{s})^2+\frac{3}{4}\theta^2(cY+eZ-fZ\frac{\theta}{s})^2<\ell(I)^2,\end{cases}$$

We shall use the substitution $x=aX+bY+dZ$, $y=cY+eZ$, $z=fZ$, having the inverse $X=\frac{cfx-bfy+(be-cd)z}{acf}$, $Y=\frac{fy-ez}{cf}$ and $Z=\frac{z}{f}$. Therefore, we see that the ideal I is reduced if and only if $(0,0,0)$ is the only solution of

$$\begin{cases}x,y,z\in\mathbb{Z}\\ f\mid z\\ cf\mid fy-ze\\ acf\mid cfx-bfy+(be-cd)z\\ \mid x+y\theta+z\frac{\theta^2}{s}\mid<\ell(I)\\ (x-\frac{y}{2}\theta-\frac{z}{2}\frac{\theta^2}{s})^2+\frac{3}{4}\theta^2(y-z\frac{\theta}{s})^2<\ell(I)^2\end{cases}$$

The theorem is proved. □

We have a similar result for a pure cubic field of the second kind.

Theorem 3.4. *Let K of the second kind, and let I be a primitive ideal of $\mathcal{O}_K$ given in term of HNF-basis $[a,b+c\theta,d+e\theta+f\delta]$. Then, I is reduced if and only if the only triple of integers (x,y,z) which satisfies the following conditions:*

- $f\mid z$,
- $3cf\mid fy-(3e+fr)z$,
- $3acf\mid cfx-bfy+(3be+dfr-3cd-cf)z$,
- $\mid x+y\theta+z\theta^2\mid<3\ell(I)$,
- $(x-\frac{y}{2}\theta-\frac{z}{2}\theta^2)^2+\frac{3}{4}\theta^2(y-z\theta)^2<9\ell(I)^2$,

is $(0,0,0)$.

Proof. Let I be a primitive ideal of $\mathcal{O}_K$ with HNF-base $[a,b+c\theta,d+e\theta+f\frac{1+r\theta+\theta^2}{3}]$. Let $\alpha\in I$, then $\alpha=Xa+Y(b+c\theta)+Z(d+e\theta+f\frac{1+r\theta+\theta^2}{3})$ for some $X,Y,Z\in\mathbb{Z}$,

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

otherwise written, $\alpha = \frac{1}{3}(3(aX+bY+dZ)+fZ+(3(cY+eZ)+frZ)\theta+fZ\theta^2)$. After the calculate of α' we get $\mid \alpha' \mid^2 = \frac{1}{9}(3(aX+bY+dZ)+fZ-(3(cY+eZ)+frZ)\frac{\theta}{2}-fZ\frac{\theta^2}{2})^2+\frac{3}{4}\theta^2(3(cY+eZ)+frZ-fZ\theta)^2)$. By the definition 3.1, the ideal I is reduced if and only if

$$\begin{cases} \alpha \in I \\ \mid \alpha \mid < \ell(I) \\ \mid \alpha' \mid < \ell(I) \end{cases} \Rightarrow \quad \alpha = 0$$

considering the following substitution: $x = 3(aX+bY+dZ)+fZ$, $y = 3(cY+eZ)+frZ$, $z = fZ$, then $3acfX = cfx - bfy + (3be+bfr-3cd-cf)z$, $3cfY = fy-(3e+rf)z$ and $fZ = z$. Hence the ideal I is reduced if and only if $(0,0,0)$ is the unique solution of the following system:

$$\begin{cases} x, y, z \in \mathbb{Z}, \\ f \mid z, \\ 3cf \mid fy-(3e+fr)z, \\ 3acf \mid cfx-bfy+(3be+bfr-3cd-cf)z, \\ \mid x+y\theta+z\theta^2 \mid < 3\ell(I), \\ (x-\frac{y}{2}\theta-\frac{z}{2}\theta^2)^2+\frac{3}{4}\theta^2(y-z\theta)^2 < 9\ell(I)^2. \end{cases}$$

□

Theorem 3.5. *Let K of the first kind, and let I be a primitive ideal of $\mathcal{O}_K$. If $\ell(I) < \frac{\theta}{s}$, then I is reduced.*

Proof. Let $[a, b+c\theta, d+e\theta+f\frac{\theta^2}{s}]$ be the HNF-basis of I. Let $(x,y,z) \in \mathbb{Z}^3$ such that $f \mid z$, $cf \mid fy-ze$, $acf \mid cfx-bfy+(be-cd)z$ and

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

If we put $\omega = x+y\theta+z\frac{\theta^2}{s}$, we have $\mid \omega \mid < \ell(I)$ and $\mid \omega' \mid < \ell(I)$, hence by lemma 3.2 we have

$$\begin{cases} \mid x \mid < \ell(I) \\ \mid y \mid < \frac{\ell(I)}{\theta} \\ \mid z \mid < \frac{s\ell(I)}{\theta^2}. \end{cases}$$

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

If $\ell(I) < \dfrac{\theta}{s}$, then $\mid z \mid< \dfrac{s\ell(I)}{\theta^2} < \dfrac{s}{\theta^2}\dfrac{\theta}{s} = \dfrac{1}{\theta} < 1$, hence $z = 0$. For y, we have $\mid y \mid< \dfrac{\ell(I)}{\theta} < \dfrac{1}{s} \leq 1$, hence $y = 0$. For x, we have $acf \mid cfx - bfy + (be - cd)z$ therefore $\ell(I) \mid x$, and $\mid x \mid< \ell(I)$, hence $x = 0$, finally we have $x = y = z = 0$, hence by definition 3.1, I is reduced. ☐

Remark 3.6. We have $\dfrac{\theta}{s} = \sqrt[3]{\dfrac{r}{s}}$, hence the last theorem is very important when we have $r >> s$, we gain more reduced ideals to less effort.

We have a similar result for K of the second kind.

Theorem 3.7. *Let K be of second kind, and let I be a primitive ideal of $\mathcal{O}_K$. If $\ell(I) < \frac{\theta}{3}$, then I is reduced.*

Proof. let $[a, b+c\theta, d+e\theta+f\dfrac{1+r\theta+\theta^2}{3}]$ be the HNF-basis of I. Let $(x, y, z) \in \mathbb{Z}^3$ satisfy

$$\begin{cases} f \mid z \\ 3cf \mid fy - (3e + fr)z \\ 3acf \mid cfx - bfy + (3be + bfr - 3cd - cf)z \\ \mid x + y\theta + z\theta^2 \mid< 3\ell(I) \\ (x - \dfrac{y}{2}\theta - \dfrac{z}{2}\theta^2)^2 + \dfrac{3}{4}\theta^2(y - z\theta)^2 < 9\ell(I)^2 \end{cases}$$

If we put $\omega = x + y\theta + z\theta^2$, then we have $\mid \omega \mid< 3\ell(I)$ et $\mid \omega' \mid< 3\ell(I)$, and by lemma 3.2 (with $s = 1$) we have

$$\begin{cases} \mid x \mid< 3\ell(I) \\ \mid y \mid< \dfrac{3\ell(I)}{\theta} \\ \mid z \mid< \dfrac{3\ell(I)}{\theta^2}. \end{cases}$$

Now, if $\ell(I) < \dfrac{\theta}{3}$, then

$$\begin{cases} \mid x \mid< 3\ell(I) \\ \mid y \mid< 1 \\ \mid z \mid< 1 \end{cases}$$

therefore $z = 0$ and $y = 0$. For x, by hypothesis we have, $3acf \mid cfx - bfy + (3be + bfr - 3cd - cf)z$, therefore $3\ell(I) \mid x$ and $\mid x \mid< 3\ell(I)$, hence $x = 0$, finally we have $x = y = z = 0$, so by theorem 3.4, I is reduced. ☐

Theorem 3.8. *Let I be an ideal of $\mathcal{O}_K$. If I is reduced, then $\ell(I) \leq \dfrac{6\sqrt{3}D}{\pi}$.*

Proof. Let I be an ideal of $\mathcal{O}_K$ with HNF-basis $[\ell(I), \alpha, \beta]$ where $\alpha = b + c\theta$ and $\beta = d + e\theta + f\delta$. By the definition 3.1, there is no element $\omega \in I$, $\omega \neq 0$

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

satisfied $\mid \omega \mid< \ell(I)$ and $\mid \omega' \mid< \ell(I)$, and by [10, Theorem 5.3, p. 32], we have $\ell(I)^3 \leq \dfrac{2}{\pi}\sqrt{|\Delta_K|}N(I)$.

- K of the first kind implies that $\ell(I)^3 \leq \dfrac{6\sqrt{3}rs}{\pi}N(I)$, therefore

$$\ell(I)^2 \leq \frac{6\sqrt{3}D}{\pi}\frac{cf}{s} \tag{3.1}$$

If we put $g = gcd(f, s)$, then $f = gf'$ and $s = gs'$ with $gcd(f', s') = 1$. By 1. theorem 2.5, we have $f \mid cs$ and $f \mid es$, therefore $gf' \mid cgs'$ and $gf' \mid egs'$ which implies that $f' \mid cs'$ and $f' \mid es'$ hence $f' \mid c$ and $f' \mid e$, and since I is primitive, then by proposition 2.8 we get $f' = 1$, thus $f = g$ and $f \mid s$. We have also $c \mid a = \ell(I)$, then we get

$$\frac{cf}{s} \leq a \tag{3.2}$$

From (3.1) and (3.2) we obtain the result.

- K of the second kind implies that $\ell(I)^3 \leq \dfrac{2\sqrt{3}rs}{\pi}N(I)$, thus

$$\ell(I)^2 \leq \frac{6\sqrt{3}D}{\pi}\frac{cf}{3s} \tag{3.3}$$

reasoning as for the first kind, we get $f|3s$, therefore

$$\frac{cf}{3s} \leq a \tag{3.4}$$

the result is obtained by (3.3) et (3.4). □

Remark 3.9. We know that every ideals class contains a reduced ideal [2]. On the other hand, by the last theorem and corollary 2.7, the number of reduced ideals of $\mathcal{O}_K$ is finite (noted $\mathfrak{r}_K$), hence we have

$$h_K \leq \mathfrak{r}_K$$

4. Principality

In this section, we will develop the notion of a minimum of an ideal which will help us to study the principality in the considered field.

Definition 4.1. 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 $|\alpha'| < |\mu'|$.

Corollary 4.2. *Let I be a primitive ideal of $\mathcal{O}_K$. Then, I is reduced if and only if $\ell(I)$ is a minimum of I.*

If I is an ideal of $\mathcal{O}_K$, then any element in I of a minimal nonzero absolute norm is a minimum of I. In particular any unit ε of K is a minimum of $\mathcal{O}_K$.
If μ is a minimum of I, then it is easy to show that $\alpha\mu$ is a minimum of αI, $\forall\alpha \in K^*$. In particular, $\mu\varepsilon$ is a minimum of I for any $\varepsilon \in \mathcal{U}_K$, hence the set of

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

minimums of an ideal I is infinite, we denote it by $\mathcal{M}_I$.
Now, we consider the following equivalence relation in $\mathcal{M}_I$, for $\mu, \nu \in \mathcal{M}_I$

$$\mu \sim \nu \Leftrightarrow \mu = \nu\varepsilon \text{ for a some unity } \varepsilon$$

We denote by $Cl(\mathcal{M}_I)$ the set of all equivalence classes of $\mathcal{M}_I$. The class of $\mu \in \mathcal{M}_I$ is denoted by $[\mu]$, and we have the following result.

Theorem 4.3. *If I is an ideal of $\mathcal{O}_K$, then $Cl(\mathcal{M}_I)$ is finite. We denote by $\mathfrak{n}_I$ its cardinal.*

Proof. Let I be an ideal of $\mathcal{O}_K$. If $[\mu]$ is an element of $Cl(\mathcal{M}_I)$, then there is no non-zero element $\alpha \in I$ verifying $|\alpha| < |\mu|$, $|\alpha'| < |\mu'|$ and $|\alpha''| < |\mu''|$, therefore by [10, Theorem 5.3, p. 32], we have $|\mu|\,|\mu'|\,|\mu''| \leq \dfrac{2}{\pi}\sqrt{|\Delta_K|}N(I)$, hence $|\mathcal{N}(\mu)| \leq \dfrac{2}{\pi}\sqrt{|\Delta_K|}N(I)$, and up to multiplication by units, there are only finitely many elements in I whose absolute norm is majorized by the constant $\dfrac{2}{\pi}\sqrt{|\Delta_K|}N(I)$, hence the result. □

Definition 4.4. A system representative of classes of $\mathcal{M}_I$ is called a cycle of minimums of I, we denote it by C_I.

In fact, we can choose a special system as follows.

Theorem 4.5. *Let I be an ideal of $\mathcal{O}_K$ and let μ be the smallest element of $\mathcal{M}_I$ which is $\geq \ell(I)$. Then, there is one and only one cycle of minimums of I in the interval $[\mu, \mu\varepsilon_0[$. We call this cycle a fundamental cycle of minimums of I, and we denote it by C_I^F.*

Proof. Let $\eta \in \mathcal{M}_I$ $(\eta > 0)$. If $\eta \geq \mu\varepsilon_0$, let k be the greatest positive integer for which we still have $\eta \geq \mu\varepsilon_0^k$ (it is clear that $k \geq 1$), therefore $\eta < \mu\varepsilon_0^{k+1}$, so

$$\mu\varepsilon_0^k \leq \eta < \mu\varepsilon_0^{k+1}$$

hence

$$\mu \leq \eta\varepsilon_0^{-k} < \mu\varepsilon_0$$

then we put $\nu = \eta\varepsilon_0^{-k}$.
If $\eta < \mu$, let k be the least positive integer for which we have $\mu\varepsilon_0^{-k} \leq \eta$, therefore $\eta < \mu\varepsilon_0^{-(k-1)}$, then we have

$$\mu\varepsilon_0^{-k} \leq \eta < \mu\varepsilon_0^{-k+1}$$

hence

$$\mu \leq \eta\varepsilon_0^{k} < \mu\varepsilon_0$$

and we put $\nu = \eta\varepsilon_0^k$. Consequently, every element η of $\mathcal{M}_I$ is associated with a minimum ν of I belonging to $[\mu, \mu\varepsilon_0[$, so, if $C_I' = \{\eta_1, ..., \eta_m\}$ is any cycle of the minimums of I, then $\forall i \in \{1, ..., m\}$ there is $\nu_i \in [\mu, \mu\varepsilon_0[$ and a unity ε_i such that $\nu_i = \varepsilon_i\eta_i$, therefore the cycle we want to find is $C_I = \{\nu_1, ..., \nu_m\}$.

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

Suppose that there is another cycle $C''_I = \{\rho_1, ..., \rho_m\}$ of minimums of I in $[\mu, \mu\varepsilon_0[$, then $\rho_j = \nu_i\varepsilon_0^k$ for some $i, j \in \{1, ..., m\}$ and $k \in \mathbb{Z}$. If $\rho_j < \nu_i$, then we will have

$$\mu \leq \nu_i\varepsilon_0^k < \nu_i < \mu\varepsilon_0.$$

So by $\nu_i\varepsilon_0^k < \nu_i$ we have $k < 0$, and by $\mu\varepsilon_0^{-k} \leq \nu_i < \mu\varepsilon_0$, we have $-1 < k$, contradiction. A similar reasoning if $\rho_j > \nu_i$. ☐

Corollary 4.6. *Let I be a reduced ideal of $\mathcal{O}_K$. Then, the fundamental cycle of the minimums of I is in $[\ell(I), \ell(I)\varepsilon_0[$. In particular, the fundamental cycle of the minimums of $\mathcal{O}_K$ is in $[1, \varepsilon_0[$.*

The notion of minimum also allow to determine the fundamental unit using any reduced ideal, namely:

Corollary 4.7. *Let I be a reduced ideal of $\mathcal{O}_K$. If μ is the smallest minimum of I such that $\mu > \ell(I)$, $\frac{\mu}{\ell(I)} \in \mathcal{O}_K$ and $\mathcal{N}(\frac{\mu}{\ell(I)}) = 1$, then*

$$\varepsilon_0 = \frac{\mu}{\ell(I)}.$$

Proof. If $\frac{\mu}{\ell(I)} \in \mathcal{O}_K$ and $\mathcal{N}(\frac{\mu}{\ell(I)}) = 1$, then $\frac{\mu}{\ell(I)} = \varepsilon_0^k$ with $(k \in \mathbb{Z})$, precisely $k > 0$ because $\ell(I) < \mu$,hence the smallest value for μ is $\ell(I)\varepsilon_0$. ☐

The following result will help us to determine the elements of an ideal I qualified to be an element of C_I^F.

Theorem 4.8. *Let K be a pure cubic field of the first kind and let I be a reduced ideal of $\mathcal{O}_K$. If $\mu = x + y\theta + z\delta \in C_I^F$ such that $\mu < \lambda$ for some $\lambda \in \mathbb{R}^+$, then*

$$\begin{cases} \frac{-\ell(I)}{3} < x < \frac{\lambda + 2\ell(I)}{3} \\ \frac{-\ell(I)}{\sqrt{3}\theta} < y < \frac{\lambda + \ell(I) + \ell(I)\sqrt{3}}{3\theta} \\ \frac{-\ell(I)}{\sqrt{3}\delta} < z < \frac{\lambda + \ell(I) + \ell(I)\sqrt{3}}{3\delta} \end{cases}$$

Proof. If $\mu = x + y\theta + z\delta$ is in C_I^F, then $\ell(I) < \mu < \lambda$ and necessarily $|\mu'| < \ell(I)$, therefore

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

which implies that

$$\ell(I) < x + y\theta + z\delta < \lambda \tag{4.1}$$

$$-\ell(I) < x - \frac{y}{2}\theta - \frac{z}{2}\delta < \ell(I) \tag{4.2}$$

$$\frac{-2\ell(I)}{\sqrt{3}} < y\theta - z\delta < \frac{2\ell(I)}{\sqrt{3}} \tag{4.3}$$

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

by (4.1) and (4.2) we get

$$\frac{-\ell(I)}{3} < x < \frac{2\ell(I)+2}{3}$$

by (4.1) and (4.3) we get

$$\ell(I) - \frac{2\ell(I)}{\sqrt{3}} < x + 2y\theta < \lambda + \frac{2\ell(I)}{\sqrt{3}} \tag{4.4}$$

and

$$\ell(I) - \frac{2\ell(I)}{\sqrt{3}} < x + 2z\delta < \lambda + \frac{2\ell(I)}{\sqrt{3}} \tag{4.5}$$

by (4.2) and (4.3) we get

$$-\ell(I) - \frac{\ell(I)}{\sqrt{3}} < x - y\theta < \ell(I) + \frac{\ell(I)}{\sqrt{3}} \tag{4.6}$$

and

$$-\ell(I) - \frac{\ell(I)}{\sqrt{3}} < x - z\delta < \ell(I) + \frac{\ell(I)}{\sqrt{3}} \tag{4.7}$$

now by (4.4) and (4.6) we get

$$\ell(I) - \frac{2\ell(I)}{\sqrt{3}} - \ell(I) - \frac{\ell(I)}{\sqrt{3}} < 3y\theta < \lambda + \ell(I) + \ell(I)\sqrt{3},$$

hence

$$\frac{-\ell(I)}{\sqrt{3}\theta} < y < \frac{\lambda + \ell(I) + \ell(I)\sqrt{3}}{3\theta}.$$

Finally, by (4.5) and (4.7) we get

$$\ell(I) - \frac{2\ell(I)}{\sqrt{3}} - \ell(I) - \frac{\ell(I)}{\sqrt{3}} < 3z\delta < \lambda + \ell(I) + \ell(I)\sqrt{3}.$$

consequently we have

$$\frac{-\ell(I)}{\sqrt{3}\delta} < z < \frac{\lambda + \ell(I) + \ell(I)\sqrt{3}}{3\delta}.$$

□

Let I be an ideal of $\mathcal{O}_K$ and $C_I^F = \{\mu_1, \mu_2, ..., \mu_t\}$ its fundamental cycle of minimums. By [2, Theorem 5.4], for all $i \in \{1, ..., t\}$ the ideal $I_i = \frac{\ell(I_i)}{\mu_i} I$ is reduced, hence we get a set

$$\{I_1, I_2, ..., I_t\}$$

of reduced ideals in the class of I. This set is called a cycle of reduced ideals of I and denoted by $\mathfrak{R}_I$.

Theorem 4.9. (1) *The ring $\mathcal{O}_K$ is principal if and only if every reduced ideal of $\mathcal{O}_K$ is principal*

(2) *If I is a principal reduced ideal of $\mathcal{O}_K$, then there exists $\mu \in C_{\mathcal{O}_K}^F$ such that $I = \frac{\ell(I)}{\mu}\mathcal{O}_K$*

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

(3) *If I is a principal ideal of $\mathcal{O}_K$, then there exists $\eta \in C_I^F$ such that $I = (\eta)$.*

Proof. (1) Suppose that every reduced ideal of $\mathcal{O}_K$ is principal. Let J be an ideal of $\mathcal{O}_K$ and let $C_J^F = \{\mu_1, \mu_2, ..., \mu_t\}$ its fundamental cycle of minimums, then $J_i = \dfrac{\ell(J_i)}{\mu_i} J$ is reduced, therefore it is principal, hence J is also principal. the reverse is clear.

(2) If $C_{\mathcal{O}_K}^F = \{\mu_1 = 1, \mu_2, ..., \mu_m\}$ is the fundamental cycle of minimums of $\mathcal{O}_K$, then the principal reduced ideals are $I_i = \dfrac{\ell(I_i)}{\mu_i}\mathcal{O}_K$, $1 \leq i \leq m$, hence $I = \dfrac{\ell(I_i)}{\mu_i}\mathcal{O}_K$ for some i.

(3) Let $C_I^F = \{\mu_1, \mu_2, ..., \mu_m\}$ be the fundamental cycle of I, since I is principal, then all the reduced ideal $I_i = \dfrac{\ell(I_i)}{\mu_i} I$ given by C_I^F are principal, hence for some i we have $\mathcal{O}_K = \dfrac{\ell(\mathcal{O}_K)}{\mu_i} I$.

□

Remark 4.10. (1) Let I be an ideal of $\mathcal{O}_K$ and $C_I^F = \{\mu_1, \mu_2, ..., \mu_m\}$ its fundamental cycle of minimums. If $\forall i \in \{1, 2, ..., m\}$ we have $N(I) \neq \mathcal{N}(\mu_i)$, then I is not principal.

(2) The ring $\mathcal{O}_K$ is principal if and only if there is an ideal I of $\mathcal{O}_K$ such that $\mathfrak{n}_I = \mathfrak{r}_K$.

5. Numerical example

Example 5.1. Let $K = \mathbb{Q}(\sqrt[3]{20})$, $\theta = \sqrt[3]{20}$, so $\delta = \dfrac{\theta^2}{2} = \dfrac{\sqrt[3]{400}}{2} = \sqrt[3]{50}$.
We have ten reduced ideals ($\mathfrak{r}_K = 10$) represented with their norms in the following table:

reduced ideal with HNF-basis	Norm
$I_1 = \mathcal{O}_K = [1, \sqrt[3]{20}, \sqrt[3]{50}]$	1
$I_2 = [2, \sqrt[3]{20}, \sqrt[3]{50}]$	2
$I_3 = [2, \sqrt[3]{20}, 2\sqrt[3]{50}]$	4
$I_4 = [3, 3\sqrt[3]{20}, 2 + \sqrt[3]{20} + \sqrt[3]{50}]$	9
$I_5 = [3, 1 + \sqrt[3]{20}, 1 + \sqrt[3]{50}]$	3
$I_6 = [6, 3\sqrt[3]{20}, 2 + \sqrt[3]{20} + \sqrt[3]{50}]$	18
$I_7 = [6, 3\sqrt[3]{20}, 4 + 2\sqrt[3]{20} + 2\sqrt[3]{50}]$	36
$I_8 = [7, 7\sqrt[3]{20}, 1 + 5\sqrt[3]{20} + \sqrt[3]{50}]$	49
$I_9 = [7, 7\sqrt[3]{20}, 4 + 3\sqrt[3]{20} + \sqrt[3]{50}]$	49
$I_{10} = [14, 7\sqrt[3]{20}, 2 + 3\sqrt[3]{20} + 2\sqrt[3]{50}]$	196

The fundamental cycle of minimums of $I_1 = \mathcal{O}_K$ is

$$C_{I_1}^F = \left\{\mu_1 = 1, \mu_2 = 3 + \sqrt[3]{20} + \sqrt[3]{50}, \mu_3 = 8 + 3\sqrt[3]{20} + 2\sqrt[3]{50}\right\}$$

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina Accepted article · Early view version
This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

and we can easily verify that

$$I_8 = \frac{7}{\mu_2} I_1 \quad \text{and} \quad I_6 = \frac{6}{\mu_3} I_1$$

therefore the the cycle of principal reduced ideals is

$$\mathfrak{R}_{I_1} = \left\{ (1), (\frac{7}{\mu_2}), (\frac{6}{\mu_3}) \right\}$$

hence by 2. remark 4.10, $\mathcal{O}_K$ is not principal.
We can verify this otherwise. In deed, if we consider the ideal $I_2 = [2, \sqrt[3]{20}, \sqrt[3]{50}] = [2, \theta, \delta]$, we get:

$$C^F_{I_2} = \{\eta_1 = 2, \eta_2 = 2 + \sqrt[3]{20} + \sqrt[3]{50}, \eta_3 = 4 + \sqrt[3]{20} + \sqrt[3]{50}, \eta_4 = 8 + 3\sqrt[3]{20} + 2\sqrt[3]{50}\}$$

and we have

$$\mathcal{N}(\eta_1) = 8, \quad \mathcal{N}(\eta_2) = 18, \quad \mathcal{N}(\eta_3) = 14, \quad \mathcal{N}(\eta_4) = 12.$$

Therefore

$$N(I_2) = 2 \neq \mathcal{N}(\eta_i), \ \forall i \in \{1, 2, 3, 4\}$$

hence by 1. remark 4.10, I_2 is not principal.

Example 5.2. Consider now the ideal $I = [6, 4 + \theta, 2 + \theta^2]$ which is not reduced because $\ell(I) = 6$ is not a minimum of I. The fundamental cycle of minimums of I is

$$C^F_I = \{\nu_1 = 4 + 2\theta + \theta^2, \quad \nu_2 = 8 + 3\theta + \theta^2, \quad \nu_3 = 4 + \theta\}$$

and we have:

$$\mathcal{N}(\nu_1) = 144, \quad \mathcal{N}(\nu_2) = 12, \quad \mathcal{N}(\nu_3) = 84.$$

Thus

$$\mathcal{N}(\nu_2) = 12 = N(I)$$

and since

$$\begin{pmatrix} 8 + 3\theta + \theta^2 \\ 20 + 8\theta + 3\theta^2 \\ 30 + 10\theta + 4\theta^2 \end{pmatrix} = \begin{pmatrix} -1 & 3 & 1 \\ -3 & 8 & 3 \\ -3 & 10 & 4 \end{pmatrix} \begin{pmatrix} 6 \\ 4 + \theta \\ 2 + \theta^2 \end{pmatrix}$$

with

$$\begin{vmatrix} -1 & 3 & 1 \\ -3 & 8 & 3 \\ -3 & 10 & 4 \end{vmatrix} = 1.$$

then I is principal generated by $\nu_2 = 8 + 3\theta + \theta^2$.

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024

Revista de la Unión Matemática Argentina **Accepted article · Early view version**

This peer-reviewed unedited article has been accepted for publication. The final copyedited version may differ in some details. Volume, issue, and page numbers will be assigned at a later stage. Cite using this DOI, which will not change in the final version: https://doi.org/10.33044/revuma.3862.

References

[1] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge Univ. Press, Cambridge, 2004. MR2031707

[2] A. Azizi et al., The reduced ideals of a special order in a pure cubic number field, Arch. Math. (Brno) **56** (2020), no. 3, 171–182. MR4156443

[3] J. A. Buchmann, On the computation of units and class numbers by a generalization of Lagrange's algorithm, J. Number Theory **26** (1987), no. 1, 8–30. MR0883530

[4] J. A. Buchmann and H. C. Williams, A key-exchange system based on imaginary quadratic fields, J. Cryptology **1** (1988), no. 2, 107–118. MR0972575

[5] J. A. Buchmann, H. C. Williams and R. Scheidler, A key-exchange protocol using real quadratic fields, J. Cryptology **7** (1994), no. 3, 171–199. MR1286662

[6] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer, Berlin, 1993. MR1228206

[7] B. N. Delone and D. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, Amer. Math. Soc., Providence, RI, 1964. MR0160744

[8] G. T. Jacobs, *Reduced ideals and periodic sequences in pure cubic fields*, ProQuest LLC, Ann Arbor, MI, 2015. MR3503469

[9] R. A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and its Applications, CRC, Boca Raton, FL, 1996. MR1383823

[10] J. Neukirch, *Algebraic number theory*, translated from the 1992 German original and with a note by Norbert Schappacher, Grundlehren der mathematischen Wissenschaften, 322, Springer, Berlin, 1999. MR1697859

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

[12] C. Prabpayak, *Orders in pure cubic number fields*, Ph.D. thesis, Univ. Graz. Grazer Math. Ber. 361, 2014. MR 3364308

Department of Mathematics, Faculty of Sciences, Mohammed First University, 60000 Oujda, Morocco.
Email address: benamarajamal@hotmail.fr

Regional Center of Education and Training, 60000 Oujda, Morocco.
Email address: talbimm@yahoo.fr

Submitted: January 16, 2023
Accepted: September 7, 2023
Published (early view): August 24, 2024