

Generators of the 5-class group of fields of degree 20

Fouad ELMOUHIB

Communicated by: Ayman Badawi

MSC 2010 Classifications: 11R04, 11R18, 11R29, 11R37.

Keywords and phrases: pure metacyclic fields, 5-class groups, generators.

The author would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Abstract Let $\Gamma = \mathbb{Q}(\sqrt[5]{n})$ be a pure quintic field, where n is a natural number 5^{th} power-free, $k_0 = \mathbb{Q}(\zeta_5)$ be the cyclotomic field containing a primitive 5^{th} root of unity ζ_5 and $k = \Gamma(\zeta_5)$ be the normal closure of Γ . Let $C_{k,5}$ be the 5-component of the class group of k . The purpose of this paper is to write down the generators of $C_{k,5}$, whenever it is of type $(5, 5)$ and the rank of the group of ambiguous classes under the action of $\text{Gal}(k/k_0)$ is 1.

1 Introduction

Let $\Gamma = \mathbb{Q}(\sqrt[5]{n})$ be a pure quintic field, where n is a 5^{th} power-free natural number, $k_0 = \mathbb{Q}(\zeta_5)$ the cyclotomic field containing a primitive 5^{th} root of unity. Then $k = \Gamma(\zeta_5)$ is the normal closure of Γ . Let $C_{k,5}$ be the 5-class group of k and $C_{k,5}^{(\sigma)}$ the subgroup of ambiguous ideal classes under the action of $\text{Gal}(k/k_0) = \langle \sigma \rangle$. In [4] we showed that there are six possible shapes of the radicand n for which it is possible that $C_{k,5}$ is of type $(5, 5)$ and $C_{k,5}^{(\sigma)} \simeq \mathbb{Z}/5\mathbb{Z}$. Based on some exhaustive numerical calculations realized by the system PARI/GP [19], we conjectured that, among the six possible forms of n , only for three of them one can have $C_{k,5}$ of type $(5, 5)$ and $C_{k,5}^{(\sigma)} \simeq \mathbb{Z}/5\mathbb{Z}$ as follows:

- (1) $n = 5^e p^{e_1} \not\equiv \pm 1, \pm 7 \pmod{25}$ such that $p \not\equiv -1 \pmod{25}$.
- (2) $n = p^{e_1} q^{e_2} \equiv \pm 1, \pm 7 \pmod{25}$ such that $p \not\equiv -1 \pmod{25}$, $q \not\equiv \pm 7 \pmod{25}$.
- (3) $n = p^{e_1} \equiv \pm 1, \pm 7 \pmod{25}$ such that $p \equiv -1 \pmod{25}$.

Here p and q are primes such that $p \equiv -1 \pmod{5}$, $q \equiv \pm 2 \pmod{5}$, $e \in \{0, 1, 2, 3, 4\}$ and $1 \leq e_1, e_2 \leq 4$.

In this paper, we will prove that $C_{k,5}$ is of type $(5, 5)$ if and only if 5 divides exactly the 5-class number of Γ and $u = 5^3$, where u is the index of the subgroup E_0 generated by the units of intermediate fields of the extension k/\mathbb{Q} in the unit group of k . Next we determine generators of $C_{k,5}$, when $C_{k,5}$ is of type $(5, 5)$ and $\text{rank } C_{k,5}^{(\sigma)} = 1$, for each of the three forms of n given above. Since k is a Kummer extension of k_0 , we begin with the decomposition laws in Kummer extensions, which is useful to give the prime factorization in the normal closure k . As the proofs of our main results are established by using the properties of the norm residue symbol, we recall the definition and the most important properties of this concept. Making use of this, we can determine the generators of the 5-class group $C_{k,5}$ of type $(5, 5)$ if $\text{rank } C_{k,5}^{(\sigma)} = 1$. Our main result will be underpinned by numerical examples, using the PARI/GP [19] in section 7. In fact, we shall prove the following Main Theorem:

Theorem 1.1. Let $k = \mathbb{Q}(\sqrt[5]{n}, \zeta_5)$, where n is a natural number 5^{th} power-free, be the normal closure of the pure quintic field $\Gamma = \mathbb{Q}(\sqrt[5]{n})$. Let $\text{Gal}(k/\Gamma) = \langle \tau \rangle$. Let p, q and l be primes such that, $p \equiv -1 \pmod{5}$, $q \equiv \pm 2 \pmod{5}$ and $l \neq p, l \neq q$. Assume that $C_{k,5}$ is of type $(5, 5)$ and $\text{rank}(C_{k,5}^{(\sigma)}) = 1$, then we have:

- (1) If $n = 5^e p^{e_1} \not\equiv \pm 1, \pm 7 \pmod{25}$, with $e \in \{0, 1, 2, 3, 4\}$, $e_1 \in \{1, 2, 3, 4\}$ and $p \not\equiv -1 \pmod{25}$. The prime p decomposes in k as $p\mathcal{O}_k = \mathcal{P}_1^5 \mathcal{P}_2^5$, where \mathcal{P}_1 and \mathcal{P}_2 are prime ideals of k . Let \mathcal{L} be a prime ideal of k above l . If 5 and l are not quintic residues modulo p , then the 5-class group $C_{k,5}$ is generated by classes $[\mathcal{P}_1]$ and $[\mathcal{L}]^{1-\tau^2}$ and we have:

$$C_{k,5} = \langle [\mathcal{P}_1] \rangle \times \langle [\mathcal{L}]^{1-\tau^2} \rangle = \langle [\mathcal{P}_1], [\mathcal{L}]^{1-\tau^2} \rangle$$

- (2) If $n = p^{e_1} q^{e_2} \equiv \pm 1, \pm 7 \pmod{25}$, with $e_1, e_2 \in \{1, 2, 3, 4\}$ and $p \not\equiv -1 \pmod{25}$, $q \not\equiv \pm 7 \pmod{25}$. The prime p decomposes in k as $p\mathcal{O}_k = \mathcal{P}_1^5 \mathcal{P}_2^5$, where \mathcal{P}_1 and \mathcal{P}_2 are prime ideals of k . Let \mathcal{L} be a prime ideal of k above l . If q and l are not a quintic residues modulo p , then the 5-class group $C_{k,5}$ is generated by classes $[\mathcal{P}_1]$ and $[\mathcal{L}]^{1-\tau^2}$ and we have:

$$C_{k,5} = \langle [\mathcal{P}_1] \rangle \times \langle [\mathcal{L}]^{1-\tau^2} \rangle = \langle [\mathcal{P}_1], [\mathcal{L}]^{1-\tau^2} \rangle$$

- (3) If $n = p^{e_1} \equiv \pm 1, \pm 7 \pmod{25}$, with $e_1 \in \{1, 2, 3, 4\}$ and $p \equiv -1 \pmod{25}$. 5 decomposes in k as $5\mathcal{O}_k = \mathcal{B}_1^4 \mathcal{B}_2^4 \mathcal{B}_3^4 \mathcal{B}_4^4 \mathcal{B}_5^4$, where \mathcal{B}_i are prime ideals of k . If 5 is not a quintic residue modulo p , then the 5-class group $C_{k,5}$ is generated by classes $[\mathcal{B}_i]$ and $[\mathcal{B}_j]$, $i \neq j \in \{1, 2, 3, 4, 5\}$ and we have:

$$C_{k,5} = \langle [\mathcal{B}_i] \rangle \times \langle [\mathcal{B}_j] \rangle = \langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle$$

Some related studies are [5], [15].

Notations.

Throughout this paper, we use the following notations:

- The lower case letters p, q and l will denote distinct prime numbers such that, $p \equiv -1 \pmod{5}$, $q \equiv \pm 2 \pmod{5}$ and $l \neq p, l \neq q$.
- $\Gamma = \mathbb{Q}(\sqrt[5]{n})$: a pure quintic field, where $n \neq 1$ is a 5^{th} power-free natural number.
- $k_0 = \mathbb{Q}(\zeta_5)$: the cyclotomic field, where $\zeta_5 = e^{\frac{2i\pi}{5}}$ a primitive 5^{th} root of unity.
- $k = \mathbb{Q}(\sqrt[5]{n}, \zeta_5)$: the normal closure of Γ , a quintic Kummer extension of k_0 .
- $\langle \tau \rangle = \text{Gal}(k/\Gamma)$ such that τ is identity on Γ , and sends ζ_5 to its square. Hence τ has order 4.
- $\langle \sigma \rangle = \text{Gal}(k/k_0)$ such that σ is identity on k_0 , and sends $\sqrt[5]{n}$ to $\zeta_5 \sqrt[5]{n}$. Hence σ has order 5.
- u : the index of the subgroup E_0 generated by the units of intermediate fields of the extension k/\mathbb{Q} in the unit group of k .
- $\lambda = 1 - \zeta_5$ is prime element above 5 in k_0 .
- $q^* = 2, 1$ or 0 , according to whether ζ_5 and $1 + \zeta_5$ are both, or only one of them, or none is norm or is norm of an element of $k^* = k \setminus \{0\}$.
- For a number field L , denote by:
 - \mathcal{O}_L : the ring of integers of L ;
 - h_L : the class number of L ;
 - $C_{L,5}$: the 5-class group of L ;
 - $[\mathcal{I}]$: the class of a fractional ideal \mathcal{I} in the class group of L .

2 Decomposition laws in Kummer extensions

Since the 5-extensions of k and k_0 are all Kummer extensions, we recall the decomposition laws of ideals in these extensions. Let L be a number field which contains the l^{th} roots of unity, where l is prime, and θ be an element of L , such that $\theta \neq \mu^l$, for any $\mu \in L$, therefore $L(\sqrt[l]{\theta})$ is cyclic extension of degree l over L . We denote by ζ a l^{th} primitive root of unity.

Proposition 2.1.

(1) We assume that a prime \mathcal{P} of L divides θ exactly to the power \mathcal{P}^a .

- If $a = 0$ and \mathcal{P} does not divide l , then \mathcal{P} splits completely in $L(\sqrt[l]{\theta})$ when the congruence $X^l \equiv \theta \pmod{\mathcal{P}}$ has a solution in L .
- If $a = 0$ and \mathcal{P} does not divide l , then \mathcal{P} is inert in $L(\sqrt[l]{\theta})$ when the congruence $\theta \equiv X^l \pmod{\mathcal{P}}$ has no solution in L .
- If $l \nmid a$, then \mathcal{P} is totally ramified in $L(\sqrt[l]{\theta})$.

(2) Let \mathcal{B} be a prime factor of $1 - \zeta$ that divides $1 - \zeta$ exactly to the a^{th} power. Suppose that $\mathcal{B} \nmid \theta$, then \mathcal{B} splits completely in $L(\sqrt[l]{\theta})$ if the congruence

$$X^l \equiv \theta \pmod{\mathcal{B}^{al+1}} \tag{*}$$

has a solution in L . The ideal \mathcal{B} is inert in $L(\sqrt[l]{\theta})$ if the congruence

$$\theta \equiv X^l \pmod{\mathcal{B}^{al}} \tag{**}$$

has a solution in L , but (*) has none. The ideal \mathcal{B} is totally ramified in L if the congruence (**) has no solution.

Proof. see [[9] Theorem 118, Theorem 119] □

3 Prime factorization in pure quintic field and in its normal closure

Let Γ , k_0 and k as above. We begin with the factorization of primes in Γ , next we give the decomposition of primes in k_0 , knowing that 5 is the unique prime ramified in k_0 . Finally the results of Proposition 2.1 allow us to state the prime factorization in k . For more details on decomposition laws, we refer the reader to [9], [10], [18].

Let $p \neq 5$ be a prime number, \mathcal{P} a prime ideal of Γ , π a prime of k_0 and \mathcal{L} a prime ideal of k . We denote by \mathcal{N} the absolute norm.

Proposition 3.1. Using the same notations as above, we have:

- (1) If p divides the radicand n then $p\mathcal{O}_\Gamma = \mathcal{P}^5$ and $\mathcal{N}(\mathcal{P}) = p$.
- (2) If $p \nmid 5n$ and $p \equiv \pm 2 \pmod{5}$ then $p\mathcal{O}_\Gamma = \mathcal{P}_1\mathcal{P}_2$ and $\mathcal{N}(\mathcal{P}_1) = p$, $\mathcal{N}(\mathcal{P}_2) = p^4$.
- (3) If $p \nmid 5n$ and $p \equiv -1 \pmod{5}$ then $p\mathcal{O}_\Gamma = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$ and $\mathcal{N}(\mathcal{P}_1) = p$, $\mathcal{N}(\mathcal{P}_2) = \mathcal{N}(\mathcal{P}_3) = p^2$.
- (4) If $p \nmid 5n$ and $p \equiv 1 \pmod{5}$ then:
 - $p\mathcal{O}_\Gamma = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4\mathcal{P}_5$ and $\mathcal{N}(\mathcal{P}_i) = p$, if n is quintic residue modulo p .
 - $p\mathcal{O}_\Gamma = \mathcal{P}$ and $\mathcal{N}(\mathcal{P}_i) = p^5$, if n is not a quintic residue modulo p .

Proof. For (1) see [[13], Lemma 3].

Since the discriminant of Γ/\mathbb{Q} is $disc(\Gamma/\mathbb{Q}) = 5^5n^4$ then if $p \nmid 5n$ we have that p is unramified in Γ . Then the decomposition of $p\mathcal{O}_\Gamma$ is governed by the factorization of $X^5 - n$ over the field \mathbb{F}_p of p elements.

- If $p \equiv 1 \pmod{5}$ then \mathbb{F}_p has five fifth roots of unity. Therefore either $X^5 - n$ splits into five linear factors, or is irreducible, according to whether or not n is a quintic residue modulo p . So in these two cases, $p\mathcal{O}_\Gamma$ splits into five ideals of norm p , or it remains inert of norm p^5 .

-If $p \not\equiv 1 \pmod{5}$ then $X^5 - n$ has a unique linear factor over \mathbb{F}_p . Let $X - a$ be the linear factor of $X^5 - n$ over \mathbb{F}_p . The remaining linear factors are $X - \zeta_5^k a$ where $k \in \{1, 2, 3, 4\}$.

If $p \equiv -1 \pmod{5}$ then $(X - \zeta_5^2 a)(X - \zeta_5^3 a)$ and $(X - \zeta_5 a)(X - \zeta_5^4 a)$ are irreducible quadratics

over \mathbb{F}_p . So $p\mathcal{O}_\Gamma$ is a product of a prime ideal of norm p and two of norm p^2 . If $p \equiv \pm 2 \pmod{5}$ then the $\zeta_5^k a$ are all conjugates over \mathbb{F}_p . Then $(X - \zeta_5 a)(X - \zeta_5^2 a)(X - \zeta_5^3 a)(X - \zeta_5^4 a)$ is irreducible over \mathbb{F}_p . So $p\mathcal{O}_\Gamma$ is a product of a prime ideal of norm p and one of norm p^4 . □

The ramification of the prime 5 needs a particular treatment.

Theorem 3.2. *Using the same notations as above. Let f be the conductor of k/k_0 , and $R = q_1 \dots q_s$ denotes the square free product of all prime divisors of the radicand n of Γ , then f satisfies the relation:*

$$f^4 = \begin{cases} 5^2 R^4 & \text{if } n^4 \not\equiv 1 \pmod{25} \text{ (field of the first kind),} \\ R^4 & \text{if } n^4 \equiv 1 \pmod{25} \text{ (field of the second kind).} \end{cases}$$

Proof. see [2]. □

Proposition 3.3. *Using the same notations as above. The decomposition into prime factors of 5 is:*

- If Γ is of first kind then: $5\mathcal{O}_\Gamma = \mathcal{P}^5$ and $\mathcal{N}(\mathcal{P}) = 5$.
- If Γ is of second kind then: $5\mathcal{O}_\Gamma = \mathcal{P}_1 \mathcal{P}_2^4$ and $\mathcal{N}(\mathcal{P}_i) = 5$.

Proof. See the proof of [[14], Theorem 1.1]. □

The decomposition law in the 5th cyclotomic field k_0 is as follows:

Proposition 3.4. *Using the same notations as above, we have :*

- $5\mathcal{O}_{k_0} = \lambda^4 = (1 - \zeta_5)^4$.
- $p\mathcal{O}_{k_0} = \pi_1 \pi_2 \pi_3 \pi_4$ in k_0 , if $p \equiv 1 \pmod{5}$.
- $p\mathcal{O}_{k_0} = \pi_1 \pi_2$ in k_0 , if $p \equiv -1 \pmod{5}$.
- $p\mathcal{O}_{k_0} = p$ in k_0 (inert), if $p \equiv \pm 2 \pmod{5}$.

Proof. Its follows from [[18], Theorem 2.13]. □

Next, let k be the normal closure of Γ . The decomposition of the prime 5 in k is the purpose of the following proposition.

Proposition 3.5. *The prime 5 decomposes in k as follows:*

- If Γ is of first kind then: $5\mathcal{O}_k = \mathcal{L}^{20}$.
- If Γ is of second kind then: $5\mathcal{O}_k = \mathcal{L}_1^4 \mathcal{L}_2^4 \mathcal{L}_3^4 \mathcal{L}_4^4 \mathcal{L}_5^4$.

Proof. We have 5 ramifies in $k_0 = \mathbb{Q}(\zeta_5)$ then:

- Suppose that Γ is of first kind, by Proposition 3.3 we have $5\mathcal{O}_\Gamma = \mathcal{P}^5$. Hence $5\mathcal{O}_k = \mathcal{L}^{20}$.
- Suppose that Γ is of second kind, by Proposition 3.3 we have $5\mathcal{O}_\Gamma = \mathcal{P}_1^4 \mathcal{P}_2$. It follows that, $5\mathcal{O}_k = \mathcal{L}_1^4 \mathcal{L}_2^4 \mathcal{L}_3^4 \mathcal{L}_4^4 \mathcal{L}_5^4$. □

However, we have the following proposition in which we characterize the decomposition into prime ideals lying above $p \neq 5$ in k .

Proposition 3.6. *Using the same notations as above, we have :*

- (1) *If p divides $\text{disc}(\Gamma/\mathbb{Q})$ then:*
 - (a) *If $p \equiv \pm 2 \pmod{5}$, then $p\mathcal{O}_k = \mathcal{L}^5$.*
 - (b) *If $p \equiv -1 \pmod{5}$, then $p\mathcal{O}_k = \mathcal{L}_1^5 \mathcal{L}_2^5$.*
 - (c) *If $p \equiv 1 \pmod{5}$, then $p\mathcal{O}_k = \mathcal{L}_1^5 \mathcal{L}_2^5 \mathcal{L}_3^5 \mathcal{L}_4^5$.*
- (2) *If p does not divide $\text{disc}(\Gamma/\mathbb{Q})$ and $p \equiv 1 \pmod{5}$ then:*
 - (a) *p decomposes completely in k if and only if $\text{disc}(\Gamma/\mathbb{Q})$ is a quintic residue modulo p .*
 - (b) *$p\mathcal{O}_k = \mathcal{L}_1 \mathcal{L}_2 \mathcal{L}_3 \mathcal{L}_4$ if and only if $\text{disc}(\Gamma/\mathbb{Q})$ is not a quintic residue modulo p .*

- (3) If p does not divide $\text{disc}(\Gamma/\mathbb{Q})$ and $p \equiv \pm 2 \pmod{5}$ then: $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2\mathcal{L}_3\mathcal{L}_4\mathcal{L}_5$.
- (4) If p does not divide $\text{disc}(\Gamma/\mathbb{Q})$ and $p \equiv -1 \pmod{5}$ then: $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2\mathcal{L}_3\mathcal{L}_4\mathcal{L}_5\mathcal{L}_6\mathcal{L}_7\mathcal{L}_8\mathcal{L}_9\mathcal{L}_{10}$.

Proof.

- (1) We use 1 of Proposition 3.1 and the decomposition of prime ideals in the cyclotomic field $k_0 = \mathbb{Q}(\zeta_5)$.
- (2) Suppose that p does not divide $\text{disc}(\Gamma/\mathbb{Q})$ and $p \equiv 1 \pmod{5}$.
 - (a) If $\text{disc}(\Gamma/\mathbb{Q})$ is a quintic residue modulo p , then by 4 of proposition 3.1 we have p splits completely in Γ , and also in k_0 . Hence p splits completely in k .
 - (b) If $\text{disc}(\Gamma/\mathbb{Q})$ is not a quintic residue modulo p , we have p remains inert in Γ . Hence $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2\mathcal{L}_3\mathcal{L}_4$.
- (3) Since $p \nmid \text{disc}(\Gamma/\mathbb{Q})$ we have that p is unramified in Γ , and also in k_0 , then p is unramified in k . Since k/\mathbb{Q} is Galois extension, if $p\mathcal{O}_k = \mathcal{L}_1 \dots \mathcal{L}_r$ then $rf = 20$, with $f = [\mathcal{O}_k/\mathcal{L}_i : \mathbb{F}_p]$ the inertia degree. It is known that f is multiplicative in towers of number fields, which implies that f is a multiple of 4 if $p \equiv \pm 2 \pmod{5}$, then $f = 4$ and $r = 5$. Otherwise $f = 20$ and $r = 1$, which means that p remains inert in k , that is impossible because according to Proposition 3.3, p decomposes in Γ as $p\mathcal{O}_\Gamma = \mathcal{P}_1\mathcal{P}_2$.
- (4) As the previous point, if $p \equiv -1 \pmod{5}$ we have that f is a multiple of 2, then $f = 2$ and $r = 10$. Otherwise $f = 10$ and $r = 2$, which means that $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2$. Since $p\mathcal{O}_\Gamma = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$ and each \mathcal{P}_i is unramified in k , furthermore k/Γ is Galois, then $r_{\mathcal{P}_i}f_{\mathcal{P}_i} = 4$. For all possible values of $r_{\mathcal{P}_i}$ and $f_{\mathcal{P}_i}$ we can not get $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2$. Hence $f = 2$ and $r = 10$. □

Remark 3.7. Let $p \neq 5$, according to Proposition 3.6, if $p \nmid \text{disc}(\Gamma/\mathbb{Q})$, then p is unramified in k and not inert in k . Let $p\mathcal{O}_k = \mathcal{L}_1\mathcal{L}_2 \dots \mathcal{L}_r$, since the elements of $\text{Gal}(k/\mathbb{Q})$ permute the set $\{\mathcal{L}_1 \dots \mathcal{L}_r\}$ then $\mathcal{L}_i^\sigma \neq \mathcal{L}_i$ for $1 \leq i \leq r$. This result has great importance in the proof of our main theorem.

4 Norm residue symbol

Let L/K be an abelian extension of number fields with conductor f . For each finite or infinite prime ideal \mathcal{P} of K , we denote by $f_{\mathcal{P}}$ the largest power of \mathcal{P} that divides f . Let $\beta \in K^*$, we determine an auxiliary number β_0 by the two conditions $\beta_0 \equiv \beta \pmod{f_{\mathcal{P}}}$ and $\beta_0 \equiv 1 \pmod{\frac{f}{f_{\mathcal{P}}}}$. Let \mathcal{Q} be an ideal co-prime with \mathcal{P} such that $(\beta_0) = \mathcal{P}^a \mathcal{Q}$ ($a = 0$ if \mathcal{P} infinite). We note by

$$\left(\frac{\beta, L}{\mathcal{P}}\right) = \left(\frac{L/K}{\mathcal{Q}}\right)$$

the Artin map in L/K applied to \mathcal{Q} .

Let K be a number field containing the m^{th} -roots of unity, where $m \in \mathbb{N}$, then for each $\alpha, \beta \in K^*$ and prime ideal \mathcal{P} of K , we define the norm residue symbol by:

$$\left(\frac{\beta, \alpha}{\mathcal{P}}\right)_m = \frac{\left(\frac{\beta, K(\sqrt[m]{\alpha})}{\mathcal{P}}\right) \sqrt[m]{\alpha}}{\sqrt[m]{\alpha}}$$

Therefore, if the prime ideal \mathcal{P} is unramified in the field $K(\sqrt[m]{\alpha})$, then we write:

$$\left(\frac{\alpha}{\mathcal{P}}\right)_m = \frac{\left(\frac{K(\sqrt[m]{\alpha})}{\mathcal{P}}\right) \sqrt[m]{\alpha}}{\sqrt[m]{\alpha}}$$

Remark 4.1. Notice that $\left(\frac{\beta, \alpha}{\mathcal{P}}\right)_m$ and $\left(\frac{\alpha}{\mathcal{P}}\right)_m$ are two m^{th} -roots of unity.

Following [8], the principal properties of the norm residue symbol are given as follows:

Property 4.2.

- (1) $\left(\frac{\beta_1\beta_2,\alpha}{\mathcal{P}}\right)_m = \left(\frac{\beta_1,\alpha}{\mathcal{P}}\right)_m \left(\frac{\beta_2,\alpha}{\mathcal{P}}\right)_m$;
- (2) $\left(\frac{\beta,\alpha_1\alpha_2}{\mathcal{P}}\right)_m = \left(\frac{\beta,\alpha_1}{\mathcal{P}}\right)_m \left(\frac{\beta,\alpha_2}{\mathcal{P}}\right)_m$;
- (3) $\left(\frac{\beta,\alpha}{\mathcal{P}}\right)_m = \left(\frac{\alpha,\beta}{\mathcal{P}}\right)_m^{-1}$;
- (4) If \mathcal{P} is not divisible by the conductor $f(\sqrt[m]{\alpha})$ of $K(\sqrt[m]{\alpha})$ and appears in (β) with the exponent b , then: $\left(\frac{\beta,\alpha}{\mathcal{P}}\right)_m = \left(\frac{\alpha}{\mathcal{P}}\right)_m^{-b}$;
- (5) $\left(\frac{\beta,\alpha}{\mathcal{P}}\right)_m = 1$ if and only if β is norm residue of $K(\sqrt[m]{\alpha})$ modulo $f(\sqrt[m]{\alpha})$;
- (6) $\left(\frac{\tau\beta,\tau\alpha}{\tau\mathcal{P}}\right)_m = \tau \left(\frac{\beta,\alpha}{\mathcal{P}}\right)_m$ for each automorphism τ of K ;
- (7) $\prod_{\mathcal{P}} \left(\frac{\beta,\alpha}{\mathcal{P}}\right)_m = 1$ for all finite or infinite prime ideals;
- (8) If K' is a finite extension of K , $\alpha \in K^*$, $\beta' \in K'$ then:

$$\prod_{\mathcal{P}'|\mathcal{P}} \left(\frac{\beta',\alpha}{\mathcal{P}'}\right)_m = \left(\frac{N_{K'/K}(\beta'),\alpha}{\mathcal{P}}\right)_m$$

- (9) Let $\alpha, \beta \in K^*$ and the conductors $f(\sqrt[m]{\alpha})$, $f(\sqrt[m]{\beta})$ of respectively $K(\sqrt[m]{\alpha})$, $K(\sqrt[m]{\beta})$ are co-prime then, the classical reciprocity law:

$$\left(\frac{\beta}{(\alpha)}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m$$

For more basic properties of the quintic norm residue symbols in the number fields, we refer the reader to [8].

Notice that in the rest of the article, we will use the quintic norm residue symbol ($m = 5$). As the ring of integer \mathcal{O}_{k_0} is principal, we will write the norm quintic residue symbol as follows:

$$\left(\frac{\beta,\alpha}{(\pi)}\right)_5 = \left(\frac{\beta,\alpha}{\pi}\right)_5 \text{ and } \left(\frac{\alpha}{(\pi)}\right)_5 = \left(\frac{\alpha}{\pi}\right)_5$$

Where $\alpha, \beta \in k_0^*$ and π is a prime integer of \mathcal{O}_{k_0} .

5 Fields $\mathbb{Q}(\sqrt[5]{n}, \zeta_5)$ whose 5-class group is of type $(5, 5)$

In this section we use the class number formula of [[16]] to give a necessary and sufficient condition such that the 5-class group of the field $\mathbb{Q}(\sqrt[5]{n}, \zeta_5)$ is of type $(5, 5)$.

Lemma 5.1. Let $\text{Gal}(k/\Gamma) = \langle \tau \rangle \cong \mathbb{Z}/4\mathbb{Z}$, and C be a $\mathbb{Z}_5[\langle \tau \rangle]$ module. Let $C^+ = \{\mathcal{A} \in C \mid \mathcal{A}^{\tau^2} = \mathcal{A}\}$ and $C^- = \{\mathcal{A} \in C \mid \mathcal{A}^{\tau^2} = \mathcal{A}^{-1}\}$. Then

$$C \cong C^+ \times C^-.$$

Proof. Let $\mathcal{A} \in C$. Write $\mathcal{A} = \mathcal{A}^{\frac{1+\tau^2}{2}} \cdot \mathcal{A}^{\frac{1-\tau^2}{2}}$. Then $\mathcal{A}^{\frac{1+\tau^2}{2}} \in C^+$ and $\mathcal{A}^{\frac{1-\tau^2}{2}} \in C^-$. Let $\mathcal{A} \in C^+ \cap C^-$, then $\mathcal{A} = \mathcal{A}^{\tau^2} = \mathcal{A}^{-1}$, that is $\mathcal{A}^2 = 1$. Thus $\mathcal{A} = 1$, since C is $\mathbb{Z}_5[\langle \tau \rangle]$ -module. Hence $C \cong C^+ \times C^-$. □

Lemma 5.2. $C_{\Gamma,5} \cong C_{k,5}^+$.

Proof. Since $C_{k,5}$ is $\mathbb{Z}_5[\langle \tau \rangle]$ -module, then $C_{k,5} \cong C_{k,5}^+ \times C_{k,5}^-$. We have a natural inclusion $C_{\Gamma,5} \hookrightarrow C_{k,5}$ as 5 is relatively prime to $[k : \Gamma] = 4$. Moreover, $C_{\Gamma,5} \hookrightarrow C_{k,5}^+$ as $\mathcal{A}^{\tau^2} = \mathcal{A}$ for all $\mathcal{A} \in C_{\Gamma,5}$. Let $\mathcal{A} \in C_{k,5}^+$, then $\mathcal{A} = 4(\frac{1}{4}\mathcal{A}) = (1 + \tau + \tau^2 + \tau^3)(\frac{1}{4}\mathcal{A}) = \mathcal{N}(\frac{1}{4}\mathcal{A})$. Thus, $\mathcal{A} \in C_{\Gamma,5}$. So $C_{\Gamma,5} \cong C_{k,5}^+$. \square

Now let u be the index of the subgroup E_0 generated by the units of intermediate fields of the extension k/\mathbb{Q} in the unit group of k . In [[16]], C.Parry proved that u is a divisor of 5^6 , and he presented the relation formula between the class numbers of k and Γ as follows: $h_k = (\frac{u}{5})(\frac{h_\Gamma}{5})^4$. The structure of the 5-class group $C_{k,5}$ is given by the following proposition:

Proposition 5.3. Let Γ be a pure quintic field, k its normal closure, and u be the index of units defined above, then

$$C_{k,5} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \iff h_\Gamma \text{ is exactly divisible by 5 and } u = 5^3.$$

Proof.

Let $C_{k,5} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ then $|C_{k,5}| = 25$. According to [[16]] $|C_{k,5}| = (\frac{u}{5})\frac{|C_{\Gamma,5}|^4}{5^4} = 25$, namely $uh_\Gamma^4 = 5^7$. Let $n = v_5(u)$, and $n' = v_5(h_\Gamma)$, so we get $n + 4n' = 7$, and the unique natural values of n and n' which satisfy this equation are $n = 3$ and $n' = 1$. Therefore we have $u = 5^3$ and h_Γ is exactly divisible by 5.

Conversely according to Lemma 5.1 and Lemma 5.2, $C_{k,5} \cong C_{k,5}^+ \times C_{k,5}^-$ and $C_{k,5}^+ \cong C_{\Gamma,5}$, then $C_{k,5}^+$ is cyclic of order 5 because $|C_{k,5}^+| = |C_{\Gamma,5}| = 5$. Since $|C_{k,5}| = |C_{k,5}^+| \cdot |C_{k,5}^-| = 25$ by the formula $|C_{k,5}| = (\frac{u}{5})\frac{|C_{\Gamma,5}|^4}{5^4}$, we get that $|C_{k,5}^-| = 5$ and $C_{k,5}^-$ is a cyclic group of order 5 and intersects $C_{k,5}^+$ trivially, then $C_{k,5} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. \square

6 Proof of the Main Theorem

We start the proof by proving some results as follows.

Proposition 6.1. Let p a prime number such that $p \equiv -1 \pmod{5}$ and $\text{Gal}(k/\Gamma) = \langle \tau \rangle$. Then we have:

- (1) $p = \pi_1\pi_2$, where π_i 's are primes of k_0 and $\pi_1^\tau = -\pi_2, \pi_2^\tau = -\pi_1$
- (2) $\left(\frac{c}{\pi_1}\right)_5 = \left(\frac{c}{\pi_2}\right)_5^2$ for all $c \in \mathbb{Z}$ such that $p \nmid c$.
- (3) $\left(\frac{c}{\pi_1}\right)_5 = \left(\frac{c}{\pi_2}\right)_5 = 1$ if and only if c is a quintic residue modulo p .
- (4) $\left(\frac{\pi_2}{\pi_1}\right)_5 = \left(\frac{\pi_1}{\pi_2}\right)_5 = 1$.

Proof. (1) According to [[1], lemma 3.1] the prime $p \equiv -1 \pmod{5}$, can be written as:

$p = a^2 + ab - b^2$, with $a, b \in \mathbb{Z}$ co-prime. Using this expression of p we define:

$$\pi_1 = a\zeta_5^3 + a\zeta_5^2 + b \quad \text{and} \quad \pi_2 = a\zeta_5^3 + a\zeta_5^2 + a - b,$$

then $p = \pi_1\pi_2$ (see [[12], theorem 5.15]). Let $\text{Gal}(k/\Gamma) = \langle \tau \rangle$ with $\tau : \zeta_5 \rightarrow \zeta_5^2$, so we get that:

$$\pi_1^\tau = (a\zeta_5^3 + a\zeta_5^2 + b)^\tau = a\zeta_5 + a\zeta_5^4 + b = a(\zeta_5 + \zeta_5^4) + b = a(-1 - \zeta_5^2 - \zeta_5^3) + b = -\pi_2.$$

$$\pi_2^\tau = (a\zeta_5^3 + a\zeta_5^2 + a - b)^\tau = a\zeta_5 + a\zeta_5^4 + a - b = a(\zeta_5 + \zeta_5^4) + a - b = a(-1 - \zeta_5^2 - \zeta_5^3) + a - b = -\pi_1.$$

(2) $\left(\frac{c}{\pi_1}\right)_5 = \left(\frac{\pi_1, c}{\pi_1}\right)_5^{-1} = \left(\frac{c, \pi_1}{\pi_1}\right)_5 = \left(\frac{c, -\pi_2^\tau}{-\pi_2^\tau}\right)_5 = \tau \left(\frac{c, \pi_2}{\pi_2}\right)_5 = \left(\frac{c, \pi_2}{\pi_2}\right)_5^2 = \left(\frac{\pi_2, c}{\pi_2}\right)_5^{-2} = \left(\frac{c}{\pi_2}\right)_5^2$, because π_1, π_2 are unramified in $k_0(\sqrt[5]{c})$ (proposition 2.1), and we use properties (3), (4), (6) of 4.2.

(3) Let $\omega \in \mathcal{O}_{k_0}$ and π a prime element of \mathcal{O}_{k_0} , such that $\pi \nmid \omega$, then $X^5 \equiv \omega \pmod{\pi}$ is soluble in \mathcal{O}_{k_0} if and only if $\omega^m \equiv 1 \pmod{\pi}$, when $m = \frac{N(\pi)-1}{5}$. If $\left(\frac{c}{\pi_1}\right)_5 = \left(\frac{c}{\pi_2}\right)_5 = 1$, we get that π_1 and π_2 split completely in $k_0(\sqrt[5]{c})$, so the equations $X^5 \equiv c \pmod{\pi_1}$ and $X^5 \equiv c \pmod{\pi_2}$ are soluble in \mathcal{O}_{k_0} , therefore $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{\pi_1}$ and $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{\pi_2}$, thus $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{p}$, and by Euler's criterion, c is a quintic residue modulo p . Conversely if c is a quintic residue modulo p we have $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{p}$, so $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{\pi_1}$ and $c^{\frac{p^2-1}{5}} \equiv 1 \pmod{\pi_2}$, therefore the equations $X^5 \equiv c \pmod{\pi_1}$ and $X^5 \equiv c \pmod{\pi_2}$ are soluble in \mathcal{O}_{k_0} , namely $\left(\frac{c}{\pi_1}\right)_5 = \left(\frac{c}{\pi_2}\right)_5 = 1$.

(4) According to [[12], theorem 5.15] we have $A = \left(\frac{\pi_1^{a_1}\pi_2^{a_2}, \pi_1, \pi_2}{\pi_1}\right)_5 = 1$ with $a_1, a_2 \in \{1, 2, 3, 4\}$ and $a_1 \neq a_2$, so using properties 4.2 we have

$$A = \left(\frac{\pi_1, \pi_1}{\pi_1}\right)_5^{a_1} \cdot \left(\frac{\pi_1, \pi_2}{\pi_1}\right)_5^{a_1} \cdot \left(\frac{\pi_2, \pi_1}{\pi_1}\right)_5^{a_2} \cdot \left(\frac{\pi_2, \pi_2}{\pi_1}\right)_5^{a_2} = 1$$

then

- $\left(\frac{\pi_1, \pi_1}{\pi_1}\right)_5^{a_1} = 1$, because π_1 is norm in $k_0(\sqrt[5]{\pi_1})/k_0$.
- $\left(\frac{\pi_1, \pi_2}{\pi_1}\right)_5^{a_1} = \left(\frac{\pi_2}{\pi_1}\right)_5^{-a_1}$ and $\left(\frac{\pi_2, \pi_1}{\pi_1}\right)_5^{a_2} = \left(\frac{\pi_2}{\pi_1}\right)_5^{a_2}$, by (4) of properties 4.2
- $\left(\frac{\pi_2, \pi_2}{\pi_1}\right)_5^{a_2} = 1$, by (2) and (4) of properties 4.2.

We get that, $A = \left(\frac{\pi_2}{\pi_1}\right)_5^{a_2-a_1} = 1$, then $a_2 - a_1 = 0$ or 5 , which is impossible because $a_1, a_2 \in \{1, 2, 3, 4\}$ and $a_1 \neq a_2$, hence $\left(\frac{\pi_2}{\pi_1}\right)_5 = 1$. Since π_1 and π_2 play symmetric roles we have also $\left(\frac{\pi_1}{\pi_2}\right)_5 = 1$. Thus we deduce that $\left(\frac{\pi_2}{\pi_1}\right)_5 = \left(\frac{\pi_1}{\pi_2}\right)_5 = 1$.

□

6.1 Case 1: $n = 5^e p^{e_1} \not\equiv \pm 1, \pm 7 \pmod{25}$ with $p \not\equiv -1 \pmod{25}$

Let $\Gamma = \mathbb{Q}(\sqrt[5]{5^e p^{e_1}})$ be a pure quintic field where $e \in \{0, 1, 2, 3, 4\}$, $e_1 \in \{1, 2, 3, 4\}$, p a prime number such that $p \not\equiv -1 \pmod{25}$ and $k = \Gamma(\zeta_5)$ its normal closure.

We have $p = \pi_1\pi_2$ in k_0 . By proposition 3.1, p is totally ramified in Γ , therefore π_1, π_2 are ramified in k . According to [[12], Lemma 5.1] we have $\lambda = 1 - \zeta_5$ is ramified in k/k_0 because $5^e p^{e_1} \not\equiv \pm 1 \pm 7 \pmod{\lambda^5}$.

If we denote by $\mathcal{P}_1, \mathcal{P}_2$ and \mathcal{I} respectively, the prime ideals of k above π_1, π_2 and λ respectively, we get that $\mathcal{P}_i^5 = \pi_i \mathcal{O}_k$ ($i = 1, 2$), $\mathcal{I}^5 = \lambda \mathcal{O}_k$, $\mathcal{P}_i^\sigma = \mathcal{P}_i$, $\mathcal{P}_1^\tau = \mathcal{P}_2$, $\mathcal{I}^\sigma = \mathcal{I}^\tau = \mathcal{I}$.

According to Proposition 5.3, we have $C_{k,5} \cong C_{k,5}^+ \times C_{k,5}^-$, such that $C_{k,5}^+$ and $C_{k,5}^-$ are cyclic subgroups of order 5. Since $\mathcal{P}_i^\sigma = \mathcal{P}_i$ ($i = 1, 2$), $\mathcal{P}_1^\tau = \mathcal{P}_2$, $\mathcal{P}_2^\tau = \mathcal{P}_1$ and $\mathcal{I}^\sigma = \mathcal{I}^\tau = \mathcal{I}$, we get that $[\mathcal{P}_1], [\mathcal{P}_2]$ and $[\mathcal{I}]$ are ambiguous classes. As $C_{k,5}^{(\sigma)}$ is an elementary group of rank 1, we can deduce that $C_{k,5}^{(\sigma)} = \langle [\mathcal{P}_1] \rangle$. Also as $[\mathcal{P}_1]^{\tau^2} = [\mathcal{P}_1]$, we have $C_{k,5}^+ = \langle [\mathcal{P}_1] \rangle$, therefore $C_{k,5}^+ = C_{k,5}^{(\sigma)} = \langle [\mathcal{P}_1] \rangle$ if and only if \mathcal{P}_1 is not principal.

we argue by reduction to absurd: Assume that \mathcal{P}_1 is principal, we have:

$$\begin{aligned} [\mathcal{P}_1] = 1 &\implies \exists \beta \in \mathcal{O}_k \mid \mathcal{P}_1 = \beta \mathcal{O}_k \\ &\implies \mathcal{N}_{k/k_0}(\mathcal{P}_1) = \mathcal{N}_{k/k_0}(\beta \mathcal{O}_k) \\ &\implies \pi_1 \mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\beta) \mathcal{O}_{k_0} \\ &\implies \exists \epsilon \in E_{k_0} \mid \pi_1 = \epsilon \mathcal{N}_{k/k_0}(\beta) \end{aligned}$$

According to the proof of [[12], theorem 5.15], we have $E_{k_0} \subset \mathcal{N}_{k/k_0}(k^*)$

$$\implies \exists \alpha \in \mathcal{O}_k \mid \pi_1 = \mathcal{N}_{k/k_0}(\alpha)$$

that is to say π_1 is norm in $k = k_0(\sqrt[5]{5^e \pi_1 \pi_2})$, where π_1, π_2 are primes above p in k_0 . Hence we have:

$$\left(\frac{\pi_1, 5^e \pi_1 \pi_2}{\mathcal{P}}\right)_5 = 1$$

for all ideals \mathcal{P} of k_0 .

In particular, we calculate this symbol for $\mathcal{P} = \pi_1 \mathcal{O}_{k_0}$ or $\mathcal{P} = \pi_2 \mathcal{O}_{k_0}$. On the one hand,

$$A = \left(\frac{\pi_1, 5^e \pi_1 \pi_2}{\pi_1 \mathcal{O}_{k_0}}\right)_5 = \left(\frac{\pi_1, 5^e}{\pi_1}\right)_5 \cdot \left(\frac{\pi_1, \pi_1}{\pi_1}\right)_5 \cdot \left(\frac{\pi_1, \pi_2}{\pi_1}\right)_5$$

On the other hand, we have:

- $\left(\frac{\pi_1, \pi_1}{\pi_1}\right)_5 = 1$, because π_1 is norm in $k_0(\sqrt[5]{\pi_1})/k_0$.
- $\left(\frac{\pi_1, \pi_2}{\pi_1}\right)_5 = \left(\frac{\pi_2}{\pi_1}\right)_5^{-1} = 1$, by (4) of properties 4.2, and (4) of 6.1.
- $\left(\frac{\pi_1, 5^e}{\pi_1}\right)_5 = \left(\frac{5}{\pi_1}\right)_5^{-e}$, by (4) of properties 4.2.

We get that, $A = \left(\frac{5}{\pi_1}\right)_5^{-e} = 1$. Since π_1 and π_2 play symmetric roles, then $B = \left(\frac{\pi_1, 5^e \pi_1 \pi_2}{\pi_2 \mathcal{O}_{k_0}}\right)_5 = \left(\frac{5}{\pi_2}\right)_5^{-e}$, and since $\left(\frac{\pi_1, 5^e \pi_1 \pi_2}{\mathcal{P}}\right)_5 = 1$, for all prime ideals of k_0 , then $A = B = 1$, namely

$$\left(\frac{5}{\pi_1}\right)_5^{-e} = \left(\frac{5}{\pi_2}\right)_5^{-e} = 1.$$

In fact that 5 is not a quintic residue modulo p , implies that

$$\left(\frac{5}{\pi_1 \pi_2}\right)_5 = \left(\frac{5}{\pi_1}\right)_5 \left(\frac{5}{\pi_2}\right)_5 \neq 1.$$

then

$$\left(\frac{5}{\pi_1}\right)_5 \neq 1 \text{ or } \left(\frac{5}{\pi_2}\right)_5 \neq 1.$$

Since 5 does not divide e , then

$$\left(\frac{5}{\pi_1}\right)_5^e \neq 1 \text{ or } \left(\frac{5}{\pi_2}\right)_5^e \neq 1.$$

Which is a contradiction. Consequently, the ideal \mathcal{P}_1 is not principal.

The second step in the proof of the case 1, is to find a non-ambiguous class, which generates the group $C_{k,5}^-$. By class field theory, the classes arise from unramified primes of k_0 , these are not ambiguous. Let l be prime integer such that $l \neq p$, then l is unramified in Γ . Let π' a prime of k_0 above l , then π' is unramified in k . Let \mathcal{L} a prime ideal of k above π' , then $C_{k,5}^- = \langle [\mathcal{L}]^{1-\tau^2} \rangle$ if and only if \mathcal{L} is not principal. we argue by reduction to absurd: Assume that \mathcal{L} is principal, we have:

$$\begin{aligned} [\mathcal{L}] = 1 &\implies \exists \beta \in \mathcal{O}_k \mid \mathcal{L} = \beta \mathcal{O}_k \\ &\implies \mathcal{N}_{k/k_0}(\mathcal{L}) = \mathcal{N}_{k/k_0}(\beta \mathcal{O}_k) \\ &\implies \pi' \mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\beta) \mathcal{O}_{k_0} \\ &\implies \exists \epsilon \in E_{k_0} \mid \pi' = \epsilon \mathcal{N}_{k/k_0}(\beta) \end{aligned}$$

By [[12], theorem 5.15] we have $E_{k_0} \subset \mathcal{N}_{k/k_0}(k^*)$, then

$$\implies \exists \alpha \in \mathcal{O}_k \mid \pi' = \mathcal{N}_{k/k_0}(\alpha)$$

that is to say π' is norm in $k = k_0(\sqrt[5]{5^e \pi_1 \pi_2})$, where π_1, π_2 are two primes of k_0 such that $p = \pi_1 \pi_2$. Hence we have:

$$\left(\frac{\pi', 5^e \pi_1 \pi_2}{\mathcal{P}}\right)_5 = 1$$

for all ideals \mathcal{P} of k_0 .

In particular, we calculate this symbol for $\mathcal{P} = \pi_1 \mathcal{O}_{k_0}$ or $\mathcal{P} = \pi_2 \mathcal{O}_{k_0}$. On one hand,

$$A = \left(\frac{\pi', 5^e \pi_1 \pi_2}{\pi_1 \mathcal{O}_{k_0}}\right)_5 = \left(\frac{\pi', 5^e}{\pi_1}\right)_5 \cdot \left(\frac{\pi', \pi_1}{\pi_1}\right)_5 \cdot \left(\frac{\pi', \pi_2}{\pi_1}\right)_5$$

On the other hand, we have:

- $\left(\frac{\pi', 5^e}{\pi_1}\right)_5 = \left(\frac{\pi', 5}{\pi_1}\right)_5^e = \left(\frac{\pi'}{\pi_1}\right)_5^{0 \times e} = 1$, by (1), (4) of properties 4.2.
- $\left(\frac{\pi', \pi_2}{\pi_1}\right)_5 = \left(\frac{\pi'}{\pi_1}\right)_5^0 = 1$, by (4) of properties 4.2.
- $\left(\frac{\pi', \pi_1}{\pi_1}\right)_5 = \left(\frac{\pi'}{\pi_1}\right)_5$, by (4) of properties 4.2.

We get that, $A = \left(\frac{\pi'}{\pi_1}\right)_5 = 1$. Since π_1 and π_2 play symmetric roles, then $B = \left(\frac{\pi', 5^e \pi_1 \pi_2}{\pi_2 \mathcal{O}_{k_0}}\right)_5 = \left(\frac{\pi'}{\pi_2}\right)_5$, and since $\left(\frac{\pi', 5^e \pi_1 \pi_2}{\mathcal{P}}\right)_5 = 1$, for all prime ideals of k_0 , then $A = B = 1$, namely

$$\left(\frac{\pi'}{\pi_1}\right)_5 = \left(\frac{\pi'}{\pi_2}\right)_5 = 1.$$

In fact that l is not a quintic residue modulo p , implies that

$$\left(\frac{\pi'}{\pi_1 \pi_2}\right)_5 = \left(\frac{\pi'}{\pi_1}\right)_5 \left(\frac{\pi'}{\pi_2}\right)_5 \neq 1.$$

then

$$\left(\frac{\pi'}{\pi_1}\right)_5 \neq 1 \text{ or } \left(\frac{\pi'}{\pi_2}\right)_5 \neq 1.$$

Which is a contradiction. Consequently, the ideal \mathcal{L} is not principal.

It is easy to see that $[\mathcal{L}]^{1-\tau^2} \in C_{k,5}^-$, and $[\mathcal{L}]^{1-\tau^2} \neq 1$, otherwise $[\mathcal{L}]^{1-\tau^2} = 1$ then $[\mathcal{L}] = [\mathcal{L}]^{\tau^2}$, therefore $[\mathcal{L}] \in C_{k,5}^+ = C_{k,5}^{(\sigma)}$, which contradicts the fact that the class $[\mathcal{L}]$ is not ambiguous. Finally we deduce that

$$C_{k,5} \cong \langle [\mathcal{P}_1] \rangle \times \langle [\mathcal{L}]^{1-\tau^2} \rangle \cong \langle [\mathcal{P}_1], [\mathcal{L}]^{1-\tau^2} \rangle$$

Remark 6.2. Since $[\mathcal{P}_2]$ and $[\mathcal{I}]$ are also ambiguous classes, we can prove by the same reasoning that:

$$C_{k,5} \cong \langle [\mathcal{P}_2], [\mathcal{L}]^{1-\tau^2} \rangle \cong \langle [\mathcal{I}], [\mathcal{L}]^{1-\tau^2} \rangle$$

6.2 Case 2: $n = p^{e_1}q^{e_2} \equiv \pm 1, \pm 7 \pmod{25}$ with $p \not\equiv -1 \pmod{25}$ and $q \not\equiv \pm 7 \pmod{25}$

Let $\Gamma = \mathbb{Q}(\sqrt[5]{p^{e_1}q^{e_2}})$ be a pure quintic field where $e_1, e_2 \in \{1, 2, 3, 4\}$, p, q primes such that $p \not\equiv -1 \pmod{25}$ and $q \not\equiv \pm 7 \pmod{25}$ and $k = \Gamma(\zeta_5)$ the normal closure. We have $p = \pi_1\pi_2$ and q is inert in k_0 from Proposition 3.4. By Proposition 3.1, p and q are totally ramified in Γ , therefore π_1, π_2 and q are ramified in k . According to [[12], Lemma 5.1] we have $\lambda = 1 - \zeta_5$ is not ramified in k/k_0 because $n \equiv \pm 1, \pm 7 \pmod{\lambda^5}$.

If we denote by $\mathcal{P}_1, \mathcal{P}_2, \mathcal{Q}$ respectively, the prime ideals of k above π_1, π_2, q respectively, we get that $\mathcal{P}_i^5 = \pi_i\mathcal{O}_k$ ($i = 1, 2$), $\mathcal{Q}^5 = q\mathcal{O}_k$. Let l be a prime integer such that $l \neq p$ and $l \neq q$, then l is unramified in Γ . Let \mathcal{L} be a prime ideal of k above l .

We prove the result of the second point of the Main Theorem 1.1, by the same reasoning as for case 1. It is sufficient to replace 5 by q . Then we have,

$$C_{k,5} \cong \langle [\mathcal{P}_1] \rangle \times \langle [\mathcal{L}]^{1-\tau^2} \rangle \cong \langle [\mathcal{P}_1], [\mathcal{L}]^{1-\tau^2} \rangle$$

Remark 6.3. Since $[\mathcal{P}_2]$ and $[\mathcal{Q}]$ are also ambiguous classes, we can prove by the same reasoning that:

$$C_{k,5} \cong \langle [\mathcal{P}_2], [\mathcal{L}]^{1-\tau^2} \rangle \cong \langle [\mathcal{Q}], [\mathcal{L}]^{1-\tau^2} \rangle$$

6.3 Case 3: $n = p^{e_1} \equiv \pm 1, \pm 7 \pmod{25}$ with $p \equiv -1 \pmod{25}$

Let $\Gamma = \mathbb{Q}(\sqrt[5]{p^{e_1}})$ be a pure quintic field, where $e_1 \in \{1, 2, 3, 4\}$, and p a prime such that, $p \equiv -1 \pmod{25}$, and $k = \Gamma(\zeta_5)$ its normal closure. Without losing generality, we can choose $e = 1$. Since the field Γ is of second kind, then by Proposition 3.5, 5 decomposes in k as $5\mathcal{O}_k = \mathcal{B}_1^4\mathcal{B}_2^4\mathcal{B}_3^4\mathcal{B}_4^4\mathcal{B}_5^4$, where \mathcal{B}_i are prime ideals of k . Since $[\mathcal{B}_i]$ and $[\mathcal{B}_j]$ with $i \neq j \in \{1, 2, 3, 4\}$ are in $C_{k,5}$ we have $\langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle \subset C_{k,5}$. To prove that $\langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle = C_{k,5}$, we should prove that $\langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle$ has order 25. It is sufficient to prove that $[\mathcal{B}_i^{a_1}\mathcal{B}_j^{a_2}] = 1$ for $a_1, a_2 \in \{0, 1, 2, 3, 4\}$ if and only if $a_1 = a_2 = 0$.

$$\begin{aligned} [\mathcal{B}_i^{a_1}\mathcal{B}_j^{a_2}] = 1 &\implies \exists \beta \in \mathcal{O}_k \mid \mathcal{B}_i^{a_1}\mathcal{B}_j^{a_2} = \beta\mathcal{O}_k \\ &\implies \mathcal{N}_{k/k_0}(\mathcal{B}_i^{a_1}\mathcal{B}_j^{a_2}) = \mathcal{N}_{k/k_0}(\beta\mathcal{O}_k) \\ &\implies \lambda^{a_1+a_2}\mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\beta)\mathcal{O}_{k_0} \text{ with } \lambda = 1 - \zeta_5 \\ &\implies \exists \epsilon \in E_{k_0} \mid \lambda^{a_1+a_2} = \epsilon\mathcal{N}_{k/k_0}(\beta) \end{aligned}$$

According to the proof of [[12], theorem 5.15], we have $E_{k_0} \subset \mathcal{N}_{k/k_0}(k^*)$
 $\implies \exists \alpha \in \mathcal{O}_k \mid \lambda^{\alpha_1+\alpha_2} = \mathcal{N}_{k/k_0}(\alpha)$

that is to say $\lambda^{\alpha_1+\alpha_2}$ is norm in $k = k_0(\sqrt[5]{p})$, where $p = \pi_1\pi_2$ in k_0 . Hence we have:

$$\left(\frac{\lambda^{\alpha_1+\alpha_2, \pi_1\pi_2}}{\mathcal{P}}\right)_5 = 1$$

for all ideals \mathcal{P} of k_0 .

In particular, we calculate this symbol for $\mathcal{P} = \pi_1\mathcal{O}_{k_0}$ or $\mathcal{P} = \pi_2\mathcal{O}_{k_0}$. Using (1) of properties 4.2 we have,

$$A = \left(\frac{\lambda^{\alpha_1+\alpha_2, \pi_1\pi_2}}{\pi_1\mathcal{O}_{k_0}}\right)_5 = \left(\frac{\lambda^{\alpha_1, \pi_1}}{\pi_1}\right)_5 \cdot \left(\frac{\lambda^{\alpha_1, \pi_2}}{\pi_1}\right)_5 \cdot \left(\frac{\lambda^{\alpha_2, \pi_1}}{\pi_1}\right)_5 \cdot \left(\frac{\lambda^{\alpha_2, \pi_2}}{\pi_1}\right)_5$$

then, we get:

- $\left(\frac{\lambda^{\alpha_1, \pi_1}}{\pi_1}\right)_5 = \left(\frac{\lambda, \pi_1}{\pi_1}\right)_5^{\alpha_1} = \left(\frac{\lambda}{\pi_1}\right)_5^{\alpha_1}$, by (1) and (9) of properties 4.2.
- $\left(\frac{\lambda^{\alpha_1, \pi_2}}{\pi_1}\right)_5 = \left(\frac{\lambda, \pi_2}{\pi_1}\right)_5^{\alpha_1} = \left(\frac{\lambda}{\pi_1}\right)_5^{0 \times \alpha_1} = 1$, by (3) and (4) of properties 4.2.
- $\left(\frac{\lambda^{\alpha_2, \pi_1}}{\pi_1}\right)_5 = \left(\frac{\lambda, \pi_1}{\pi_1}\right)_5^{\alpha_2} = \left(\frac{\lambda}{\pi_1}\right)_5^{\alpha_2}$, by (1) and (9) of properties 4.2.
- $\left(\frac{\lambda^{\alpha_2, \pi_2}}{\pi_1}\right)_5 = \left(\frac{\lambda, \pi_2}{\pi_1}\right)_5^{\alpha_2} = \left(\frac{\lambda}{\pi_1}\right)_5^{0 \times \alpha_2} = 1$, by (3) and (4) of properties 4.2.

we get that, $A = \left(\frac{\lambda}{\pi_1}\right)_5^{\alpha_1+\alpha_2} = 1$. Since π_1 and π_2 play symmetric roles, then $B = \left(\frac{\lambda^{\alpha_1+\alpha_2, \pi_1\pi_2}}{\pi_2\mathcal{O}_{k_0}}\right)_5 = \left(\frac{\lambda}{\pi_2}\right)_5^{\alpha_1+\alpha_2}$, and since $\left(\frac{\lambda^{\alpha_1+\alpha_2, \pi_1\pi_2}}{\mathcal{P}}\right)_5 = 1$, for all prime ideals of k_0 , then $A = B = 1$, namely $\left(\frac{\lambda}{\pi_1}\right)_5^{\alpha_1+\alpha_2} = \left(\frac{\lambda}{\pi_2}\right)_5^{\alpha_1+\alpha_2} = 1$. Since 5 is not a quintic residue modulo p , we have $\alpha_1 + \alpha_2 = 0$ or 5, then $\alpha_1 = \alpha_2 = 0$, because otherwise $\alpha_1 + \alpha_2 = 5$, so we need to distinguish two cases:

- If $\alpha_1 = 1$ and $\alpha_2 = 4$, then $[\mathcal{B}_i\mathcal{B}_j^4] = 1$ means that $[\mathcal{B}_i] = [\mathcal{B}_j]^{-4}$ and since $[\mathcal{B}_j]^5 = 1$ because $[\mathcal{B}_i]$ is 5-class, we get $[\mathcal{B}_i] = [\mathcal{B}_j]$ which is impossible.

- If $\alpha_1 = 2$ and $\alpha_2 = 3$, then $[\mathcal{B}_i^2\mathcal{B}_j^3] = 1$ means that $[\mathcal{B}_i]^2 = [\mathcal{B}_j]^{-3}$, so $[\mathcal{B}_i] = [\mathcal{B}_j]$ which is impossible.

Thus the case $\alpha_1 + \alpha_2 = 5$ cannot occur. Hence $\langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle$ has order 25, and since $\langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle \subset C_{k,5}$ we deduce that $C_{k,5} = \langle [\mathcal{B}_i], [\mathcal{B}_j] \rangle$.

Corollary 6.4. Using the same notation as above, we have:

- (1) $C_{k,5}^{(\sigma)} = C_{k,5}^+ = \langle [\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5] \rangle$.
- (2) $C_{k,5}^- = \langle [\mathcal{B}_i]^{1-\tau^2} \rangle$ for $(i = 1, 2, 3, 4, 5)$.
- (3) The 5-class group can be generated also by:

$$C_{k,5} = \langle [\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5], [\mathcal{B}_i]^{1-\tau^2} \rangle \text{ for } (i = 1, 2, 3, 4, 5).$$

Proof.

- (1) The fact that the ideals \mathcal{B}_i are not principal by the same reasoning as above, we prove that $[\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5]^\sigma = [\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5]$ and $[\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5]^{\tau^2} = [\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5]$ by applying the decomposition of 5 in the normal closure k .
- (2) Since \mathcal{B}_i are not principal then $[\mathcal{B}_i]^{1-\tau^2} \in C_{k,5}^-$
- (3) That comes from $C_{k,5} \cong C_{k,5}^+ \times C_{k,5}^-$ □

7 Numerical examples

Using the system PARI/GP [[19]], we illustrate our main result Theorem 1.1 by numerical examples.

7.1 Case 1: $n = 5^e p^{e_1} \not\equiv \pm 1, \pm 7 \pmod{25}$ with $p \not\equiv -1 \pmod{25}$

In this case we have: $C_{k,5} = \langle [\mathcal{P}], [\mathcal{L}]^{1-\tau^2} \rangle$, where \mathcal{P} is a prime ideal of k above p , and \mathcal{L} is prime ideals of k above l such that $l \neq p$. The following table verifies, for some primes $p \not\equiv -1 \pmod{25}$ and $l \neq p$, such that 5 and l are not quintic residues modulo p and $C_{k,5}$ is of type $(5, 5)$, that the ideals \mathcal{P} and \mathcal{L} are not principal, and are of order 5.

Table 1:

p	l	Type of $C_{k,5}$	Is principal \mathcal{P}	Is principal \mathcal{L}	Is principal \mathcal{P}^5	Is principal \mathcal{L}^5
19	2	(5,5)	[4,0]	[1,0]	[0,0]	[0,0]
19	113	(5,5)	[4,0]	[4,0]	[0,0]	[0,0]
29	43	(5,5)	[6,0,0,0]	[6,0,1,0]	[0,0,0,0]	[0,0,0,0]
29	149	(5,5)	[6,0,0,0]	[2,0,0,0]	[0,0,0,0]	[0,0,0,0]
59	67	(5,5)	[4,0,0,0]	[6,0,0,0]	[0,0,0,0]	[0,0,0,0]
79	97	(5,5)	[21,21,0,0]	[28,28,0,0]	[0,0,0,0]	[0,0,0,0]
79	307	(5,5)	[21,21,0,0]	[7,7,0,0]	[0,0,0,0]	[0,0,0,0]
89	19	(5,5)	[1,0]	[4,0]	[0,0]	[0,0]
89	101	(5,5)	[1,0]	[4,4]	[0,0]	[0,0]
109	13	(5,5)	[2,0]	[1,0]	[0,0]	[0,0]
109	103	(5,5)	[2,0]	[1,0]	[0,0]	[0,0]
179	157	(5,5)	[3,0]	[2,0]	[0,0]	[0,0]
299	83	(5,5)	[8,12,0,0]	[12,8,0,0]	[0,0]	[0,0]
239	3	(5,5)	[3,0]	[2,0]	[0,0]	[0,0]
269	157	(5,5)	[1,0]	[3,0]	[0,0]	[0,0]

7.2 Case 2: $n = p^{e_1} q^{e_2} \equiv \pm 1, \pm 7 \pmod{25}$ with $p \not\equiv -1 \pmod{25}$ and $q \not\equiv \pm 7 \pmod{25}$

In this case we have: $C_{k,5} = \langle [\mathcal{P}], [\mathcal{L}]^{1-\tau^2} \rangle$, where \mathcal{P}, \mathcal{L} as above.

Table 2

p	q	l	Type of $C_{k,5}$	Is principal \mathcal{P}_1	Is principal \mathcal{P}_2	Is principal \mathcal{P}_1^5	Is principal \mathcal{P}_2^5
19	3	53	(5,5)	[1,0]	[3,0]	[0,0]	[0,0]
19	3	67	(5,5)	[1,0]	[4,0]	[0,0]	[0,0]
19	53	7	(5,5)	[3,0]	[1,0]	[0,0]	[0,0]
19	53	23	(5,5)	[3,0]	[1,0]	[0,0]	[0,0]
29	17	157	(5,5)	[28,14,0,0]	[14,7,0,0]	[0,0,0,0]	[0,0,0,0]
59	2	13	(5,5)	[0,2]	[0,2]	[0,0]	[0,0]
59	2	47	(5,5)	[0,2]	[0,3]	[0,0]	[0,0]
59	23	127	(5,5)	[2,0,0,0]	[6,0,0,0]	[0,0,0,0]	[0,0,0,0]
89	37	61	(5,5)	[3,0]	[3,0]	[0,0]	[0,0]
89	37	73	(5,5)	[3,0]	[2,0]	[0,0]	[0,0]
109	23	47	(5,5)	[28,0,0,0]	[14,0,0,0]	[0,0,0,0]	[0,0,0,0]
359	2	61	(5,5)	[2,1]	[3,1]	[0,0]	[0,0]
359	2	97	(5,5)	[2,1]	[4,2]	[0,0]	[0,0]
409	2	157	(5,5)	[2,0]	[1,0]	[0,0]	[0,0]
409	2	163	(5,5)	[2,0]	[3,0]	[0,0]	[0,0]
509	2	53	(5,5)	[2,0]	[3,0]	[0,0]	[0,0]
509	2	79	(5,5)	[2,0]	[4,0]	[0,0]	[0,0]

7.3 Case 3: $n = p^{e_1} \equiv \pm 1, \pm 7 \pmod{25}$ with $p \equiv -1 \pmod{25}$

In this case we have: $C_{k,5} = \langle [\mathcal{B}_1], [\mathcal{B}_2] \rangle$, where \mathcal{B}_i are prime ideals of k above 5. The following table verifies that the ideals \mathcal{B}_1 and \mathcal{B}_2 are not principal and are of order 5 such that $\left(\frac{5}{p}\right)_5 \neq 1$

Table 3:

p	Type of $C_{k,5}$	Is principal \mathcal{B}_1	Is principal \mathcal{B}_2	Is principal \mathcal{B}_1^5	Is principal \mathcal{B}_2^5
149	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
199	(5,5)	[6,0,0,0]	[6,0,0,0]	[0,0,0,0]	[0,0,0,0]
499	(5,5)	[1,4]	[1,4]	[0,0]	[0,0]
599	(5,5)	[3,0]	[3,0]	[0,0]	[0,0]
2099	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
2549	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
2699	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
2749	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
3299	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
4049	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
4099	(5,5)	[8,0,0,0]	[8,0,0,0]	[0,0,0,0]	[0,0,0,0]
4349	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
4549	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
4999	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
5099	(5,5)	[8,0,0,0]	[8,0,0,0]	[0,0,0,0]	[0,0,0,0]
5399	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
5749	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
6299	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]
6599	(5,5)	[1,0]	[1,0]	[0,0]	[0,0]

References

[1] K. Bahmanpour, Prime numbers p with expression $p = a^2 \pm ab \pm b^2$, *Journal of Number Theory* 166 (2016) 208-218.

[2] W.E.H. Berwick, Integral bases, *Cambridge Tracts in Math. and Math.Phys*, Vol 22, 1927.

[3] R.Dedekind. Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, *J für reine und angewandte mathematik*, Bd 121 (1900), 40-123.

[4] F.El mouhib, M.Talbi, and A.Azizi, 5-rank of ambiguous class groups of quintic Kummer extensions, *Proc Math Sci* 132, 12 (2022). <https://doi.org/10.1007/s12044-022-00660-z>

[5] F.El mouhib, M.Talbi, and A.Azizi, On the capitulation problem of some pure metacyclic fields of degree 20, *Palestine Journal of Mathematics*, (2024), 13 (Special Issue II), pp. 73–80.

[6] D. Grant, A proof of quintic reciprocity using the arithmetic of $y^2 = x^5 + \frac{1}{4}$. *ACTA ARITHMETICA* (1996).

[7] G.Gras, Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier impaire l . *Annales de l'institut Fourier*, (1973).

[8] H. Hasse, Neue Begründung und Verallgemeinerung der Theorie des Normenrest Symbols, *Journal für reine und ang. Math.* 162 (1930), 134-143.

[9] E.Hecke, Lectures on the Theory of Algebraic Numbers, *GTM*, Vol. 77, Springer-Verlag 1981.

[10] K.Ireland and M.Rosen, A Classical Introduction to modern Number Theory. *Graduate Texts in Mathematics* 84, Springer-Verlag (1982).

[11] G.J Janus, Algebraic Number Fields. *Academic Press, New York-London* (1973).

[12] M.Kulkarni, D. Majumdar and B.Sury l -class groups of cyclic extension of prime degree l , *J. Ramanujan Math. Soc.* 30, No.4 (2015), 413-454.

[13] H. Kobayashi, Class numbers of pure quintic fields, *Journal of Number Theory* 160 (2016) 463-477.

[14] D.C. Mayer, Differential Principal Factors and Polya Property of Pure Metacyclic Fields, *International Journal of Number Theory*, Vol. 15, No. 10 (2019), pp. 1983-2025.

[15] R.C Martha, V.S Gabriel, Congruence function fields with class number one, *Palestine Journal of Mathematics*. 5, No 1 (2016).

- [16] C. Parry, Class number relations in pure quintic fields, *Symposia Mathematica*. 15 (1975), 475-485.
- [17] P. Samuel. Théorie algébrique des nombres. *Hermann, éditeurs des sciences et des arts* (1971).
- [18] L.C. Washington, Introduction to Cyclotomic Fields, *Springer-Verlag New York Inc* (1982).
- [19] The PARI Group, *PARI/GP, Version 2.4.9, Bordeaux, 2017*, <http://pari.math.u-bordeaux.fr>.

Author information

Fouad ELMOUHIB, Department of Mathematics and Computer Sciences
Faculty of Science
Mohammed First University
, Morocco.
E-mail: fouad.cd@gmail.com

Received: 2025-04-09

Accepted: 2025-09-11