THE 3-CLASS GROUP OF $\mathbb{Q}(\sqrt[3]{p})$

JIANING LI AND SHENXING ZHANG

Abstract. We determine the 3-class groups of $\mathbb{Q}(\sqrt[3]{p})$ and $K = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-3})$ when $p \equiv 4, 7 \bmod 9$ is a prime and 3 is a cubic modulo p. This confirms a conjecture made by Barrucand-Cohn, and proves the last remaining case of a conjecture of Lemmermeyer on the 3-class group of K.

1. Introduction

Let p be a prime. Let $F = \mathbb{Q}(\sqrt[3]{p})$ and $K = \mathbb{Q}(\sqrt[3]{p}, \mu_3)$ the normal closure of F. Let A_F (resp. A_K) be the 3-class group (i.e., 3-Sylow subgroup of the class group) of F (resp. K). The paper aims to prove the following result.

Theorem 1.1. *Assume that $p \equiv 4, 7 \mod 9$ is a prime such that the cubic residue symbol $\left(\frac{3}{p}\right)_3 = 1$. Then $A_F \cong \mathbb{Z}/3\mathbb{Z}$ and $A_K \cong (\mathbb{Z}/3\mathbb{Z})^2$.*

This result confirms a conjecture made by Barrucand-Cohn in [BC70, §8], and later mentioned by Barrucand-Williams-Baniuk, Williams and Gerth in [BWB76, §8, Conjecture 1], [Wil82, p. 273] and [Ger05, p. 474]. Theorem 1.1 also completes a proof of a Lemmermeyer's conjecture on A_K in [Lem10, Conjecture 5, §1.10] when combining with the following known results:

(1) If $p \equiv 2 \bmod 3$, then the groups A_F and A_K are both trivial; see [Hon71].
(2) If $p \equiv 1 \bmod 3$, then A_F is cyclic non-trivial and $\mathrm{rk}(A_K) = 1$ or 2 where $\mathrm{rk}(A_K)$ is the 3-rank of A_K; see [Ger05].
(3) If $p \equiv 1 \bmod 9$, then $\mathrm{rk}(A_K) = 1$ if and only if 9 divides $|A_F|$; see [CE05, Lemma 5.11] and [Ger05].
(4) If $p \equiv 4, 7 \bmod 9$ and $\left(\frac{3}{p}\right)_3 \neq 1$; then $A_F \cong A_K \cong \mathbb{Z}/3\mathbb{Z}$; see [BWB76] or [Ger05].

We give two consequences of Theorem 1.1. Let E_K be the group of units of K. Let E_K' be the subgroup of E_K generated by the units of non-trivial subfields of K. Write $q = [E_K : E_{K'}]$. One has ([BC71, Theorem 12.1, 14.1])

$$q = 1 \text{ or } 3 \quad \text{and} \quad h_K = \frac{q}{3} h_F^2.$$

Here h_K (resp. h_F) is the class number of K (resp. F). Thus, if $p \equiv 4, 7 \bmod 9$ and $\left(\frac{3}{p}\right)_3 = 1$, Theorem 1.1 implies that $q = 3$. This confirms a conjecture made in [ATIA20].

Assume $p \equiv 4, 7 \bmod 9$. Theorem 1.1 implies that the norm equation $\mathbf{N}_{F/\mathbb{Q}}(x) = 3$ has a solution $x \in \mathcal{O}_F$ if and only if $\left(\frac{3}{p}\right)_3 = 1$, as mentioned in [Wil82, p. 273]. Since $\mathcal{O}_F = \mathbb{Z}[\sqrt[3]{p}]$, this is to say, the Diophantine equation

$$x_1^3 + p x_2^3 + p^2 x_3^3 - 3p x_1 x_2 x_3 = 3$$

has solutions $(x_1, x_2, x_3) \in \mathbb{Z}$ if and only if $\left(\frac{3}{p}\right)_3 = 1$.

2010 *Mathematics Subject Classification.* 11R29, 11R16.
Key words and phrases. class groups, pure cubic fields, ambiguous class number formulas.

2. The proof

2.1. **Chevalley's ambiguous class number formula.** We first review Chevalley's S-version ambiguous class number formula which will be used. For a finite set S of prime ideals of a number field T, the *S-class group* of T is defined as

$$\mathrm{Cl}_{T,S} := \mathrm{Cl}_T/\langle[\mathfrak{p}] : \mathfrak{p} \in S\rangle,$$

where Cl_T denotes the class group of T and $[\mathfrak{p}]$ denotes the ideal class of $\mathfrak{p}$. Let $E_{T,S} := \mathcal{O}_{T,S}^{\times}$ denote the group of S-units of T. Let R/T be a finite cyclic extension with Galois group G. For a finite set S of prime ideals of T, we denote by $\mathrm{Cl}_{R,S} = \mathrm{Cl}_{R,S_R}$ for simplicity, where S_R is the set of primes of R lying above those in S. Chevalley's ambiguous class number formula states that the order of the G-invariant subgroup of $\mathrm{Cl}_{R,S}$ is given by

$$|\mathrm{Cl}_{R,S}^G| = |\mathrm{Cl}_{T,S}| \cdot \frac{\prod\limits_{v\notin S} e_v \cdot \prod\limits_{v\in S} e_v f_v}{[R:T]\cdot[E_{T,S} : E_{T,S}\cap \mathbf{N}R^{\times}]}. \tag{2.1}$$

Here the first product runs over all places of T not in S, e_v and f_v are the ramification index and the residue degree of v respectively, and $\mathbf{N} = \mathbf{N}_{R/T}$ is the norm map. For a proof of this formula, see [LY20] for example. The unit index in (2.1) can be computed by Hilbert symbols provided that R/T is a Kummer extension.

Proposition 2.1. *Let R/T be a cyclic extension of degree d and $\mu_d \subset T$. Then $R = T(\sqrt[d]{a})$ for some $a \in T$. Let* Ram *be the set of ramified places of T. Define*

$$\rho : \frac{E_{T,S}}{(E_{T,S})^d} \longrightarrow \prod_{v\in S\cup \mathrm{Ram}} \mu_d$$
$$x \longmapsto \left(\left(\frac{x,a}{v}\right)_d\right)_{v\in S\cup\mathrm{Ram}}.$$

Then the kernel of ρ is given by

$$\operatorname{Ker}\rho = \frac{E_{T,S}\cap \mathbf{N}R^{\times}}{(E_{T,S})^d}$$

and hence the size of the image is given by

$$|\mathrm{Im}(\rho)| = [E_{T,S} : E_{T,S}\cap \mathbf{N}R^{\times}],$$

which is at most $d^{|S\cup\mathrm{Ram}|-1}$.

Proof. This result is a standard direct consequence of local class field theory, Hasse's norm theorem, and the product formula for Hilbert symbols. For details, see [LOXZ20, §2]. □

If $\sigma \in \mathrm{Aut}(T)$ and v is a prime of T, we have (*loc. cit.*)

$$\sigma\left(\frac{a,b}{v}\right)_d = \left(\frac{\sigma(a),\sigma(b)}{\sigma(v)}\right)_d, \quad a,b\in T^{\times}. \tag{2.2}$$

For our applications, the degree $[R:T]$ is a power of a prime ℓ. For any finite generated abelian group A, we denote by $A_\ell = A\otimes\mathbb{Z}_\ell$ where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. If A is finite, A_ℓ is the ℓ-primary subgroup of A. If there is no ambiguity, we write a for $a\otimes 1\in A_\ell$ for $a\in A$. Clearly, the formula (2.1) still holds by replacing $(\mathrm{Cl}_{R,S})^G$ and $\mathrm{Cl}_{T,S}$ with $\big((\mathrm{Cl}_{R,S})_\ell\big)^G = (\mathrm{Cl}_{R,S}^G)_\ell$ and $(\mathrm{Cl}_{T,S})_\ell$ respectively.

The following well known fact which is proved by counting the orbits of the G-action or by Nakayama's Lemma will be used frequently:

$$(\mathrm{Cl}_{R,S})_\ell = 0 \text{ if and only if } (\mathrm{Cl}_{R,S}^G)_\ell = 0.$$

2.2. **Proof of Theorem 1.1.** From now on, assume $p \equiv 1 \bmod 3$. Denote by

- $k = \mathbb{Q}(\mu_3)$;
- M^+ the unique cubic subfield of $\mathbb{Q}(\mu_p)$, which is real;
- $M = M(\mu_3)$ a quadratic extension of M^+;
- $L = KM = M(\sqrt[3]{p}, \mu_3)$;
- $A_T = (\mathrm{Cl}_T)_3$ for any number field T.

$$\begin{tikzcd}
 & L = KM \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt[3]{p}, \mu_3) \arrow[d, dash] \arrow[dr, dash] & FM^+ \arrow[dl, dash] \arrow[dr, dash] & M = kM^+ \arrow[dl, dash] \arrow[d, dash] \\
F = \mathbb{Q}(\sqrt[3]{p}) \arrow[dr, dash] & k = \mathbb{Q}(\mu_3) \arrow[d, dash] & M^+ \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Proposition 2.2. *Assume $p \equiv 1 \bmod 3$.*

(1) There exists $\alpha \in \mathcal{O}_k$ such that $M = k(\sqrt[3]{p\alpha})$ and $p = \alpha\overline{\alpha}$;

(2) $A_M = 0$ if and only if $p \equiv 4, 7 \bmod 9$.

Proof. (1) Since $p \equiv 1 \bmod 3$, we can write $p = \alpha\overline{\alpha}$ for some $\alpha \in \mathcal{O}_k$. Note that (α) and $(\overline{\alpha})$ are exactly the ramified primes of k in M. Now, since the class number of k is 1 and M/k is a Kummer extension, we have

$$M = \mathbb{Q}(\sqrt[3]{\gamma}) \quad \text{and} \quad \gamma = \zeta_3^a \alpha^b \overline{\alpha}^c$$

with $a, b, c \in \{0, 1, 2\}$ and $bc \neq 0$. Since $(3-a, 3-b, 3-c)$ give the same field as (a, b, c), we conclude that $M = k(\sqrt[3]{\zeta_3^a p})$ or $k(\sqrt[3]{\zeta_3^a p\alpha})$ for some $a = 0, 1, 2$. Since M is abelian over $\mathbb{Q}$ but $k(\sqrt[3]{\zeta_3^a p})/\mathbb{Q}$ is not, M must coincide with $k(\sqrt[3]{\zeta_3^a p\alpha})$. By replacing α with $\zeta_3^a\alpha$, we have $M = k(\sqrt[3]{p\alpha})$ and $p = \alpha\bar{\alpha}$. This proves (1).

(2) We apply (2.1) and Proposition 2.1 to the cyclic cubic extension M/k. Let $\iota : k \hookrightarrow \mathbb{Q}_p$ be the embedding induced by (α). Then we have the following equalities of cubic Hilbert symbols:

$$\left(\frac{\zeta_3, p\alpha}{\alpha}\right) = \iota^{-1}\left(\frac{\iota(\zeta_3), p\iota(\alpha)}{\mathbb{Q}_p}\right) = \iota^{-1}\left(\frac{\iota\zeta_3, \iota(\alpha)}{\mathbb{Q}_p}\right)^{-1} = \zeta_3^{(p-1)/3}. \tag{2.3}$$

Hence this symbol as well as the index $[E_k : E_k \cap \mathbf{N}M^\times]$ is trivial if and only if $p \equiv 1 \bmod 9$. Thus

$$|A_M^G| = \frac{3^2}{3 \cdot [E_k : E_k \cap \mathbf{N}M^\times]} = 1$$

if and only if $p \equiv 4, 7 \bmod 9$. By Nakayama's lemma, it turns out that A_M is trivial if and only if $p \equiv 4, 7 \bmod 9$. This completes the proof of Proposition 2.2. $\square$

Let $\mathfrak{p}$ (resp. $\mathfrak{p}'$) be the unique prime of M (resp. K) lying above $\alpha\mathcal{O}_k$. Then $\alpha\mathcal{O}_M = \mathfrak{p}^3$ and $\alpha\mathcal{O}_K = \mathfrak{p}'^3$.

Proposition 2.3. *Assume that $p \equiv 1 \bmod 3$ and $\left(\frac{3}{p}\right)_3 = 1$.*

(1) The extensions L/K and FM^+/F are both abelian unramified cubic extensions.

(2) The primes $\mathfrak{p}$ and $\mathfrak{p}'$ both split in L.

Proof. (1) Since $L = KM^+$, we have that L/K is unramified outside the primes above p. Denote by $I_{(\alpha)}$ the inertia group of $(\alpha) = \alpha\mathcal{O}_k$ in the abelian extension L/k. By local class field theory and noting that the completion of k at (α) is $\mathbb{Q}_p$, we have a surjection

$$\mathbb{Z}_p^\times \twoheadrightarrow I_{(\alpha)}.$$

It follows that $I_{(\alpha)}$ can not be $\mathrm{Gal}(L/k) \cong (\mathbb{Z}/3\mathbb{Z})^2$. On the other hand, $I_{(\alpha)}$ is non-trivial since (α) is ramified in K and M. This shows that $\mathfrak{p}$ and $\mathfrak{p}'$ must be unramified in L. An entirely same argument for the prime $(\overline{\alpha}) = \overline{\alpha}\mathcal{O}_k$ shows that L/M and L/K are both unramified outside the primes above $\overline{\alpha}$. This shows that L/K is unramified everywhere.

For the extension FM^+/F, first note that it is unramified outside $\sqrt[3]{p}\mathcal{O}_F$ as $M^+/\mathbb{Q}$ is unramified outside p. We claim that $\sqrt[3]{p}\mathcal{O}_F$ is also unramified in FM^+. Otherwise, since K/F is unramified at $\sqrt[3]{p}\mathcal{O}_F$, the prime of K above $\sqrt[3]{p}$ would be ramified in L. But this contradicts that L/K is unramified whence the claim holds. This proves (1).

(2) We just show that FM^+ is contained in the Hilbert class field of F. By class field theory, the principal prime $\sqrt[3]{p}\mathcal{O}_F$ splits in FM^+. It follows that $\mathfrak{p}'$ and $\mathfrak{p}$ both split in L. $\square$

Lemma 2.4. *(1) If $p \equiv 4, 7 \bmod 9$, then 3 is totally ramified in K.*

(2) If $p \equiv 1 \bmod 3$ and 3 is a cubic modulo p, then $(1 - \zeta_3)\mathcal{O}_k$ splits in M.

Proof. (1) Since $(x + p)^3 - p$ is an Eisenstein polynomial, 3 is totally ramified in F. Since 3 is also ramified in k, it follows that 3 is totally ramified in K by counting the ramification degrees.

(2) Fix the canonical isomorphism

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^\times &\cong \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \\ a &\mapsto (\sigma_a : \zeta_p \mapsto \zeta_p^a).\end{aligned}$$

By definition, M^+ is the subfield of $\mathbb{Q}(\mu_p)$ fixed by $(\mathbb{Z}/p\mathbb{Z})^{\times 3}$. Our assumptions imply that σ_3 is trivial on M^+ whence 3 splits in M^+. It follows that $(1 - \zeta_3)\mathcal{O}_k$ must split in M. $\square$

We need the following elementary fact on the local field $\mathbb{Q}_3(\mu_3)$.

Lemma 2.5. *If $a, b \in \mathbb{Z}$ with $3 \nmid ab$, then the cubic Hilbert symbol of a and b in $\mathbb{Q}_3(\mu_3)$ is trivial.*

Proof. By convergence of the Taylor expansion of $(1+9x)^{1/3}$ on $\mathbb{Z}_3[\mu_3]$, every element in $1 + 9\mathbb{Z}_3[\mu_3]$ is a cubic. Note that -1 is a cubic whence the cubic Hilbert symbol $\left(\frac{a,a}{\mathbb{Q}_3(\mu_3)}\right) = 1$. Thus, we only need to show the triviality of the symbol

$$\left(\frac{4,7}{\mathbb{Q}_3(\zeta_3)}\right) = \left(\frac{4,2}{\mathbb{Q}_3(\zeta_3)}\right) = \left(\frac{2,2}{\mathbb{Q}_3(\zeta_3)}\right)^2 = 1. \qquad \square$$

Theorem 2.6. *Assume that $p \equiv 4, 7 \bmod 9$ and $\left(\frac{3}{p}\right)_3 = 1$. Then A_L is non-trivial and 3 does not divides $|\mathrm{Cl}_{L,\{\mathfrak{p}\}}|$.*

Proof. We first apply (2.1) on L/M with $S = \emptyset$ to prove 3 divides $|A_L^G|$ where $G = \mathrm{Gal}(L/M)$. By Proposition 2.3 and Lemma 2.4, exactly the three primes $\mathfrak{l}, \sigma(\mathfrak{l}), \sigma^2(\mathfrak{l})$ of M lying above $(1-\zeta_3)\mathcal{O}_k$ are ramified in L/M, where σ is a generator of $\mathrm{Gal}(M/k)$. By Proposition 2.2, we know that $|A_M| = 1$. It remains to compute the unit index. Note that $L = M(\sqrt[3]{p})$. To apply Proposition 2.1, we define

$$\begin{aligned}\rho : E_M &\longrightarrow \mu_3^3 \\ u &\longmapsto \left(\left(\frac{u,p}{\mathfrak{l}}\right), \left(\frac{u,p}{\sigma(\mathfrak{l})}\right), \left(\frac{u,p}{\sigma^2(\mathfrak{l})}\right)\right).\end{aligned}$$

Since M/M^+ is a CM-extension, the group $(E_M)_3$ is generated by $(E_{M^+})_3$ and ζ_3 by [Was82, Theorem 4.12]. The completion of M^+ at a prime above 3 is $\mathbb{Q}_3$. It follows that $\eta \equiv a \bmod 9$ with $a \in \mathbb{Z}$ for any $\eta \in E_{M^+}$. Then by Lemma 2.5,

$$|\rho(E_{M^+})| = 1. \tag{2.4}$$

Now we compute $\rho(\zeta_3)$. Since $\sigma(\zeta_3) = \zeta_3$, by (2.2) we have

$$\left(\frac{\zeta_3, p}{\mathfrak{l}}\right) = \left(\frac{\zeta_3, p}{\sigma(\mathfrak{l})}\right) = \left(\frac{\zeta_3, p}{\sigma^2(\mathfrak{l})}\right).$$

By Lemma 2.4, the completion of M at $\mathfrak{l}$ is $\mathbb{Q}_3(\mu_3)$. Applying the product formula for cubic Hilbert symbols on the field $\mathbb{Q}(\mu_3)$ gives

$$\left(\frac{\zeta_3, p}{(\alpha)}\right)\left(\frac{\zeta_3, p}{(\overline{\alpha})}\right)\left(\frac{\zeta_3, p}{(1-\zeta_3)}\right) = 1.$$

By (2.3) and our assumption $p \equiv 4, 7 \bmod 9$, we obtain that

$$\left(\frac{\zeta_3, p}{(1-\zeta_3)}\right) \neq 1 \text{ and } \left(\frac{\zeta_3, p}{\mathbb{Q}_3(\mu_3)}\right) \neq 1. \tag{2.5}$$

This proves that $\rho(\zeta_3) = \zeta_3^{\pm 1}(1,1,1)$. Combining with (2.4), we conclude that $|\rho(E_M)_3| = 3$. Then Chevalley's formula gives

$$|A_L^G| = \frac{3^3}{3 \times 3} = 3.$$

In particular, $|A_L| \geq 3$.

Next, we apply Chevalley's formula on L/M with $S = \{\mathfrak{p}\}$ to compute $\mathrm{Cl}_{L,\{\mathfrak{p}\}}^G$. Define

$$\beta = \frac{\sqrt[3]{p\alpha}}{\mathbf{N}_{\mathbb{Q}(\mu_p)/M^+}(1-\zeta_p)}.$$

Note that β^3 generates the ideal $\alpha\mathcal{O}_M$ whence $\beta\mathcal{O}_M = \mathfrak{p}$. It follows that $(E_{M,\{\mathfrak{p}\}})_3$ is generated by β, ζ_3 and E_{M^+}. We claim that

$$\left(\frac{\beta, p}{\mathfrak{l}}\right) \neq \left(\frac{\beta, p}{\sigma(\mathfrak{l})}\right).$$

Indeed, by (2.2), the right hand side equals the Hilbert symbol of $\sigma^{-1}(\beta)$ and p at $\mathfrak{l}$. Note that $\sigma^{-1}(\beta) = \zeta_3^{\pm 1}\beta\eta$ for some $\eta \in E_{M^+}$. Thus the inequality follows from (2.4) and (2.5). By Proposition 2.1, this shows that the index

$$[E_{M,\{\mathfrak{p}\}} : E_{M,\{\mathfrak{p}\}} \cap \mathbf{N}L^\times] = 9.$$

By Proposition 2.3, the prime $\mathfrak{p}$ splits in L. It follows from (2.1) that 3 does not divide $|\mathrm{Cl}_{L,\{\mathfrak{p}\}}^G|$ whence 3 does not divide $|\mathrm{Cl}_{L,\{\mathfrak{p}\}}|$ by Nakayama's Lemma. This completes the proof. □

Proof of Theorem 1.1. By Theorem 2.6, A_L is non-trivial. It follows that, by Nakayama's lemma, we have $|A_L^{\mathrm{Gal}(L/K)}| \geq 3$. Since L/K is unramified everywhere, by Hasse's norm theorem and local class field theory (or Proposition 2.3), we have the unit index $[E_K : E_K \cap \mathbf{N}(L^\times)] = 1$. Then applying Chevalley's formula with $S = \emptyset$ to the extension L/K gives

$$|A_K| \geq 9.$$

Recall that $\mathfrak{p}'$ is the prime of K lying above $\alpha\mathcal{O}_k$. Note that $\mathfrak{p}'\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$, we have $\mathrm{Cl}_{L,\{\mathfrak{p}'\}} = \mathrm{Cl}_{L,\{\mathfrak{p}\}}$ by definition. Since 3 does not divide $|\mathrm{Cl}_{L,\{\mathfrak{p}'\}}|$ by Theorem 2.6 and $\mathfrak{p}'$ splits in L by Proposition 2.3, Chevalley's formula with $S = \{\mathfrak{p}'\}$ will imply that $(\mathrm{Cl}_{K,\{\mathfrak{p}'\}})_3 \cong \mathbb{Z}/3\mathbb{Z}$ if we can show that

$$[E_{K,\{\mathfrak{p}'\}} : E_{K,\{\mathfrak{p}'\}} \cap \mathbf{N}(L^\times)] = 1.$$

Because $\mathfrak{p}'$ splits in L/K by Proposition 2.3, the local extension at $\mathfrak{p}'$ is trivial. Thus any $\{\mathfrak{p}'\}$-unit is a local norm at $\mathfrak{p}'$ whence is a local norm at every place of K as L/K is unramified. By Hasse's norm theorem, the above unit index is indeed trivial.

The equality $\mathfrak{p}'^3 = \alpha\mathcal{O}_K$ implies that $|\mathrm{Cl}_K| \leq 3|\mathrm{Cl}_{K,\{\mathfrak{p}'\}}|$. It follows that

$$|A_K| \leq 9.$$

Hence $|A_K| = 9$ and then $|A_F| = 3$ by [Hon71, Lemma 1].

Let τ be the non-trivial element of $\Delta = \mathrm{Gal}(K/F)$. Since Δ is of order 2, we have a decomposition of $\mathbb{Z}_3[\Delta]$-modules

$$A_K = A_K^+ \oplus A_K^-, \text{ where } A_K^\pm = \{a \in A_K | \tau(a) = a^{\pm 1}\}.$$

It is well known that $|A_K^+| = |A_F| = 3$ (for example, using (2.1)). Thus A_K has a direct factor $\mathbb{Z}/3\mathbb{Z}$. This implies that $A_K \cong (\mathbb{Z}/3\mathbb{Z})^2$, completing the proof of Theorem 1.1. □

Acknowledgment. The authors are partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and by the Fundamental Research Funds for the Central Universities (Grant No. WK0010000058 and Grant No. WK0010000061 respectively). The second named author is also supported by NSFC (Grant No. 12001510).

References

[ATIA20] S. Aouissi, M. Talbi, M. C. Ismaili and A. Azizi. *On a conjecture of Lemmermeyer*, Int. J. Number Theory, 16(7):1407–1424, 2020, doi:10.1142/S1793042120500748.

[BC70] P. Barrucand and H. Cohn. *A rational genus, class number divisibility, and unit theory for pure cubic fields*, J. Number Theory, 2:7–21, 1970, doi:10.1016/0022-314X(70)90003-X.

[BC71] P. Barrucand and H. Cohn. *Remarks on principal factors in a relative cubic field*, J. Number Theory, 3:226–239, 1971, doi:10.1016/0022-314X(71)90040-0.

[BWB76] P. Barrucand, H. C. Williams and L. Baniuk. *A computational technique for determining the class number of a pure cubic field*, Math. Comp., 30(134):312–323, 1976, doi:10.2307/2005974.

[CE05] F. Calegari and M. Emerton. *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math., 160(1):97–144, 2005, doi:10.1007/s00222-004-0406-z.

[Ger05] F. E. Gerth III. *On 3-class groups of certain pure cubic fields*, Bull. Austral. Math. Soc., 72(3):471–476, 2005, doi:10.1017/S0004972700035292.

[Hon71] T. Honda. *Pure cubic fields whose class numbers are multiples of three*, J. Number Theory, 3(1):7–12, 1971, doi:10.1016/0022-314X(71)90045-X.

[Lem10] F. Lemmermeyer. *Class field towers*, preprint, 2010, available at `http://www.rzuser.uni-heidelberg.de/~hb3/publ/pcft.pdf`.

[LOXZ20] J. Li, Y. Ouyang, Y. Xu and S. Zhang. *ℓ-class groups of fields in Kummer towers*, *to appear in* Publ. Mat., 2020, arXiv:1905.04966

[LY20] J. Li and C. F. Yu. *The Chevalley-Gras formula over global fields*, *appearing in* J. Thor. Nombres Bordeaux, 2020, arXiv:2001.11413.

[Was82] L. C. Washington. *Introduction to cyclotomic fields*, 2nd ed. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997, doi:10.1007/978-1-4612-1934-7.

[Wil82] H. C. Williams. *Determination of principal factors in $\mathcal{Q}(\sqrt{D})$ and $\mathcal{Q}(\sqrt[3]{D})$*, Math. Comp., 38(157):261–274, 1982, doi:10.2307/2007484.

CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China
E-mail address: `lijn@ustc.edu.cn`

CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China
E-mail address: `zsxqq@mail.ustc.edu.cn`