On a conjecture of Lemmermeyer

S. AOUISSI, M. TALBI, M. C. ISMAILI and A. AZIZI

Abstract: Let \( p \equiv 1 \pmod{3} \) be a prime and denote by \( \zeta_3 \) a primitive third root of unity. Recently, Lemmermeyer presented a conjecture about 3-class groups of pure cubic fields \( L = \mathbb{Q}(\sqrt[3]{p}) \) and of their normal closures \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \). The purpose of this paper is to prove Lemmermeyer’s conjecture.

Keywords: Pure cubic fields, Galois closure, 3-class groups, abelian type invariants.
Mathematics Subject Classification 2010: 11R11, 11R16, 11R20, 11R27, 11R29, 11R37.

1 Introduction

Let \( L = \mathbb{Q}(\sqrt[3]{d}) \) be a pure cubic field, where \( d > 1 \) is a cubefree positive integer, \( k = \mathbb{Q}(\sqrt[3]{d}, \zeta_3) \) be its normal closure, and \( C_{k,3} \) be the 3-component of the class group of \( k \).

In a collection of unsolved problems, Lemmermeyer proposed a conjecture for the special pure cubic field \( \mathbb{Q}(\sqrt[3]{p}) \), where \( p \equiv 1 \pmod{3} \) is a prime number [20, Conjecture 5, § 1.10, p. 44]. This conjecture gives a necessary and sufficient condition for the 3-class group \( C_{k,3} \) to be isomorphic to either \( \mathbb{Z}/3\mathbb{Z} \) or \( \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \), and thus specifies the rank of \( C_{k,3} \) as follows:

**Conjecture 1.1.** Let \( L = \mathbb{Q}(\sqrt[3]{p}) \) be a pure cubic field, where \( p \) is a prime number such that \( p \equiv 1 \pmod{3} \), and \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \) be its normal closure. Let \( C_{L,3} \) (resp. \( C_{k,3} \)) be the 3-component of the class group of \( L \) (resp. \( k \)). Then:

1) \( C_{L,3} \) is a cyclic 3-group, and if it contains a cyclic subgroup of order 9, then \( p \equiv 1 \pmod{9} \).

2) If \( p \equiv 4, 7 \pmod{9} \), then:

\[
C_{k,3} \simeq \begin{cases} 
\mathbb{Z}/3\mathbb{Z} & \text{if } \left( \frac{3}{p} \right)_3 \neq 1, \\
(\mathbb{Z}/3\mathbb{Z})^2 & \text{if } \left( \frac{3}{p} \right)_3 = 1.
\end{cases}
\]

3) If \( p \equiv 1 \pmod{9} \), then rank \( C_{k,3} \in \{1, 2\} \), independently of the value of \( \left( \frac{3}{p} \right)_3 \).

Here \( \left( \frac{3}{p} \right)_3 \) is the cubic residue symbol.

In fact, Conjecture 1.1 for \( p \equiv 4, 7 \pmod{9} \) was first expressed in 1970 by Barrucand and Cohn [5, § 8, p. 19], partially proved in 1976 by Barrucand, H. C. Williams and Baniuk [6, § 7, Thm. 1, p. 321, and § 8, Cnj. 1, p. 322], and mentioned again in 1982 by H. C. Williams [24, § 6, p. 273]. Conjecture 1.1 for \( p \equiv 1 \pmod{9} \) was proved partially in 2005 by Gerth [12, Formulas p. 474, and Case 4, pp. 475–476], who also pointed out that Conjecture 1.1 for \( p \equiv 4, 7 \pmod{9} \) is still an open problem.

Based on results concerning the 3-class group \( C_{k,3} \) in § 2.1, we shall prove Conjecture 1.1 in § 2.2. It will be underpinned by numerical examples obtained with the Computational Number Theory System PARI [23] in § 3.1. Throughout this paper, we will use the following notations:
• \( p \) is a prime number such that \( p \equiv 1 \pmod{3} \);
• \( L = \mathbb{Q}(\sqrt[3]{d}) \) is a pure cubic field, where \( d > 1 \) is a cube-free positive integer;
• \( k_0 = \mathbb{Q}(\zeta_3) \), where \( \zeta_3 = e^{2\pi i/3} \) denotes a primitive third root of unity;
• \( k = \mathbb{Q}(\sqrt[3]{d}, \zeta_3) \) is the normal closure of \( L \);
• \( \langle \tau \rangle = \text{Gal}(k/L) \) such that \( \tau^2 = id \), \( \tau(\zeta_3) = \zeta_3^2 \) and \( \tau(\sqrt[3]{d}) = \sqrt[3]{d} \);
• \( \langle \sigma \rangle = \text{Gal}(k/k_0) \) such that \( \sigma^3 = id \), \( \sigma(\zeta_3) = \zeta_3 \), \( \sigma(\sqrt[3]{d}) = \zeta_3 \sqrt[3]{d} \) and \( \tau \sigma = \sigma^2 \tau \);
• \( \lambda = 1 - \zeta_3 \) and \( \pi \) are prime elements of \( k_0 \);
• \( q^* = 1 \) or 0 according to whether \( \zeta_3 \) is or is not norm of an element of \( k \setminus \{0\} \);
• \( u \) denotes the index of the subgroup \( E_0 \) generated by the units of intermediate fields of the extension \( k/\mathbb{Q} \) in the group of units of \( k \);
• \( \mathcal{N}_{k/k_0} \) denotes the norm of \( k \) on \( k_0 \);
• \( t \) denotes the number of prime ideals ramified in \( k/k_0 \);
• \( \left( \frac{p}{3} \right) \) is the cubic residue symbol such that \( \left( \frac{p}{3} \right) = 1 \iff X^3 \equiv c \pmod{p} \) has a solution in \( \mathbb{Z} \iff c^{(p-1)/3} \equiv 1 \pmod{p} \), where \( c \in \mathbb{Z} \), and \( p \) is a prime number such that \( p \nmid c \) and \( p \equiv 1 \pmod{3} \);
• For an algebraic number field \( F \):
  - \( \mathcal{O}_F, E_F \) : the ring of integers and the group of units of \( F \);
  - \( C_{F,3}, F_3^{(1)} \) : the 3-class group and the Hilbert 3-class field of \( F \);
  - \( [\mathcal{I}] \) : the class of a fractional ideal \( \mathcal{I} \) in the class group of \( F \);

2 Proof of Conjecture 1.1

2.1 Preliminary results

Let \( d > 1 \) be a cubefree integer, and let \( L = \mathbb{Q}(\sqrt[3]{d}) \) be the pure cubic field with radicand \( d \). We denote by \( \zeta_3 = (-1 + i\sqrt{3})/2 \) a primitive cube root of unity. By \( k_0 \) we denote the third cyclotomic field \( \mathbb{Q}(\zeta_3) \), by \( k = \mathbb{Q}(\sqrt[3]{d}, \zeta_3) \) the normal closure of the pure cubic field \( L \), and by \( C_{k,3} \) the 3-component of the class group of \( k \). Further, let \( \langle \tau \rangle = \text{Gal}(k/L) \) and \( \langle \sigma \rangle = \text{Gal}(k/k_0) \).

The 3-class group \( C_{k,3} \) can be viewed as a \( \mathbb{Z}_3[\zeta_3]- \) module. According to [11, § 2, Lemma 2.1 and Lemma 2.2, p. 53] we have:

\[
C_{k,3} \cong C_{k,3}^+ \times C_{k,3}^- \quad \text{and} \quad C_{k,3}^+ \cong C_{L,3}.
\]

Define the 3-group \( C_{k,3}^{(1-\sigma)^i} \) for each \( i \in \mathbb{N} \) by \( C_{k,3}^{(1-\sigma)^i} = \{ A^{(1-\sigma)^i} \mid A \in C_{k,3} \} \). Since we always have \( (1 - \zeta_3)^2 \cdot \mathbb{Z}_3[\zeta_3] = 3 \cdot \mathbb{Z}_3[\zeta_3] \), then for each \( i \in \mathbb{N} \) we have \( C_{k,3}^{(1-\sigma)^{i+2}} = (C_{k,3}^{(1-\sigma)^i})^3 \). Consequently, we have the following equation for the rank of the group \( C_{k,3} \):

\[
\text{rank } C_{k,3} = \text{rank } (C_{k,3}/C_{k,3}^3) = \text{rank } (C_{k,3}/C_{k,3}) + \text{rank } (C_{k,3}^{(1-\sigma)^i}/C_{k,3}^{(1-\sigma)^{i+1}}) \quad (1)
\]

The fact that, for each \( i \in \mathbb{N} \), \( C_{k,3}^{(1-\sigma)^i}/C_{k,3}^{(1-\sigma)^{i+1}} \) is a \( \mathbb{Z}_3[\langle \tau \rangle] \) -module implies that:

\[
\text{rank } (C_{k,3}^{(1-\sigma)^i}/C_{k,3}^{(1-\sigma)^{i+1}}) = \text{rank } (C_{k,3}^{(1-\sigma)^i}/C_{k,3}^{(1-\sigma)^{i+1}}) + \text{rank } (C_{k,3}^{(1-\sigma)^i}/C_{k,3}^{(1-\sigma)^{i+1}}).
\]
So, for each $i \in \mathbb{N}$, we consider the homomorphism $\varphi_i$ as follows:

$$\varphi_i : \frac{C^{i(\sigma)^i}}{C^{(i-1)(\sigma)^{i+1}}} \rightarrow \frac{C^{(i-1)(\sigma)^{i+1}}}{C^{(i-2)(\sigma)^{i+2}}}$$

where $A \equiv C^{(i)(\sigma)^{i+1}} \mod C^{(i-1)(\sigma)^{i+2}}$.

Let $B \equiv C^{(i)(\sigma)^{i+1}} / C^{(i-1)(\sigma)^{i+2}}$, then:

$$\text{if } B \equiv C^{(i)(\sigma)^{i+1}} / C^{(i-1)(\sigma)^{i+2}} \text{, then: }$$

$$\begin{align*}
(B^1)^{i-1} & = B^1 - B^1 \equiv B^1 - 1 \mod C^{(i-1)(\sigma)^{i+2}} \nonumber
\end{align*}$$

If $B \equiv (C^{(i)(\sigma)^{i+1}} / C^{(i-1)(\sigma)^{i+2}})$, then:

$$\begin{align*}
(B^1)^{i-1} & = (B^1)^{i-2} = (B^1)^{i-2} \equiv B^1 - \sigma \mod C^{(i-1)(\sigma)^{i+2}} \nonumber
\end{align*}$$

The number of primes ramified in $k/k_0$ and $C^{(i)} = \{ A \in C_{k,3}/ A^\sigma = A \}$ be the ambiguous index class group of $k/k_0$, where $\sigma$ is a generator of $\text{Gal}(k/k_0)$. Then, according to [10, § 5, pp 91-92] we have

$$|C^{(i)}| = 3^{t-2+\sigma^*}.$$ (2)

If we denote by $C_{k,3}$ the Sylow 3-subgroup of the ideal class group of $k_0$, then $C_{k,3} = \{1\}$, and by the exact sequence:

$$1 \rightarrow C^{(i)} \rightarrow C_{k,3} \rightarrow \frac{C_{k,3}}{C^{i-1}C_{k,3}} \rightarrow 1$$

we deduce that

$$|C^{(i)}| = |C_{k,3}/C^{1-i}C_{k,3}|.$$ (3)

The fact that $C^{i(\sigma)} / C^{i-1}C_{k,3}$ are elementary abelian 3-groups implies that:

$$\text{rank } C^{i(\sigma)} = \text{rank } (C_{k,3} / C^{1-i}C_{k,3}).$$

Next, we define the important index of subfield units for the normal closure of a pure cubic field as follows: Put $L' = \mathbb{Q}(\zeta_3, \sqrt[3]{d})$ and $L'' = \mathbb{Q}(\zeta_3, \sqrt[3]{d})$. Let $O_{L}$, $O_{L'}$, $O_{L''}$ and $O_{k_0}$, respectively, be the rings of integers of $k$, $L$, $L'$, and $L''$. Let $E_{k,3}$ be the unit’s group in $O_{k,3}$, and let $E_0$ be the subgroup of $E_{k,3}$ generated by the units in the ring of integers $O_{L}$, $O_{L'}$, $O_{L''}$ and $O_{k_0}$. We let $u$ denote the index $[E_{k,3} : E_0]$. According to [4, § 12, Theorem 12.1, p. 229], there are two possibilities, either $u = 1$ or $u = 3$.

To prove Conjecture 1.1, we must employ the following Lemmas:

**Lemma 2.1.** Let $L = \mathbb{Q}(\sqrt[3]{d})$ be a pure cubic field, where $d > 1$ is a cubefree natural number, and $k = \mathbb{Q}(\sqrt[3]{d}, \zeta_3)$ be its normal closure. Let $C_{L,3}$ (resp. $C_{k,3}$) be the 3-component of the class group of $L$ (resp. $k$), $h_L$ the class number of $L$, and $u$ the index of subfield units, defined as above. Then:

1) $C_{k,3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ($3$ divides $h_L$ exactly and $u = 3$).

2) $C_{L,3} \simeq C_{k,3} \simeq \mathbb{Z}/3\mathbb{Z}$ ($3$ divides $h_L$ exactly and $u = 1$).
Proof.
1) If $C_{k,3} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then $|C_{k,3}| = 9$ and by [4, § 14, Theorem 14.1, p. 232] we have $|C_{k,3}| = \frac{1}{3}(C_{L,3})^2 = 9$. We deduce that $u = 3$ and $|C_{L,3}| = 3$, since the other value for $u$, namely 1, is not possible because otherwise 27 would be a square.

Conversely, if 3 divides $h_2$ exactly and $u = 3$, then $3^2$ divides the class number $h_k$ of $k$ exactly and $|C_{k,3}| = 9$. By [11, § 2, Lemma 2.2, p. 53], the group $C_{k,3}$ is cyclic of order 3. On the other hand, by [11, § 2, Lemma 2.1, p. 53], $C_{k,3} \cong C_{k,3}^+ \times C_{k,3}^-$. Thus we have $|C_{k,3}| = |C_{k,3}^+| \cdot |C_{k,3}^-| = 9$, so $|C_{k,3}^+| = 3$ and $C_{k,3}^-$ is also a cyclic group of order 3. As $C_{k,3}$ is the direct product of two cyclic subgroups of order 3, then $C_{k,3} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2) We have the same proof as above. □

Lemma 2.2. Let $p$ be a prime number such that $p \equiv 1 \pmod{3}$. Let $L = \mathbb{Q}((\sqrt[3]{p}),$, and $k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ be its normal closure. Then, $p = \pi_1 \pi_2$, with $\pi_1$ and $\pi_2$ are two primes of $k_0$ such that $\pi_2 = \pi_1^3$ and $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathbb{O}_{k_0}}$, where $(\tau) = \text{Gal}(k/L)$. Furthermore:

\[ \left( \frac{\zeta_3}{\pi_1} \right)_3 = \left( \frac{\zeta_3}{\pi_2} \right)_3 = 1 \iff \left( \frac{\zeta_3}{p} \right)_3 = 1, \]

where $\left( \frac{\cdot}{\cdot} \right)_3$ is the cubic residue symbol.

Proof. Let $p$ be a prime number such that $p \equiv 1 \pmod{3}$. Then according to [17, § 9, Section 1, prop. 9.1.4, p.110] there is two primes $\pi_1$ and $\pi_2$ of $k_0$ such that $p = \pi_1 \pi_2$, $\pi_2 = \pi_1^3$ and $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathbb{O}_{k_0}}$.

$\Leftarrow$: It is clear that if $\left( \frac{\zeta_3}{\pi_1} \right)_3 = 1$ then $\left( \frac{\zeta_3}{\pi_2} \right)_3 = \left( \frac{\zeta_3}{p} \right)_3 = 1$.

$\Rightarrow$: If $\left( \frac{\zeta_3}{\pi_1} \right)_3 = \left( \frac{\zeta_3}{\pi_2} \right)_3 = 1$, then the equations

\[ \begin{cases} \zeta_3 \equiv X^3 \pmod{\pi_1}, \\ \zeta_3 \equiv Y^3 \pmod{\pi_2}, \end{cases} \]

are solvable in $\mathbb{O}_{k_0}$, and we have $X \equiv Z(\pmod{\pi_1})$ and $Y \equiv Z(\pmod{\pi_2})$ because $\mathbb{O}_{k_0}/(\pi_1)$ is a field. Then $X = Z \not\equiv 0$ in $\mathbb{O}_{k_0}/(\pi_1)$, then $X^3 = Z^3$ in $\mathbb{O}_{k_0}/(\pi_1)$, thus $X^3 \equiv Z^3(\pmod{\pi_1})$ is solvable in $\mathbb{O}_{k_0}$. Similarly for $Y$, we obtain $Y^3 \equiv Z^3(\pmod{\pi_2})$ is solvable in $\mathbb{O}_{k_0}$. Then

\[ \begin{cases} \zeta_3 \equiv Z^3 \pmod{\pi_1}, \\ \zeta_3 \equiv Z^3 \pmod{\pi_2}, \end{cases} \]

are solvable in $\mathbb{O}_{k_0}$. So $(\zeta_3 - Z^3)$ is in $\mathbb{O}_{k_0}$ because $\pi_1$ and $\pi_2$ are two different primes of $k_0$. Since $(\pi_1, \pi_2) = 1$, then according to Gauss’s Theorem we get $\pi_1 \pi_2 | (\zeta_3 - Z^3)$ in $\mathbb{O}_{k_0}$, which implies that $\zeta_3 \equiv Z^3(\pmod{p})$ is solvable in $\mathbb{O}_{k_0}$, since $p = \pi_1 \pi_2$. Thus $\left( \frac{\zeta_3}{p} \right)_3 = 1$.

□

Lemma 2.3. Let $p$ be a prime number such that $p \equiv 1 \pmod{3}$. If $\left( \frac{\zeta_3}{p} \right)_3 = 1$, then $p \equiv 1 \pmod{9}$, where $\left( \frac{\cdot}{\cdot} \right)_3$ is the cubic residue symbol.

Proof. Let $p$ be a prime number such that $p \equiv 1 \pmod{3}$. Let us assume $\left( \frac{\zeta_3}{p} \right)_3 = 1$.

Since $p \equiv 1 \pmod{3}$, then according to [17, § 9, Section 1, prop. 9.1.4, p.110], $p = \pi_1 \pi_2$ where $\pi_1$ and $\pi_2$ are two primes of $k_0$ such that $\pi_2 = \pi_1^3$. According to [19, § 7.3, Theorem 7.8, p. 217]
we obtain \( \pi_1 = a + b\zeta_3 \) and \( \pi_2 = a + b\zeta_3^2 \), with \( a = 3m + 1 \) and \( b = 3n \), where \((n, m) \in \mathbb{N}^2\). Then:

\[
p = \pi_1\pi_2 = (a + b\zeta_3)(a + b\zeta_3^2) = a^2 + b^2 - ab = (3m + 1)^2 + (3n)^2 - (3m + 1)(3n) = 9m^2 + 9n^2 - 9mn + 6m - 3n + 1 \equiv 6m - 3n + 1 \pmod{9}
\]

According to [19, § 7.3, Theorem 7.8, p. 217] we have

\[
\left( \frac{\zeta_3}{p} \right)_3 = \zeta_3^{-\frac{m+n}{3}} = \zeta_3^{-(m+n)},
\]

then

\[
\left( \frac{\zeta_3}{p} \right)_3 = \begin{cases} 
1, & \text{if } m+n \equiv 0 \pmod{3}, \\
\zeta_3, & \text{if } m+n \equiv -1 \pmod{3}, \\
\zeta_3^2, & \text{if } m+n \equiv -2 \pmod{3},
\end{cases}
\]

since \( \left( \frac{\zeta}{p} \right)_3 = 1 \), then there exist \( k \in \mathbb{N} \) such that \( m+n = 3k \). So

\[
p \equiv 6m - 3n + 1 \pmod{9} = 6m - 3(3k - m) + 1 \pmod{9} = 9m - 9k + 1 \pmod{9} \equiv 1 \pmod{9}.
\]

\[\square\]

**Lemma 2.4.** Let \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \), where \( p \) is a prime number such that \( p \equiv 1 \pmod{3} \). Let \( C^{(\sigma)}_{k,3} \) be the ambiguous ideal class group of \( k/k_0 \), where \( \sigma \) is a generator of \( \text{Gal}(k/k_0) \). Then \( |C^{(\sigma)}_{k,3}| = 3 \).

**Proof.** Since \( p \equiv 1 \pmod{3} \), then according to [17, § 9, Section 1, prop. 9.1.4, p.110] we have \( p = \pi_1\pi_2 \), where \( \pi_1 \) and \( \pi_2 \) are two primes of \( k_0 \) such that \( \pi_2 = \pi_1^\tau \) and \( \pi_1 \equiv \pi_2 \equiv 1 \pmod{3}\mathcal{O}_{k_0} \). We study all cases depending on the congruence class of \( p \) modulo 9, then:

- If \( p \equiv 4 \) or \( 7 \pmod{9} \), then according to [9, § 4, pp. 51-55], the prime \( 3 \) is ramified in the field \( L \), so the prime ideal \( (1 - \zeta_3) \) is ramified in \( k/k_0 \). Also \( \pi_1 \) and \( \pi_2 \) are totally ramified in \( k \). So \( t = 3 \). As \( p \equiv 4 \) or \( 7 \pmod{9} \), then \( \pi_1\pi_2 = p \equiv 4 \) or \( 7 \pmod{(1 - \zeta_3)^3} \) because \( 9 = 3^2 = (\zeta_3^3(1 - \zeta_3)^3)^2 = \zeta_3(1 - \zeta_3)^3 \) (cf. [17, § 9, Section 1, prop. 9.1.4, p.110]), so \( p = \pi_1\pi_2 \equiv 4 \) or \( 7 \pmod{(1 - \zeta_3)^3} \). Thus \( \pi_1 \) and \( \pi_2 \neq 1 \pmod{(1 - \zeta_3)^3} \), and according to [10, § 5, pp. 91-92] we obtain

\[
\left( \frac{\zeta_3, p}{\pi_1} \right)_3 \neq 1
\]

where the symbol \((\cdot)_3 \) is the cubic Hilbert symbol. We deduce that \( \zeta_3 \) is not a norm in the extension \( k/k_0 \), so \( q^* = 0 \). By Equation (2) we get \( |C^{(\sigma)}_{k,3}| = 3 \).

- If \( p \equiv 1 \pmod{9} \), then the prime ideals which ramify in \( k/k_0 \) are \( (\pi_1) \) and \( (\pi_2) \), so \( t = 2 \). Moreover, \( \pi_1 \equiv \pi_2 \equiv 1 \pmod{(1 - \zeta_3)^3} \). Thus, according to [10, § 5, pp. 91-92], the cubic Hilbert symbol is:

\[
\left( \frac{\zeta_3, p}{\pi_1} \right)_3 = \left( \frac{\zeta_3, p}{\pi_2} \right)_3 = 1.
\]

We conclude that \( \zeta_3 \) is a norm in the extension \( k/k_0 \), that is, \( q^* = 1 \), so according to Equation (2) we obtain \( |C^{(\sigma)}_{k,3}| = 3 \).
Next, we specify the rank of $C_{k,3}$ as follows:

**Lemma 2.5.** Let $k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$, where $p$ is a prime number such that $p \equiv 1 \pmod{3}$. Let $s$ be the non-null positive integer such that $C_{k,3}^{(s)} \subseteq C_{k,3}^{(1-s)}$ but $C_{k,3}^{(s)} \nsubseteq C_{k,3}^{(1-s)}$, where $C_{k,3}^{(s)}$ denotes the ambiguous ideal class group of $k/\mathbb{Q}(\zeta_3)$ and $s$ is a generator of $\text{Gal}(k/\mathbb{Q}(\zeta_3))$. Let $C_{k,3}$ be the 3-component of the class group of $k$, then $|C_{k,3}| = 3^s$, and rank $C_{k,3} = 1$ or 2. Furthermore

$$C_{k,3} \simeq \begin{cases} \left(\mathbb{Z}/3^\frac{s}{2}\mathbb{Z}\right)^2, & \text{if } s \text{ is even}, \\ \mathbb{Z}/3 \times \mathbb{Z}/3^\frac{s}{2}\mathbb{Z}, & \text{if } s \text{ is odd}, \end{cases}$$

*Proof.* We have $p \equiv 1 \pmod{3}$, then by Lemma 2.4, $|C_{k,3}^{(s)}| = 3$. Since $|C_{k,3}^{(s)}| = |C_{k,3}/C_{k,3}^{(1-s)}|$, then

$$|C_{k,3}/C_{k,3}^{(1-s)}| = |C_{k,3}^{(1-s)}/C_{k,3}^{(1-s)}| = \ldots = |C_{k,3}^{(1-s)^{s-1}}/C_{k,3}^{(1-s)^s}| = 3,$$

where $s$ is the positive integer defined above, and we have

$$|C_{k,3}| = |C_{k,3}^{(1-s)}| \times |C_{k,3}^{(1-s)}/C_{k,3}^{(1-s)}|^2 \times \ldots \times |C_{k,3}^{(1-s)^{s-1}}/C_{k,3}^{(1-s)^s}| = 3^s.$$

According to Equation (1), it is easy to see that

$$\text{rank } C_{k,3} = \begin{cases} 1 & \text{if } s = 1, \\ 2 & \text{if } s > 1. \end{cases}$$

Next, let $k_3^{(1)}$ be the maximal abelian unramified 3-extension of $k$. So $k_3^{(1)}/k_0$ is Galois, and according to class field theory we have

$$\text{Gal} \left( k_3^{(1)}/k \right) \cong C_{k,3}. \quad (3)$$

We denote by $(k/k_0)^*$ the maximal abelian extension of $k_0$ contained in $k_3^{(1)}$, which is called the *relative genus field* of $k/k_0$ (cf. [15, § 2, p. VII-3]). So the commutator subgroup of $\text{Gal} \left( k_3^{(1)}/k_0 \right)$ coincides with $\text{Gal} \left( k_3^{(1)}/(k/k_0)^* \right)$ and thus

$$\text{Gal} \left( (k/k_0)^*/k_0 \right) \cong \text{Gal} \left( k_3^{(1)}/k_0 \right)/\text{Gal} \left( k_3^{(1)}/(k/k_0)^* \right).$$

The fact that $k/k_0$ is abelian and that $k \subseteq (k/k_0)^*$ implies that $\text{Gal} \left( k_3^{(1)}/(k/k_0)^* \right)$ coincides with $C_{k,3}^{1-s}$, with the aid of the isomorphism (3) above and by Artin’s reciprocity law. $C_{k,3}^{1-s}$ is called the *principal genus* of $C_{k,3}$. Thus

$$\text{Gal} \left( (k/k_0)^*/k \right) \cong C_{k,3}/C_{k,3}^{1-s}.$$

Since $|C_{k,3}/C_{k,3}^{1-s}| = |C_{k,3}^{(s)}| = 3$, then $(k/k_0)^*$ is an unramified cyclic cubic extension of $k$ of degree 3 which is an abelian extension of $k_0$.

Since $p \equiv 1 \pmod{3}$, then according to [17, § 9, Section 1, prop. 9.1.4, p.110] we have $p = \pi_1\pi_2$, where $\pi_1$ and $\pi_2$ are two primes in $k_0$ such that $\pi_2 = \pi_1^3$. Let $\zeta_p$ be a primitive $p$th root of unity. If we denote by $k_p$ the unique sub-field of $\mathbb{Q}((\zeta_p))$ of degree 3 in which only $p$ ramifies, then $k_pk_0 = \mathbb{Q}(\zeta_3, \sqrt[3]{\pi_1\pi_2})$. Hence $(k/k_0)^* = k(\sqrt[3]{\pi_1\pi_2})$. From the congruence:

$$(\pi_1\pi_2)^3 = \pi_2\pi_1^2 \equiv (\pi_1\pi_2)^{-1} \mod (k^*)^3,$$

we conclude by Kummer theory and according to [11, Proposition 2.4, p. 54] that:

\[\square\]
\[ |\left(\frac{C_{k,3}}{C_{k,3}^{1-\sigma}}\right)^+| = 3 \quad \text{and} \quad |\left(\frac{C_{k,3}}{C_{k,3}^{1-\sigma}}\right)^-| = 1. \]

However, by the observations on the surjective maps \( \varphi_i \), above, for each integer \( i \) such that \( 0 \leq i \leq s-1 \) we have:

\[ |\left(\frac{C_{k,3}^{(1-\sigma)^i}}{C_{k,3}}\right)^+| = \begin{cases} 3, & \text{if } s \text{ is even}, \\ 1, & \text{if } s \text{ is odd}. \end{cases} \]

and

\[ |\left(\frac{C_{k,3}^{(1-\sigma)^i}}{C_{k,3}}\right)^-| = \begin{cases} 1, & \text{if } s \text{ is even}, \\ 3, & \text{if } s \text{ is odd}. \end{cases} \]

We conclude that:

\[ |C^+_k| = \begin{cases} 3^\frac{s}{2}, & \text{if } s \text{ is even}, \\ 3^\frac{s+1}{2}, & \text{if } s \text{ is odd}. \end{cases} \]

and

\[ |C^-_k| = \begin{cases} 3^\frac{s}{2}, & \text{if } s \text{ is even}, \\ 3^\frac{s+1}{2}, & \text{if } s \text{ is odd}. \end{cases} \]

Since rank \( C_{k,3} \in \{1, 2\} \), then \( C^+_k \) and \( C^-_k \) are a cyclic 3-groups. Hence:

\[ C_{k,3} \cong \begin{cases} (\mathbb{Z}/3^\frac{s}{2}\mathbb{Z})^2, & \text{if } s \text{ is even}, \\ \mathbb{Z}/3^\frac{s+1}{2}\mathbb{Z} \times \mathbb{Z}/3^\frac{s+1}{2}\mathbb{Z}, & \text{if } s \text{ is odd}. \end{cases} \]

**Lemma 2.6.** Let \( k = \mathbb{Q}(\sqrt[p]{\zeta}_3) \), where \( p \) is a prime number such that \( p \equiv 1 \pmod{3} \). Let \( C^{(\sigma)}_{k,3} = \{A \in C_{k,3} / A^\sigma = A\} \) be the ambiguous ideal class group of \( k/k_0 \), and \( u \) be the index of subfield units defined as above.

(i) If \( |\left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^+| = 3 \), then \( u = 1 \),

(ii) If \( |\left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^+| = 1 \), then \( u = 3 \),

where \( \left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^+ \) and \( \left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^- \) are defined in [11, § 2, Lemma 2.1, p. 53].

**Proof.** Let \( C_{k,3} \) be the 3-component of the class group of \( k \). According to [11, § 2, Lemma 2.1 and Lemma 2.2, p. 53], \( C_{k,3} \cong C_{L,3} \times C_{k,3}^- \), where \( C_{L,3} \) is the 3-component of the class group of \( L = \mathbb{Q}(\sqrt[p]{\zeta}) \). Let \( s \) be the positive integer defined in Lemma 2.5. From proof of Lemma 2.5 we obtain:

\[ |C_{L,3}| = \begin{cases} 3^\frac{s}{2}, & \text{if } s \text{ is even}, \\ 3^\frac{s+1}{2}, & \text{if } s \text{ is odd}, \end{cases} \]

and

\[ |C^-_{k,3}| = \begin{cases} 3^\frac{s}{2}, & \text{if } s \text{ is even}, \\ 3^\frac{s+1}{2}, & \text{if } s \text{ is odd}. \end{cases} \]

According to [4, § 14, Theorem 14.1, p. 232], \( C_{k,3} = \frac{u}{3} |C_{L,3}|^2 \), where \( u = 1 \) or \( 3 \). By Lemma 2.5, we have \( |C_{k,3}| = 3^s \), thus:

(i) If \( |\left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^+| = 3 \) and \( |\left(\frac{C^{(\sigma)}_{k,3}}{C_{k,3}}\right)^-| = 1 \), the integer \( s \) is odd, whence \( |C_{k,3}| \) is not a square, and thus \( u = 1 \).
(ii) Conversely, if $|C_{k,3}^{(\sigma)}|^+ = 1$ and $|C_{k,3}^{(\sigma)}|^- = 3$, the integer $s$ is even, whence $|C_{k,3}|$ is a square, and thus $u = 3$.

\[ \square \]

**Lemma 2.7.** Let $L = \mathbb{Q}(\sqrt{p})$, where $p$ is a prime number such that $p \equiv 1 \pmod{3}$, and $k = \mathbb{Q}(\sqrt{p},\zeta_3)$. The prime $p$ decomposes in the field $k$ as $P^3Q^3$, where $P$ and $Q$ are two prime ideals of $k$, and $Q$ is the conjugate of $P$. Let $u$ and $s$ be the integers defined as above. Then the following statements are equivalent:

1) $u = 3$;

2) $s$ is even;

3) $P$ is not principal.

**Proof.** Let $C_{k,3}^{(\sigma)}$ be the group of ambiguous ideal classes of $k/k_0$. Since $p \equiv 1 \pmod{3}$, then by Lemma 2.4, $|C_{k,3}^{(\sigma)}| = 3$. If we denote by $I_k$ the group of fractional ideals of $k$, we let $S_{k,3}^{(\sigma)} = \{A \in C_{k,3} | \exists B \in I_k \text{ such that } A = [B] \text{ and } B^{1-\sigma} = (1)\}$ be the group of strongly ambiguous ideal classes of the cyclic extension $k/k_0$. It is known that $S_{k,3}^{(\sigma)}$ is generated by the ideal classes of the primes ramified in $k/k_0$.

1) $\Rightarrow$ 2) Let $h_{L,3}$ (resp. $h_{k,3}$) be the 3-class number of $L$ (resp $k$). By [4, § 14, Theorem 14.1, p. 232] we have $h_{k,3} = \frac{u}{3}h_{L,3}$. If $u = 3$, then $h_{k,3}$ is a square, so the integer $s$ is even.

2) $\Rightarrow$ 3) First, since $p \equiv 1 \pmod{3}$, then by [17, § 9, Section 1, prop. 9.1.4, p.110] we have $p = \pi_1\pi_2$, where $\pi_1$ and $\pi_2$ are two primes of $k_0$ such that $\pi_1 = \pi_2^2$ and $\pi_2 = \pi_1^2$ and $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3O_{k_0}}$. Furthermore, $\pi_1$ and $\pi_2$ are ramified in $k_0$, so there exist two prime ideals $P$ and $Q$ of $k$ such that $\pi_1O_k = P^3$ and $\pi_2O_k = Q^3$. Then $pO_k = P^3Q^3$.

Next, let $s$ be even, where $s$ is the non-null positive integer defined in Lemma 2.5. We shall prove that the prime ideal $P$ is not principal. Assume that $P$ is principal. The fact that $p \equiv 1 \pmod{3}$ implies that $|C_{k,3}^{(\sigma)}| = 3$ according to Lemma 2.4. We study all cases in dependence on the congruence class of $p$ modulo 9:

- If $p \equiv 1 \pmod{9}$, then $3$ is decomposes in $L$ by [9, § 4, pp. 51-55]. The prime ideals which ramify in $k/k_0$ are $(\pi_1)$ and $(\pi_2)$. Since $P$ is principal, the prime ideal $Q$ is also principal. Thus a generator of $C_{k,3}^{(\sigma)}$ does not contain the classes of prime ideals lying above the primes ramified in the extension $k/k_0$. So, a generator of $C_{k,3}^{(\sigma)}$ comes from $C_{k,3}^+$ (cf. [13, Proposition 2, part (1), p. 679]). This implies that

$$|C_{k,3}^{(\sigma)}|^+ = 3 \quad \text{and} \quad |C_{k,3}^{(\sigma)}|^- = 1,$$

where $C_{k,3}^{(\sigma)}$ and $C_{k,3}^{(\sigma)}$ are defined in [11, § 2, Lemma 2.1, p. 53]. By Lemma 2.6 we see that the integer $s$ is odd. This contradicts the fact that $s$ is even. Thus $P$ is not principal.

- If $p \equiv 4$ or $7 \pmod{9}$, then $3$ is ramified in $L$ by [9, § 4, pp. 51-55], so the prime ideals which ramify in $k/k_0$ are $(1 - \zeta_3)$, $(\pi_1)$ and $(\pi_2)$. Let $I$ be the unique prime ideal above $(1 - \zeta_3)$ in $k$. The fact that $p \equiv 4$ or $7 \pmod{9}$ implies according to [1, § 3, Lemma 3.1, p. 16] that $\pi_i \not\equiv 1 \pmod{(1 - \zeta_3)^3}$ for $i = \{1,2\}$. Thus, according to [1, § 3, Lemma 3.3, p. 17] we get $\zeta_3$ is not a norm in the extension $k/k_0$, so $S_{k,3}^{(\sigma)} = C_{k,3}^{(\sigma)}$. Hence, $C_{k,3}^{(\sigma)}$ is generated by the ideal classes of the primes ramified in $k/k_0$.  

8
* If $I$ is not principal, then the ideal class $[I]$ of $I$ generates the group $C_{k,3}^{(\sigma)}$ and it is not contained in $C_{k,3}^{1-\sigma}$. We see that $s = 1$ which contradicts the fact that $s$ is even.

* If $I$ is principal, and since $P$ and $Q$ are also principal, then $C_{k,3}^{(\sigma)}$ will be reduced to $\{1\}$, which contradict the fact that $|C_{k,3}^{(\sigma)}| = 3$.

Hence, the prime ideal $P$ is not principal.

3) $\Rightarrow$ 1): We note that $PQ = (\sqrt{P})$ is a principal ideal. Assume that $P$ is not principal, then the prime ideal $Q = P^r$ is also not principal. Then $PQ^2$ is also not principal and the ideal class of $PQ^2$ generates the group $C_{k,3}^{(\sigma)}$. In addition, we have $(PQ^2)^r = PQ^2$ which implies that $|PQ^2|^r = |PQ^2| = |PQ^2|^{-1}$. Thus, $[PQ^2] \in \left( C_{k,3}^{(\sigma)} \right)^{-1}$. According to [11, § 2, Lemma 2.1, p. 53], $C_{k,3}^{(\sigma)} \simeq (C_{k,3}^{(\sigma)})^+ \times (C_{k,3}^{(\sigma)})^-$. Since $p \equiv 1 \pmod{3}$, then by Lemma 2.4, $|C_{k,3}^{(\sigma)}| = 3$, and as $[PQ^2] \in \left( C_{k,3}^{(\sigma)} \right)^-$, we obtain:

$$\left| C_{k,3}^{(\sigma)} \right|^+ = 1 \quad \text{and} \quad \left| C_{k,3}^{(\sigma)} \right|^- = 3.$$

We see that the integer $s$ is even, so the class number $h_{k,3}$ is a square. Hence $u = 3$.

\[\square\]

**Lemma 2.8.** Let $k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$, where $p$ is a prime number such that $p \equiv 4$ or $7 \pmod{9}$. Let $u$ be the index of subfield units defined as above. Then:

$$\left( \frac{3}{p} \right)_3 \neq 1 \iff (3 \mid |C_{L,3}| \text{ and } u = 3),$$

where $\left( \frac{3}{p} \right)_3$ is the cubic residue symbol.

**Proof.** Lemma 2.8 is due to Ismaili and El Mesaoudi for $e = 0$ in assertion (1) of [18, Thm. 3.2, p. 104]. \[\square\]

### 2.2 Final Proof of Conjecture 1.1

Let $L = \mathbb{Q}(\sqrt[3]{p})$ be a pure cubic field, where $p$ is a prime number such that $p \equiv 1 \pmod{3}$, and let $k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ be its normal closure. Let $C_{L,3}$ (resp. $C_{k,3}$) be the 3-component of the class group of $L$ (resp $k$).

1) It is clear that $C_{L,3}$ is a cyclic group when $s = 1$. Assume that $s \geq 2$. From the proof of Lemma 2.5, $C_{k,3}^{+}$ and $C_{k,3}^{-}$ are two non-trivial groups, and according to Lemma 2.5 we deduce that $C_{k,3}^{+}$ is a cyclic group, because otherwise the rank of $C_{k,3}$ will be greater than or equal to $3$. According to [11, § 2, Lemma 2.2, p. 53], we conclude that $C_{L,3}$ is a cyclic group.

Now, let us show that $p \equiv 1 \pmod{9}$ when $C_{L,3}$ contains a cyclic subgroup of order 9. This equivalent to the statement that if $p \equiv 4$ or $7 \pmod{9}$ then the class number of $L$ is divisible exactly by $3$.

Assume that $p \equiv 4$ or $7 \pmod{9}$ and $9$ divides the class number of $L$, then $\left( \frac{2}{p} \right)_3 = 1$. In fact, if $\left( \frac{2}{p} \right)_3 \neq 1$, then from the proof of Lemma 2.8 the class number of $L$ is divisible exactly by $3$ which is absurd.

Since $p = \pi_1 \pi_2$, where $\pi_1$ and $\pi_2$ are two primes of $k_0$ such that $\pi_2 = \pi_1^7$, then the equations $3 \equiv X^3 \pmod{\pi_1}$ and $3 \equiv X^3 \pmod{\pi_2}$ are solvable in $\mathcal{O}_{k_0}$ (cf. [17, § 9, Section 3, prop. 9.3.3], [17, § 9, Section 3, prop. 9.3.3], 9)
so $3$ is a cubic residue modulo $\pi_1$ and $3$ is a cubic residue modulo $\pi_2$. According to [17, §9, Section 1, prop. 9.1.4, p.110], we have $3 = -\zeta_3^2\lambda^2$, where $\lambda = 1 - \zeta_3$ is a prime of $k_0$, thus:

$$\left(\frac{-\zeta_3^2\lambda^2}{\pi_1}\right)_3 = \left(\frac{-\zeta_3^2\lambda^2}{\pi_2}\right)_3 = 1.$$ 

Since $-1$ is a norm in $k_0(\sqrt[3]{\pi_1})/k_0$ and a norm in $k_0(\sqrt[3]{\pi_2})/k_0$, then

$$\left(\frac{-1}{\pi_1}\right)_3 = \left(\frac{-1}{\pi_2}\right)_3 = 1,$$

so

$$\left(\frac{\zeta_3^2\lambda^2}{\pi_1}\right)_3 = \left(\frac{\zeta_3^2\lambda^2}{\pi_2}\right)_3 = 1.$$

Hence

$$\left(\frac{\zeta_3\lambda}{\pi_1}\right)_3 = \left(\frac{\zeta_3\lambda}{\pi_2}\right)_3 = 1.$$

The fields $k_0(\sqrt[3]{\lambda})$ and $k_0(\sqrt[3]{\zeta_3})$ are different. Put $F_1 = k_0(\sqrt[3]{\zeta_3})$ and $F_2 = k_0(\sqrt[3]{\lambda})$. We have $F_1 \neq F_2$, and $F_1 \cap F_2 = k_0$. Let $F = F_1F_2 = k_0(\sqrt[3]{\zeta_3}, \sqrt[3]{\lambda})$. Then in the subfield diagram

$$F = F_1F_2$$

$$F_1 = k_0(\sqrt[3]{\zeta_3})$$

$$F_2 = k_0(\sqrt[3]{\lambda})$$

$$k_0 = \mathbb{Q}(\zeta_3)$$

we have $\text{Gal}(F_1/k_0)$ and $\text{Gal}(F_2/k_0)$ are cyclic of order 3, and $\text{Gal}(F/k_0)$ is abelian. Since $\pi_1$ is not ramified in $F_1$ and $F_2$, then $\pi_1$ is also not ramified in $F$. We will calculate the Artin symbol $\left(\frac{F/k_0}{\pi_1}\right)$. On the one hand:

$$\left(\frac{F/k_0}{\pi_1}\right) = \left(\frac{F_1F_2/k_0}{\pi_1}\right) = \left(\frac{F_1/k_0}{\pi_1}\right) \left(\frac{F_2/k_0}{\pi_1}\right) = \left(\frac{k_0(\sqrt[3]{\zeta_3})/k_0}{\pi_1}\right) \left(\frac{k_0(\sqrt[3]{\lambda})/k_0}{\pi_1}\right) = \left(\frac{\zeta_3}{\pi_1}\right)_3 \left(\frac{\lambda}{\pi_1}\right)_3 = \left(\frac{\zeta_3\lambda}{\pi_1}\right)_3 = 1.$$
On the other hand, since $k_0(\sqrt[3]{3}) = k_0(\sqrt[3]{2})$, we get:

\[
\left(\frac{F/k_0}{\pi_1}\right) = \left(\frac{F_1F_2/k_0}{(\pi_1)}\right)
= \left(\frac{F_1/k_0}{(\pi_1)}\right) \left(\frac{F_2/k_0}{(\pi_1)}\right)
= \left(\frac{k_0(\sqrt[3]{3})/k_0}{(\pi_1)}\right) \left(\frac{k_0(\sqrt[3]{2})/k_0}{(\pi_1)}\right)
= \left(\frac{\zeta_3^2}{\pi_1}\right) \left(\frac{\lambda}{\pi_1}\right)_{3}
= \left(\frac{\zeta_3^2\lambda}{\pi_1}\right)_{3}
\]

We see that $\left(\frac{\zeta_3^2\lambda}{\pi_1}\right)_{3} = 1$, and since $\left(\frac{\zeta_3\lambda}{\pi_1}\right)_{3} = 1$, we conclude that

\[
\left(\frac{\zeta_3}{\pi_1}\right)_{3} = 1,
\]

(4)

However, since $\pi_2$ is not ramified in $F_1$ and $F_2$, then $\pi_2$ is also not ramified in $F$. As above, we calculate the Artin symbol $\left(\frac{F/k_0}{\pi_2}\right)$, we obtain $\left(\frac{\zeta_3\lambda}{\pi_2}\right)_{3} = 1$, and since $\left(\frac{\zeta_3\lambda}{\pi_2}\right)_{3} = 1$, we get

\[
\left(\frac{\zeta_3}{\pi_2}\right)_{3} = 1,
\]

(5)

From the cubic symbols (4) and (5) we conclude according to Lemma 2.2 that $\left(\frac{\zeta_3}{\pi}\right)_{3} = 1$, so by Lemma 2.3 we obtain $p \equiv 1 \pmod{9}$ which contradicts the hypothesis that $p \equiv 4$ or $7 \pmod{9}$. Hence, if $p \equiv 4$ or $7 \pmod{9}$ then the class number of $L$ is divisible exactly by 3.

2) Let $p$ be a prime number such that $p \equiv 4$ or $7 \pmod{9}$.

- If $\left(\frac{2}{p}\right)_{3} \neq 1$, then according to Lemma 2.8 we get $|C_{L,3}| = 3$ and $u = 1$, and by Lemma 2.1 we deduce that $C_{k,3} \simeq \mathbb{Z}/3\mathbb{Z}$.

- If $\left(\frac{2}{p}\right)_{3} = 1$, then by Lemma 2.8 we have either 3 is not divide $|C_{L,3}|$ or $u = 3$. Assume that 3 is not divide $|C_{L,3}|$, then according to [16, §1, Thm. p. 8] the prime $p$ is congruent to $-1 \pmod{3}$, which is a contradiction because $p \equiv 4$ or $7 \pmod{9}$. Hence, we have necessary $u = 3$ and 3 divide $|C_{L,3}|$, then $|C_{L,3}| = 3$ from assertion 1) above. By Lemma 2.1 we deduce that $C_{k,3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

3) According to Lemma 2.5, we get rank $C_{k,3} \in \{1, 2\}$. On the one hand, for the prime numbers $p = 271$ and $p = 307$, we have $\left(\frac{2}{p}\right)_{3} = 1$ and $p \equiv 1 \pmod{9}$, moreover for $p = 271$, rank $C_{k,3} = 2$ and for $p = 307$, rank $C_{k,3} = 1$.

On the other hand, the primes $p = 379$ and $p = 487$ satisfy $\left(\frac{2}{p}\right)_{3} \neq 1$ and $p \equiv 1 \pmod{9}$, moreover for $p = 379$, rank $C_{k,3} = 1$ and for $p = 487$, rank $C_{k,3} = 2$.

This shows that, if $p \equiv 1 \pmod{9}$, then rank $C_{k,3} \in \{1, 2\}$, independently of the value of $\left(\frac{3}{p}\right)_{3}$.
From Lemmas 2.7 and 2.8, we propose the following Corollary and Proposition:

**Corollary 2.0.1.** Let \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \), where \( p \) is a prime number such that \( p \equiv 4 \) or \( 7 \) (mod 9). Let \( u \) be the index of subfield units defined as above. Then:

\[
\left( \frac{3}{p} \right)_3 \neq 1 \Leftrightarrow u = 3,
\]

where \( \left( \frac{3}{p} \right)_3 \) is the cubic residue symbol.

**Proposition 2.1.** Let \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \), where \( p \) is a prime number such that \( p \equiv 4 \) or \( 7 \) (mod 9). Let \( I, P \) and \( Q \) be the prime ideals defined in the proof of Lemma 2.7. Then:

(i) The unique prime ideal \( P_0 \) above \( p \) in \( \mathbb{Q}(\sqrt[3]{p}) \) is principal independently of the value of \( \left( \frac{3}{p} \right)_3 \).

(ii) \( \left( \frac{3}{p} \right)_3 = 1 \) if and only if \( I \) is principal and \( P \) (resp. \( Q \)) is not principal.

(iii) \( \left( \frac{3}{p} \right)_3 \neq 1 \) if and only if \( I \) is not principal and \( P \) (resp. \( Q \)) is principal.

where \( \left( \frac{3}{p} \right)_3 \) is the cubic residue symbol.

The Proposition 2.1 will be underpinned by numerical examples obtained with the computational number theory system PARI [23] in § 3.

**Proof.** Since \( p \equiv 1 \) (mod 3), then according to [17, § 9, Section 1, prop. 9.1.4, p.110], \( p = \pi_1 \pi_2 \), where \( \pi_1 \) and \( \pi_2 \) are two primes of \( k_0 \) such that \( \pi_2 = \pi_1^3 \) and \( \pi_1 \equiv \pi_2 \equiv 1 \) (mod 3\( \mathcal{O}_{k_0} \)). As \( p \equiv 4 \) or \( 7 \) (mod 9), then \( 3 \) is ramified in \( L \) by [9, § 4, pp. 51-55], so the primes ramified in \( k/k_0 \) are \( (1 - \zeta_3) \pi_1 \) and \( \pi_2 \). Put \( (\pi_1) = P_0^3 \), \( (\pi_2) = Q^3 \) and \( (1 - \zeta_3) = I^3 \).

The fact that \( p \equiv 4 \) or \( 7 \) (mod 9) implies that \( S_k(\sigma) = C_k(\sigma) \), where \( S_k(\sigma) \) and \( C_k(\sigma) \) are defined in the proof of Lemma 2.7. Then \( C_k(\sigma) \) is generated by the ideal classes of the primes ramified in \( k/k_0 \).

(i) Let \( P_0 \) be the unique prime ideal above \( p \) in \( \mathbb{Q}(\sqrt[3]{p}) \), we have \( p\mathcal{O}_L = P_0^3 \), and since \( p\mathcal{O}_k = \mathcal{O}_k^3 \mathcal{O}_Q^3 \), then the ideal \( P_0 = P \mathcal{O}_L = (\sqrt[3]{p}) \) is principal.

(ii) Assume that \( \left( \frac{3}{p} \right)_3 = 1 \), then according to Corollary 2.0.1 we have \( u = 3 \), and by Lemma 2.7 the prime ideal \( P \) is not principal, so \( Q = P^\sigma \) is also not principal. Since \( |C_k(\sigma)| = 3 \) by Lemma 2.4, then \( I \) is principal.

(iii) Reasoning as in (ii). Assume that \( \left( \frac{3}{p} \right)_3 \neq 1 \), then according to Corollary 2.0.1 we have \( u = 3 \), and by Lemma 2.7 the ideal \( P \) is principal, so \( Q = P^\sigma \) is also principal. Since \( |C_k(\sigma)| = 3 \) by Lemma 2.4, then \( I \) is not principal.

\[ \Box \]

**Remark 2.1.** Let \( L = \mathbb{Q}(\zeta_3) \), where \( d > 1 \) is a cube-free integer, let \( k = \mathbb{Q}(\sqrt[3]{d}, \zeta_3) \) be the normal closure of the pure cubic field \( L \) and \( C_{L,3} \) (resp. \( C_{k,3} \)) be the 3-component of the class group of \( L \) (resp. \( k \)).

1) If \( |C_{L,3}| = 3 \), then rank \( C_{k,3} \leq 2 \).
2) If \( |C_{L,3}| = 9 \), then rank \( C_{k,3} \leq 3 \) if \( u = 1 \), and rank \( C_{k,3} \leq 4 \) otherwise.
3) If \( d = p \) or \( p^2 \), with \( p \) is a prime number such that \( p \equiv 1 \) (mod 9), and if 9 divide exactly the class number of \( \mathbb{Q}(\sqrt[3]{d}) \) and \( u = 1 \), then according to [2, § 1, Theorem 1.1, p. 1], the 3-class group of \( \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \) is of type (9, 3). Furthermore, if 3 is not residue cubic modulo \( p \), then a generators of 3-class group of \( \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \) can be deduced by [3, § 3, Theorem 3.2, p. 10].

12
3 Appendix

3.1 Illustrations of Conjecture 1.1

Let \( p \equiv 1 \pmod{3} \) be a prime, \( L = \mathbb{Q}(\sqrt[3]{p}) \), and \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \). Let \( u \) be the index of subfield units defined as above, \( C_{L,3} \) (resp. \( C_{k,3} \)) be the 3-class group of \( L \) (resp. \( k \)).

Table 1: Some numerical examples for Conjecture 1.1.

| \( p \)   | \( p \pmod{9} \) | \( u \) | \( \left(\frac{3}{p}\right)_3 \) | \( C_{L,3} \) | \( \text{rank} \ C_{k,3} \) |
|---------|-----------------|------|-----------------|---------|-----------------|
| 199     | 1               | 1    | 1               | [9]     | 2               |
| 211     | 4               | 1    | \neq 1          | 3       | 1               |
| 223     | 7               | 1    | \neq 1          | 3       | 1               |
| 367     | 7               | 3    | 1               | 3       | 2               |
| 499     | 4               | 3    | 1               | 3       | 2               |
| 541     | 1               | 3    | 1               | [9]     | 2               |

Moreover, in Section 17 of [4, Numerical Data, p. 238], and also in the tables of [7] which give the class number of a pure cubic field, the prime numbers \( p = 61, 67, 103, \) and \( 151 \), which are all congruend to 4 or 7 (mod 9), verify the following properties:

i) 3 is a residue cubic modulo \( p \);

ii) 3 divide exactly the class number of \( L \);

iii) \( u = 3 \);

iv) \( C_{L,3} \simeq \mathbb{Z}/3\mathbb{Z} \), and \( C_{k,3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \).

3.2 Illustrations of Proposition 2.1 and Corollary 2.0.1

Let \( L = \mathbb{Q}(\sqrt[3]{p}) \), and \( k = \mathbb{Q}(\sqrt[3]{p}, \zeta_3) \), where \( p \) is a prime such that \( p \equiv 4 \) or 7 (mod 9). We put \( 3\mathcal{O}_L = I_0^3, p\mathcal{O}_L = \mathcal{P}_0^3, 3\mathcal{O}_k = I^3, \) and \( p\mathcal{O}_k = \mathcal{P}^3Q^3 \).

Table 2: Case where \( p \equiv 4 \) or 7 (mod 9) and \( \left(\frac{3}{p}\right)_3 = 1 \).

| \( p \) | \( u \) | \( \left(\frac{3}{p}\right)_3 \) | \( C_{L,3} \) | \( C_{k,3} \) | \( I_0 \) | \( I \) | \( \mathcal{P}_0 \) | \( \mathcal{P} \) |
|---------|------|-----------------|---------|---------|---------|------|-------------|------|
| 61      | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 67      | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 103     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 151     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 193     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 367     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 439     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 499     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 547     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 619     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 643     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 661     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 727     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 787     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 853     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 967     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
| 997     | 3    | 1               | [3]     | [3, 3]  | [0]     | [0]  | \neq [0]   | \neq 0|
Table 3: Case where $p \equiv 4$ or $7 \pmod{9}$ and $(\frac{2}{p})_3 \neq 1.$

| $p$ | $u$ | $(\frac{2}{p})_3$ | $C_{L,3}$ | $C_{k,3}$ | $I_0$ | $I$ | $P_0$ | $P$ |
|-----|-----|-----------------|-------------|------------|-------|-----|-------|-----|
| 7   | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 13  | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 31  | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 43  | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 79  | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 97  | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 139 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 157 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 211 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 223 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 229 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 241 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 277 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 283 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 313 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |
| 331 | 1   | $\neq 1$        | 3           | $\neq 0$   | $\neq 0$| 0   | 0     | 0   |

4 Acknowledgements
The authors would like to thank Professor Daniel C. Mayer who was of a great help concerning correcting the spelling mistakes and making some precious modifications that gave more value and meaning to the work.

References
[1] S. Aouissi, D. C. Mayer, M. C. Ismaili, M. Talbi, and A. Azizi, 3-rank of ambiguous class groups in cubic Kummer extensions, arXiv preprint, 2018, arXiv:1804.00767v3.
[2] S. Aouissi, M. Talbi, M. C. Ismaili and A. Azizi. Fields $\mathbb{Q}(\sqrt[3]{d},\zeta_3)$ whose 3-class group is of type $(9,3)$. arXiv preprint, 2018, arXiv:1805.04963.
[3] S. Aouissi, M. C. Ismaili, M. Talbi and A. Azizi. The generators of 3-class group of some fields of degree 6 over $\mathbb{Q}$. arXiv preprint, 2018, arXiv:1804.00692.
[4] P. Barrucand and H. Cohn, Remarks on principal factors in a relative cubic field, J. Number Theory 3 (1971), No. 2, 226–239.
[5] P. Barrucand and H. Cohn, A rational genus, class number divisibility, and unit theory for pure cubic fields, J. Number Theory 2 (1970), No. 1, 7–21.
[6] P. Barrucand, H. C. Williams and L. Baniuk, A computational technique for determining the class number of a pure cubic field, Math. Comp. 30 (1976), No. 134, 312–323.
[7] B. D. Beach, H. C. Williams, C. R. Zarnke Some computer results on units in quadratic and cubic fields, Proceeding of the twenty-fifth summer meeting of the Canadian Mathematical Congress (Lake Head Univ., Thunder Bay, Out. 1971), 609-648.
[8] R. A. Mollin, Algebraic number theory, London, UK: Chapman and Hall (1999).
[9] R. Dedekind, Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, J. Reine Angew. Math. 121 (1900), 40–123.
[10] F. Gerth III, *On 3-class groups of cyclic cubic extensions of certain number fields*, J. Number Theory *8* (1976), No. 1, 84–98.

[11] F. Gerth III, *On 3-class groups of pure cubic fields*, J. Reine Angew. Math *278/279* (1975), 52–62.

[12] F. Gerth III, *On 3-class groups of certain pure cubic fields*, Bull. Austral. Math. Soc. *72* (2005), 471–476.

[13] G. Gras, *Sur les ℓ-classes d'idéaux des extensions non galoisiennes de ℚ de degré premier impair ℓ a clôture galoisienne diédrale de degré 2ℓ*, J. Math. Soc. Japan *26* (1974), 677-685.

[14] H. Hasse, *The class number formula of Dedekind-Meyer for simply real cubic fields*, unpublished manuscript.

[15] C. S. Herz, *Construction of Class Fields*, Chapter VII in: A. Borel, et al., Seminar on Complex Multiplication (Inst. Advanced Study, Princeton, 1957–58), Lecture Notes in Math. *21*, Springer-Verlag, New York, 1966.

[16] T. Honda, *Pure cubic fields whose class numbers are multiples of three*, J. Number Theory *3* (1971), No. 1, 7–12.

[17] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math. *84*, Springer-Verlag, New York, 1982.

[18] M. C. Ismaili and R. El Mesaoudi, *Corps cubiques purs dont le nombre de classes est exactement divisible par 3*, Ann. Sci Math. Québec *28* (2004), No. 1–2, 103–112 (2005).

[19] F. Lemmermeyer, *Reciprocity laws: from Euler to Eisenstein*. Springer Science and Business Media, 2013.

[20] F. Lemmermeyer, *Class field towers*, Chapter 1, Section 1.10. Unsolved Problems, Conjecture 5, page 44 (2010).

[21] A. A. Markoff, *Sur les nombres entiers dépendants d’une racine cubique d’un nombre entier ordinaire*, Mém. Acad. Imp. Sci. St. Pétersbourg (Série VII) *38* (1892), No. 9, 1–37.

[22] C. Meyer, *Die Berechnung der Klassenzahl Abelscher Zahlkörper über quadratischen Zahlkörpern*, Akademie Verlag, Berlin, 1957.

[23] PARI Developer Group, PARI/GP, Version 2.9.4, Bordeaux, 2017, http://pari.math.u-bordeaux.fr.

[24] H. C. Williams, *Determination of principal factors in ℚ(√D) and ℚ(√D)*, Math. Comp. *38* (1982), No. 157, 261–274.