Publ. Mat. **66** (2022), 235–267
DOI: 10.5565/PUBLMAT6612210

ℓ-CLASS GROUPS OF FIELDS IN KUMMER TOWERS

Jianing Li, Yi Ouyang, Yue Xu, and Shenxing Zhang

Abstract: Let ℓ and p be prime numbers and $K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^m}}, \zeta_{2\ell^m})$. We study the ℓ-class group of $K_{n,m}$ in this paper. When $\ell = 2$, we determine the structure of the 2-class group of $K_{n,m}$ for all $(n,m) \in \mathbb{Z}^2_{\geq 0}$ in the case $p \equiv 3, 5 \bmod 8$, and for $(n,m) = (n,0)$, $(n,1)$, or $(1,m)$ in the case $p \equiv 7 \bmod 16$, generalizing the results of Parry about the 2-divisibility of the class number of $K_{2,0}$. We also obtain results about the ℓ-class group of $K_{n,m}$ when ℓ is odd and in particular when $\ell = 3$. The main tools we use are class field theory, including Chevalley's ambiguous class number formula and its generalization by Gras, and a stationary result about the ℓ-class groups in the 2-dimensional Kummer tower $\{K_{n,m}\}$.

2010 Mathematics Subject Classification: 11R29, 11R11, 11R16, 11R18, 11R20.

Key words: Kummer tower, class group, ambiguous class number formula.

1. Introduction

In this paper we let ℓ and p be prime numbers. For n and m non-negative integers, let $K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^n}}, \zeta_{2\ell^m})$. Let $A_{n,m}$ and $h_{n,m}$ be the ℓ-part of the class group and the class number of $K_{n,m}$. The aim of this paper is to study the ℓ-class groups of $K_{n,m}$ when n and m vary.

First let us assume $\ell = 2$. In 1886, Weber ([**21**]) proved that the class number $h_{0,m}$ of $\mathbb{Q}(\zeta_{2^{m+1}})$ is odd for any $m \geq 0$. In fact, by inductively using a result of Iwasawa [**9**], one easily obtains that $2 \nmid h_{n,m}$ for any n, m in the case $p = 2$. For odd primes p, it is well known that the class number $h_{1,0}$ of $\mathbb{Q}(\sqrt{p})$ is odd by the genus theory of Gauss. By a more careful application of genus theory for quartic fields, Parry ([**19**]) showed that $A_{2,0}$ is cyclic and

(i) If $p \equiv 3, 5 \bmod 8$, then $2 \nmid h_{2,0}$.
(ii) If $p \equiv 7 \bmod 16$, then $2 \parallel h_{2,0}$.
(iii) If $p \equiv 15 \bmod 16$, then $2 \mid h_{2,0}$.
(iv) If $p \equiv 1 \bmod 8$, then $2 \mid h_{2,0}$. Moreover, if 2 is not a fourth power modulo p, then $2 \parallel h_{2,0}$.

For $p \equiv 9 \bmod 16$, Lemmermeyer showed that $2 \parallel h_{2,0}$; see [**17**]. For $p \equiv 15 \bmod 16$, one can show that $4 \mid h_{2,0}$; see [**14**].

Our first result of this paper is

Theorem 1.1. *Let p be a prime number, $K_{n,m} = \mathbb{Q}(p^{\frac{1}{2^n}}, \zeta_{2^{m+1}})$. Let $A_{n,m}$ be the 2-part of the class group and $h_{n,m}$ the class number of $K_{n,m}$.*

(1) *If $p \equiv 3 \bmod 8$, then $h_{n,m}$ is odd for $n, m \geq 0$.*
(2) *If $p \equiv 5 \bmod 8$, then $h_{n,0}$ and $h_{1,m}$ are odd for $n, m \geq 0$ and $2 \parallel h_{n,m}$ for $n \geq 2$ and $m \geq 1$.*
(3) *If $p \equiv 7 \bmod 16$, then $A_{n,0} \cong \mathbb{Z}/2\mathbb{Z}$, $A_{n,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $n \geq 2$, and $A_{1,m} \cong \mathbb{Z}/2^{m-1}\mathbb{Z}$ for $m \geq 1$.*

We give an interesting consequence on 2-adic properties of units. Let $p \equiv 3 \bmod 8$ and $\epsilon = a + b\sqrt{p}$ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Parry ([**19**]) and Zhang–Yue ([**22**]) showed that $a \equiv -1 \bmod p$ and $v_2(a) = 1$. Applying Theorem 1.1, we obtain the following analogue of their results.

Theorem 1.2. *Assume $p \equiv 7 \bmod 16$. Let ϵ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$.*

(1) *There exists a totally positive unit η of $\mathbb{Q}(\sqrt[4]{p})$ such that $\mathbf{N}(\eta) = \epsilon$ and the group of units $\mathcal{O}^\times_{\mathbb{Q}(\sqrt[4]{p})} = \langle \eta, \epsilon, -1 \rangle$.*
(2) *For any unit $\eta' \in \mathbf{N}^{-1}(\epsilon)$ in $\mathbb{Q}(\sqrt[4]{p})$, one has $v_{\mathfrak{l}}(\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{p})/\mathbb{Q}(\sqrt{p})}(\eta')) = 3$ and $\eta' \equiv -\operatorname{sgn}(\eta') \bmod \sqrt[4]{p}$, where $\mathfrak{l}$ is the unique prime of $\mathbb{Q}(\sqrt{p})$ above 2 and* sgn *is the signature function.*

Remark 1.3. (1) We may call the unit η the relative fundamental unit of $\mathbb{Q}(\sqrt[4]{p})$. The first part of this theorem is due to Parry; see [**19**, Theorem 3]. We include a proof here for completeness.
(2) For $\eta' \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt[4]{p})}$ such that $\mathbf{N}(\eta') = \epsilon$, we know η' is either totally positive or totally negative since ϵ is totally positive. Therefore the sign of η' is well defined.

Now assume ℓ is odd. Recall that ℓ is called regular if ℓ does not divide $h_{0,1}$, the class number of $\mathbb{Q}(\zeta_\ell)$. We have the following result:

Theorem 1.4. *Assume ℓ is an odd regular prime, and p is either ℓ or a prime generating the group $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Then $\ell \nmid h_{n,m}$, the class number of $K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^n}}, \zeta_{\ell^m})$ for any $n, m \geq 0$.*

Again the case $p = \ell$ can be deduced from [**9**]. For the particular case $\ell = 3$, the following results about the 3-class groups of $\mathbb{Q}(\sqrt[3]{p})$ and $\mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ were obtained by several authors:

(i) If $p = 3$ or $p \equiv 2 \bmod 3$, then $3 \nmid h_{1,1}$ and $3 \nmid h_{1,0}$ ([**8**]).
(ii) If $p \equiv 1 \bmod 3$, then $\operatorname{rank}_3 A_{1,0} = 1$ and $\operatorname{rank}_3 A_{1,1} = 1$ or 2 ([**4**]).

(iii) If $p \equiv 4, 7 \bmod 9$, then $A_{1,0} \cong \mathbb{Z}/3\mathbb{Z}$; moreover $A_{1,1} \cong \mathbb{Z}/3\mathbb{Z}$ if $\left(\frac{3}{p}\right)_3 \neq 1$ and $A_{1,1} \cong (\mathbb{Z}/3\mathbb{Z})^2$ if $\left(\frac{3}{p}\right)_3 = 1$. See [**16**].
(iv) If $p \equiv 1 \bmod 9$, then $\operatorname{rank}_3 A_{1,1} = 1$ if and only if $9 \mid h_{1,0}$ ([**1**], [**5**]).

We refer to [**5**] and [**16**] for more details. However, $h_{n,m}$ and $A_{n,m}$ for general n and m has rarely been studied in the literature as far as we know. We have the following result in this case:

Theorem 1.5. *Let p be a prime number. Let $A_{n,m}$ be the 3-part of the class group and $h_{n,m}$ the class number of $K_{n,m} = \mathbb{Q}(p^{\frac{1}{3^n}}, \zeta_{3^m})$.*

(1) *If $p = 3$ or $p \equiv 2, 5 \bmod 9$, then $3 \nmid h_{n,m}$ for $n, m \geq 0$.*
(2) *If $p \equiv 4, 7 \bmod 9$ and the cubic residue symbol $\left(\frac{3}{p}\right)_3 \neq 1$, then $A_{n,m} \cong \mathbb{Z}/3\mathbb{Z}$ for $n \geq 1$, $m \geq 0$.*

Remark 1.6. A. Lei ([**12**]) obtained the growth formula of class numbers in $\mathbb{Z}_\ell^{d-1} \rtimes \mathbb{Z}_\ell$-extensions for an odd prime ℓ. Under the conditions in Theorem 1.4 or 1.5, the Kummer tower $K_{\infty,\infty}/K_{0,1}$ satisfies the conditions in Lei's paper. Then by [**12**, Corollary 3.4], one has that for each m, there exist integers μ_m and λ_m such that

$$v_\ell(h_{n,m}) = \mu_m \ell^n + \lambda_m n + O(1) \text{ for } n \gg 0.$$

Theorems 1.4 and 1.5 thus imply that the invariants $\mu_m = \lambda_m = 0$ for all m.

To prove our results, we need to use Chevalley's ambiguous class number formula and its generalization by Gras. The most technical part of our paper is a stationary result of ℓ-class groups in a cyclic $\mathbb{Z}/\ell^2\mathbb{Z}$-extension under certain conditions, and its application to the study of ℓ-class groups in the 2-dimensional Kummer tower $\{K_{n,m}\}$. We emphasize that the stationary result could be used in other situations. Due to the computational nature of our results, we impose conditions to simplify computation. It would be of interest to study other cases, for example, replacing p by some positive integer with two or more prime factors.

The organization of this paper is as follows. In §2 we introduce notation and conventions for the paper, and present basic properties of Hilbert symbols and Gras' formula on genus theory. In §3 we prove our stationary result on ℓ-class groups in certain cyclic ℓ-extensions by using arguments from Iwasawa theory, and then prove a stationary result about the ℓ-class groups of $K_{n,m}$. We devote §4 to the proof of results for the easier case that ℓ is odd and §5 to the more complicated case $\ell = 2$.

2. Preliminary

2.1. Notations and conventions. The numbers ℓ and p are always prime numbers. The ℓ-Sylow subgroup of a finite abelian group M is denoted by $M(\ell)$. ζ_n is a primitive n-th root of unity and μ_n is the group of n-th roots of unity.

For a number field K, we denote by Cl_K, h_K, $\mathcal{O}_k$, E_K, and cl the class group, the class number, the ring of integers, the unit group of the ring of integers, and the ideal class map of K respectively. For w a place of K, K_w is the completion of K by w. For $\mathfrak{p}$ a prime of K, $v_\mathfrak{p}$ is the additive valuation associated with $\mathfrak{p}$.

For an extension K/F of number fields, v, a place of F, and w, a place of K above v, let $e_{w/v} = e(w/v, K/F)$ be the ramification index in K/F if v is finite and $e_{w/v} = [K_w : F_v]$ if v is infinite. We say that w/v is ramified if $e_{w/v} > 1$, and that w/v is totally ramified if $e_{w/v} = [K : F]$; in this case w is the only place above v and we can also say that v is totally ramified in K/F. Note that when v is infinite, w/v is ramified if and only if w is complex and v is real, and in this case $e_{w/v} = 2$. Hence an infinite place v is totally ramified if and only if K/F is quadratic, $F_v = \mathbb{R}$, and $K_w = \mathbb{C}$. When K/F is Galois, then $e_{w/v}$ is independent of w and we denote it by e_v.

Denote by $\mathbf{N}_{K/F}$ the norm map from K to F, and the induced norm map from Cl_K to Cl_F. If the extension is clear, we use $\mathbf{N}$ instead of $\mathbf{N}_{K/F}$.

When $K = K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^m}}, \zeta_{2^{m+1}})$, we write $\mathrm{Cl}_{n,m} = \mathrm{Cl}_K$, $h_{n,m} = h_K$, $\mathcal{O}_{n,m} = \mathcal{O}_K$, and $E_{n,m} = E_K$ for simplicity. The group $A_{n,m}$ is the ℓ-Sylow subgroup of $\mathrm{Cl}_{n,m}$.

2.2. Hilbert symbol. Let $n \geq 2$ be an integer. Let k be a finite extension of $\mathbb{Q}_p$ containing μ_n. Let ϕ_k be the local reciprocity map $\phi_k \colon k^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$. Given $a, b \in k^\times$, the n-th Hilbert symbol is defined by

$$\left(\frac{a,b}{k}\right)_n = \frac{\phi_k(a)(\sqrt[n]{b})}{\sqrt[n]{b}} \in \mu_n \subset k.$$

The following results about the Hilbert symbol can be found in standard textbooks on number theory, for example [**18**, Chapters IV and V].

Proposition 2.1. *Let $a, b \in k^\times$.*

(1) $\left(\frac{a,b}{k}\right)_n = 1 \Leftrightarrow a$ *is a norm from the extension* $k(\sqrt[n]{b})/k$.

(2) $\left(\frac{aa',b}{k}\right)_n = \left(\frac{a,b}{k}\right)_n \left(\frac{a',b}{k}\right)_n$ *and* $\left(\frac{a,bb'}{k}\right)_n = \left(\frac{a,b}{k}\right)_n \left(\frac{a,b'}{k}\right)_n$.

(3) $\left(\frac{a,b}{k}\right)_n = \left(\frac{b,a}{k}\right)_n^{-1}$.

(4) $\left(\frac{a,1-a}{k}\right)_n = 1$ *and* $\left(\frac{a,-a}{k}\right)_n = 1$.

(5) *Let* ϖ *be a uniformizer of* k. *Let* $q = |\mathcal{O}_k/(\varpi)|$ *be the cardinality of the residue field of* k. *If* $p \nmid n$, *then* $\left(\frac{\varpi,u}{k}\right)_n = \omega(u)^{\frac{q-1}{n}}$, *where* $\omega\colon \mathcal{O}_k^\times \to \zeta_{q-1}$ *is the unique map such that* $u \equiv \omega(u) \bmod \varpi$ *for* $u \in \mathcal{O}_k^\times$.

(6) *Let* M/k *be a finite extension. For* $a \in M^\times$, $b \in k^\times$, *one has the following norm-compatible property:*

$$\left(\frac{a,b}{M}\right)_n = \left(\frac{\mathbf{N}_{M/k}(a),b}{k}\right)_n.$$

When $k = \mathbb{R}$, $\mu_n \subset \mathbb{R}$ if and only if $n = 1$ or 2. For $a, b \in k^\times$ define

$$\left(\frac{a,b}{k}\right)_2 = \begin{cases} -1 & \text{if } a < 0 \text{ and } b < 0; \\ 1 & \text{otherwise.} \end{cases}$$

When $k = \mathbb{C}$, define $\left(\frac{a,b}{k}\right)_n = 1$ for any $a, b \in k^\times$.

The following is the product formula of Hilbert symbols; see [**18**, Chapter VI, Theorem 8.1].

Proposition 2.2. *Let* K *be a number field containing* μ_n. *For any place* v *of* K, *set* $\left(\frac{a,b}{v}\right)_n := \iota_v^{-1}\left(\left(\frac{\iota_v(a),\iota_v(b)}{K_v}\right)_n\right)$, *where* ι_v *is the canonical embedding* $K \to K_v$. *Then for* $a, b \in K^\times$, *one has*

$$\prod_v \left(\frac{a,b}{v}\right)_n = 1,$$

where v *runs over all places of* K.

Hilbert symbols are invariant under Galois actions as follows. Let K be a number field containing μ_n. Let v be a prime ideal of K. Suppose $\sigma \in \mathrm{Hom}(K, K)$. Then $\sigma(v)$ is also a prime ideal of K. Note that $\iota_v \circ \sigma^{-1}$ is an embedding from K to the completion of K at $\sigma(v)$. We shall often say that this embedding is the corresponding embedding induced by the prime ideal $\sigma(v)$. By definition, we have

$$\sigma\left(\left(\frac{a,b}{v}\right)_n\right) = \left(\frac{\sigma(a),\sigma(b)}{\sigma(v)}\right)_n. \tag{2.1}$$

2.3. Three useful lemmas.

Lemma 2.3. *Suppose* K/F *is a cyclic* ℓ*-extension with Galois group* G *and* C *is a* G*-submodule of* Cl_K. *Then* $\ell \nmid |(\mathrm{Cl}_K/C)^G|$ *implies that* $\mathrm{Cl}_K(\ell) = C(\ell)$. *In particular,* $\ell \nmid |\mathrm{Cl}_K^G|$ *implies that* $\ell \nmid h_K$.

Proof: Consider the action of G on $(\mathrm{Cl}_K/C)(\ell)$. The cardinality of the orbit of $c \in (\mathrm{Cl}_K/C)(\ell) \backslash (\mathrm{Cl}_K/C)(\ell)^G$ is a multiple of ℓ. Thus $|(\mathrm{Cl}_K/C)(\ell)| \equiv |(\mathrm{Cl}_K/C)(\ell)^G| \bmod \ell$. Hence $\ell \nmid |(\mathrm{Cl}_K/C)^G|$ implies $(\mathrm{Cl}_K/C)(\ell) = 0$ and then $\mathrm{Cl}_K(\ell) = C(\ell)$ by the exact sequence $0 \to C(\ell) \to \mathrm{Cl}_K(\ell) \to (\mathrm{Cl}_K/C)(\ell)$. □

Lemma 2.4. *Let K_n/K_0 be a cyclic extension of number fields of degree ℓ^n. Let K_i be the unique intermediate field such that $[K_i : K_0] = \ell^i$ for $0 \le i \le n$. If a prime ideal $\mathfrak{p}$ of K_0 is ramified in K_1/K_0, then $\mathfrak{p}$ is totally ramified in K_n/K_0.*

Proof: Let $I_\mathfrak{p}$ be the inertia group of $\mathfrak{p}$. Then $K_n^{I_\mathfrak{p}} = K_i$ for some i and $K_n^{I_\mathfrak{p}}/K$ is unramified at $\mathfrak{p}$. Since K_1/K_0 is ramified at $\mathfrak{p}$, we must have $K_n^{I_\mathfrak{p}} = K_0$. In other words, $\mathfrak{p}$ is totally ramified. □

Lemma 2.5. *Suppose the number field extension M/K contains no unramified abelian subextension other than K. Then the norm map $\mathrm{Cl}_M \to \mathrm{Cl}_K$ is surjective. In particular, $h_K \mid h_M$.*

Proof: This is [**20**, Theorem 10.1]. □

2.4. Gras' formula on class groups in cyclic extensions.

Theorem 2.6 (Gras)**.** *Let K/F be a cyclic extension of number fields with Galois group G. Let C be a G-submodule of Cl_K. Let D be a subgroup of fractional ideals of K such that $\mathrm{cl}(D) = C$. Denote by $\Lambda_D = \{x \in F^\times \mid (x)\mathcal{O}_F \in \mathbf{N}D\}$. Then*

$$|(\mathrm{Cl}_K/C)^G| = \frac{|\mathrm{Cl}_F|}{|\mathbf{N}C|} \cdot \frac{\prod_v e_v}{[K:F]} \cdot \frac{1}{[\Lambda_D : \Lambda_D \cap \mathbf{N}K^\times]}, \tag{2.2}$$

where the product runs over all places of F.

Proof: See [**6**, Section 3]. Alternatively, an adelic proof is given by the first named author and Yu in [**15**]. □

Remark 2.7. (1) The index $[\Lambda_D : \Lambda_D \cap \mathbf{N}K^\times]$ is independent of the choice of D.

(2) Take $C = \{1\}$ and $D = \{1\}$, then Λ_D is the unit group E_F, and Gras' formula is nothing but the ambiguous class number formula of Chevalley:

$$|\mathrm{Cl}_K^G| = |\mathrm{Cl}_F| \cdot \frac{\prod_v e_v}{[K:F]} \cdot \frac{1}{[E_F : E_F \cap \mathbf{N}K^\times]}. \tag{2.3}$$

In fact, the proof of Gras' formula is based on Chevalley's formula, whose proof can be found in [**11**, Chapter 13, Lemma 4.1].

One can use Hilbert symbols to compute the index $[\Lambda_D : \Lambda_D \cap \mathbf{N}K^\times]$.

Lemma 2.8. *Let F be a number field and $\mu_d \subset F$. Assume $K = F(\sqrt[d]{a})$ is a Kummer extension of F of degree d. Let D be any subgroup of the group of fractional ideals of K and $\Lambda_D = \{x \in F^\times \mid (x)\mathcal{O}_F \in \mathbf{N}D\}$. Define*

$$\rho = \rho_{D,K/F} \colon \Lambda_D \longrightarrow \prod_v \mu_d, \quad x \longmapsto \left(\left(\frac{x,a}{v} \right)_d \right)_v,$$

where v passes through all places of F ramified in K/F. Then

(1) $\mathrm{Ker}(\rho) = \Lambda_D \cap \mathbf{N}K^\times$. *In particular,* $[\Lambda_D : \Lambda_D \cap \mathbf{N}K^\times] = |\rho(\Lambda_D)|$.
(2) *Let Π be the product map $\prod_v \mu_d \to \mu_d$, then $\Pi \circ \rho = 1$ and hence* $\rho(\Lambda_D) \subset \ker \Pi := (\prod_v \mu_d)^{\Pi=1}$.
(3) $\mathrm{Ker}(\rho)$ *and* $|\rho(\Lambda_D)|$ *are independent of the choice of a.*

Proof: Let I_K be the group of fraction ideals of K. Note that if $D \subset I_K$, then $\Lambda_D \subset \Lambda := \Lambda_{I_K}$. Therefore it suffices to prove the results in the case $D = I_K$.

(1) For v, a place of F, let w be a place of K above v. Recall that $\left(\frac{x,a}{v}\right)_d = 1$ if and only if $x \in \mathbf{N}_{K_w/F_v}(K_w^\times)$. We claim that if v is unramified, then $x \in \mathbf{N}_{K_w/F_v}(K_w^\times)$ for $x \in \Lambda$. Suppose v is an infinite unramified place. Then $F_v = K_w$ and clearly $x \in \mathbf{N}_{K_w/F_v}(K_w^\times)$. Suppose v is a finite unramified place. Since $x \in \Lambda$, we have $(x)\mathcal{O}_F = \mathbf{N}(I)$. Then locally $(x)\mathcal{O}_{F_v} = \mathbf{N}_{K_w/F_v}(J)$ for some fractional ideal J of $\mathcal{O}_{K_w}$. Since $\mathcal{O}_{K_w}$ is a principal ideal domain, $J = (\alpha)$ for some $\alpha \in K_w^\times$. Hence $x = u\mathbf{N}_{K_w/F_v}(\alpha)$ with $u \in \mathcal{O}_{F_v}^\times$. Since v is unramified, we have $u \in \mathbf{N}_{K_w/F_v}(K_w^\times)$ by local class field theory. Therefore $x \in \mathbf{N}_{K_w/F_v}(K_w^\times)$.

Now for $x \in \mathrm{Ker}(\rho)$, we have $x \in \mathbf{N}_{K_w/F_v}(K_w^\times)$ for every place v of F. Hasse's norm theorem ([**18**, Chapter VI, Corollary 4.5]) gives $x \in \mathbf{N}K^\times$. So $\mathrm{Ker}(\rho) \subset \Lambda \cap \mathbf{N}K^\times$. The other direction is clear. This proves (1).

(2) We have proved that if v is unramified, then $\left(\frac{x,a}{v}\right)_d = 1$ for $x \in \Lambda$. Therefore (2) follows from the product formula of Hilbert symbols.

(3) is a consequence of (1). □

3. Stability of ℓ-class groups

We now give a stationary result about ℓ-class groups in a finite cyclic ℓ-extension. We first introduce the ramification hypothesis RamHyp. Let

F be a number field and K an algebraic extension (possibly infinite) of F. Then K/F satisfies the ramification hypothesis RamHyp if

> Every place of K ramified in K/F is totally ramified in K/F and there is at least one prime ramified in K/F.

Lemma 3.1. *Let G be a finite ℓ-cyclic group with generator σ. Then $\mathbb{Z}_\ell[G]$ is a local ring with maximal ideal $(\ell, \sigma - 1)$.*

Proof: Note that $\mathbb{Z}_\ell[G] \cong \mathbb{Z}_\ell[T]/(T^{\ell^n} - 1)$ by sending σ to T, where ℓ^n is the order of G. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{Z}_\ell[T]/(T^{\ell^n} - 1)$. Then $\mathfrak{m} \cap \mathbb{Z}_\ell$ is a prime ideal of $\mathbb{Z}_\ell$. We claim that $\mathfrak{m} \cap \mathbb{Z}_\ell = \ell\mathbb{Z}_\ell$.

Otherwise $\mathfrak{m} \cap \mathbb{Z}_\ell = 0$, namely $\mathfrak{m}$ is disjoint with the multiplicative subset $\mathbb{Z}_\ell \setminus \{0\}$. Then $\mathfrak{m}$ corresponds to a prime ideal of the ring $\mathbb{Q}_\ell[T]/(T^{\ell^n} - 1)$. Each prime ideal of $\mathbb{Q}_\ell[T]/(T^{\ell^n} - 1)$ is generated by a monic irreducible polynomial $f(T)$ with $f(T) \mid T^{\ell^n} - 1$. By Gauss' lemma, $f(T)$ has $\mathbb{Z}_\ell$-coefficients. Then $\mathfrak{m} = (f(T))$. But $\mathbb{Z}_\ell[T]/(f(T))$ is not a field since $\mathbb{Z}_\ell[T]/(f(T))$ is integral over $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell$ is not a field. So $\mathfrak{m} \cap \mathbb{Z}_\ell = \ell\mathbb{Z}_\ell$.

Then $\mathfrak{m}$ corresponds to a maximal ideal of $\mathbb{F}_\ell[T]/(T^{\ell^n}-1) = \mathbb{F}_\ell[T]/(T-1)^{\ell^n}$. The latter is obviously a local ring with maximal ideal $(T-1)$. Hence $\mathfrak{m} = (\ell, T-1)$. Therefore the maximal ideal of $\mathbb{Z}_\ell[G]$ is $(\ell, \sigma - 1)$. □

Proposition 3.2. *Let K_2/K_0 be a cyclic extension of number fields of degree ℓ^2 satisfying RamHyp. Let K_1 be the unique non-trivial intermediate field of K_2/K_0. Then for any $n \geq 1$,*

$$|\mathrm{Cl}_{K_0}/\ell^n \mathrm{Cl}_{K_0}| = |\mathrm{Cl}_{K_1}/\ell^n \mathrm{Cl}_{K_1}|$$

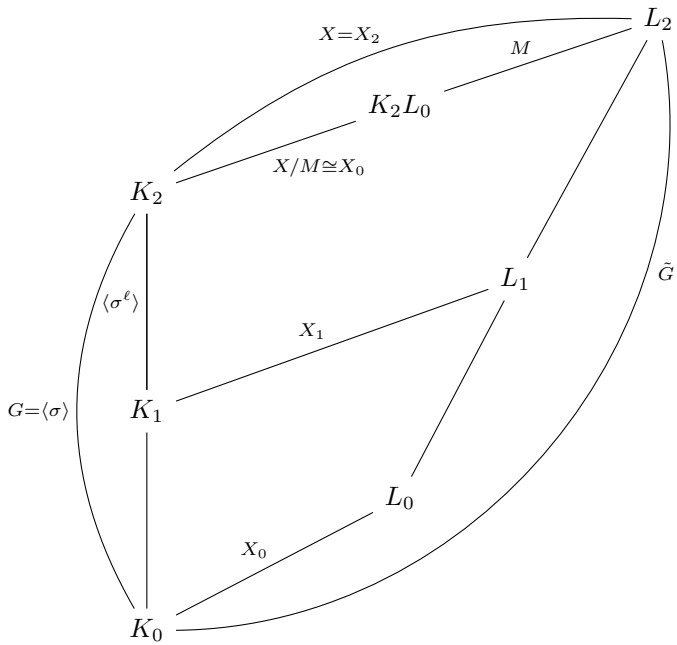
implies that

$$\mathrm{Cl}_{K_2}/\ell^n \mathrm{Cl}_{K_2} \cong \mathrm{Cl}_{K_1}/\ell^n \mathrm{Cl}_{K_1} \cong \mathrm{Cl}_{K_0}/\ell^n \mathrm{Cl}_{K_0}.$$

In particular, $|\mathrm{Cl}_{K_0}(\ell)| = |\mathrm{Cl}_{K_1}(\ell)|$ implies that $\mathrm{Cl}_{K_0}(\ell) \cong \mathrm{Cl}_{K_1}(\ell) \cong \mathrm{Cl}_{K_2}(\ell)$.

Proof: Denote by $G = \mathrm{Gal}(K_2/K_0) = \langle\sigma\rangle$. Let L_i be the maximal unramified abelian ℓ-extension of K_i and $X_i = \mathrm{Gal}(L_i/K_i)$. By class field theory $X_i \cong \mathrm{Cl}_{K_i}(\ell)$. By the maximal property, L_2/K_0 is a Galois extension. Let $\widetilde{G} := \mathrm{Gal}(L_2/K_0)$. The Galois group G acts on $X := X_2$ via $x^\sigma = \widetilde{\sigma} x \widetilde{\sigma}^{-1}$, where $\widetilde{\sigma} \in \widetilde{G}$ is any lifting of σ. By this action X becomes a module over the local ring $\mathbb{Z}_\ell[G]$. Since $K_0 \subset K_1 \subset K_2$ satisfies RamHyp, we have $L_0 \cap K_2 = K_0$. Then $X/M = \mathrm{Gal}(K_2L_0/K_2) \cong X_0$,

where $M = \mathrm{Gal}(L_2/K_2L_0)$. Note that K_2L_0/K_0 is Galois, so M and X/M are also $\mathbb{Z}_\ell[G]$-modules.



We have the following claim:

Claim. $X/\omega M \cong X_1$, where $\omega = 1 + \sigma + \cdots + \sigma^{\ell-1} \in \mathbb{Z}_\ell[G]$.

Now for any $n \geq 1$, by the claim,

$$X_0/\ell^n X_0 \cong \frac{X}{M + \ell^n X} \text{ and } X_1/\ell^n X_1 \cong \frac{X}{\omega M + \ell^n X}.$$

By the assumptions, $M + \ell^n X = \omega M + \ell^n X$. Since ω lies in the maximal ideal of $\mathbb{Z}_\ell[G]$, we have $M \subset \ell^n X$ by Nakayama's lemma. Hence we have isomorphisms which are induced by the restrictions

$$X/\ell^n X \cong X_1/\ell^n X_1 \cong X_0/\ell^n X_0.$$

By class field theory we have isomorphisms which are induced by the norm maps

$$\mathrm{Cl}_{K_2}/\ell^n \mathrm{Cl}_{K_2} \cong \mathrm{Cl}_{K_1}/\ell^n \mathrm{Cl}_{K_1} \cong \mathrm{Cl}_{K_0}/\ell^n \mathrm{Cl}_{K_0}.$$

Let $n \to +\infty$; we get $\mathrm{Cl}_{K_2}(\ell) \cong \mathrm{Cl}_{K_1}(\ell) \cong \mathrm{Cl}_{K_0}(\ell)$.

Let us prove the claim. Note that $G = \widetilde{G}/X$. Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ be the set of places of K_0 ramified in K_2/K_0. Note that $\mathfrak{p}_i$ is not an infinite place by RamHyp. For each $\mathfrak{p}_i$, choose a prime ideal $\widetilde{\mathfrak{p}}_i$ of L_2 above $\mathfrak{p}_i$. Let $I_i \subset \widetilde{G}$ be the inertia subgroup of $\widetilde{\mathfrak{p}}_i$. The map $I_i \hookrightarrow \widetilde{G} \twoheadrightarrow G$ induces an isomorphism $I_i \cong G$, since L_2/K_2 is unramified and K_2/K_0 is totally ramified. Let $\sigma_i \in I_i$ such that $\sigma_i \equiv \tilde{\sigma} \bmod X$. Then $I_i = \langle \sigma_i \rangle$. Let $a_i = \sigma_i \sigma_1^{-1} \in X$. Then $\langle I_1, \dots, I_t \rangle = \langle \sigma_1, a_2, \dots, a_t \rangle$. Since L_0 is the maximal unramified abelian ℓ-extension of K_0, we have

$$\mathrm{Gal}(L_2/L_0) = \langle \widetilde{G}', I_1, \dots, I_t \rangle = \langle \widetilde{G}', \sigma_1, a_2, \dots, a_t \rangle,$$

where $\widetilde{G}'$ is the commutator subgroup of $\widetilde{G}$. In fact, $\widetilde{G}' = (\sigma - 1)X$. The inclusion $(\sigma - 1)X \subset \widetilde{G}'$ is clear. Furthermore, it is easy to check that $(\sigma - 1)X$ is normal in $\widetilde{G}$ and $X/(\sigma - 1)X$ is in the center of $\widetilde{G}/(\sigma - 1)X$. Since $\widetilde{G}/X \cong G$ is cyclic, from the exact sequence

$$1 \longrightarrow X/(\sigma - 1)X \longrightarrow \widetilde{G}/(\sigma - 1)X \longrightarrow G \longrightarrow 1,$$

we obtain that $\widetilde{G}/(\sigma - 1)X$ is abelian. Thus we have

$$\mathrm{Gal}(L_2/L_0) = \langle (\sigma - 1)X, \sigma_1, a_2, \dots, a_t \rangle.$$

Since $a_i \in X$ and $X \cap I_1 = \{1\}$, we have

$$X \cap \mathrm{Gal}(L_2/L_0) = \langle (\sigma - 1)X, a_2, \dots, a_t \rangle.$$

Thus the map $X \hookrightarrow \widetilde{G}$ induces the following isomorphism:

$$X/\langle (\sigma - 1)X, a_2, \dots, a_t \rangle \cong \widetilde{G}/\mathrm{Gal}(L_2/L_0) = X_0.$$

Therefore $\langle (\sigma - 1)X, a_2, \dots, a_t \rangle = M$. By repeating the above argument to L_2/K_1, we obtain

$$X/\langle (\sigma^\ell - 1)X, b_2, \dots, b_t \rangle \cong X_1,$$

where $b_i = \sigma_i^\ell \sigma_1^{-\ell}$ for each i. Obviously, $(\sigma^\ell - 1)X = \omega(\sigma - 1)X$. Recall that σ_i is a lifting of σ, so by definition $x^\sigma = \sigma_i x \sigma_i^{-1}$ for $x \in X$. We have

$$\begin{aligned} b_i &= \sigma_i^\ell \sigma_1^{-\ell} = \sigma_i^{\ell-1} a_i \sigma_1^{-(\ell-1)} = \sigma_i^{\ell-2} a_i \sigma_1 a_i \sigma_1^{-1} \sigma_1^{-(\ell-2)} \\ &= \sigma_i^{\ell-2} a_i^{1+\sigma} \sigma_1^{-(\ell-2)} = \cdots = a_i^{1+\sigma+\cdots+\sigma^{\ell-1}} = \omega a_i. \end{aligned}$$

So $\langle (\sigma^\ell - 1)X, b_2, \dots, b_t \rangle = \omega M$ and then $X_1 = X/\omega M$. This finishes the proof of the claim. □

Remark 3.3. (1) Let K_∞/K be a $\mathbb{Z}_\ell$-extension and K_n its n-th layer. It is well known that there exists n_0 such that K_∞/K_{n_0} satisfies RamHyp. Then Proposition 3.2 recovers the following result of Fukuda [**3**]: If $|\mathrm{Cl}_{K_m}(\ell)| = |\mathrm{Cl}_{K_{m+1}}(\ell)|$ (resp. $|\mathrm{Cl}_{K_m}/\ell\mathrm{Cl}_{K_m}| =$

$|\mathrm{Cl}_{K_{m+1}}/\ell\mathrm{Cl}_{K_{m+1}}|$) for some $m \geq n_0$, then $|\mathrm{Cl}_{K_m}(\ell)| = |\mathrm{Cl}_{K_{m+i}}(\ell)|$ (resp. $|\mathrm{Cl}_{K_m}/\ell\mathrm{Cl}_{K_m}| = |\mathrm{Cl}_{K_{m+i}}/\ell\mathrm{Cl}_{K_{m+i}}|$) for any $i \geq 1$. In fact, our proof is essentially the same as the proof of the corresponding results for $\mathbb{Z}_\ell$-extensions; see [**20**, Lemmas 13.14 and 13.15] and [**3**].

(2) Let K be a number field containing μ_{ℓ^2}. Let $a \in K^\times \backslash K^{\times\ell}$ and $K_n = K(\sqrt[\ell^n]{a})$. Then $\mathrm{Gal}(K_{m+2}/K_m) \cong \mathbb{Z}/\ell^2\mathbb{Z}$ for any integer $m \geq 0$. One can show that there exists some n_0 such that K_∞/K_{n_0} satisfies RamHyp. If $|\mathrm{Cl}_{K_m}(\ell)| = |\mathrm{Cl}_{K_{m+1}}(\ell)|$ for some $m \geq n_0$, then by repeatedly applying Proposition 3.2, one obtains $|\mathrm{Cl}_{K_{m+i}}(\ell)| = |\mathrm{Cl}_{K_m}(\ell)|$ for any $i \geq 0$.

Now let ℓ and p be prime numbers and $K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^n}}, \zeta_{2\ell^m})$. The following result is a consequence of Proposition 3.2. Since we know that $2 \nmid h_{n,m}$ if $(\ell, p) = (2, 2)$, we assume for simplicity that $(\ell, p) \neq (2, 2)$ in the following proposition.

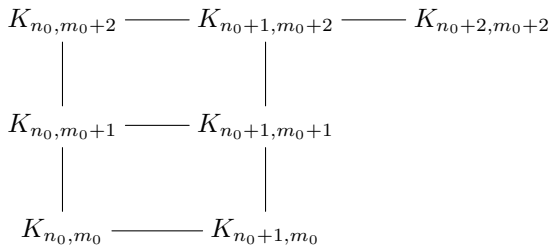
Proposition 3.4. *Suppose $(\ell, p) \neq (2, 2)$. Assume that all the primes above ℓ in K_{n_0,m_0} are totally ramified in K_{n_0+1,m_0+1} for some integers $n_0 \geq 0$ and $m_0 \geq 1$. Then*

(1) *All primes above ℓ in K_{n_0,m_0} are totally ramified in $K_{n,m}/K_{n_0,m_0}$ for all $(n, m) \geq (n_0, m_0)$.*
(2) *If $|A_{n_0,m_0}| = |A_{n_0+1,m_0+1}|$, then $A_{n,m} \cong A_{n_0,m_0}$ for all $(n, m) \geq (n_0, m_0)$.*
(3) *If $\ell \nmid h_{n_0+1,m_0+1}$, then $\ell \nmid h_{n,m}$ for all $(n, m) \geq (n_0, m_0)$.*

Proof: By the assumption for n_0 and m_0, one has $[K_{n_0+1,m_0+1} : K_{n_0,m_0}] = \ell^2$ and

$$\begin{aligned}\mathrm{Gal}(K_{n_0,m_0+2}/K_{n_0,m_0}) &\cong \mathrm{Gal}(K_{n_0+1,m_0+2}/K_{n_0+1,m_0}) \\ &\cong \mathrm{Gal}(K_{n_0+2,m_0+2}/K_{n_0,m_0+2}) \cong \mathbb{Z}/\ell^2\mathbb{Z}.\end{aligned}$$

Consider the following diagram.



For (1), let $\mathfrak{l}$ be a prime of K_{n_0,m_0} above ℓ. Apply Lemma 2.4 to the two vertical lines in the diagram; we obtain that $\mathfrak{l}$ is totally ramified

in $K_{n_0+1,m_0+2}/K_{n_0,m_0}$. Apply Lemma 2.4 to the top horizontal line in the diagram; we get that $\mathfrak{l}$ is totally ramified in $K_{n_0+2,m_0+2}/K_{n_0+2,m_0}$. Hence $\mathfrak{l}$ is totally ramified in $K_{n_0+2,m_0+2}/K_{n_0,m_0}$. Repeatedly using the above argument, we obtain that $\mathfrak{l}$ is totally ramified in $K_{n,m}/K_{n_0,m_0}$ for all $n \geq n_0$ and $m \geq m_0$.

For (2), by Lemma 2.5, $|A_{n_0,m_0}| = |A_{n_0+1,m_0+1}|$ implies that

$$A_{n_0+1,m_0+1} \cong A_{n_0+1,m_0} \cong A_{n_0,m_0+1} \cong A_{n_0,m_0}.$$

If $p = \ell$, the two vertical lines and the top horizontal line in the diagram satisfy RamHyp by (1). If $p \neq \ell$, let $\mathfrak{p}$ be a prime of $K_{0,m}$ above p. For any $n \geq 1$, note that $x^{\ell^n} - p$ is a $\mathfrak{p}$-Eisenstein polynomial in $K_{0,m}[x]$. Therefore $K_{n,m}/K_{0,m}$ is totally ramified at $\mathfrak{p}$ for each n, m. In particular the horizontal line is totally ramified at $\mathfrak{p}$. Since $K_{\infty,\infty}/K_{n_0,m_0}$ is unramified outside ℓ and p, the two horizontal lines and the rightmost vertical line in the diagram all satisfy RamHyp by (1).

Since $K_{n_0,m_0+2}/K_{n_0,m_0}$ is a cyclic extension of degree ℓ^2, applying Proposition 3.2 to this extension, we get

$$A_{n_0,m_0+2} \cong A_{n_0,m_0+1} \cong A_{n_0,m_0}.$$

Similarly, applying Proposition 3.2 to $K_{n_0+1,m_0+2}/K_{n_0+1,m_0}$, we obtain

$$A_{n_0+1,m_0+2} \cong A_{n_0+1,m_0+1} \cong A_{n_0+1,m_0}.$$

Therefore $A_{n_0+2,m_0+1} \cong A_{n_0+2,m_0}$. Note that $K_{n_0+2,m_0+2}/K_{n_0,m_0+2}$ is also a cyclic extension of degree ℓ^2. Applying Proposition 3.2 to this extension, we obtain

$$A_{n_0+2,m_0+2} \cong A_{n_0+1,m_0+2} \cong A_{n_0,m_0+2}.$$

Thus $A_{n_0+2,m_0+2} \cong A_{n_0+1,m_0+1}$. Using the above argument inductively, we have $A_{n_0+k,m_0+k} \cong A_{n_0,m_0}$ for any $k \geq 1$. Finally we have $A_{n,m} \cong A_{n_0,m_0}$ by Lemma 2.5.

For (3), $\ell \nmid h_{n_0+1,m_0+1}$ implies that $\ell \nmid h_{n_0,m_0}$ by Lemma 2.5. Then the result follows from (2). □

4. The case in which ℓ is odd

Lemma 4.1. *Assume that $p = \ell$ or $p^{\ell-1} \not\equiv 1 \bmod \ell^2$. Then ℓ is totally ramified in $K_{n,m}$ for any $(n, m) > (0, 0)$.*

Proof: For $n \geq 1$, $(x + p)^{\ell^n} - p$ is an Eisenstein polynomial in $\mathbb{Q}_\ell[x]$ by the assumptions on p and ℓ, hence is irreducible in $\mathbb{Q}_\ell[x]$. This implies that the extension $\mathbb{Q}_\ell(p^{\frac{1}{\ell^n}})/\mathbb{Q}_\ell$ is totally ramified of degree ℓ^n and

$\mu_\ell \not\subset \mathbb{Q}_\ell(p^{\frac{1}{\ell^n}})$. As a result, $\mathbb{Q}_\ell(p^{\frac{1}{\ell^n}})/\mathbb{Q}_\ell(p^{\frac{1}{\ell^{n-1}}})$ is non-Galois of degree ℓ, and one has that $\mathbb{Q}_\ell(p^{\frac{1}{\ell^n}}, \zeta_{\ell^m})/\mathbb{Q}_\ell(p^{\frac{1}{\ell^{n-1}}}, \zeta_{\ell^m})$ is also of degree ℓ. By induction,

$$[\mathbb{Q}_\ell(p^{\frac{1}{\ell^n}}, \zeta_{\ell^m}) : \mathbb{Q}_\ell] = \ell \cdot [\mathbb{Q}_\ell(p^{\frac{1}{\ell^{n-1}}}, \zeta_{\ell^m}) : \mathbb{Q}_\ell] = \ell^n(\ell^m - \ell^{m-1}).$$

Then the extension $\mathbb{Q}_\ell(p^{\frac{1}{\ell^n}}, \zeta_{\ell^n})/\mathbb{Q}_\ell(\zeta_{\ell^n})$ is cyclic of degree ℓ^n, with the only subextensions of the form $\mathbb{Q}_\ell(p^{\frac{1}{\ell^k}}, \zeta_{\ell^n})$ for $0 \le k \le n$. If $\mathbb{Q}_\ell^{\mathrm{ab}} \cap \mathbb{Q}_\ell(p^{\frac{1}{\ell^n}}, \zeta_{\ell^n}) \supsetneq \mathbb{Q}_\ell(\zeta_{\ell^n})$, then there exists $k > 0$ such that $p^{\frac{1}{\ell^k}} \in \mathbb{Q}_\ell^{\mathrm{ab}}$ and hence $p^{\frac{1}{\ell}} \in \mathbb{Q}_\ell^{\mathrm{ab}}$, impossible. Hence $\mathbb{Q}_\ell^{\mathrm{ab}} \cap \mathbb{Q}_\ell(p^{\frac{1}{\ell^n}}, \zeta_{\ell^n}) = \mathbb{Q}_\ell(\zeta_{\ell^n})$. Thus ℓ is totally ramified in $K_{n,n}$ for any $n \ge 1$, and therefore totally ramified in $K_{n,m}$ for all $(n, m) > (0, 0)$. □

Proof of Theorem 1.4: By Proposition 3.4 and Lemma 4.1, if $\ell \nmid h_{1,2}$, then $\ell \nmid h_{n,m}$ for any $(n, m) \ge (1, 2)$ and then $\ell \nmid h_{n,m}$ for any $(n, m) \ge (0, 0)$ by Lemma 2.5. We prove $\ell \nmid h_{1,2}$ by applying Chevalley's formula (2.3) to $K_{1,2}/K_{0,2}$. We deal with the case $p \ne \ell$ and leave the case $p = \ell$ to the readers.

Since p is inert in $K_{0,2}$, the ramified primes in $K_{1,2}/K_{0,2}$ are $p\mathcal{O}_{0,2}$ and $(1-\zeta_{\ell^2})\mathcal{O}_{0,2}$. As ℓ is regular, one has that ℓ does not divide the class number $K_{0,m}$ for any $m \ge 1$; see [**20**, Corollary 10.5]. We now calculate the unit index in Chevalley's formula. Recall the following map as in Lemma 2.8 (let $D = \{1\}$ so that $\Lambda_D = E_{0,2}$):

$$\begin{aligned} \rho\colon E_{0,2} &\longrightarrow \mu_\ell \times \mu_\ell \\ x &\longmapsto \left(\left(\frac{x, p}{p\mathcal{O}_{0,2}} \right)_\ell, \left(\frac{x, p}{(1-\zeta_{\ell^2})} \right)_\ell \right). \end{aligned}$$

We have the index $[E_{0,2} : E_{0,2} \cap \mathbf{N}K_{0,2}^\times] = |\rho(E_{0,2})| \le \ell$ by product formula. Since p is a primitive root modulo ℓ^2, we have $\ell^2 \nmid p^{\ell-1} - 1$. Then by Proposition 2.1(6) and (5), we have

$$\left(\frac{\zeta_{\ell^2}, p}{p\mathcal{O}_{0,2}} \right)_\ell = \left(\frac{\zeta_\ell, p}{p\mathcal{O}_{0,1}} \right)_\ell = \zeta_\ell^{-\frac{p^{\ell-1}-1}{\ell}} \ne 1.$$

Thus $|\rho(E_{0,2})| = \ell$ and Chevalley's formula gives $\ell \nmid |\operatorname{Cl}_{1,2}^G|$, where $G = \operatorname{Gal}(K_{1,2}/K_{0,2})$. Therefore $\ell \nmid h_{1,2}$ by Lemma 2.3. □

Proof of Theorem 1.5: (1) is a special case of Theorem 1.4.

For (2), by Lemma 4.1, we obtain that 3 is totally ramified in $K_{n,n}/\mathbb{Q}$ for any $n \geq 1$. To prove (2), we first show that $A_{2,2} \cong A_{1,1} \cong \mathbb{Z}/3\mathbb{Z}$. We apply Gras' formula (2.2) in the case

$$K_{2,2}/K_{0,2}, \quad C = \langle \mathrm{cl}(\mathfrak{l}_{2,2}) \rangle, \quad D = \langle \mathfrak{l}_{2,2} \rangle,$$

where $\mathfrak{l}_{2,2}$ is the unique prime ideal of $K_{2,2}$ above 3. In this case

$$\Lambda_D = \langle \pm\zeta_9, 1-\zeta_9, 1-\zeta_9^2, 1-\zeta_9^4 \rangle.$$

Since $p \equiv 4, 7 \bmod 9$, we have $p\mathcal{O}_{0,2} = \mathfrak{p}_1\mathfrak{p}_2$. The ramified primes of $K_{0,2}$ in $K_{2,2}$ are $\mathfrak{l}_{0,2}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$. For the map

$$\rho\colon \Lambda_D \longrightarrow \mu_9 \times \mu_9 \times \mu_9$$
$$x \longmapsto \left(\left(\frac{x,p}{\mathfrak{p}_1}\right)_9, \left(\frac{x,p}{\mathfrak{p}_2}\right)_9, \left(\frac{x,p}{\mathfrak{l}_{0,2}}\right)_9 \right)$$

defined in Lemma 2.8, we know $\rho(\Lambda_D) \subset (\mu_9 \times \mu_9 \times \mu_9)^{\Pi=1}$, $[\Lambda_D : \Lambda_D \cap \mathbf{N}(K_{2,2}^\times)] = |\rho(\Lambda_D)|$ and $[E_{0,2} : E_{0,2} \cap \mathbf{N}(K_{2,2}^\times)] = |\rho(E_{0,2})|$.

Now Lemma 4.2 tells us that $|\rho(\Lambda_D)| = 81$ and $|\rho(E_{0,2})| = 27$. Hence Gras' formula implies that $3 \nmid (\mathrm{Cl}_{2,2}/C)^G$, where $G = \mathrm{Gal}(K_{2,2}/K_{0,2})$. This means $A_{2,2} = C$ by Lemma 2.3. In particular, $A_{2,2} = \mathrm{Cl}_{2,2}^G(3)$. By Chevalley's formula (2.3), we have $|A_{2,2}| = |\,\mathrm{Cl}_{2,2}^G\,| = 3$. For $m \leq 2, n \leq 2$, the norm map from $A_{2,2}$ to $A_{m,n}$ is surjective. It has been shown in [**4**] that 3 divides $|A_{1,0}|$, whence $A_{1,0} \cong \mathbb{Z}/3\mathbb{Z}$. The inequalities $|A_{1,0}| \leq |A_{1,1}| \leq |A_{2,2}|$ then imply that $A_{2,2} \cong A_{1,1} \cong \mathbb{Z}/3\mathbb{Z}$.

By Proposition 3.4, we have $A_{n,m} \cong \mathbb{Z}/3\mathbb{Z}$ for any $n \geq 1, m \geq 1$. For $n \geq 1$, note that $3 = |A_{1,0}| \leq |A_{n,0}| \leq |A_{n,1}| = 3$, then $A_{n,0} \cong \mathbb{Z}/3\mathbb{Z}$. This completes the proof of (2). □

Lemma 4.2. *We have* $|\rho(\Lambda_D)| = 81$ *and* $|\rho(E_{0,2})| = 27$.

Proof: By the product formula, $|\rho(\Lambda_D)| \leq 81$. To get equality, it suffices to show $|\rho(\Lambda_D)| \geq 81$.

We first compute $\rho(\zeta_9)$. In the local field $\mathbb{Q}_p(\zeta_9)$, one has

$$\left(\frac{\zeta_9, p}{\mathbb{Q}_p(\zeta_9)}\right)_9 = \zeta_9^{-\frac{p^3-1}{9}}$$

which is a primitive 9-th root of unity since $p \equiv 4, 7 \bmod 9$. The prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above p induce two embeddings from $K_{0,2}$ to $\mathbb{Q}_p(\zeta_9)$ which are not $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugate. We choose the corresponding embeddings by setting $\iota_1(\zeta_9) = \zeta_9 \in (K_{0,2})_{\mathfrak{p}_1} = \mathbb{Q}_p(\zeta_9)$ and $\iota_2(\zeta_9) = \zeta_9^{-1} \in (K_{0,2})_{\mathfrak{p}_1}$; here we use the convention for the embedding below Proposition 2.2. Then

$$\left(\frac{\zeta_9, p}{\mathfrak{p}_1}\right)_9 = \left(\frac{\zeta_9, p}{\mathfrak{p}_2}\right)_9 = \zeta_9^{-\frac{p^3-1}{9}}.$$

By the product formula, one has

$$\rho(\zeta_9) = (\zeta_9^{-\frac{p^3-1}{9}}, \zeta_9^{-\frac{p^3-1}{9}}, \zeta_9^{\frac{2(p^3-1)}{9}}), \quad \text{whence} \quad |\langle \rho(\zeta_9)\rangle| = 9.$$

To prove $|\rho(\Lambda_D)| \geq 81$, it suffices to show that $\rho(1-\zeta_9)^3 \notin \langle \rho(\zeta_9)\rangle$. We have

$$\left(\frac{1-\zeta_9, p}{\mathbb{Q}_p(\zeta_9)}\right)_9^3 = \left(\frac{1-\zeta_9, p}{\mathbb{Q}_p(\zeta_9)}\right)_3 = \left(\frac{1-\zeta_3, p}{\mathbb{Q}_p}\right)_3.$$

For $a \in (\mathbb{Z}/9\mathbb{Z})^\times$, let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ be given by $\sigma_a(\zeta_9) = \zeta_9^a$. So we have $\sigma_{-1}(\mathfrak{p}_1) = \mathfrak{p}_2$. We have

$$\begin{aligned}
\left(\frac{1-\zeta_9, p}{\mathfrak{p}_1}\right)_9^3 \cdot \sigma_{-1}\left(\left(\frac{1-\zeta_9, p}{\mathfrak{p}_2}\right)_9^3\right) &= \left(\frac{1-\zeta_9, p}{\mathfrak{p}_1}\right)_9^3 \left(\frac{1-\zeta_9^{-1}, p}{\mathfrak{p}_1}\right)_9^3 \\
&= \left(\frac{1-\zeta_9, p}{\mathbb{Q}_p(\zeta_9)}\right)_3 \left(\frac{1-\zeta_9^{-1}, p}{\mathbb{Q}_p(\zeta_9)}\right)_3 \\
&= \left(\frac{1-\zeta_3, p}{\mathbb{Q}_p}\right)_3 \left(\frac{1-\zeta_3^{-1}, p}{\mathbb{Q}_p}\right)_3 \\
&= \left(\frac{3, p}{\mathbb{Q}_p}\right)_3 \neq 1,
\end{aligned}$$

where the first equality is by (2.1), the second equality is by definition (more precisely, here we identify $K_{0,2}$ with $\iota_1(K_{0,2}) \subset \mathbb{Q}_p(\zeta_9)$), the third equality is by the norm compatibility of Hilbert symbols, and the last equality is by assumptions on p. Comparing with $\rho(\zeta_9)$, we conclude that $\rho(1-\zeta_9)^3 \notin \langle \rho(\zeta_9)\rangle$. This proves that $|\rho(\Lambda_D)| = 81$.

Now we compute $|\rho(E_{0,2})|$. Since $3 \mid h_{1,0}$, one has $3 \mid h_{2,2}$ by Lemma 2.5. By Chevalley's formula and Lemma 2.3, we must have

$$|\rho(E_{0,2})| \leq 27.$$

Since $p \equiv 4, 7 \bmod 9$, we have $\sigma_4(\mathfrak{p}_i) = \mathfrak{p}_i$ $(i = 1, 2)$. It then follows that

$$\left(\frac{1-\zeta_9^4, p}{\mathfrak{p}_i}\right)_9 \equiv (1-\zeta_9^4)^{\frac{p^3-1}{9}} \bmod \mathfrak{p}_i = \sigma_4\left(\left(\frac{1-\zeta_9, p}{\mathfrak{p}_i}\right)_9\right) = \left(\frac{1-\zeta_9, p}{\mathfrak{p}_i}\right)_9^4.$$

Therefore $\rho\left(\frac{1-\zeta_9^4}{1-\zeta_9}\right) = \rho(1-\zeta_9)^3$. As we have proved,

$$|\rho(E_{0,2})| \geq \left|\left\langle \rho(\zeta_9), \rho\left(\frac{1-\zeta_9^4}{1-\zeta_9}\right)\right\rangle\right| = 27.$$

Hence $|\rho(E_{0,2})| = 27$. □

5. The case $\ell = 2$

In this section, $K_{n,m} = \mathbb{Q}(p^{\frac{1}{2^n}}, \zeta_{2^{m+1}})$, $A_{n,m}$, and $h_{n,m}$ are the 2-part of the class group and the class number of $K_{n,m}$ respectively.

5.1. The cases $p \equiv 3, 5 \bmod 8$.

Lemma 5.1. *Suppose $p \equiv 3 \bmod 8$.*

(1) *The unique prime above 2 in $K_{1,1}$ is totally ramified in $K_{\infty,\infty}/K_{1,1}$.*
(2) *$\prod_v e_v = 32$ where v runs over the places of $K_{0,2}$ and e_v is the ramification index of v in $K_{2,2}/K_{0,2}$.*
(3) *$[E_{0,2} : E_{0,2} \cap \mathbf{N}K_{2,2}^{\times}] = 8$.*

Proof: (1) We only need to show that the unique prime above 2 in $K_{1,1}$ is totally ramified in $K_{2,2}/K_{1,1}$ by Proposition 3.4.

It is easy to see that $K_{1,2}/K_{1,1}$ is ramified at the prime above 2. To see that the prime above 2 is also ramified in $K_{2,2}/K_{1,2}$, we consider the local field extension $\mathbb{Q}_2(\zeta_8, \sqrt[4]{p})/\mathbb{Q}_2(\zeta_8, \sqrt{p})$. Note that

$$\mathbb{Q}_2(\sqrt[4]{p}) = \begin{cases} \mathbb{Q}_2(\sqrt[4]{3}) & \text{if } p \equiv 3 \bmod 16, \\ \mathbb{Q}_2(\sqrt[4]{11}) & \text{if } p \equiv 11 \bmod 16. \end{cases}$$

Since the fields $\mathbb{Q}_2(\sqrt[4]{3})$ and $\mathbb{Q}_2(\sqrt[4]{11})$ are not Galois over $\mathbb{Q}_2$,

$$\mathbb{Q}_2^{\mathrm{un}} \cap \mathbb{Q}_2(\zeta_8, \sqrt[4]{p}) \subset \mathbb{Q}_2^{\mathrm{ab}} \cap \mathbb{Q}_2(\zeta_8, \sqrt[4]{p}) = \mathbb{Q}_2(\zeta_8, \sqrt{p}),$$

where $\mathbb{Q}_2^{\mathrm{un}}$ (resp. $\mathbb{Q}_2^{\mathrm{ab}}$) is the maximal unramified (resp. abelian) extension of $\mathbb{Q}_2$. Thus $\mathbb{Q}_2(\zeta_8, \sqrt[4]{p})/\mathbb{Q}_2(\zeta_8, \sqrt{p})$ is totally ramified. So $K_{2,2}/K_{1,1}$ is totally ramified at 2.

(2) Since $p \equiv 3 \bmod 8$, we have $p\mathcal{O}_{0,2} = \mathfrak{p}_1\mathfrak{p}_2$, with $\mathfrak{p}_1$, $\mathfrak{p}_2$ totally ramified in $K_{\infty,2}$. Then $e_{\mathfrak{p}_i} = [\mathbb{Q}_p(\sqrt[4]{p}, \zeta_8) : \mathbb{Q}_p(\zeta_8)] = 4$. Let $\mathfrak{l}_{0,2}$ be the unique prime ideal above 2 in $K_{0,2}$. Then $e_{\mathfrak{l}_{0,2}} = 2$ as $\mathbb{Q}_2(\sqrt{p}, \zeta_8)/\mathbb{Q}_2(\zeta_8)$ is unramified. Since $K_{2,2}/K_{0,2}$ is unramified outside 2 and p, we have $\prod_v e_v = 32$.

(3) Note that $E_{0,2} = \langle \zeta_8, 1 + \sqrt{2} \rangle$. Recall the following map as in Lemma 2.8:

$$\begin{aligned} \rho\colon E_{0,2} &\longrightarrow \mu_4 \times \mu_4 \times \mu_4 \\ x &\longmapsto \left(\left(\frac{x,p}{\mathfrak{p}_1} \right)_4, \left(\frac{x,p}{\mathfrak{p}_2} \right)_4, \left(\frac{x,p}{\mathfrak{l}_{0,2}} \right)_4 \right). \end{aligned}$$

We have $|\rho(E_{0,2})| = [E_{0,2} : E_{0,2} \cap \mathbf{N}K_{2,2}^{\times}]$ and $\rho(E_{0,2}) \subset (\mu_4 \times \mu_4 \times \mu_4)^{\prod=1}$.

Let $\iota_1, \iota_2 \colon \mathbb{Q}(\zeta_8) \to \mathbb{Q}_p(\zeta_8)$ be the corresponding embeddings of $\mathfrak{p}_1$, $\mathfrak{p}_2$ such that $\iota_1(\zeta_8) = \zeta_8$ and $\iota_2(\zeta_8) = \zeta_8^{-1}$. By definition $\left(\frac{x,p}{\mathfrak{p}_j}\right)_4 = \iota_j^{-1}\left(\frac{\iota_j(x),p}{\mathbb{Q}_p(\zeta_8)}\right)_4$ for $j = 1, 2$.

We first compute $\rho(\zeta_8)$. Since the residue field of $\mathbb{Q}_p(\zeta_8)$ is $\mathbb{F}_{p^2}$, we have

$$\left(\frac{\zeta_8^{\pm 1}, p}{\mathbb{Q}_p(\zeta_8)}\right)_4 = \left(\frac{p, \zeta_8^{\pm 1}}{\mathbb{Q}_p(\zeta_8)}\right)_4^{-1} = \zeta_8^{\mp \frac{p^2-1}{4}}.$$

Thus

$$\left(\frac{\zeta_8, p}{\mathfrak{p}_1}\right)_4 = \left(\frac{\zeta_8, p}{\mathfrak{p}_2}\right)_4 = \zeta_8^{-\frac{p^2-1}{4}} = \pm i.$$

By the product formula $\left(\frac{\zeta_8,p}{\mathfrak{l}_{0,2}}\right)_4 = -1$. Therefore $\rho(\zeta_8) = (\pm i, \pm i, -1)$.

Now we compute $\rho(1+\sqrt{2})$. In the local field $\mathbb{Q}_p(\zeta_8)$,

$$\left(\frac{1+\sqrt{2}, p}{\mathbb{Q}_p(\sqrt{2})}\right)_4^2 = \left(\frac{1+\sqrt{2}, p}{\mathbb{Q}_p(\sqrt{2})}\right)_2 = \left(\frac{-1, p}{\mathbb{Q}_p}\right)_2 = -1.$$

Hence

$$\left(\frac{1+\sqrt{2}, p}{\mathbb{Q}_p(\sqrt{2})}\right)_4 = \pm i.$$

Since $\iota_1(1+\sqrt{2}) = \iota_2(1+\sqrt{2}) = 1+\sqrt{2}$ and $\iota_1(i) = i, \iota_2(i) = -i$, we have

$$\left(\frac{1+\sqrt{2}, p}{\mathfrak{p}_1}\right)_4 = \pm i, \quad \left(\frac{1+\sqrt{2}, p}{\mathfrak{p}_2}\right)_4 = \mp i.$$

By the product formula, $\left(\frac{1+\sqrt{2},p}{\mathfrak{l}_{0,2}}\right)_4 = 1$.

Therefore, $\rho(\zeta_8) = (\pm i, \pm i, -1)$ and $\rho(1+\sqrt{2}) = (\pm i, \mp i, 1)$. In each case, we have $|\rho(E_{0,2})| = 8$. □

Proof of Theorem 1.1 for $p \equiv 3 \bmod 8$: We know that the class number of $K_{0,2} = \mathbb{Q}(\zeta_8)$ is 1, the product of the ramification indices is 32, and the index $[E_{0,2} : E_{0,2} \cap \mathbf{N}K_{2,2}^{\times}] = 8$ by Lemma 5.1, then $|\mathrm{Cl}_{2,2}^G| = 1$ by Chevalley's formula (2.3). Thus $2 \nmid h_{2,2}$ by Lemma 2.3. Now Proposition 3.4 implies $2 \nmid h_{n,m}$ for $n, m \geq 1$. Since $K_{n,1}/K_{n,0}$ is ramified at the real places, we have $2 \nmid h_{n,0}$ by Lemma 2.5. □

Lemma 5.2. *Suppose $p \equiv 5 \bmod 8$.*

(1) *The unique prime in $K_{1,0}$ above 2 is totally ramified in $K_{\infty,\infty}/K_{1,0}$.*
(2) $\prod_v e(v, K_{3,2}/K_{0,2}) = 2^8$ *where v runs over the places of $K_{0,2}$.*
(3) $\prod_v e(v, K_{2,1}/K_{0,1}) = 2^5$ *where v runs over the places of $K_{0,1}$.*
(4) $\prod_v e(v, K_{1,2}/K_{0,2}) = 4$ *where v runs over the places of $K_{0,2}$.*

Proof: (1) Note that $\mathbb{Q}_2(\sqrt[4]{p})/\mathbb{Q}_2$ is not Galois, so $\sqrt[4]{p} \notin \mathbb{Q}_2^{\mathrm{ab}}$. Then the proof is the same as the case $p \equiv 3 \bmod 8$.

(2) We only need to consider the primes above 2 and p. Since $p\mathcal{O}_{0,2} = \mathfrak{p}_1\mathfrak{p}_2$ and $e(p, K_{3,0}/\mathbb{Q}) = 8$, we have $e(\mathfrak{p}_1, K_{3,2}/K_{0,2}) = e(\mathfrak{p}_2, K_{3,2}/K_{0,2}) = 8$. From (1), we can easily obtain that $e(\mathfrak{l}_{0,2}, K_{3,2}/K_{0,2}) = 4$ for $\mathfrak{l}_{0,2}$, the only prime above 2 in $K_{0,2}$. Hence the product of ramification indices is 2^8.

The proofs of (3) and (4) are easy; we leave them to the readers. □

Lemma 5.3. *Let* $p \equiv 5 \bmod 8$. *Let* $\Lambda_{0,2} = \langle (1-\zeta_8)^2, \zeta_8, 1+\sqrt{2}\rangle \subset K_{0,2}^{\times}$ *and* $\Lambda_{0,1} = \langle (1-i)^2, i\rangle \subset K_{0,1}^{\times}$. *We have*

(1) $[\Lambda_{0,2} : \Lambda_{0,2} \cap \mathbf{N}K_{3,2}^{\times}] = 32$ *and* $[E_{0,2} : E_{0,2} \cap \mathbf{N}K_{3,2}^{\times}] = 16$.
(2) $[\Lambda_{0,1} : \Lambda_{0,1} \cap \mathbf{N}K_{2,1}^{\times}] = 8$ *and* $[E_{0,1} : E_{0,1} \cap \mathbf{N}K_{2,1}^{\times}] = 4$.
(3) $[E_{0,2} : E_{0,2} \cap \mathbf{N}K_{1,2}^{\times}] = 2$.

Proof: Denote by $\mathfrak{l}_{n,m}$ the unique prime ideal of $K_{n,m}$ above 2 for each $n, m \geq 0$. Note that $E_{0,2} = \langle \zeta_8, 1+\sqrt{2}\rangle$. Then $\Lambda_{0,2} = \Lambda_{\langle \mathfrak{l}_{3,2}\rangle}$ corresponds to the extension $K_{3,2}/K_{0,2}$ and $\Lambda_{0,1} = \Lambda_{\langle \mathfrak{l}_{2,1}\rangle}$ corresponds to the extension $K_{2,1}/K_{0,1}$ as in Lemma 2.8.

Since $p \equiv 5 \bmod 8$, we have $p\mathcal{O}_{0,1} = \mathfrak{p}_1\mathfrak{p}_2$ and $p\mathcal{O}_{0,2} = \mathfrak{P}_1\mathfrak{P}_2$. Note that $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{l}_{0,2}$ are exactly the ramified places in $K_{3,2}/K_{0,2}$. For (1), we study the map as in Lemma 2.8:

$$\rho := \rho_{\langle \mathfrak{l}_{3,2}\rangle, K_{3,2}/K_{0,2}} \colon \Lambda_{0,2} \longrightarrow \mu_8 \times \mu_8 \times \mu_8$$
$$x \longmapsto \left(\left(\frac{x,p}{\mathfrak{P}_1}\right)_8, \left(\frac{x,p}{\mathfrak{P}_2}\right)_8, \left(\frac{x,p}{\mathfrak{l}_{0,2}}\right)_8 \right).$$

By Lemma 2.8, $\rho(\Lambda_{0,2}) \subset (\mu_8 \times \mu_8 \times \mu_8)^{\Pi=1}$, $[\Lambda_{0,2} : \Lambda_{0,2} \cap \mathbf{N}(K_{3,2}^{\times})] = |\rho(\Lambda_{0,2})|$, and $[E_{0,2} : E_{0,2} \cap \mathbf{N}(K_{3,2}^{\times})] = |\rho(E_{0,2})|$.

Let $\iota_j \colon \mathbb{Q}(\zeta_8) \to \mathbb{Q}_p(\zeta_8)$ be the corresponding embeddings for $\mathfrak{P}_j$ for$j = 1, 2$. We choose ι_j so that $\iota_1(\zeta_8) = \zeta_8$ (and hence $\iota(i) = i, \iota(\sqrt{2}) = \sqrt{2}$) and $\iota_2(\zeta_8) = \zeta_8^{-1}$ (and hence $\iota_2(i) = -i, \iota_2(\sqrt{2}) = \sqrt{2}$). The Hilbert symbol $\left(\frac{x,p}{\mathfrak{P}_i}\right)_8$ by definition is $\iota_i^{-1}\left(\frac{\iota_i(x),p}{\mathbb{Q}_p(\zeta_8)}\right)_8$.

We first compute $\rho(\zeta_8)$. In the local field $\mathbb{Q}_p(\zeta_8)$,

$$\left(\frac{\zeta_8^{\pm 1}, p}{\mathbb{Q}_p(\zeta_8)}\right)_8 = \left(\frac{p, \zeta_8^{\pm}}{\mathbb{Q}_p(\zeta_8)}\right)_8^{-1} = \zeta_8^{\mp \frac{p^2-1}{8}},$$

we have

$$\left(\frac{\zeta_8, p}{\mathfrak{P}_1}\right)_8 = \left(\frac{\zeta_8, p}{\mathfrak{P}_2}\right)_8 = \zeta_8^{-\frac{p^2-1}{8}}.$$

Hence $\rho(\zeta_8) = (\zeta_8^{-\frac{p^2-1}{8}}, \zeta_8^{-\frac{p^2-1}{8}}, \pm i)$ by the product formula.

Now we compute $\rho(1+\sqrt{2})$. In $\mathbb{Q}_p(\zeta_8)$,

$$\left(\frac{1+\sqrt{2},p}{\mathbb{Q}_p(\zeta_8)}\right)_8^2 = \left(\frac{1+\sqrt{2},p}{\mathbb{Q}_p(\zeta_8)}\right)_4 = \left(\frac{-1,p}{\mathbb{Q}_p}\right)_4 = -1,$$

where the second equality is due to the norm-compatible property of Hilbert symbols and the fact that $i \in \mathbb{Q}_p$ for $p \equiv 5 \bmod 8$. The last equality is due to the fact that -1 is a square but not a fourth power in $\mathbb{Z}/p\mathbb{Z}$ for $p \equiv 5 \bmod 8$. Therefore

$$\left(\frac{1+\sqrt{2},p}{\mathbb{Q}_p(\zeta_8)}\right)_8 = \pm i.$$

Since $\iota_1(\sqrt{2}) = \iota_2(\sqrt{2}) = \sqrt{2}$ and $\iota_1(i) = i, \iota_2(i) = -i$, we have

$$\left(\frac{1+\sqrt{2},p}{\mathfrak{P}_1}\right)_8 = \pm i, \quad \left(\frac{1+\sqrt{2},p}{\mathfrak{P}_2}\right)_8 = \mp i.$$

Hence $\rho(1+\sqrt{2}) = (\pm i, \mp i, 1)$ by the product formula. In each case, we always have $|\rho(E_{0,2})| = |\langle \rho(\zeta_8), \rho(1+\sqrt{2})\rangle| = 16$.

Finally we compute $\rho((1-\zeta_8)^2)$. In $\mathbb{Q}_p(\zeta_8)$,

$$\begin{aligned} a^{\pm} &:= \left(\frac{(1-\zeta_8^{\pm 1})^2,p}{\mathbb{Q}_p(\zeta_8)}\right)_8 = \left(\frac{1-\zeta_8^{\pm 1},p}{\mathbb{Q}_p(\zeta_8)}\right)_4 \\ &= \left(\frac{(1-\zeta_8^{\pm 1})(1+\zeta_8^{\pm 1}),p}{\mathbb{Q}_p}\right)_4 = \left(\frac{1\mp i,p}{\mathbb{Q}_p}\right)_4. \end{aligned}$$

Then $a^+a^- = \left(\frac{2,p}{\mathbb{Q}_p}\right)_4 = \pm i$ and $\frac{a^-}{a^+} = \left(\frac{i,p}{\mathbb{Q}_p}\right)_4 = \pm i$. Therefore

$$(a^+, a^-) = (\pm i, 1), (\pm i, -1), (1, \pm i), (-1, \pm i).$$

By definition, $\left(\frac{(1-\zeta_8)^2,p}{\mathfrak{P}_1}\right)_8 = a^+$ and $\left(\frac{(1-\zeta_8)^2,p}{\mathfrak{P}_2}\right)_8 = \iota_2^{-1}(a^-)$. Therefore

$$\left(\left(\frac{(1-\zeta_8)^2,p}{\mathfrak{P}_1}\right)_8, \left(\frac{(1-\zeta_8)^2,p}{\mathfrak{P}_2}\right)_8\right) = (\pm i, 1), (\pm i, -1), (1, \mp i), (-1, \mp i).$$

In each case, we always have $|\rho(\Lambda_{0,2})| = |\langle \rho((1-\zeta_8)^2), \rho(\zeta_8), \rho(1+\sqrt{2})\rangle| = 32$. This proves (1).

For (2), we study the map

$$\begin{aligned} \rho_4 := \rho_{\langle \mathfrak{l}_{2,1}\rangle, K_{2,1}/K_{0,1}} \colon \Lambda_{0,1} &\longrightarrow \mu_4 \times \mu_4 \times \mu_4 \\ x &\longmapsto \left(\left(\frac{x,p}{\mathfrak{p}_1}\right)_4, \left(\frac{x,p}{\mathfrak{p}_2}\right)_4, \left(\frac{x,p}{\mathfrak{l}_{0,1}}\right)_4\right). \end{aligned}$$

We always have

$$\left(\frac{i,p}{\mathbb{Q}_p}\right)_4 = \left(\frac{p,i}{\mathbb{Q}_p}\right)_4^{-1} = i^{-\frac{p-1}{4}} = \pm i.$$

Let τ_1, τ_2 be the embeddings corresponding to $\mathfrak{p}_1$, $\mathfrak{p}_2$ respectively. We assume that $\tau_1(i) = i$ and $\tau_2(i) = -i$. Then

$$\left(\frac{i,p}{\mathfrak{p}_1}\right)_4 = \tau_1^{-1}\left(\frac{\tau_1(i),p}{\mathbb{Q}_p}\right)_4 = \pm i = \tau_2^{-1}\left(\frac{\tau_2(i),p}{\mathbb{Q}_p}\right)_4 = \left(\frac{i,p}{\mathfrak{p}_2}\right)_4.$$

Hence $\rho_4(i) = (\pm i, \pm i, -1)$ by the product formula. So $[E_{0,1} : E_{0,1} \cap \mathbf{N}K_{2,1}^{\times}] = |\rho_4(E_{0,1})| = |\langle \rho_4(i)\rangle| = 4$.

Now we compute $\rho_4((1+i)^2)$. Since

$$\left(\frac{(1-i)^2,p}{\mathbb{Q}_p}\right)_4\left(\frac{(1+i)^2,p}{\mathbb{Q}_p}\right)_4 = \left(\frac{1-i,p}{\mathbb{Q}_p}\right)_2\left(\frac{1+i,p}{\mathbb{Q}_p}\right)_2 = \left(\frac{2,p}{\mathbb{Q}_p}\right)_2 = -1,$$

we have

$$\left(\frac{(1-i)^2,p}{\mathfrak{p}_1}\right)_4 = \pm 1, \quad \left(\frac{(1-i)^2,p}{\mathfrak{p}_2}\right)_4 = \mp 1.$$

Hence $\rho_4((1-i)^2) = (\pm 1, \mp 1, -1)$. Therefore, $[\Lambda_{0,1} : \Lambda_{0,1} \cap \mathbf{N}K_{2,1}^{\times}] = |\langle \rho_4((1-i)^2), \rho_4(i)\rangle| = 8$. This proves (2).

(3) follows from the values of the following quadratic Hilbert symbols:

$$\left(\frac{\zeta_8,p}{\mathbb{Q}_p(\zeta_8)}\right)_2 = \left(\frac{-i,p}{\mathbb{Q}_p}\right)_2 = -1, \quad \left(\frac{1+\sqrt{2},p}{\mathbb{Q}_p(\zeta_8)}\right)_2 = \left(\frac{-1,p}{\mathbb{Q}_p}\right)_2 = 1. \qquad \square$$

Proof of Theorem 1.1 for $p \equiv 5 \bmod 8$: We first prove that $2\|h_{3,2}, 2\|h_{2,1}$ and $2 \nmid h_{1,2}$.

We apply Gras' formula (2.2) to the case

$$K_{3,2}/K_{0,2}, \quad C = \langle \mathrm{cl}(\mathfrak{l}_{3,2})\rangle, \quad D = \langle \mathfrak{l}_{3,2}\rangle,$$

where $\mathfrak{l}_{n,m}$ is the unique prime ideal of $K_{n,m}$ above 2. Then $\Lambda_D = \Lambda_{0,2}$ as in Lemma 5.3. By the above computation and Lemma 2.3, $A_{3,2} = \langle \mathrm{cl}(\mathfrak{l}_{3,2})\rangle(2)$. Note that C is invariant under the action of $G := \mathrm{Gal}(K_{3,2}/K_{0,2})$. We have $A_{3,2} = A_{3,2}^G$. Chevalley's formula (2.3) and the above computation imply that $|A_{3,2}| = |A_{3,2}^G| = 2$.

Similarly, applying Gras' formula to the case

$$K_{2,1}/K_{0,1}, \quad C = \langle \mathrm{cl}(\mathfrak{l}_{2,1})\rangle, \quad D = \langle \mathfrak{l}_{2,1}\rangle$$

shows that $A_{2,1} = \langle \mathrm{cl}(\mathfrak{l}_{2,1})\rangle(2)$. In particular, $A_{2,1}$ is invariant under the action of $\mathrm{Gal}(K_{2,1}/K_{0,1})$. Apply Chevalley's formula to $K_{2,1}/K_{0,1}$, we obtain $|A_{2,1}| = 2$.

By Applying Chevalley's formula to the extension $K_{1,2}/K_{0,2}$ and Lemma 2.3, we have $2 \nmid h_{1,2}$. Hence $2 \nmid h_{1,1}$ by Lemma 2.5.

We have $2 \parallel h_{n,m}$ for $n \geq 2, m \geq 1$ by Proposition 3.4 and $2 \nmid h_{1,m}$ for $n = 1, m \geq 1$ by Proposition 3.2.

It remains to prove that $2 \nmid h_{n,0}$. The proof consists of three steps:

Step 1: Let ϵ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$. We show that $\left(\frac{\epsilon,\sqrt{p}}{\sqrt{p}}\right)_2 = -1$.

Write $\epsilon = \frac{a+b\sqrt{p}}{2}, a, b \in \mathbb{Z}$. Then

$$\left(\frac{\epsilon,\sqrt{p}}{(\sqrt{p})}\right)_2 = \left(\frac{a/2,\sqrt{p}}{(\sqrt{p})}\right)_2 = \left(\frac{a/2,-p}{p}\right)_2 = \left(\frac{a/2}{p}\right).$$

It is well known that $\mathbf{N}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\epsilon) = \left(\frac{a}{2}\right)^2 - p\left(\frac{b}{2}\right)^2 = -1$. Since $\left(\frac{a}{2}\right)^2 \equiv -1 \bmod p$ and $p \equiv 5 \bmod 8$, we have $\left(\frac{a/2}{p}\right) \equiv \left(\frac{a}{2}\right)^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Step 2: We show that $[E_{n,0} : E_{n,0} \cap \mathbf{N}K_{n+1,0}^{\times}] = 4$ for each $n \geq 1$.

Consider the map as in Lemma 2.8,

$$\begin{aligned} \rho\colon E_{n,0} &\longrightarrow \mu_2 \times \mu_2 \times \mu_2 \\ x &\longmapsto \left(\left(\frac{x, p^{\frac{1}{2^n}}}{\infty_n}\right)_2, \left(\frac{x, p^{\frac{1}{2^n}}}{(p^{\frac{1}{2^n}})}\right)_2, \left(\frac{x, p^{\frac{1}{2^n}}}{\mathfrak{l}_{n,0}}\right)_2\right), \end{aligned}$$

where ∞_n is the real place of $K_{n,0}$ such that $\infty_n(p^{\frac{1}{2^n}}) < 0$. We know $[E_{n,0} : E_{n,0} \cap \mathbf{N}K_{n,0}^{\times}] = |\rho(E_{n,0})|$ and $\rho(E_{n,0}) \subset (\zeta_2 \times \zeta_2 \times \zeta_2)^{\Pi=1}$. In particular, $|\rho(E_{n,0})| \leq 4$.

Since $-1, \epsilon \in E_{n,0}$, it is enough to prove that $|\langle \rho(-1), \rho(\epsilon)\rangle| = 4$. By Step 1, we have

$$\left(\frac{\epsilon, p^{\frac{1}{2^n}}}{(p^{\frac{1}{2^n}})}\right)_2 = \left(\frac{\epsilon, -p^{\frac{1}{2^{n-1}}}}{(p^{\frac{1}{2^{n-1}}})}\right)_2 = \cdots = \left(\frac{\epsilon, -\sqrt{p}}{(\sqrt{p})}\right)_2 = -1.$$

Therefore, $\rho(\epsilon) = (\pm 1, -1, \mp 1)$. Since $\rho(-1) = (-1, 1, -1)$, we have $|\langle \rho(-1), \rho(\epsilon)\rangle| = 4$ and hence $|\rho(E_{n,0})| = 4$.

Step 3: We prove $2 \nmid h_{n,0}$ for any $n \geq 1$.

We prove it by induction on n. The case $n = 1$ is well known. Assume that $2 \nmid h_{n,0}$. The product of ramification indices of $K_{n+1,0}/K_{n,0}$ is 8. Using the result in Step 2, Chevalley's formula (2.3) for the extension $K_{n+1,0}/K_{n,0}$, and Lemma 2.3 then imply $2 \nmid h_{n+1,0}$. □

5.2. The case $p \equiv 7 \bmod 16$. The main purpose of this subsection is to prove Theorem 1.1(3). We first give a brief description of the proof.

- Apply Gras' formula (2.2) inductively to the extension $K_{n,0}/K_{n-1,0}$ to show that $A_{n,0}$ is generated by the unique prime above 2. Then apply (2.2) to $K_{n,1}/K_{n,0}$ to show that $A_{n,1}$ equals the 2-primary part of $\langle$classes of primes above 2$\rangle$. Next we apply Chevalley's formula (2.3) to the extensions $K_{3,1}/K_{1,1}$ and $K_{2,1}/K_{1,1}$ to deduce $A_{2,1} \cong A_{3,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Proposition 3.2 then implies $A_{n,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $n \geq 2$. Finally from this one can get $A_{n,0} \cong \mathbb{Z}/2\mathbb{Z}$ for $n \geq 2$.
- Apply (2.2) inductively to $K_{1,m}/K_{0,m}$ to show that $A_{1,m}$ is a quotient of $\mathbb{Z}/2^{m-1}\mathbb{Z}$, then use Kida's λ-invariant formula to get $|A_{1,m}| \geq 2^{m-1}$. This leads to $A_{1,m} \cong \mathbb{Z}/2^{m-1}\mathbb{Z}$ for any $m \geq 1$.

For each $n \geq 1$, $K_{n,0}$ has two real places. Let ∞_n be the real place such that $\infty_n(p^{\frac{1}{2^n}}) < 0$. Then ∞_n is ramified in $K_{n+1,0}/K_{n,0}$, while the other real place is unramified in $K_{n+1,0}/K_{n,0}$.

The prime p is totally ramified as $p\mathcal{O}_{n,0} = \mathfrak{p}_{n,0}^{2^n}$ in $K_{n,0}$, where $\mathfrak{p}_{n,0} = (p^{\frac{1}{2^n}})$. Since p is inert in $K_{0,1}$, $\mathfrak{p}_{n,0}$ is inert in $K_{n,1}$. Write $\mathfrak{p}_{n,0}\mathcal{O}_{n,1} = \mathfrak{p}_{n,1}$. The prime $\mathfrak{p}_{0,1} = (p)$ is totally ramified in $K_{\infty,1}/K_{0,1}$.

Since $(x+1)^{2^n} - p$ is a 2-Eisenstein polynomial, 2 is totally ramified as $2\mathcal{O}_{n,0} = \mathfrak{l}_{n,0}^{2^n}$ in $K_{n,0}$. Since 2 splits in $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$, $\mathfrak{l}_{n,0}$ splits as $\mathfrak{l}_{n,0}\mathcal{O}_{n,1} = \mathfrak{l}_{n,1}\mathfrak{l}'_{n,1}$ in $K_{n,1}/K_{n,0}$ for each $n \geq 1$. The primes $\mathfrak{l}_{1,1}$ and $\mathfrak{l}'_{1,1}$ are totally ramified in $K_{\infty,1}/K_{1,1}$.

The prime 2 is also totally ramified as $2\mathcal{O}_{0,m} = \mathfrak{l}_{0,m}^{2^n}$ in $K_{0,m}$, where $\mathfrak{l}_{0,m} = (1 - \zeta_{2^{m+1}})\mathcal{O}_{0,m}$. The prime $\mathfrak{l}_{0,m}$ splits as $\mathfrak{l}_{0,m}\mathcal{O}_{1,m} = \mathfrak{l}_{1,m}\mathfrak{l}'_{1,m}$ in $K_{1,m}$ for each $m \geq 1$.

Since $2 \nmid h_{1,0}$, $\mathfrak{l}_{1,0}$ is principal. Let $\pi = u + v\sqrt{p}$ be a totally positive generator of $\mathfrak{l}_{1,0}$. We must have $\mathbf{N}(\pi) = u^2 - pv^2 = 2$, since -2 is not a square modulo p. Let ϵ be the fundamental unit of $K_{1,0}$. Note that $\frac{\pi^2}{2}$ is a unit. We must have $\frac{\pi^2}{2} = \epsilon^k$ for some odd integer k; otherwise, $\sqrt{2}$ would belong in $K_{1,0} = \mathbb{Q}(\sqrt{p})$, which is plainly impossible. Replace the generator π by $\pi\epsilon^{\frac{1-k}{2}}$. We may assume that $\frac{\pi^2}{2} = \epsilon$. So $E_{1,0} = \left\langle -1, \frac{\pi^2}{2} \right\rangle$.

Lemma 5.4. *The class number $h_{1,1}$ of $K_{1,1} = \mathbb{Q}(\sqrt{p}, i)$ is odd and $E_{1,1} = \left\langle \frac{\pi}{1+i}, i \right\rangle$.*

Proof: Apply Chevalley's formula to the extension $K_{1,1}/K_{0,1}$ and Lemma 2.3; one has $2 \nmid h_{1,1}$.

By [**2**, Theorem 42, p. 195],

$$\left[E_{1,1} : \left\langle \frac{\pi^2}{2}, i \right\rangle \right] = 1 \text{ or } 2.$$

Note that $\frac{\pi}{1+i}$ is a unit and $\left[\left\langle \frac{\pi}{1+i}, i\right\rangle : \left\langle \frac{\pi^2}{2}, i\right\rangle\right] = 2$; we must have $E_{1,1} = \left\langle \frac{\pi}{1+i}, i\right\rangle$. □

Lemma 5.5. *We have*

(1) $\left(\frac{\pi,\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = -1$ *and* $\left(\frac{\pi,\sqrt{p}}{\mathfrak{l}_{1,0}}\right)_2 = -1$.

(2) $[E_{1,0} : E_{1,0} \cap \mathbf{N}K_{2,0}^{\times}] = 2$.

(3) $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{3,1}^{\times}] = 4$ *and* $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{2,1}^{\times}] = 1$.

Proof: (1) Since $\pi = u + v\sqrt{p}$ is totally positive, we have $u > 0$, $u^2 - pv^2 = 2$, and $2 \nmid uv$. Note that 2 is a square modulo v, so $v \equiv \pm 1 \bmod 8$. Then $u^2 \equiv 9 \bmod 16$ since $p \equiv 7 \bmod 16$. In other words, $u \equiv \pm 3 \bmod 8$. We have

$$\left(\frac{\pi,\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = \left(\frac{u,\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = \left(\frac{u,-p}{p}\right)_2 = \left(\frac{u}{p}\right) = \left(\frac{-p}{u}\right) = \left(\frac{2}{u}\right) = -1.$$

The fourth equality is due to the quadratic reciprocity law. We have $\left(\frac{\pi,\sqrt{p}}{\infty_1}\right)_2 = 1$ as π is totally positive, thus $\left(\frac{\pi,\sqrt{p}}{\mathfrak{l}_{1,0}}\right)_2 = -1$ by the product formula.

(2) Since the infinite place ∞_1 is ramified, -1 is not a norm of $K_{2,0}$. For the fundamental unit $\frac{\pi^2}{2}$, we have

$$\left(\frac{\frac{\pi^2}{2},\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = \left(\frac{2,\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = \left(\frac{2,-p}{p}\right)_2 = 1, \quad \left(\frac{\frac{\pi^2}{2},\sqrt{p}}{\infty_1}\right)_2 = 1.$$

By the product formula,

$$\left(\frac{\frac{\pi^2}{2},\sqrt{p}}{\mathfrak{l}_{1,0}}\right)_2 = 1.$$

Then $\frac{\pi^2}{2}$ is a norm of $K_{2,0}$ by Hasse's norm theorem. This proves (2).

(3) We need to study the map

$$\begin{aligned} \rho\colon \rho\colon E_{1,1} &\longrightarrow \mu_4 \times \mu_4 \times \mu_4 \\ x &\longmapsto \left(\left(\frac{x,\sqrt{p}}{\mathfrak{p}_{1,1}}\right)_4, \left(\frac{x,\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_4, \left(\frac{x,\sqrt{p}}{\mathfrak{l}'_{1,1}}\right)_4\right). \end{aligned}$$

Then $\rho(E_{1,1}) \subset (\mu_4 \times \mu_4 \times \mu_4)^{\prod=1}$ and $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{3,1}^{\times}] = |\rho(E_{1,1})|$.

We first compute $\rho(i)$. Since $p \equiv 7 \bmod 16$ and the residue field of $\mathfrak{p}_{1,1}$ is $\mathbb{F}_{p^2}$, we have

$$\left(\frac{i,\sqrt{p}}{\mathbb{Q}_p(\sqrt{p},i)}\right)_4 = \left(\frac{\sqrt{p},i}{\mathbb{Q}_p(\sqrt{p},i)}\right)_4^{-1} = i^{-\frac{p^2-1}{4}} = 1.$$

Thus

$$\left(\frac{i,\sqrt{p}}{\mathfrak{p}_{1,1}}\right)_4 = 1.$$

Note that the localization of $K_{1,1}$ at $\mathfrak{l}_{1,1}$ is $\mathbb{Q}_2(\sqrt{p},i) = \mathbb{Q}_2(i)$. Note that $\sqrt{-p} \in \mathbb{Q}_2$. Since

$$\left(\frac{i,i}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,-1}{\mathbb{Q}_2(i)}\right) 9_4 \left(\frac{i,-i}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,-1}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,i}{\mathbb{Q}_2(i)}\right)_2 = 1,$$

we have

$$\left(\frac{i,\sqrt{p}}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,\sqrt{-p}}{\mathbb{Q}_2(i)}\right)_4 = \begin{cases} \left(\frac{i,\sqrt{-7}}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,11}{\mathbb{Q}_2(i)}\right)_4 & \text{if } p \equiv 7 \bmod 32; \\ \left(\frac{i,\sqrt{-23}}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,3}{\mathbb{Q}_2(i)}\right)_4 & \text{if } p \equiv 23 \bmod 32. \end{cases}$$

Applying the product formula to the quartic Hilbert symbols on $\mathbb{Q}(i)$ gives

$$\left(\frac{i,11}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,11}{\mathbb{Q}_{11}(i)}\right)_4^{-1} = i^{-\frac{11^2-1}{4}} = -1,$$
$$\left(\frac{i,3}{\mathbb{Q}_2(i)}\right)_4 = \left(\frac{i,3}{\mathbb{Q}_3(i)}\right)_4^{-1} = i^{-\frac{3^2-1}{4}} = -1.$$

Therefore, $\left(\frac{i,\sqrt{p}}{\mathbb{Q}_2(i)}\right)_4 = -1$ and we have $\rho(i) = (1,-1,-1)$.

Next we compute $\rho\left(\frac{\pi}{1+i}\right)$. By (1), we have $\pi^{\frac{p-1}{2}} \equiv -1 \bmod \mathfrak{p}_{1,0}$. Since $p \equiv 7 \bmod 16$, $\pi^{\frac{p^2-1}{4}} \equiv 1 \bmod \mathfrak{p}_{1,0}$. Hence $\left(\frac{\pi,\sqrt{p}}{\mathfrak{p}_{1,1}}\right)_4 = 1$. Since $(1+i)^{\frac{p^2-1}{4}} = (2i)^{\frac{p^2-1}{8}} = -2^{\frac{p^2-1}{8}} \equiv -1 \bmod p$, we have $\left(\frac{1+i,\sqrt{p}}{\mathfrak{p}_{1,1}}\right)_4 = -1$. Thus

$$\left(\frac{\frac{\pi}{1+i},\sqrt{p}}{\mathfrak{p}_{1,1}}\right)_4 = -1.$$

To compute $\left(\frac{\frac{\pi}{1+i},\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_4$, we first compute its square:

$$\left(\frac{\frac{\pi}{1+i},\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_4^2 = \left(\frac{\frac{\pi}{1+i},\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_2 = \left(\frac{\pi,\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_2 \left(\frac{1+i,\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_2.$$

Note that $\mathbb{Q}_2(\sqrt{p}) = \mathbb{Q}_2(i)$. By part (1) of Lemma 5.5, we have

$$-1 = \left(\frac{\pi,\sqrt{p}}{\mathfrak{l}_{0,1}}\right)_2 = \left(\frac{\pi,\sqrt{p}}{\mathbb{Q}_2(\sqrt{p})}\right)_2 = \left(\frac{\pi,\sqrt{p}}{\mathfrak{l}_{1,1}}\right)_2.$$

Note that $\sqrt{-p} \equiv \pm 3 \bmod 8$. So we have the following equality of quadratic Hilbert symbols:

$$\left(\frac{1 \pm i, \sqrt{p}}{\mathbb{Q}_2(i)}\right)_2 = \left(\frac{1 \pm i, \sqrt{-p}}{\mathbb{Q}_2(i)}\right)_2 = \left(\frac{2, \sqrt{-p}}{\mathbb{Q}_2}\right)_2 = -1.$$

Therefore

$$\left(\frac{\frac{\pi}{1+i}, \sqrt{p}}{\mathfrak{l}_{1,1}}\right)_4^2 = 1 = \left(\frac{\frac{\pi}{1+i}, \sqrt{p}}{\mathfrak{l}'_{1,1}}\right)_4^2.$$

By the product formula we must have $\rho\big(\frac{\pi}{1+i}\big) = (-1, \pm 1, \mp 1)$. Hence $|\rho(E_{1,1})| = 4$. This implies $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{3,1}^{\times}] = 4$.

To compute $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{2,1}^{\times}]$, we need to consider the following map:

$$\begin{aligned} \rho' \colon E_{1,1} &\longrightarrow \mu_2 \times \mu_2 \times \mu_2 \\ x &\longmapsto \left(\left(\frac{x, \sqrt{p}}{\mathfrak{p}_{1,1}}\right)_2, \left(\frac{x, \sqrt{p}}{\mathfrak{l}_{1,1}}\right)_2, \left(\frac{x, \sqrt{p}}{\mathfrak{l}'_{1,1}}\right)_2\right). \end{aligned}$$

Then $\rho' = \rho^2$ by Proposition 2.1(7). Thus $\rho'(i) = \rho(i)^2 = (1,1,1)$ and $\rho'\big(\frac{\pi}{1+i}\big) = \rho\big(\frac{\pi}{1+i}\big)^2 = (1,1,1)$. Therefore $[E_{1,1} : E_{1,1} \cap \mathbf{N}K_{2,1}^{\times}] = |\rho'(E_{1,1})| = 1$. □

Proposition 5.6. *We have*

(1) $A_{n,0} = \langle \mathrm{cl}(\mathfrak{l}_{n,0}) \rangle$ *for* $n \geq 1$ *and* $A_{2,0} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) $A_{n,1} = \langle \mathrm{cl}(\mathfrak{l}_{n,1}), \mathrm{cl}(\mathfrak{l}'_{n,1}) \rangle(2)$ *for* $n \geq 2$.

Proof: (1) We prove this by induction. The case $n = 1$ is well known. Suppose the result holds for n. We apply Gras' formula (2.2) to

$$K_{n+1,0}/K_{n,0}, C = \langle \mathrm{cl}(\mathfrak{l}_{n+1,0}) \rangle, D = \langle \mathfrak{l}_{n+1,0} \rangle.$$

Note that $\mathbf{N}(C) = \langle \mathrm{cl}(\mathfrak{l}_{n,0}) \rangle = A_{n,0}$ by the assumption. The product of ramification indices is 8. Consider the map

$$\begin{aligned} \rho := \rho_{D, K_{n+1,0}/K_{n,0}} \colon \Lambda_D &\longrightarrow \mu_2 \times \mu_2 \times \mu_2 \\ x &\longmapsto \left(\left(\frac{x, p^{\frac{1}{2^n}}}{\infty_n}\right)_2, \left(\frac{x, p^{\frac{1}{2^n}}}{\mathfrak{p}_{n,0}}\right)_2, \left(\frac{x, p^{\frac{1}{2^n}}}{\mathfrak{l}_{n,0}}\right)_2\right). \end{aligned}$$

We have $|\rho(\Lambda_D)| = [\Lambda_D : \Lambda_D \cap \mathbf{N}K_{n+1,0}^{\times}]$ and $\rho(\Lambda_D) \subset (\mu_2 \times \mu_2 \times \mu_2)^{\prod = 1}$, in particular, $|\rho(\Lambda_D)| \leq 4$. Notice that $\Lambda_D \supset \big\langle \pi, \frac{\pi^2}{2}, -1 \big\rangle$.

Since $\infty_n(p^{\frac{1}{2^n}}) < 0$,

$$\left(\frac{-1, p^{\frac{1}{2^n}}}{\infty_n}\right)_2 = -1.$$

By the norm compatibility of Hilbert symbols,

$$\left(\frac{-1, p^{\frac{1}{2^n}}}{\mathfrak{p}_{n,0}}\right)_2 = \left(\frac{-1, -p^{\frac{1}{2^{n-1}}}}{\mathfrak{p}_{n-1,0}}\right)_2 = \cdots = \left(\frac{-1, -p}{(p)}\right)_2 = -1.$$

Then $\rho(-1) = (-1, -1, 1)$. Since π is totally positive,

$$\left(\frac{\pi, p^{\frac{1}{2^n}}}{\infty_n}\right)_2 = 1.$$

By the norm compatibility of Hilbert symbols and the above lemma,

$$\left(\frac{\pi, p^{\frac{1}{2^n}}}{\mathfrak{p}_{n,0}}\right)_2 = \left(\frac{\pi, -\sqrt{p}}{\mathfrak{p}_{1,0}}\right)_2 = -1.$$

Hence $\rho(\pi) = (1, -1, -1)$. Therefore $|\rho(\Lambda_D)| \geq |\langle \rho(\pi), \rho(-1)\rangle| = 4$. This shows that $|\rho(\Lambda_D)| = 4$. Then Gras' formula and Lemma 2.3 tell us $A_{n+1,0} = \langle \mathrm{cl}(\mathfrak{l}_{n+1,0})\rangle(2)$. Note that $\mathfrak{l}_{n+1,0}^{2^n} = \mathfrak{l}_{1,0} = (\pi)$, so $\langle \mathrm{cl}(\mathfrak{l}_{n+1,0})\rangle(2) = \langle \mathrm{cl}(\mathfrak{l}_{n+1,0})\rangle$. By induction, $A_{n+1,0} = \langle \mathrm{cl}(\mathfrak{l}_{n+1,0})\rangle$.

In particular, $A_{2,0}$ is invariant under the action of $\mathrm{Gal}(K_{2,0}/K_{1,0})$. Since $E_{1,0} = \langle -1, \frac{\pi^2}{2}\rangle$ and $[E_{1,0} : E_{1,0} \cap \mathbf{N}K_{2,0}^{\times}] = 2$ by the above lemma, applying Chevalley's formula (2.3) to $K_{2,0}/K_{1,0}$ gives $A_{2,0} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) We apply Gras' formula to

$$K_{n,1}/K_{n,0}, \quad C = \langle \mathrm{cl}(\mathfrak{l}_{n,1}), \mathrm{cl}(\mathfrak{l}'_{n,1})\rangle, \quad D = \langle \mathfrak{l}_{n,1}, \mathfrak{l}'_{n,1}\rangle.$$

Then $\mathbf{N}C = \langle \mathrm{cl}(\mathfrak{l}_{n,0})\rangle = A_{n,0}$ by (1). Only the two infinite places are ramified in $K_{n,1}/K_{n,0}$, so -1 is not a norm. This shows that the index $[\Lambda_D : \Lambda_D \cap \mathbf{N}K_{n+1,0}^{\times}] \geq 2$. By Gras' formula and Lemma 2.3, $A_{n,1} = \langle \mathrm{cl}(\mathfrak{l}_{n,1}), \mathrm{cl}(\mathfrak{l}'_{n,1})\rangle(2)$. □

Theorem 5.7. *For $p \equiv 7 \mod 16$, we have $A_{n,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $A_{n,0} \cong \mathbb{Z}/2\mathbb{Z}$ for any $n \geq 2$.*

Proof: The extension $K_{\infty,1}/K_{1,1}$ satisfies RamHyp and $\mathrm{Gal}(K_{n+2,1}/K_{n,1})$ is cyclic of order 4 for each $n \geq 1$. By Proposition 3.2, to show $A_{n,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it suffices to show $A_{2,1} \cong A_{3,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let $G_{2,1} = \mathrm{Gal}(K_{2,1}/K_{1,1})$. We have $A_{2,1} = \langle \mathrm{cl}(\mathfrak{l}_{2,1}), \mathrm{cl}(\mathfrak{l}'_{2,1})\rangle(2) = A_{2,1}^{G_{2,1}}$ by Proposition 5.6. Since $h_{1,1}$ is odd, $\mathrm{cl}(\mathfrak{l}_{2,1})^2 = \mathrm{cl}(\mathfrak{l}_{1,1}\mathcal{O}_{2,1})$ has odd order. In other words, $A_{2,1}$ is a quotient of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that

$A_{2,1} = A_{2,1}^{G_{2,1}}$. The product of ramification indices of $K_{2,1}/K_{1,1}$ is 8. By Lemma 5.5 and Chevalley's formula (2.3) for $K_{2,1}/K_{1,1}$, we obtain $|A_{2,1}| = |A_{2,1}^{G_{2,1}}| = 4$. So $A_{2,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

By Proposition 5.6, $A_{3,1} = A_{3,1}^{G_{3,1}}$, where $G_{3,1} = \mathrm{Gal}(K_{3,1}/K_{1,1})$. The product of ramification indices of $K_{3,1}/K_{1,1}$ is 64. By Lemma 5.5 and Chevalley's formula for $K_{3,1}/K_{1,1}$, we get $|A_{3,1}| = |A_{3,1}^{G_{3,1}}| = 4$. Since the norm map from $A_{3,1}$ to $A_{2,1}$ is surjective by Lemma 2.5, we must have $A_{3,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now we compute $A_{n,0}$. Since $K_{n,1}/K_{n,0}$ is ramified at the real places of $K_{n,0}$, the norm map from $A_{n,1}$ to $A_{n,0}$ is surjective by Lemma 2.5. In particular, $A_{n,0}$ is a quotient of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We know that $A_{n,0}$ is cyclic by Proposition 5.6. Since the norm map from $A_{n,0}$ to $A_{2,0} \cong \mathbb{Z}/2\mathbb{Z}$ is surjective, we must have $A_{n,0} \cong \mathbb{Z}/2\mathbb{Z}$ for $n \geq 2$. □

To compute the 2-class group of $K_{1,m}$ for $m \geq 1$, we first note that $K_{1,m}$ is the m-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $K_{1,1}$.

Proposition 5.8. *For $p \equiv 7 \mod 16$, we have $A_{1,m} = \langle \mathrm{cl}(\mathfrak{l}_{1,m})\rangle(2)$ for $m \geq 1$.*

Proof: We first reduce the result to the case $m = 2$. Suppose $A_{1,2} = \langle \mathrm{cl}(\mathfrak{l}_{1,2})\rangle(2)$. Note that $K_{1,\infty}/K_{1,1}$ is totally ramified at $\mathfrak{l}_{1,1}$ and $\mathfrak{l}'_{1,1}$, and unramified outside $\mathfrak{l}_{1,1}$ and $\mathfrak{l}'_{1,1}$. Applying Gras' formula (2.2) to

$$K_{1,2}/K_{1,1}, \quad C_1 = \langle \mathrm{cl}(\mathfrak{l}_{1,2})\rangle, \quad D_1 = \langle \mathfrak{l}_{1,2}\rangle$$

gives

$$[\Lambda_{D_1} : \Lambda_{D_1} \cap \mathbf{N}K_{1,2}^{\times}] = 2.$$

Next we apply Gras' formula to

$$K_{1,3}/K_{1,2}, \quad C_2 = \langle \mathrm{cl}(\mathfrak{l}_{1,3})\rangle, \quad D_2 = \langle \mathfrak{l}_{1,3}\rangle.$$

Note that $\mathbf{N}(C)(2) = A_{1,2}$. To prove $A_{1,3} = C_2$, we need to prove that $[\Lambda_{D_2} : \Lambda_{D_2} \cap \mathbf{N}K_{1,3}^{\times}] = 2$ by Lemma 2.3. Note that $K_{1,2} = K_{1,1}(\sqrt{-i})$ and $K_{1,3} = K_{1,2}(\sqrt{\zeta_8})$. We need to study the following two maps:

$$\rho_1 = \rho_{D_1,K_{1,2}/K_{1,1}} : \Lambda_{D_1} \longrightarrow \mu_2 \times \mu_2$$
$$x \longmapsto \left(\left(\frac{x, -i}{\mathfrak{l}_{1,1}} \right)_2, \left(\frac{x, -i}{\mathfrak{l}'_{1,1}} \right)_2 \right)$$

and

$$\rho_2 = \rho_{D_2,K_{1,3}/K_{1,2}} : \Lambda_{D_2} \longrightarrow \mu_2 \times \mu_2$$
$$x \longmapsto \left(\left(\frac{x, \zeta_8}{\mathfrak{l}_{1,2}} \right)_2, \left(\frac{x, \zeta_8}{\mathfrak{l}'_{1,2}} \right)_2 \right).$$

We have $|\rho_2(\Lambda_2)| = [\Lambda_{D_2} : \Lambda_{D_2} \cap \mathbf{N}K_{1,3}^{\times}] \le 2$ by Lemma 2.8. Note that $\Lambda_{D_1} \subset \Lambda_{D_2}$. By the norm-compatible property of Hilbert symbols, $\left(\frac{x,\zeta_8}{\mathfrak{l}_{1,2}}\right)_2 = \left(\frac{x,-i}{\mathfrak{l}_{1,1}}\right)_2$. So the following diagram is commutative:

$$\begin{array}{ccc} \Lambda_{D_2} & \xrightarrow{\rho_2} & \mu_2 \times \mu_2 \\ \uparrow & \nearrow_{\rho_1} & \\ \Lambda_{D_1} & & \end{array}$$

Thus $2 = |\rho_1(\Lambda_{D_1})| \le |\rho_2(\Lambda_{D_2})| \le 2$ and $[\Lambda_{D_2} : \Lambda_{D_2} \cap \mathbf{N}K_{1,3}^{\times}] = 2$, which implies that $A_{1,3} = \langle \mathrm{cl}(\mathfrak{l}_{1,3})\rangle(2)$ by Lemma 2.3. Repeating this argument, we get $A_{1,m} = \langle \mathrm{cl}(\mathfrak{l}_{1,m})\rangle(2)$ for $m \ge 2$.

Consider the case

$$K/F = K_{1,2}/K_{0,2}, \quad C = \langle \mathrm{cl}(\mathfrak{l}_{1,2})\rangle, \quad D = \langle \mathfrak{l}_{1,2}\rangle.$$

Note that C is a $\mathrm{Gal}(K_{1,2}/K_{0,2})$-submodule of $A_{1,2}$. This can be seen from that, for $\sigma \in \mathrm{Gal}(K_{1,2}/K_{0,2})$, we have $\sigma(\mathfrak{l}_{1,2})\mathfrak{l}_{1,2} = \mathfrak{l}_{0,2}\mathcal{O}_{1,2} = (1-\zeta_8)\mathcal{O}_{1,2}$ and therefore $\sigma(\mathrm{cl}(\mathfrak{l}_{1,2})) = \mathrm{cl}(\mathfrak{l}_{1,2})^{-1}$. If we can show $[\Lambda_D : \Lambda_D \cap \mathbf{N}K_{1,2}^{\times}] = 2$, then by Gras' formula (2.2) and Lemma 2.3, we have $A_{1,2} = \langle \mathrm{cl}(\mathfrak{l}_{1,2})\rangle(2)$.

Note that $\Lambda_D = \langle 1-\zeta_8, \zeta_8, 1+\sqrt{2}\rangle$ and the ramified places in $K_{1,2}/K_{0,2}$ are $\mathfrak{p}_{0,2}$ and $\mathfrak{p}'_{0,2}$, where $\mathfrak{p}_{0,2}\mathfrak{p}'_{0,2} = p\mathcal{O}_{0,2}$. By Lemma 2.8, for the map

$$\begin{aligned} \rho = \rho_{D,K_{1,2}/K_{0,2}} \colon \ &\longrightarrow \Lambda_D \mu_2 \times \mu_2 \\ x &\longmapsto \left(\left(\frac{x,p}{\mathfrak{p}_{0,2}}\right)_2, \left(\frac{x,p}{\mathfrak{p}'_{0,2}}\right)_2 \right), \end{aligned}$$

we have $|\rho(\Lambda_D)| = [\Lambda_D : \Lambda_D \cap \mathbf{N}K_{1,2}^{\times}] \le 2$. To show $|\rho(\Lambda_D)| = 2$, it suffices to show that ρ is not trivial. Let us compute $\rho(1-\zeta_8)$. For $p \equiv 7 \bmod 16$, the conjugate of ζ_8 over $\mathbb{Q}_p$ is ζ_8^{-1}. By the norm-compatible property of Hilbert symbols, we have

$$\begin{aligned} \left(\frac{1-\zeta_8,p}{\mathfrak{p}_{0,2}}\right)_2 = \left(\frac{1-\zeta_8,p}{\mathbb{Q}_p(\zeta_8)}\right)_2 &= \left(\frac{(1-\zeta_8)(1-\zeta_8^{-1}),p}{\mathbb{Q}_p}\right)_2 \\ &= \left(\frac{2+\zeta_8+\zeta_8^{-1},p}{\mathbb{Q}_p}\right)_2. \end{aligned}$$

By Hensel's lemma, we have that

$$\begin{aligned} \left(\frac{2+\zeta_8+\zeta_8^{-1},p}{\mathbb{Q}_p}\right)_2 = 1 &\Leftrightarrow 2+\zeta_8+\zeta_8^{-1} \bmod p \text{ is a square} \\ &\Leftrightarrow 2+\zeta_8+\zeta_8^{-1} \in (\mathbb{Q}_p^{\times})^2. \end{aligned}$$

Notice that $(\zeta_{16}+\zeta_{16}^{-1})^2 = 2+\zeta_8+\zeta_8^{-1}$. Since $p \equiv 7 \bmod 16$, $\mathrm{Frob}_p(\zeta_{16}+\zeta_{16}^{-1}) = \zeta_{16}^7+\zeta_{16}^{-7} = -(\zeta_{16}+\zeta_{16}^{-1})$, where Frob_p is the Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Thus $\zeta_{16}+\zeta_{16}^{-1} \notin \mathbb{Q}_p$ and we have $\left(\frac{1-\zeta_8,p}{\mathfrak{p}_{0,2}}\right)_2 = -1$. □

Theorem 5.9. *For $p \equiv 7 \bmod 16$ and $m \geq 1$, $A_{1,m} \cong \mathbb{Z}/2^{m-1}\mathbb{Z}$.*

Proof: Note that $A_{1,1}$ is trivial and $\mathfrak{l}_{1,m}^{2^{m-1}} = \mathfrak{l}_{1,1}$. We have that $A_{1,m} = \langle \mathrm{cl}(\mathfrak{l}_{1,m})\rangle(2)$ is a quotient of $\mathbb{Z}/2^{m-1}\mathbb{Z}$. Since $h_{1,m} \mid h_{1,m+1}$ by Lemma 2.5, if $|A_{1,m}| < 2^{m-1}$ for some m, we must have $|A_{1,k}| = |A_{1,k+1}|$ for some k. Then $|A_{1,n}| = |A_{1,k}|$ for any $n \geq k$ by Proposition 3.2. But Kida's formula ([**10**, Theorem 1]) shows that the λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{-p})$ is 1. In particular, the 2-class numbers of $\mathbb{Q}(\sqrt{-p}, \zeta_{2^{m+1}}+\zeta_{2^{m+1}}^{-1})$ are unbounded when $m \to \infty$. Thus the 2-class numbers of $\mathbb{Q}(\sqrt{-p}, \zeta_{2^{m+1}}) = K_{1,m}$ are also unbounded by Lemma 2.5. We get a contradiction. □

Proof of Theorem 1.1(3): Theorem 1.1(3) is just the combination of Theorem 5.7 and Theorem 5.9. □

5.3. Congruence property of the relative fundamental unit. We are now ready to prove Theorem 1.2. We assume $p \equiv 7 \bmod 16$ and use the same notations as in §5.2.

To prove this theorem, we need an explicit reciprocity law for a real quadratic field F. We view $F \subset \mathbb{R}$ by fixing an embedding. For a prime ideal $\mathfrak{p}$ with odd norm and $\gamma \in \mathcal{O}_F$ prime to $\mathfrak{p}$, define the Legendre symbol $\left[\frac{\gamma}{\mathfrak{p}}\right] \in \{\pm 1\}$ by the congruence $\left[\frac{\gamma}{\mathfrak{p}}\right] \equiv \gamma^{\frac{\mathbf{N}\mathfrak{p}-1}{2}} \bmod \mathfrak{p}$. For coprime $\gamma, \delta \in \mathcal{O}_F$ with $(2,\delta) = 1$, define $\left[\frac{\gamma}{\delta}\right] := \prod_{\mathfrak{p}\mid\delta}\left[\frac{\gamma}{\mathfrak{p}}\right]^{v_{\mathfrak{p}}(\delta)}$. So by definition $\left[\frac{\gamma}{\delta}\right] = 1$ if $\delta \in \mathcal{O}_F^\times$.

For $\gamma, \delta \in \mathcal{O}_F \setminus \{0\}$, define

$$\{\gamma,\delta\} = (-1)^{\frac{\mathrm{sgn}(\gamma)-1}{2}\cdot\frac{\mathrm{sgn}(\delta)-1}{2}},$$

where $\mathrm{sgn}(x) = 1$ if $x > 0$ and $\mathrm{sgn}(x) = -1$ if $x < 0$. Note that $\{\gamma,\delta_1\}\{\gamma,\delta_2\} = \{\gamma,\delta_1\delta_2\}$.

Theorem 5.10. *Assume that $\gamma_1, \delta_1, \gamma_2, \delta_2 \in \mathcal{O}_F$ have odd norms, γ_1 and δ_1 are coprime, γ_2 and δ_2 are coprime, and $\gamma_1 \equiv \gamma_2, \delta_1 \equiv \delta_2 \bmod 4$. Then*

$$\left[\frac{\gamma_1}{\delta_1}\right]\left[\frac{\delta_1}{\gamma_1}\right]\left[\frac{\gamma_2}{\delta_2}\right]\left[\frac{\delta_2}{\gamma_2}\right] = \{\gamma_1,\delta_1\}\{\gamma_1',\delta_1'\}\{\gamma_2,\delta_2\}\{\gamma_2',\delta_2'\},$$

where ξ' is the conjugate of $\xi \in F$.

Proof: This follows from [**13**, Lemmas 12.12, 12.13, and 12.16] directly. □

Proof of Theorem 1.2: (1) Note that $E_{2,0}/E_{1,0}$ is an abelian group of rank 1. We claim that $E_{2,0}/E_{1,0}$ is torsion-free. Otherwise, there exists $u \in E_{2,0} \setminus E_{1,0}$ such that $u^j \in E_{1,0}$ for some $j \geq 2$. Then $K_{2,0} = K_{1,0}(u)$. The norm of u with respect to the extension $K_{2,0}/K_{1,0}$ is $u\zeta u = \zeta u^2 \in E_{1,0}$ for some $\zeta \in \mu_j \cap K_{2,0}$. So $\zeta = \pm 1$. Thus $u^2 \in E_{1,0}$ and this implies that $K_{2,0}/K_{1,0}$ is unramified at p. This contradicts the fact that $K_{2,0}/K_{1,0}$ is ramified at p. This proves the claim.

Let $\eta \in E_{2,0}$ such that its image in $E_{2,0}/E_{1,0}$ is a generator of $E_{2,0}/E_{1,0}$. Then clearly $E_{2,0} = \langle \eta, \epsilon, -1 \rangle$. By Lemma 5.5, $\epsilon \in \mathbf{N}K_{2,0}^{\times}$. Let $G = \mathrm{Gal}(K_{2,0}/K_{1,0})$. Since $A_{2,0}^G = \langle \mathrm{cl}(\mathfrak{l}_{2,0}) \rangle$ and $\mathfrak{l}_{2,0}$ is a G-invariant fractional ideal, by [**7**, Proposition 1.3.4], $E_{1,0} \cap \mathbf{N}K_{2,0}^{\times} = \mathbf{N}E_{2,0}$ and in particular $\epsilon \in \mathbf{N}E_{2,0}$. Therefore we must have $\mathbf{N}(\pm\eta\epsilon^k) = \epsilon$. Replacing η by $\mathrm{sgn}(\eta)\eta\epsilon^k$, then η is totally positive since ϵ is totally positive, $\mathbf{N}(\eta) = \epsilon$, and $E_{2,0} = \langle \eta, \epsilon, -1 \rangle$.

(2) We first reduce it to the case $\eta' = \eta$. Suppose the result holds for η. For any $\eta' \in E_{2,0}$ such that $\mathbf{N}(\eta') = \epsilon$, we can write $\eta' = \mathrm{sgn}(\eta')\eta^k\epsilon^s$ with $k = 1 - 2s$. Firstly, one can easily see that $\epsilon \equiv \pm 1 \bmod \sqrt{p}$. We claim that $\epsilon \equiv 1 \bmod \sqrt{p}$. Since $\epsilon = \mathbf{N}(\eta) = \eta\overline{\eta}$, we have $\epsilon \equiv \eta\overline{\eta} \equiv \eta^2 \bmod \sqrt[4]{p}$. Therefore, ϵ is a square in $\mathcal{O}_{2,0}/(\sqrt[4]{p}) \cong \mathbb{F}_p$. Because -1 is not a square in $\mathbb{F}_p$, we obtain $\epsilon \equiv 1 \bmod \sqrt{p}$. Then $\eta' \equiv \mathrm{sgn}(\eta')(-1)^k \equiv -\mathrm{sgn}(\eta') \bmod \sqrt[4]{p}$. Write $\eta = \alpha + \beta\sqrt[4]{p}$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$. By the assumption we have $\mathfrak{l} \parallel \alpha$ and $\mathfrak{l} \nmid \beta$. It is easy to check that for odd k, $\mathfrak{l} \parallel \alpha_k$ also, where $\eta^k = \alpha_k + \beta_k\sqrt[4]{p}$ with $\alpha_k, \beta_k \in \mathbb{Z}[\sqrt{p}]$. Thus we have $v_{\mathfrak{l}}(\mathrm{Tr}(\eta')) = v_{\mathfrak{l}}(2\epsilon^s\alpha_k) = v_{\mathfrak{l}}(2\epsilon^s\alpha) = 3$.

From now on we prove the result holds for $\eta = \alpha + \beta\sqrt[4]{p}$. Write $\alpha = a + b\sqrt{p}$ and $\beta = c + d\sqrt{p}$ with $a, b, c, d \in \mathbb{Z}$. Since the infinite place is ramified in $K_{2,0}$, we have $\mathbf{N}_{K_{2,0}/\mathbb{Q}}(\eta) = 1$. Hence $\mathbf{N}_{K_{2,0}/\mathbb{Q}}(\eta) \equiv a^4 \equiv 1 \bmod \sqrt[4]{p}$. Since $p \equiv 7 \bmod 16$, we have $\eta \equiv a \equiv \pm 1 \bmod \sqrt[4]{p}$.

Let $G = \mathrm{Gal}(K_{3,0}/K_{2,0})$. Proposition 5.6 and Theorem 5.7 tell us that $|A_{3,0}| = |A_{3,0}^G| = |A_{2,0}| = 2$. Applying Chevalley's formula (2.3) on $K_{3,0}/K_{2,0}$ gives $[E_{2,0} : \mathbf{N}K_{3,0}^{\times} \cap E_{2,0}] = 4$. This implies $\left(\left(\frac{\eta, \sqrt[4]{p}}{\infty_2}\right), \left(\frac{\eta, \sqrt[4]{p}}{(\sqrt[4]{p})}\right), \left(\frac{\eta, \sqrt[4]{p}}{\mathfrak{l}_{2,0}}\right)\right) \neq (1, 1, 1)$. Therefore $\left(\frac{\eta}{\sqrt[4]{p}}(\sqrt[4]{p})\right) = \left(\frac{\eta}{\sqrt[4]{p}}\mathfrak{l}_{2,0}\right) = -1$ by the total positivity of η and the product formula. Hence η is not a square modulo $\sqrt[4]{p}$ and we must have $\eta \equiv -1 \bmod \sqrt[4]{p}$.

Write $\alpha = \pi^t\alpha_0$ with $\pi \nmid \alpha_0$, and recall that π is the totally positive generator of $\mathfrak{l}$ such that $\epsilon = \frac{\pi^2}{2}$. Now $t = v_{\mathfrak{l}}(\mathrm{Tr}(\frac{\eta}{2})) = v_{\mathfrak{l}}(\mathrm{Tr}(\eta)) - 2$,

so our goal is to prove $t = 1$. Note that α and α_0 are positive. Write $\epsilon = x + y\sqrt{p}$, $\pi = u + v\sqrt{p}$. By Lemma 5.5, u and v are both odd and $v \equiv \pm 1 \bmod 8$. From $\epsilon = \frac{\pi^2}{2}$ and $\mathbf{N}(\pi) = u^2 - pv^2 = 2$, we obtain $8 \parallel x = u^2 - 1 = pv^2 + 1$ and $y \equiv \pm 3 \bmod 8$.

If $y \equiv 3 \bmod 8$, then $\epsilon \equiv -\sqrt{p} \bmod 4$. Take $(\alpha_0, -\sqrt{p}, \alpha_0, \epsilon)$ in Theorem 5.10; since $\alpha_0 > 0$, $\sqrt{p}\epsilon' > 0$, we have

$$\left[\frac{\alpha_0}{-\sqrt{p}}\right]\left[\frac{-\sqrt{p}}{\alpha_0}\right]\left[\frac{\alpha_0}{\epsilon}\right]\left[\frac{\epsilon}{\alpha_0}\right] = \{\alpha_0, -\sqrt{p}\epsilon\}\{\alpha_0', \sqrt{p}\epsilon'\} = 1.$$

Since $\alpha^2 - \sqrt{p}\beta^2 = \epsilon$, we have

$$\left[\frac{\alpha^2 - \sqrt{p}\beta^2}{\alpha_0}\right] = \left[\frac{-\sqrt{p}}{\alpha_0}\right] = \left[\frac{\epsilon}{\alpha_0}\right].$$

By definition, $\left[\frac{\alpha_0}{\epsilon}\right] = 1$. Combine the above two equalities, $\left[\frac{\alpha_0}{-\sqrt{p}}\right] = 1$. By Lemma 5.5, $\left[\frac{\pi}{-\sqrt{p}}\right] = \left(\frac{\pi}{\sqrt{p}}\sqrt{p}\right)_2 = -1$. Thus we have

$$-1 = \left[\frac{\alpha}{-\sqrt{p}}\right] = \left[\frac{\pi}{-\sqrt{p}}\right]^t \left[\frac{\alpha_0}{-\sqrt{p}}\right] = (-1)^t,$$

which means that t is odd in this case.

If $y \equiv -3 \bmod 8$, then $\epsilon^{-1} = x - y\sqrt{p}$ with $-y \equiv 3 \bmod 8$ and $\mathbf{N}(\eta^{-1}) = \epsilon^{-1}$. Repeating the above argument, we obtain that $v_{\mathfrak{l}}\big(\mathrm{Tr}\big(\frac{\eta^{-1}}{2}\big)\big)$ is odd. Let $\bar{\eta} = \alpha - \beta\sqrt[4]{p}$. We have $\mathrm{Tr}(\eta^{-1}) = \mathrm{Tr}(\bar{\eta}\epsilon^{-1}) = \epsilon^{-1}\,\mathrm{Tr}(\bar{\eta}) = \epsilon^{-1}\,\mathrm{Tr}(\eta)$. Therefore $t = v_{\mathfrak{l}}\big(\frac{\mathrm{Tr}(\eta)}{2}\big) = v_{\mathfrak{l}}\big(\frac{\mathrm{Tr}(\eta^{-1})}{2}\big) + v_{\mathfrak{l}}(\epsilon^{-1}) = v_{\mathfrak{l}}\big(\frac{\mathrm{Tr}(\eta^{-1})}{2}\big)$ is also odd.

Finally let us prove $t = 1$. Recall that $\eta = a + b\sqrt{p} + (c + d\sqrt{p})\sqrt[4]{p}$ with $a, b, c, d \in \mathbb{Z}$. Since t is odd, we have $\pi \mid a + b\sqrt{p}$ and $\pi \nmid c + d\sqrt{p}$. Then $c \not\equiv d \bmod 2$. From $\mathbf{N}(\eta) = \epsilon = x + y\sqrt{p}$ we have $a^2 + pb^2 - 2cdp = x$. Assume $t \geq 3$, i.e. $2\pi \mid a + b\sqrt{p}$. We must have $2 \parallel a$ and $2 \parallel b$ or $4 \mid a$ and $4 \mid b$. In both cases, $x \equiv -2cdp \bmod 8$. Since $8 \mid x$, we have $4 \mid cd$. But exactly one of c and d is odd, $y = 2ab - c^2 - pd^2 \equiv d^2 - c^2 \equiv \pm 1 \bmod 8$, which is a contradiction of $y \equiv \pm 3 \bmod 8$. Thus $t = 1$. □

Acknowledgments. The authors thank heartily the anonymous referees for their careful and helpful reports. The authors are partially supported by the Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200), NSFC (Grant No. 11571328). The fourth named author is supported by NSFC (Grant No. 12001510).

References

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

[2] A. Fröhlich and M. J. Taylor, *"Algebraic Number Theory"*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, Cambridge, 1993. DOI: 10.1017/CBO9781139172165.

[3] T. Fukuda, Remarks on $\mathbf{Z}_p$-extensions of number fields, *Proc. Japan Acad. Ser. A Math. Sci.* **70(8)** (1994), 264–266. DOI: 10.3792/pjaa.70.264.

[4] F. Gerth, III, Ranks of 3-class groups of non-Galois cubic fields, *Acta Arith.* **30(4)** (1976), 307–322. DOI: 10.4064/aa-30-4-307-322.

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

[6] G. Gras, Invariant generalized ideal classes—structure theorems for p-class groups in p-extensions, *Proc. Indian Acad. Sci. Math. Sci.* **127(1)** (2017), 1–34. DOI: 10.1007/s12044-016-0324-1.

[7] R. Greenberg, *"Topics in Iwasawa Theory"*. https://sites.math.washington.edu/∼greenber/book.pdf.

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

[9] K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258. DOI: 10.1007/BF03374563.

[10] Y. Kida, On cyclotomic $\mathbf{Z}_2$-extensions of imaginary quadratic fields, *Tohoku Math. J. (2)* **31(1)** (1979), 91–96. DOI: 10.2748/tmj/1178229880.

[11] S. Lang, *"Cyclotomic Fields I and II"*, Combined second edition, With an appendix by Karl Rubin, Graduate Texts in Mathematics **121**, Springer-Verlag, New York, 1990. DOI: 10.1007/978-1-4612-0987-4.

[12] A. Lei, Estimating class numbers over metabelian extensions, *Acta Arith.* **180(4)** (2017), 347–364. DOI: 10.4064/aa170216-27-4.

[13] F. Lemmermeyer, Quadratic reciprocity in number fields (2005). http://www.fen.bilkent.edu.tr/∼franz/rl2/rlb12.pdf.

[14] J. Li and Y. Xu, On class numbers of pure quartic fields, *Ramanujan J.* **56(1)** (2021), 235–248. DOI: 10.1007/s11139-020-00253-2.

[15] J. Li and C.-F. Yu, The Chevalley–Gras formula over global fields, *J. Théor. Nombres Bordeaux* **32(2)** (2020), 525–543. DOI: 10.5802/jtnb.1133.

[16] J. Li and S. Zhang, The 3-class groups of $\mathbb{Q}(\sqrt[3]{p})$ and its normal closure, *Math. Z.* (2021). DOI: 10.1007/s00209-021-02797-5.

[17] P. Monsky, A result of Lemmermeyer on class numbers. Preprint (2010). arXiv:1009.3990.

[18] J. Neukirch, *"Algebraic Number Theory"*, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999. DOI: 10.1007/978-3-662-03983-0.

[19] C. J. Parry, A genus theory for quartic fields, *J. Reine Angew. Math.* **314** (1980), 40–71. DOI: 10.1515/crll.1980.314.40.

[20] L. C. Washington, *"Introduction to Cyclotomic Fields"*, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997. DOI: 10.1007/978-1-4612-1934-7.

[21] H. Weber, Theorie der Abel'schen Zahlkörper, *Acta Math.* **8(1)** (1886), 193–263. DOI: 10.1007/BF02417089.

[22] Z. Zhang and Q. Yue, Fundamental units of real quadratic fields of odd class number, *J. Number Theory* **137** (2014), 122–129. DOI: 10.1016/j.jnt.2013.10.019.

Jianing Li
Research Center for Mathematics and Interdisciplinary Sciences, Shandong University, Qingdao 266237, PR China
E-mail address: lijn@ustc.edu.cn

Yi Ouyang and Yue Xu
CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China
E-mail address: yiouyang@ustc.edu.cn
E-mail address: wasx250@mail.ustc.edu.cn

Shenxing Zhang
School of Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China
E-mail address: zsxqq@mail.ustc.edu.cn

Received on April 21, 2020.
Accepted on September 15, 2020.