Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–3.
ISSN-0037-8712
doi:10.5269/bspm.66679

Class number and fundamental units of certain pure cubic fields

Jamal Benamara

ABSTRACT: Let $K_{m\pm} = \mathbb{Q}(\sqrt[3]{m^3 \pm 1})$ be a pure cubic number field where m is an integer. We prove that if $m \geq 2$ and $m^3 \pm 1$ is square-free then the class number of $K_{m\pm}$ is a multiple of 3 we also give the fundamental unit of $K_{m\pm}$ when $m^3 \pm 1 \not\equiv \pm 1 \pmod 9$.

Key Words: Cubic field; Class number; Fundamental unit.

Contents

1. Introduction

We consider a pure cubic number field $K_{m\pm} = \mathbb{Q}(\sqrt[3]{m^3 \pm 1})$ where m is an integer such that $d_{m\pm} = m^3 \pm 1$ is a cube-free. In [6], Louboutin obtained a lower bound for class numbers of pure cubic number fields and applied this bound to prove that there are 2 such $K_{m\pm}$ with class number one, namely K_{1+} and K_{2+}; there does not exist any such $K_{m\pm}$ with class number two; and there are 3 such $K_{m\pm}$ with class number three, namely K_{2-} and $K_{3\pm}$. Another work concerning this family of fields, is in [2], where the authors explicitly determine the reduced principal ideals. In [[5], p8], Honda improved the results of Barrucand and Cohn [3], and gave the list of all the pure cubic fields $\mathbb{Q}(\sqrt[3]{n})$ whose class numbers are not divisible by 3.
Recall that we may assume with no loss of generality that $d_{m\pm} = rs^2$ where r and s are square-free and $(r, s) = 1$. It is well known (see for example [1,4]) that if $d_{m\pm} \not\equiv \pm 1 \pmod 9$, then the ring of integers $\mathcal{O}_{K_{m\pm}}$ of $K_{m\pm}$ has a basis $[1, \theta_{m\pm}, \delta_{m\pm} = \theta_{m\pm}/s]$ where $\theta_{m\pm} = \sqrt[3]{d_{m\pm}}$ and the discriminant of $K_{m\pm}$ is $\Delta_{K_{m\pm}} = -27r^2s^2$. In this case, $K_{m\pm}$ is called a pure cubic field of the first kind. If $d_{m\pm} \equiv \pm 1 \pmod 9$, then $\mathcal{O}_{K_{m\pm}} = \left[1, \theta_{m\pm}, \delta_{m\pm} = (1 + r\theta_{m\pm} + \theta_{m\pm}^2)/3\right]$, $\Delta_{K_{m\pm}} = -27r^2s^2$ and K is called a pure cubic field of the second kind. We also know that the norm of $\alpha = x + y\theta_{m\pm} + z\theta_{m\pm}^2 \in K_{m\pm}$ is $\mathcal{N}(\alpha) = x^3 + y^3 d_{m\pm} + z^3 d_{m\pm}^2 - 3xyzd_{m\pm}$.
In this paper we prove that if $m^3 \pm 1$ is square-free, then the class number of $K_{m\pm}$ is divided by three except K_{1+}, we also determine the fundamental unit of $K_{m\pm}$ when $m \equiv 1, 2 \pmod 3$.

2. The class number of $K_{m\pm}$

Theorem 2.1 *Let $K_{m\pm} = \mathbb{Q}(\sqrt[3]{m^3 \pm 1})$ where $m \geq 1$ is an integer such that $d_{m\pm} = m^3 \pm 1$ is square-free. Then the class number $h_{m\pm}$ of $K_{m\pm}$ is a multiple of three, except $h_{1+} = 1$.*

Proof: To prove this theorem we will study the decomposition of $d_{m\pm}$ and use the result obtained in [[5],p8].
Since $d_{m\pm} = m^3 \pm 1$ is square-free, then $d_{m\pm} = p_1p_2...p_k$ where $p_1, p_2, ..., p_k$ are the distinct primes occur in this factorization.
First case $(k = 1)$ is when $d_{m\pm} = m^3 \pm 1 = (m \pm 1)(m^2 \mp m + 1) = p$ is a prime number, this is verified for K_{m+} when $m = 1$ and where we have $d_{m+} = 2 \equiv -1 \pmod 3$ and for K_{m-} when $m = 2$ and where we have $d_{+m} = 7 \not\equiv -1 \pmod 3$.
Second case $(k = 2)$ is when $d_{m\pm} = m^3 \pm 1 = (m \pm 1)(m^2 \mp m + 1) = 3p$, in this case, four situations are possible for K_{m+}:

Submitted January 16, 2023. Published January 01, 2025
2010 *Mathematics Subject Classification:* Primary 11R16, 11R27, 11R29.

1. $m+1=3p$ and $m^2-m+1=1$ hence $3p=2$ and $m=1$.
2. $m+1=1$ and $m^2-m+1=3p$.
3. $m+1=3$ and $m^2-m+1=p$.
4. $m+1=p$ and $m^2-m+1=3$ hence $p=3$.

And four situations for K_{m-}:

1. $m-1=3p$ and $m^2+m+1=1$.
2. $m-1=1$ and $m^2+m+1=3p$ hence $m=2$ and $7=3p$.
3. $m-1=3$ and $m^2+m+1=p$ hence $m=4$ and $21=p$.
4. $m-1=p$ and $m^2+m+1=3$ hence $0=p$ and $m=1$.

Third case $k=2$, $d_{m\pm}=(m\pm 1)(m^2\mp m+1)=pq$, also four situation are possible for K_{m+}:

1. $m+1=pq$ and $m^2-m+1=1$ hence $pq=2$ and $m=1$.
2. $m+1=1$ and $m^2-m+1=pq$.
3. $m+1=p$ and $m^2-m+1=q$ with $p\equiv 2 \pmod 9$ and $q\equiv 5 \pmod 9$ i.e $m\equiv 1 \pmod 9$ and $m^2-m\equiv 4 \pmod 9$.
4. $m+1=q$ and $m^2-m+1=p$ with $p\equiv 2 \pmod 9$ and $q\equiv 5 \pmod 9$ i.e $m^2-m\equiv 1 \pmod 9$ and $m\equiv 4 \pmod 9$ therefore $m^2-m\equiv 1 \pmod 9$ and $m^2-m\equiv 3 \pmod 9$.

And four situation for K_{m-}:

1. $m-1=pq$ and $m^2+m+1=1$ hence $pq=2$ and $m=0$.
2. $m-1=1$ and $m^2+m+1=pq$ hence $m=2$ and $7=pq$.
3. $m-1=p$ and $m^2+m+1=q$ with $p\equiv 2 \pmod 9$ and $q\equiv 5 \pmod 9$ i.e $m\equiv 3 \pmod 9$ and $m^2+m\equiv 4 \pmod 9$.
4. $m-1=q$ and $m^2+m+1=p$ with $p\equiv 2 \pmod 9$ and $q\equiv 5 \pmod 9$ i.e $m^2+m\equiv 1 \pmod 9$ and $m\equiv 6 \pmod 9$.

It follows that all the possible forms of $d_{m\pm}$ do not appear in the main result of [[5], p8], except for the case $d_{m\pm}=p=2$, $(m=1)$. Which proves our theorem. □

3. Fundamental unit of $K_{m\pm}$

Theorem 3.1 *Let $K_{m\pm}=\mathbb{Q}(\sqrt[3]{m^3\pm 1})$ where $m\geq 1$ is an integer such that $d_{m\pm}=m^3\pm 1$ is square-free and $d_{m\pm}\not\equiv \pm 1 \pmod 9$. Then the fundamental unit of $K_{m\pm}$ is $\eta_{m\pm}=m^2+m\theta_{m\pm}+\theta^2_{m\pm}$, where $\theta_{m\pm}$ is defined in the introduction.*

Proof: We prove this theorem for K_{m+}. For $m=1$ we have $K_{1+}=\mathbb{Q}(\sqrt[3]{2})$ and $\eta_{1+}=1+\sqrt[3]{2}+\sqrt[3]{2}^2$ is the fundamental unit of K_{1+}, (see [[7],p1135]). For $m\geq 2$, let η_{m+} be the fundamental unit of K_{m+} and let be $\varepsilon_{m+}=m^2+m\theta_{m+}+\theta^2_{m+}$. We can verify by a simple calculation that $\mathcal{N}(\varepsilon_{m+})=1$ which means that ε_{m+} is a unit of K_{m+}. Since $m\geq 2$, then $|\Delta_{K_{m\pm}}|=27(m^3+1)^2\geq 33$, hence by [[1], Theorem 13.6.1] we get

$$\eta^3_{m+}>\frac{|\Delta_{K_{m+}}|-27}{4}$$

it follows that

$$\eta^3_{m+}>\frac{27}{4}m^3(m^3+2)>\frac{27}{8}m^3(m^3+1)$$

therefore $\eta_{m+} > \dfrac{3}{2}m\theta_{m+}$, so $\eta_{m+}^2 > \dfrac{9}{4}m^2\theta_{m+}^2$. Since $\dfrac{9}{4}m^2\theta_{m+}^2 > 3m^2$, $\dfrac{9}{4}m^2\theta_{m+}^2 > 3m\theta_{m+}$ and $\dfrac{9}{4}m^2\theta_{m+}^2 > 3\theta_{m+}^2$, then , $\eta_{m+}^2 > 3m^2$, $\eta_{m+}^2 > 3m\theta_{m+}$ and $\eta_{m+}^2 > 3\theta_{m+}^2$, which means that

$$1 < \varepsilon_{m+} < \eta_{m+}^2.$$

But by Dirichlet's unit theorem we have $\varepsilon_{m+} = \pm\eta_{m+}^k, k \in \mathbb{Z}$, hence we must have $\eta_{m+} = \varepsilon_{m+}$. A similar reasoning for K_{m-}. $\square$

References

1. S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*. Cambridge University Press, New York, 2004.
2. A. Azizi and J. Benamara and M. C. Ismaili and M. Talbi, *On the key-exchange protocol using real quadratic fields*. Annals of the University of Craiova, Mathematics and Computer Science, **48**(2021), 53–62.
3. P. Barrucand and H.Cohn; A rational Genus, Class Number Divisibility, and Unit Theory for Pure Cubic Fields J. Number Theory, 2(1970), 7-21.
4. B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*. American Mathematical, Society, Providence, Rhode Island, 1964.
5. T. Honda, *Pure Cubic Fields whose Class Numbers are Multiples of Three*, J. Number Theory, **3**(1971), 7-12.
6. S. Louboutin, *Class number problems for cubic number fields*. Nagoya Math. J. **138**(1995), 199-208.
7. H. Wada, *A Table of Fundamental Units of Purely Cubic Fields*. Proc. Japan Acad., **46**(1970), 1135-1140.

J. Benamara,

Department of Mathematics, Faculty of Sciences,

Mohammed First University, 60000 Oujda, Morocco.

E-mail address: `benamarajamal@hotmail.fr`