On the Class Groups of Certain Real Cyclic Fields of 2-power Degree

By

Humio Ichimura and Hiroki Sumida-Takahashi

Humio Ichimura
Professor Emeritus, Ibaraki University,
Mito, Ibaraki 310-8512, JAPAN
e-mail: humio.ichimura.sci@vc.ibaraki.ac.jp
and
Hiroki Sumida-Takahashi*
Department of Mathematical Sciences,
Tokushima University, Tokushima 770-8506, JAPAN
e-mail: hirokit@tokushima-u.ac.jp

(Received January 6, 2023)

Abstract

Let $e \geq 2$ be a fixed integer, and let $p = 2^{e+1}q + 1$ be an odd prime number with $2 \nmid q$. For $0 \leq n \leq e$, let k_n be the subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ of degree 2^n. For $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with an odd prime number ℓ, we put $L_n = L_0 k_n$. For each $0 \leq n \leq e-1$, we denote by $\mathcal{F}_n$ the quadratic subextension of the $(2,2)$-extension L_{n+1}/k_n with $\mathcal{F}_n \neq L_n$, k_{n+1}. It is a real cyclic field of degree 2^{n+1}. We study the Galois module structure of the 2-parts of the narrow and the ordinary class groups of $\mathcal{F}_n$. This generalizes a classical result of Rédei and Reichardt for the case $n = 0$.

2010 Mathematics Subject Classification. Primary 11R29; Secondary 11R18, 11R23

*The author was partially supported by JSPS KAKENHI Grant Number JP17K05176 and JP20H00115.

1 Introduction

Let $e \geq 2$ be a fixed integer, and let $p = 2^{e+1}q + 1$ be an odd prime number with $2 \nmid q$. For each $0 \leq n \leq e+1$, we denote by k_n the subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ of degree 2^n. We denote by $\mathbb{P}$ the set of prime numbers ℓ satisfying

$$\left(\frac{p}{\ell}\right) = -1 \quad \text{and} \quad \ell \equiv \pm 1 \bmod 8. \tag{1.1}$$

Let $L_0 = \mathbb{Q}(\sqrt{\pm 2})$ or $\mathbb{Q}(\sqrt{\pm 2\ell})$ with $\ell \in \mathbb{P}$, and put $L_n = L_0 k_n$. For each $0 \leq n \leq e$, L_{n+1}/k_n is a $(2,2)$-extension with quadratic subextensions k_{n+1} and L_n. We denote by $\mathcal{F}_n$ the third quadratic subextension of the $(2,2)$-extension L_{n+1}/k_n. It is a cyclic extension over $\mathbb{Q}$ of degree 2^{n+1}. The cyclic field $\mathcal{F}_n$ is real when L_0 is real and $0 \leq n \leq e-1$ or when L_0 is imaginary and $n = e$. It is imaginary otherwise. When $n = 0$, Rédei and Reichardt [11] studied the 2-part of the class group of the quadratic field $\mathcal{F}_0 = \mathbb{Q}(\sqrt{\pm 2p})$ or $\mathbb{Q}(\sqrt{\pm 2p\ell})$. In the previous papers [5, 6], we studied the Galois module structure of the 2-part of the class group of $\mathcal{F}_n$ when $\mathcal{F}_n$ is imaginary, and generalized the classical result on $\mathcal{F}_0$. In this paper, we study the class group of $\mathcal{F}_n$ when $\mathcal{F}_n$ is real. To avoid confusion, we only deal with the case where L_0 is real and $0 \leq n \leq e-1$.

In all what follows, we let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$. Let $\tilde{Cl}_F$ and Cl_F be the ideal class groups of a number field F in the narrow sense and in the ordinary sense, respectively, and let $\tilde{A}_F$ and A_F be the 2-parts of $\tilde{Cl}_F$ and Cl_F, respectively. We put $\tilde{h}_n = |\tilde{Cl}_{\mathcal{F}_n}|$, $h_n = |Cl_{\mathcal{F}_n}|$, $\tilde{A}_n = \tilde{A}_{\mathcal{F}_n}$ and $A_n = A_{\mathcal{F}_n}$. Let $\mathbb{P}_+$ (resp. $\mathbb{P}_-$) be the subset of $\mathbb{P}$ consisting of those $\ell \in \mathbb{P}$ with $\ell \equiv 1 \bmod 8$ (resp. $\ell \equiv -1 \bmod 8$), so that we have $\mathbb{P} = \mathbb{P}_+ \sqcup \mathbb{P}_-$. It is well known that

$$\tilde{A}_0 \cong \begin{cases} \mathbb{Z}/2^j & \text{when } L_0 = \mathbb{Q}(\sqrt{2}), \\ \mathbb{Z}/2 \oplus \mathbb{Z}/2^j & \text{when } L_0 = \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_+, \\ \mathbb{Z}/2 \oplus \mathbb{Z}/2 & \text{when } L_0 = \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_-, \end{cases}$$

for some $j \geq 2$ depending on L_0. This is due to Rédei and Reichardt [11]. There are many other papers and results on the 2-part of class groups of quadratic fields, such as [1, 3, 7, 8, 10, 14, 15]. We generalize the above classical result for $n \geq 1$. We fix a generator γ_n of the cyclic group $\Gamma_n = \mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$ of order 2^{n+1}. Let $R_n = \mathbb{Z}_2[\Gamma_n]$ be the group ring associated to Γ_n over the ring $\mathbb{Z}_2$ of 2-adic integers. Let $\Lambda = \mathbb{Z}_2[[T]]$ be the 2-adic power series ring with an indeterminate T. We identify the group ring $R_n = \mathbb{Z}_2[\Gamma_n]$ with the residue ring $\Lambda/((1+T)^{2^{n+1}} - 1)$ by the correspondence $\gamma_n \leftrightarrow 1 + T$:

$$R_n = \Lambda/((1+T)^{2^{n+1}} - 1). \tag{1.2}$$

The class groups $\tilde{A}_n$ and A_n are naturally regarded as modules over R_n, and hence as modules over Λ. In this paper, we study the structure of these Λ-modules when $0 \leq n \leq e-1$. As in [5, 6], our arguments are based upon the following fact.

Lemma 1.1. *Under the above setting,* $(1+T)^{2^n}+1$ *annihilates the* Λ*-modules* $\tilde{A}_n$ *and* A_n*.*

Let κ_p be the smallest non-negative integer κ such that p splits completely in $\mathbb{Q}(2^{1/2^{e-\kappa+1}})$. It is known that $0 \le \kappa_p \le e$ and that for each i with $0 \le i \le e$, there exist infinitely many prime numbers p of the form $p = 2^{e+1}q + 1$ with $\kappa_p = i$ ([5, Lemma 1]). We put

$$\tilde{f} = e - \kappa_p + 1 \quad \text{and} \quad f = \min\{e, \tilde{f}\}.$$

We have $1 \le f \le e$ as $\kappa_p \le e$. We have $f = \tilde{f}$ when $\kappa_p \ge 1$, and $f = \tilde{f} \le e-1$ if and only if $\kappa_p \ge 2$. In the following, we simply write "$f \le n \le e-1$" when $\kappa_p \ge 2$ and $f \le n \le e-1$. It is also known that the prime number 2 splits completely in $k_{\tilde{f}}$ and that the primes over 2 remain prime in $k_{e+1}/k_{\tilde{f}}$ ([5, Lemma 3]). For a finite abelian group A and an integer $t \ge 1$, let

$$r_{2^t}(A) = \dim_{\mathbb{F}_2}(2^{t-1}A/2^tA)$$

be the 2^t-rank of A, where $\mathbb{F}_2$ is the field of 2 elements. On the 2-rank of the narrow class group $\tilde{A}_n$, the following assertion holds.

Proposition 1.1. *According as* $L_0 = \mathbb{Q}(\sqrt{2})$ *or* $\mathbb{Q}(\sqrt{2\ell})$ *with* $\ell \in \mathbb{P}$*, the* 2*-rank* $r_2(\tilde{A}_n)$ *equals* 2^n *or* $1+2^n$ *for* $0 \le n \le f-1$*, and it equals* 2^f *or* $1+2^f$ *for* $f \le n \le e-1$*.*

Remark 1.1. As the ordinary class group A_n is a quotient of the narrow one $\tilde{A}_n$, we have $r_{2^t}(A_n) \le r_{2^t}(\tilde{A}_n)$ for every n and L_0.

Proposition 1.2. (I) *Let* $L_0 = \mathbb{Q}(\sqrt{2})$*. The* Λ*-modules* $\tilde{A}_n$ *and its quotient* A_n *are cyclic.*

(II) *The case* $L_0 = \mathbb{Q}(\sqrt{2\ell})$ *with* $\ell \in \mathbb{P}$*. The* Λ*-module* $\tilde{A}_n$ *is isomorphic to* $\Lambda/(2,T) \oplus \tilde{B}_n$ *for some cyclic* Λ*-module* $\tilde{B}_n$*. Further, when* $\ell \in \mathbb{P}_+$*,* A_n *is isomorphic to* $\Lambda/(2,T) \oplus B_n$ *for some cyclic* Λ*-module* B_n*, which is a quotient of the* Λ*-module* $\tilde{B}_n$*.*

Let A be a finite cyclic Λ-module which is annihilated by $(1+T)^{2^n}+1$. Then, we see that $r_2(A) \le 2^n$ since the quotient $\Lambda/((1+T)^{2^n}+1)$ is isomorphic to $\mathbb{Z}_2^{\oplus 2^n}$ as an abelian group. When $r_2(A) = 2^n$ (and hence $\mathrm{ord}_2(|A|) \ge 2^n$), we put

$$s_n(A) = \left\lceil \frac{\mathrm{ord}_2(|A|)}{2^n} \right\rceil,$$

and

$$a_n(A) = 2^n s_n(A) - \mathrm{ord}_2(|A|), \quad b_n(A) = 2^n - a_n(A).$$

Here, $\lceil x \rceil$ denotes the smallest integer $\ge x$, and $\mathrm{ord}_2(*)$ the 2-adic additive valuation on $\mathbb{Q}$ with $\mathrm{ord}_2(2) = 1$. Then, we have $s_n(A) \ge 1$, $a_n(A) \ge 0$ and $b_n(A) \ge 1$. Further, we define an ideal $\Theta_n(A)$ of Λ by

$$\Theta_n(A) = \left(2^{s_n(A)},\, 2^{s_n(A)-1}T^{b_n(A)},\, (1+T)^{2^n}+1\right).$$

Note that the integers $s_n(A)$, $a_n(A)$, $b_n(A)$ and the ideal $\Theta_n(A)$ depend only on the cardinality $|A|$. We see that

$$\Lambda/\Theta_n(A) \cong (\mathbb{Z}/2^{s_n(A)-1})^{\oplus a_n(A)} \oplus (\mathbb{Z}/2^{s_n(A)})^{\oplus b_n(A)} \tag{1.3}$$

as abelian groups. For a cyclic Λ-module A, the following holds.

Proposition 1.3. *Let A be a finite cyclic Λ-module which is annihilated by $(1+T)^{2^n}+1$. Then,*

$$A \cong \begin{cases} \Lambda/\Theta_n(A) & \text{when } r_2(A) = 2^n \\ \Lambda/(2, T^{r_2(A)}) & \text{when } r_2(A) < 2^n \text{ or } r_4(A) = 0 \end{cases}$$

as Λ-modules.

Because of the above results, we can determine the Λ-module structures of $\tilde{A}_n$ and A_n once we know the (2-parts of the) class numbers $\tilde{h}_n$ and h_n of $\mathcal{F}_n$, respectively.

Now, we shall write down several results first on the narrow class group $\tilde{A}_n$ and next on the ordinary one A_n. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$, $\tilde{B}_n$ (resp. B_n) denotes the cyclic Λ-submodule of $\tilde{A}_n$ (resp. A_n) in Proposition 1.2. We have $r_4(\tilde{B}_n) = r_4(\tilde{A}_n)$ and $r_4(B_n) = r_4(A_n)$ by Proposition 1.2.

Proposition 1.4. *When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_-$, $r_4(\tilde{A}_n) = r_4(A_n) = 0$.*

From Propositions 1.1–1.4, we obtain the following:

Corollary 1.1. *When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_-$, the Λ-module $\tilde{B}_n$ is isomorphic to $\Lambda/(2, T^{2^n})$ or $\Lambda/(2, T^{2^f})$ according as $0 \le n \le f-1$ or $f \le n \le e-1$.*

In view of Corollary 1.1, we let $\ell \in \mathbb{P}_+$.

Proposition 1.5. *Let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. For $0 \le n \le e-1$, $r_4(\tilde{A}_n) \ge 1$ if and only if $0 \le n \le f-1$.*

From Propositions 1.1–1.3 and 1.5, we obtain the following:

Corollary 1.2. *Let $f \le n \le e-1$. According as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, the Λ-module $\tilde{A}_n$ or $\tilde{B}_n$ is isomorphic to $\Lambda/(2, T^{2^f})$.*

In view of Corollaries 1.1 and 1.2, we let $0 \le n \le f-1$ and $\ell \in \mathbb{P}_+$. We already know that $r_4(\tilde{A}_n) \ge 1$ by Proposition 1.5. The following assertion gives a relation between the 4 and 8-ranks of the class groups $\tilde{A}_n$.

Proposition 1.6. *Let $L_0 = \mathbb{Q}(\sqrt{2})$. For $0 \le n \le f-2$, we have $r_8(\tilde{A}_n) \ge 1$ if and only if $r_4(\tilde{A}_{n+1}) \ge 2^n + 1$.*

Let $L_0 = \mathbb{Q}(\sqrt{2})$. When there exists an integer $0 \le m \le f-1$ with $r_8(\tilde{A}_m) = 0$, let m_p be the smallest such integer and put $b_p = r_4(\tilde{A}_{m_p})$. Then, it follows from Propositions 1.1 and 1.6 that

$$2^{m_p-1} + 1 \le b_p \le 2^{m_p} \ \text{if } m_p \ge 1, \quad \text{and} \quad b_p = 1 \ \text{if } m_p = 0. \tag{1.4}$$

When $r_8(\tilde{A}_m) \ge 1$ for all $0 \le m \le f-1$, we simply put $m_p = \infty$. Thus, the condition $m_p < \infty$ means $0 \le m_p \le f-1$. In general, when $0 \le n \le f-1$, the submodule $\tilde{B}_n$ of $\tilde{A}_n$ depends on ℓ. However, there are cases where it does not depend on ℓ.

Theorem 1.1. *When the base field L_0 moves over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, the following assertions hold.*

(I) *For $0 \le n \le f-1$, the 4-rank $r_4(\tilde{A}_n)$ depends only on n and not on individual L_0's.*

(II) *Assume that $m_p < \infty$.*

  (II-i) *Let $0 \le n \le m_p - 1$. Then, $r_4(\tilde{A}_n) = 2^n$ and $r_8(\tilde{A}_n) \ge 1$ when $L_0 = \mathbb{Q}(\sqrt{2})$, and $r_4(\tilde{B}_n) = 2^n$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$.*

  (II-ii) *Let $m_p \le n \le f-1$. Put $\Theta_n = (4, 2T^{b_p}, (1+T)^{2^n} + 1)$. Then, the Λ-module $\tilde{A}_n$ is isomorphic to Λ/Θ_n when $L_0 = \mathbb{Q}(\sqrt{2})$, and $\tilde{B}_n$ is isomorphic to Λ/Θ_n and* **independent** *of ℓ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$ and $(n, b_p) \ne (m_p, 2^{m_p})$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ and $b_p = 2^{m_p}$, we only have $r_4(\tilde{B}_{m_p}) = 2^{m_p}$.*

(III) *Assume that $m_p = \infty$. Then, for each $0 \le n \le f-1$, $r_4(\tilde{A}_n) = 2^n$ and $r_8(\tilde{A}_n) \ge 1$ when $L_0 = \mathbb{Q}(\sqrt{2})$, and $r_4(\tilde{B}_n) = 2^n$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$.*

Next, let us write down our results on the ordinary class group A_n.

Proposition 1.7. *When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_-$, $A_n \cong \mathbb{Z}/2$ for every $0 \le n \le e-1$.*

In view of this proposition, we let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. Let $L_0 = \mathbb{Q}(\sqrt{2})$. By Proposition 1.5 (and Remark 1.1), we already know that $r_4(A_n) = 0$ for $f \le n \le e-1$. When there exists an integer $0 \le n \le f-1$ with $r_4(A_n) = 0$, let n_p be the smallest such integer and put $c_p = r_2(A_{n_p})$. When $r_4(A_n) \ge 1$ for all $0 \le n \le f-1$, we put $n_p = \infty$. Then, the condition $n_p < \infty$ means $0 \le n_p \le f-1$. When $n_p = \infty$ and $f \le e-1$ (or equivalently $\kappa_p \ge 2$), we put $d_p = r_2(A_f)$. When $n_p = \infty$ and $f = e$ (or equivalently, $\kappa_p = 0$, 1), we do not define d_p. The following two assertions are analogous to the assertion (1.4) and Theorem 1.1 for the narrow class group $\tilde{A}_n$.

Proposition 1.8. *When $n_p < \infty$, we have*

$$2^{n_p-1} + 1 \le c_p \le 2^{n_p} \quad \textit{if } n_p \ge 1, \quad \textit{and} \quad c_p = 1 \quad \textit{if } n_p = 0. \tag{1.5}$$

When $n_p = \infty$ and $f \le e-1$, we have

$$2^{f-1} + 1 \le d_p \le 2^f. \tag{1.6}$$

Theorem 1.2. *When the base field L_0 moves over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, the following assertions hold.*

(I) *Let $0 \le n \le e-1$. The 2-rank $r_2(A_n)$ for $L_0 = \mathbb{Q}(\sqrt{2})$ and $r_2(B_n)$ for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ depend only on n and not on individual L_0's.*

(II) *Assume that $n_p < \infty$.*

- (II-i) *Let $0 \le n \le n_p - 1$. Then, $r_2(A_n) = 2^n$ and $r_4(A_n) \ge 1$ when $L_0 = \mathbb{Q}(\sqrt{2})$, and $r_2(B_n) = 2^n$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$.*
- (II-ii) *Let $n_p \le n \le e-1$. Then, the Λ-module A_n is isomorphic to $\Lambda/(2, T^{c_p})$ when $L_0 = \mathbb{Q}(\sqrt{2})$, and B_n is isomorphic to $\Lambda/(2, T^{c_p})$ and* **independent** *of ℓ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$ and $(n, c_p) \ne (n_p, 2^{n_p})$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ and $c_p = 2^{n_p}$, we only have $r_2(B_{n_p}) = c_p$.*

(III) *Assume that $n_p = \infty$.*

- (III-i) *Let $0 \le n \le f-1$. Then, $r_2(A_n) = 2^n$ and $r_4(A_n) \ge 1$ when $L_0 = \mathbb{Q}(\sqrt{2})$, and $r_2(B_n) = 2^n$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$.*
- (III-ii) *Let $f \le n \le e-1$. The Λ-module A_n or B_n is isomorphic to $\Lambda/(2, T^{d_p})$ according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$.*

This paper is organized as follows. In Section 2, we give some related results and remarks. In Section 3, we give several lemmas which are necessary to show our results. Proposition 1.3 is shown in Section 3. In Section 4, we introduce several submodules of $k_n^\times/(k_n^\times)^2$ which play important roles for showing the results. In Section 5, we construct the class fields of $\mathcal{F}_n$ corresponding to $\tilde{A}_n/\tilde{A}_n^2$ and A_n/A_n^2, respectively. Lemma 1.1 and Propositions 1.1, 1.2 are shown in Section 5. In Section 6, we prove Theorems 1.1, 1.2 and Propositions 1.4–1.8. In Section 7, we give several numerical examples mainly related to Theorems 1.1 and 1.2.

2 Related results and remarks

In this section, we give some related results and remarks. First, we show the following simple assertion on the invariants m_p and n_p.

Lemma 2.1. *We have $n_p \geq m_p$.*

Proof. Let L/F be a cyclic extension of degree 8 unramified at all finite prime divisors. Then, the quartic subextension N/F is everywhere unramified (including the infinite ones). Therefore, it follows that $r_4(A_F) \geq r_8(\tilde{A}_F)$. From this, we obtain the assertion. □

In [10], Morton studied the narrow class number $\tilde{h}_0$ and the fundamental unit of the real quadratic field $\mathcal{F}_0 = \mathbb{Q}(\sqrt{2p})$ (associated to $L_0 = \mathbb{Q}(\sqrt{2})$). We already know that $4|\tilde{h}_0$ by [11]. From Lemma 2.1, we see that $m_p = 0$ if $n_p = 0$, and that $n_p \geq m_p \geq 1$ if $8|\tilde{h}_0$. The following assertion is essentially due to Morton.

Proposition 2.1. (i) *We have $8|\tilde{h}_0$ (or equivalently, $m_p \geq 1$) if and only if $e \geq 3$ and $f \geq 2$.*

(ii) *When $e = f = 2$, we have $n_p = 0$ and $c_p = 1$.*

(iii) *When $e = 2$ and $f = 1$, we have $n_p = \infty$ and $d_p = 2$.*

(iv) *When $e \geq 3$ and $f = 1$, we have $n_p = 0$ and $c_p = 1$.*

Proof. The first assertion (i) is nothing but [10, Theorem 3]. For showing (ii) and (iv), let us assume that $e = f = 2$ or that $e \geq 3$ and $f = 1$. Then, by (i), we have $4\|\tilde{h}_0$. Let ϵ be the fundamental unit of $\mathcal{F}_0 = \mathbb{Q}(\sqrt{2p})$. By [10, Theorem 5], we have $N\epsilon = 1$. Therefore, we obtain $2\|h_0$. This implies that $n_p = 0$, and hence $c_p = 1$ by (1.5). Next, for showing (iii), assume that $e = 2$ and $f = 1$. Then, we have $4\|\tilde{h}_0$ by (i), and $N\epsilon = -1$ by [10, Theorem 5]. Hence, it follows that $4\|h_0$. This implies $n_p = \infty$, and hence $d_p = 2$ by (1.6). □

The following assertion is an immediate consequence of Theorems 1.1, 1.2 and Proposition 2.1.

Proposition 2.2. *Let $L_0 = \mathbb{Q}(\sqrt{2})$, and assume that $e \geq 3$ and $f \geq 2$.*

(i) *Assume further that $r_8(\tilde{A}_1) = 0$. Then the abelian group $\tilde{A}_n$ is isomorphic to $(\mathbb{Z}/2)^{\oplus(2^n-2)} \oplus (\mathbb{Z}/4)^{\oplus 2}$ for $1 \leq n \leq f-1$.*

(ii) *Assume further that $r_4(A_1) = 0$. Then the abelian group A_n is isomorphic to $(\mathbb{Z}/2)^{\oplus 2}$ for $1 \leq n \leq e-1$.*

Proof. As $e \geq 3$ and $f \geq 2$, we have $r_8(\tilde{A}_0) = 1$ by Proposition 2.1(i). Therefore, if $r_8(\tilde{A}_1) = 0$, then we have $m_p = 1$, and hence $b_p = 2$ by (1.4). Thus, we obtain the assertion (i) from Theorem 1.1(II-ii) and (1.3). We have $r_4(A_0) = 1$ as $r_8(\tilde{A}_0) = 1$. Therefore, if $r_4(A_1) = 0$, then we have $n_p = 1$, and hence $c_p = 2$ by (1.5). Thus, we obtain the assertion (ii) from Theorem 1.2(II-ii). □

Remark 2.1. (I) As we will see in Section 7, there are several examples with $n_p = m_p$ or $n_p = m_p + 1$ when $n_p < \infty$. However, we have at present no example with $m_p + 2 \le n_p < \infty$.

(II) Let $p = 2593$, 4513 or 7489. Then, by Table 3 in Section 7, we see that $f = 4$ and that $r_8(\tilde{A}_1) = 0$ and $r_4(A_1) = 0$ for $L_0 = \mathbb{Q}(\sqrt{2})$. Hence, these p satisfy the assumptions in Proposition 2.2.

Remark 2.2. (I) When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, it is shown that $r_8(\tilde{A}_0) = 1$ if and only if $p \equiv \ell \bmod 16$ and $\left(\dfrac{2}{p\ell}\right)_4 = 1$ by Zhang and Yue [15, Corollary 2].

(II) In Theorem 1.1(II-ii), the group $\tilde{B}_{m_p}$ for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ depends on ℓ when $b_p = 2^{m_p}$. Let us give some example. Let $e = 2$ or $f = 1$, so that $m_p = 0$ and $b_p = 1 = 2^{m_p}$ by Proposition 2.1(i) and (1.4). The above mentioned result [15, Corollary 2] tells us how $r_8(\tilde{B}_0)$ depends on ℓ for such a case. For example, let $p = 73$. Then, $e = 2$, $\kappa_p = 0$ and $f = 2$. Further $\tilde{A}_0 \cong \mathbb{Z}/4$ for $L_0 = \mathbb{Q}(\sqrt{2})$ and $m_p = 0$. The group $\tilde{B}_0$ for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ is isomorphic to $\mathbb{Z}/2$ when $\ell = 113$, 313; to $\mathbb{Z}/4$ when $\ell = 17$, 193; to $\mathbb{Z}/8$ when $\ell = 41$, 89; to $\mathbb{Z}/16$ when $\ell = 97$, 601; to $\mathbb{Z}/32$ when $\ell = 641$. These are found in the table of Wada [12] on class numbers of real quadratic fields.

(III) In Theorem 1.2(II-ii), the group B_{n_p} for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ depends on ℓ when $c_p = 2^{n_p}$. For example, let $p = 73$ as above. Then, we have $A_0 \cong \mathbb{Z}/2$ for $L_0 = \mathbb{Q}(\sqrt{2})$, and $n_p = 0$ and $c_p = 1 = 2^{n_p}$. From the table [12], we find that B_0 is isomorphic to $\mathbb{Z}/2$ when $\ell = 113$, 313; to $\mathbb{Z}/4$ when $\ell = 17$, 41; to $\mathbb{Z}/8$ when $\ell = 97$, 401; to $\mathbb{Z}/16$ when $\ell = 601$, 641.

(IV) Several related examples are given in Section 7.

Remark 2.3. Let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. Then, we see from Proposition 1.5 that $r_4(\tilde{A}_n) \ge 1$ if and only if p splits completely in $\mathbb{Q}(2^{1/2^{n+1}})$ similarly to [6, Remark 2.4]. Thus, we can say that $\mathbb{Q}(2^{1/2^{n+1}})$ is a "governing field" for the 4-rank of $\tilde{A}_n$ to be positive.

3 Several lemmas

In this section, we collect several general lemmas, which are necessary to prove our results. We also show Proposition 1.3 on a finite cyclic Λ-module at the end of this section.

For a number field F, let $\mathcal{O}_F$ be the ring of integers and $E_F = \mathcal{O}_F^\times$ the group of units of F. The following lemma is shown in [5, Lemma 6].

Lemma 3.1. *Let F be a real abelian field of degree n. Assume that the narrow class number $\tilde{h}_F$ is odd and that the prime number 2 splits completely in F; $(2) = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Then, the map*

$$E_F \longrightarrow (O_F/4)^\times = (\mathcal{O}_F/\mathfrak{q}_1^2)^\times \oplus \cdots \oplus (\mathcal{O}_F/\mathfrak{q}_n^2)^\times;\ \epsilon \to \epsilon \bmod 4$$

is surjective.

The following lemma is well known (Washington [13, Exercise 9.3]).

Lemma 3.2. *Let F be a number field. Let $\mathfrak{q}$ be a prime ideal of F over 2, and let $a \geq 1$ be an integer with $\mathfrak{q}^a \| 2$. Let $K = F(\sqrt{w})$ be a quadratic extension over F with $w \in F^\times$ relatively prime to $\mathfrak{q}$. Then,* (i) *the prime ideal $\mathfrak{q}$ is unramified in K if and only if $w \equiv u^2 \bmod \mathfrak{q}^{2a}$ for some $u \in \mathcal{O}_F$, and* (ii) *it splits in K if and only if $w \equiv u^2 \bmod \mathfrak{q}^{2a+1}$ for some $u \in \mathcal{O}_F$. In particular, when $\mathfrak{q}$ is unramified over $\mathbb{Q}$ ($a = 1$) and its degree is one,* (i') *$\mathfrak{q}$ is unramified in K if and only if $w \equiv 1 \bmod \mathfrak{q}^2$, and* (ii') *it splits in K if and only if $w \equiv 1 \bmod \mathfrak{q}^3$.*

For an integer $s \geq 1$, C_{2^s} denotes a cyclic group of order 2^s. We call a cyclic extension of degree 2^s over a number field simply as a C_{2^s}-extension. For a finite abelian group A, let ${}_2A$ be the subgroup of A consisting of elements $a \in A$ with $a^2 = 1_A$, where 1_A is the identity element of A.

We say that an extension K/F is "narrowly unramified" when it is unramified at all finite prime divisors, and that it is "unramified" when it is unramified at all prime divisors including the infinite ones. Let $\tilde{\mathcal{M}}_F/F$ and $\mathcal{M}_F/F$ be the class fields corresponding to the class groups $\tilde{A}_F$ and A_F of F, respectively. Then, we have the following identifications via the reciprocity law map:

$$\mathrm{Gal}(\tilde{\mathcal{M}}_F/F) = \tilde{A}_F : \tilde{\rho}_c \leftrightarrow c, \quad \text{and} \quad \mathrm{Gal}(\mathcal{M}_F/F) = A_F : \rho_c \leftrightarrow c.$$

Here, $\tilde{\rho}_c$ (resp. ρ_c) is the Frobenius automorphism on $\tilde{\mathcal{M}}_F$ (resp. $\mathcal{M}_F$) associated to a narrow (resp. an ordinary) ideal class c. The following lemma has its origin in [11] and was repeatedly used in the study of 4, 8 and 16-ranks of class groups of quadratic fields, and it is an immediate consequence of class field theory. For a proof, see [6, Lemma 3.3].

Lemma 3.3. (I) *An unramified C_{2^s}-extension K/F extends to an unramified $C_{2^{s+1}}$-extension if and only if* (i) *ρ_c acts trivially on K for every $c \in {}_2A_F$.*

(II) *A narrowly unramified C_{2^s}-extension K/F extends to a narrowly unramified $C_{2^{s+1}}$-extension if and only if* (ii) *$\tilde{\rho}_c$ acts trivially on K for every $c \in {}_2\tilde{A}_F$.*

Remark 3.1. Let $\wp_i$ ($1 \leq i \leq r$) be some prime ideals of F, and let h be an odd integer. When ${}_2A_F$ is generated by the ordinary classes $[\wp_i^h]$, the condition (i) in Lemma 3.3 holds if and only if the prime ideals $\wp_i$ split completely in K. When the base field F is totally real and ${}_2\tilde{A}_F$ is generated by the narrow classes $[\wp_i^h]$ and $[(x)]$ for all $x \in F^\times$, the condition (ii) in Lemma 3.3 holds if and only if K is totally real and the prime ideals $\wp_i$ split completely in K.

The following lemma is an exercise in Galois theory, and is quite easy to show.

Lemma 3.4. *Let K/F be a quadratic extension, and let σ be the nontrivial automorphism of K/F. Let $N = K(\sqrt{\alpha})/K$ be a quadratic extension with $\alpha \in K^\times \setminus (K^\times)^2$. The extension N is Galois over F if and only if $\alpha^{1+\sigma} = a^2$ for some $a \in K^\times$. Further, N/F is a C_4-extension if and only if $a^{1-\sigma} = -1$, and it is a $(2,2)$-extension if and only if $a \in F^\times$.*

Lemma 3.5. *Let K/F be a narrowly unramified quadratic extension, and let $N = K(\sqrt{\alpha})/F$ be a narrowly unramified C_4-extension with $\alpha \in K^\times$. Then, every narrowly unramified C_4-extension over F containing K is given by the form $K(\sqrt{\alpha c})$ with some $c \in F^\times$ for which $F(\sqrt{c})/F$ is narrowly unramified.*

Proof. Let $K(\sqrt{\beta})/F$ with $\beta \in K^\times$ be another narrowly unramified C_4-extension containing K. Then, we see from Lemma 3.4 that $\alpha^{1+\sigma} = a^2$ and $\beta^{1+\sigma} = b^2$ for some a, $b \in K^\times$ such that $a^{1-\sigma} = b^{1-\sigma} = -1$. Thus, $(\alpha\beta)^{1+\sigma} = (ab)^2$ with $(ab)^{1-\sigma} = 1$. It follows from Lemma 3.4 that $K(\sqrt{\alpha\beta}) = K(\sqrt{c})$ for some $c \in F^\times$. Therefore, we see that $K(\sqrt{\beta}) = K(\sqrt{\alpha c})$ and that the extension $F(\sqrt{c})/F$ is narrowly unramified as $F(\sqrt{c}) \subseteq K(\sqrt{\alpha}, \sqrt{\beta})$. □

Let $G = \langle \rho \rangle$ be a cyclic group of order 2^f, and let $\mathcal{R} = \mathbb{F}_2[G]$. For $0 \le i \le 2^f$, let U_i be the principal ideal of $\mathcal{R}$ generated by $(1+\rho)^i$. Then, we have a filtration

$$U_0 = \mathcal{R} \supset U_1 \supset \cdots \supset U_{2^f-1} \supset U_{2^f} = \{0\}.$$

For $0 \le n \le f$, let

$$N_{f/n} = \sum_{j=0}^{2^{f-n}-1} (\rho^{2^n})^j = (1+\rho)^{2^f - 2^n} \tag{3.1}$$

be a norm element in $\mathcal{R}$. Here, the second equality is shown in the proof of [6, Lemma 4.3]. Let $J_n = (N_{f/n})$ be the ideal of $\mathcal{R}$ generated by $N_{f/n}$. On these ideals, we showed in [6, Lemma 4.3], the following:

Lemma 3.6 ([6])**.** (I) *The ideals U_i are all the ideals of $\mathcal{R}$, and* $\dim_{\mathbb{F}_2} U_i = 2^f - i$*. In particular, the ideals of $\mathcal{R}$ are parametrized by their dimensions over $\mathbb{F}_2$.*

(II) *For $0 \le n \le f$, $J_n = U_{2^f - 2^n}$ and hence $J_0 = U_{2^f-1}$ is the smallest nontrivial ideal of $\mathcal{R}$.*

In the later sections, we use this lemma for the cyclic Galois group $G = G_f = \mathrm{Gal}(k_f/\mathbb{Q})$ of order 2^f.

Remark 3.2. For ideals I and J of $\mathcal{R}$, Lemma 3.6(I) implies that $I \cap J \subsetneq J$ if and only if $I \subsetneq J$.

Proof of Proposition 1.3. When $r_2(A) = 2^n$ and $r_4(A) \ge 1$, the assertion is already shown in [6, Lemma 3.5]. So it suffices to show the assertion when

$r_2(A) = 2^n$ and $r_4(A) = 0$ and when $r_2(A) < 2^n$.

First, let $r_2(A) = 2^n$ and $r_4(A) = 0$. Then, $A \cong \Lambda/(2, T^{2^n})$ as A is cyclic over Λ. On the other hand, we observe that $s_n(A) = 1$, $a_n(A) = 0$, $b_n(A) = 2^n$ from the assumptions, and hence $\Theta_n(A) = (2, T^{2^n}) = (2, T^{r_2(A)})$. Therefore, we obtain the assertion under this setting.

Next, let $r = r_2(A) < 2^n$. It suffices to show that $r_4(A) = 0$. Assume to the contrary that $r_4(A) \geq 1$. We can write

$$A = \bigoplus_{i=1}^{s} (\mathbb{Z}/2^i)^{\oplus t_i}$$

as abelian groups for some integers $s \geq 1$, $t_i \geq 0$ $(1 \leq i \leq s-1)$ and $t_s \geq 1$. As $r_2(A) = r$, we have

$$\sum_{i=1}^{s} t_i = r \quad \text{and} \quad \sum_{i=1}^{s} i t_i = \mathrm{ord}_2(|A|). \tag{3.2}$$

The assumption $r_4(A) \geq 1$ means that $\mathrm{ord}_2(|A|) \geq r + 1$. Then, it follows that $s \geq 2$. Put $B = A^{2^{s-2}}$. Then, B is a cyclic Λ-module annihilated by $(1+T)^{2^n} + 1$ and it is isomorphic to

$$(\mathbb{Z}/2)^{\oplus t_{s-1}} \oplus (\mathbb{Z}/4)^{\oplus t_s} \quad \text{with} \quad t_s \geq 1$$

as an abelian group. From these conditions on B, we see that $t_{s-1} + t_s = 2^n$ immediately from [5, Proposition 3]. Then it follows from (3.2) that $r \geq 2^n$, a contradiction. Thus we have shown $r_4(A) = 0$. □

4 Submodules of $k_n^\times/(k_n^\times)^2$

We use the same notation as in Sections 1 and 2. In particular, $p = 2^{e+1}q + 1$ is a prime number with $e \geq 2$ and $2 \nmid q$, and k_n $(0 \leq n \leq e+1)$ is the subfield of $\mathbb{Q}(\zeta_p)$ of degree 2^n. In this section, we introduce submodules $\tilde{V}_n$, V_n and Q_n of $k_n^\times/(k_n^\times)^2$, which play important roles in the proofs of our results. In all what follows, we let

$$h = \tilde{h}_{k_e}$$

be the narrow class number of k_e. By Conner and Hurrelbrink [2, Corollary 12.9], h is odd and hence it coincides with the ordinary class number of k_e. The narrow class number $\tilde{h}_{k_n}$ of k_n $(0 \leq n \leq e)$ is a divisor of h as $k_e/\mathbb{Q}$ is totally ramified at p, and hence it is odd. Let $\mathfrak{p}_n$ be the unique prime ideal of k_n over p, so that we have $(p) = \mathfrak{p}_n^{2^n}$ in k_n. For each $0 \leq n \leq e$, there exists an element δ_n of k_n such that $k_{n+1} = k_n(\sqrt{\delta_n})$. The element δ_n is totally positive when $0 \leq n \leq e-1$, and it is totally negative when $n = e$. Since k_{n+1}/k_n is ramified only at $\mathfrak{p}_n$ and h is odd, we can choose the element δ_n so that

$$(\delta_n) = \mathfrak{p}_n^h \quad \text{and} \quad \delta_n \equiv u^2 \bmod 4 \tag{4.1}$$

for some $u \in \mathcal{O}_{k_n}$. Here, the congruence holds by Lemma 3.2(i). Further, since 2 splits completely in $k_{\tilde{f}}/\mathbb{Q}$ and the primes over 2 remain prime in $k_{e+1}/k_{\tilde{f}}$ ([5, Lemma 3]), we see from Lemma 3.2(ii), (ii') that

$$\delta_n \equiv 1 \bmod 8 \quad \text{when } 0 \le n \le \tilde{f} - 1 \tag{4.2}$$

but

$$\delta_n \not\equiv u^2 \bmod 8 \text{ for any } u \in \mathcal{O}_{k_n} \quad \text{when } \tilde{f} \le n \le e. \tag{4.3}$$

We see that

$$\mathcal{F}_n = k_n(\sqrt{2\delta_n}) \quad \text{or} \quad k_n(\sqrt{2\ell\delta_n}) \tag{4.4}$$

according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$.

We put $G_n = \mathrm{Gal}(k_n/\mathbb{Q})$, which is a cyclic group of order 2^n. Let $\mathfrak{q}_f$ be a fixed prime ideal of k_f over 2, and set $\mathfrak{q}_n = N_{f/n}\mathfrak{q}_f$ for $0 \le n \le f-1$, where $N_{f/n}$ is the norm map from k_f to k_n. Then, since 2 splits completely in k_f ([5, Lemma 3]), $\mathfrak{q}_n$ is a prime ideal of k_n over 2 and

$$(2) = \prod_{\sigma \in G_n} \mathfrak{q}_n^{\sigma}.$$

When ($\kappa_p \ge 2$ and) $f \le n \le e-1$, the prime ideals over 2 remain prime in k_n/k_f by [5, Lemma 3]. We denote the unique prime ideal of k_n over $\mathfrak{q}_f^{\sigma}$ ($\sigma \in G_f$) by $\mathfrak{q}_n^{\sigma}$; $\mathfrak{q}_f^{\sigma} = \mathfrak{q}_n^{\sigma}$ in k_n. In the following, we choose and fix a prime number $\ell \in \mathbb{P}$. We put

$$2^* = \begin{cases} 2 & \text{when } L_0 = \mathbb{Q}(\sqrt{2}) \text{ or } \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_+ \\ -2 & \text{when } L_0 = \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_-, \end{cases}$$

and

$$\ell^* = \begin{cases} \ell & \text{when } L_0 = \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_+ \\ -\ell & \text{when } L_0 = \mathbb{Q}(\sqrt{2\ell}) \text{ with } \ell \in \mathbb{P}_-. \end{cases}$$

Then, by (1.1), we have

$$2^*\ell^* = 2\ell, \quad \ell^* \equiv 1 \bmod 8, \quad \text{and} \quad \left(\frac{\ell^*}{p}\right) = -1 \tag{4.5}$$

for every $\ell \in \mathbb{P}$.

Recall that the narrow class number $h = \tilde{h}_{k_e}$ of k_e is odd and hence that of k_f is also odd. Then, by virtue of Lemma 3.1, we can choose an element ω of k_f such that $\mathfrak{q}_f^h = (\omega)$ and

$$\frac{\omega}{(2^*)^h} \equiv 1 \bmod \mathfrak{q}_f^2 \quad \text{and} \quad \omega \equiv 1 \bmod (\mathfrak{q}_f^{\sigma})^2 \tag{4.6}$$

for $\sigma \in G_f$ with $\sigma \ne 1_f$. Here, 1_n is the identity element of G_n. For $0 \le n \le f-1$, we put $\omega_n = N_{f/n}\omega$ so that we have $\mathfrak{q}_n^h = (\omega_n)$ and

$$\frac{\omega_n}{(2^*)^h} \equiv 1 \bmod \mathfrak{q}_n^2 \quad \text{and} \quad \omega_n \equiv 1 \bmod (\mathfrak{q}_n^{\sigma})^2 \tag{4.7}$$

for $\sigma \in G_n$ with $\sigma \neq 1_n$. In particular, we have $\omega_0 = (2^*)^h$. When $L_0 = \mathbb{Q}(\sqrt{2})$, we put $\omega_f = \omega$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$, we put $\omega_f = \omega$ or $\omega\ell^*$ according as ω is a square modulo $\mathfrak{p}_f$ or not, so that ω_f is a quadratic residue modulo $\mathfrak{p}_f$ by (4.5). For $f \leq n \leq e$, we put $\omega_n = \omega_f$. Though our target is the class groups $\tilde{A}_n$ and A_n for $0 \leq n \leq e-1$, it is convenient to define ω_n (and the modules $\tilde{V}_n$, V_n) also for $n = e$. In any case, we see that ω_n satisfies the congruence (4.7) for any n as $\ell^* \equiv 1 \bmod 8$, and that

$$\omega_n \equiv N_{f/n}\omega_f \bmod (k_n^\times)^2 \tag{4.8}$$

for $0 \leq n \leq f-1$. From $(2^*)^h = \omega_0$ and (4.8), we have

$$(2^*)^h = N_{n/0}\omega_n \equiv N_{f/0}\omega_f \bmod (\mathbb{Q}^\times)^2 \tag{4.9}$$

for $0 \leq n \leq f-1$. From the choice of ω_f and (4.8), we have

Lemma 4.1. *When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$, ω_n is a quadratic residue modulo the prime ideal $\mathfrak{p}_n$ for $0 \leq n \leq e$.*

Let $\tilde{V}_n$ be the submodule of $k_n^\times/(k_n^\times)^2$ generated by the class $[\omega_n]$ over the group ring $\mathbb{F}_2[G_n]$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$, let $\tilde{W}_n$ be the submodule of $k_n^\times/(k_n^\times)^2$ generated by the class $[\ell^*]$ and the submodule $\tilde{V}_n$.

Lemma 4.2. *Under the above setting, the following assertions hold.*

(I) *When $0 \leq n \leq f-1$, the submodule $\tilde{V}_n$ of $k_n^\times/(k_n^\times)^2$ does not depend on individual L_0's.*

(II) *According as $0 \leq n \leq f-1$ or $f \leq n \leq e$, we have*

$$\dim_{\mathbb{F}_2} \tilde{V}_n = 2^n \quad \text{or} \quad 2^f$$

and

$$\dim_{\mathbb{F}_2} \tilde{W}_n = 1 + 2^n \quad \text{or} \quad 1 + 2^f$$

for any L_0's. Further, the natural lifting map φ_n from $k_n^\times/(k_n^\times)^2$ to $\mathcal{F}_n^\times/(\mathcal{F}_n^\times)^2$ is injective on $\tilde{V}_n$ and $\tilde{W}_n$.

Proof. The assertion (I) is obvious from the definition of ω_n for $0 \leq n \leq f-1$. Let us show the second one (II) when $L_0 = \mathbb{Q}(\sqrt{2\ell})$. It suffices to show that the dimension of $\varphi_n(\tilde{W}_n)$ over $\mathbb{F}_2$ equals $1 + 2^n$ or $1 + 2^f$. Let us show this when $f \leq n \leq e$ (so that $\omega_n = \omega_f$). Put

$$x = (\ell^*)^s \prod_{\sigma \in G_f} (\omega_f^\sigma)^{t_\sigma} \in k_n$$

with s, $t_\sigma = 0, 1$. Assume that x is a square in $\mathcal{F}_n$. By (4.4) and (4.5), we have $\mathcal{F}_n = k_n(\sqrt{2^*\ell^*\delta_n})$. Then, it follows from the assumption that x or $y = 2^*\ell^*\delta_n x$ is a square in k_n. When x is a square in k_n, we see that the principal ideal

$$(x) = (\ell)^{s+u} \prod_{\sigma \in G_f} (\mathfrak{q}_f^\sigma)^{ht_\sigma}$$

is a square of an ideal of k_n, where $u = 0$ or $\sum_\sigma t_\sigma$ according as $\omega_f = \omega$ or $\omega\ell^*$. Since the prime numbers ℓ and 2 are unramified in k_n and h is odd, we see that $s + u$ is even and $t_\sigma = 0$. Hence, $s = t_\sigma = 0$. Further, we see that y is not a square in k_n because $\mathfrak{p}_n^h \| \delta_n$, $2 \nmid h$ and x is relatively prime to $\mathfrak{p}_n$. Thus, we have shown (II) when $L_0 = \mathbb{Q}(\sqrt{2\ell})$ and $f \le n \le e$. It is shown similarly for the other cases. □

By Lemma 4.2(II) and (4.8), we see that the natural lifting map from $k_n^\times/(k_n^\times)^2$ to $k_{n+1}^\times/(k_{n+1}^\times)^2$ induces an injection $\tilde{V}_n \to \tilde{V}_{n+1}$ for $0 \le n \le f-1$ and an isomorphism $\tilde{V}_n \cong \tilde{V}_{n+1}$ for $f \le n \le e-1$. Therefore, letting $\tilde{V} = \tilde{V}_f$, we regard $\tilde{V}_n$ $(0 \le n \le f-1)$ as a submodule of $\tilde{V}$, and we identify $\tilde{V}_n$ $(f \le n \le e)$ with $\tilde{V}$. We can naturally regard the modules $\tilde{V}_n$ as modules over the group ring $\mathcal{R} = \mathbb{F}_2[G_f]$. By Lemma 4.2(II), we have an isomorphism

$$\iota : \tilde{V} \longrightarrow \mathcal{R}$$

of $\mathcal{R}$-modules sending the class $[\omega_f]$ to 1_f. We denote the element of $\mathcal{R}$ associated to the norm map $N_{f/n}$ from k_f to k_n by the same letter $N_{f/n}$. Let $J_n = (N_{f/n})$ be the ideal of $\mathcal{R}$ generated by $N_{f/n}$. Then, we see from (4.8) that

$$\iota(\tilde{V}_n) = J_n \tag{4.10}$$

for $0 \le n \le f$. Further, by virtue of the last assertion of Lemma 4.2(II), we may and shall denote the submodules $\varphi_n(\tilde{V}_n)$ and $\varphi_n(\tilde{W}_n)$ of $\mathcal{F}_n^\times/(\mathcal{F}_n^\times)^2$ simply by the same symbols $\tilde{V}_n$ and $\tilde{W}_n$, respectively.

Remark 4.1. The module $\tilde{V} = \tilde{V}_f$ depends on L_0's by the definition of ω_f, while its proper submodules $\tilde{V}_n$ $(0 \le n \le f-1)$ do not depend on L_0's by Lemma 4.2(I).

In the rest of this section, we let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, so that we have $2^* = 2$ and $\ell^* = \ell$. In this case, we define submodules V and V_n of $\tilde{V}$ by

$$V = \{[\alpha] \in \tilde{V} \mid \alpha \gg 0\} \quad \text{and} \quad V_n = V \cap \tilde{V}_n = \{[\alpha] \in \tilde{V}_n \mid \alpha \gg 0\}$$

for $0 \le n \le e$. Here, for $x \in k_n$, we write $x \gg 0$ when x is totally positive. Clearly, these are $\mathcal{R}$-submodules of $\tilde{V}$. For $f \le n \le e$, since $\tilde{V}_n = \tilde{V}$, we have $V_n = V$. For each $0 \le n \le f-1$, consider an element

$$\alpha = \prod_{\sigma \in G_n} (\omega_n^\sigma)^{a_\sigma} \quad \text{with} \quad a_\sigma = 0, 1$$

of $k_n^\times$. By (4.7), it satisfies the congruence

$$\frac{\alpha}{2^h} \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^2 \quad \text{or} \quad \alpha \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^2 \tag{4.11}$$

according as $a_\sigma = 1$ or 0. For $0 \le n \le f-1$, let Q_n be the subset of V_n consisting of the classes $[\alpha]$ for all such α satisfying the stronger condition

$$\alpha \gg 0, \quad \text{and} \quad \frac{\alpha}{2^h} \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^3 \quad \text{or} \quad \alpha \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^3 \tag{4.12}$$

according as $a_\sigma = 1$ or 0. We easily see that Q_n is an $\mathcal{R}$-submodule of $\tilde{V}$, and that $Q_n = Q_{f-1} \cap \tilde{V}_n$ from the norm relation (4.8). Let $\mathcal{Q}$ and $\mathcal{Q}_n$ be the ideals of $\mathcal{R}$ corresponding to the $\mathcal{R}$-submodules Q_{f-1} and Q_n of $\tilde{V}$:

$$\mathcal{Q} = \iota(Q_{f-1}), \quad \text{and} \quad \mathcal{Q}_n = \iota(Q_n).$$

Then, as $Q_n = Q_{f-1} \cap \tilde{V}_n$, we see from (4.10) that

$$\mathcal{Q}_n = \mathcal{Q} \cap J_n. \tag{4.13}$$

By (4.9), we observe that $[2] \in Q_n$ for every n and that Q_n is nontrivial.

Lemma 4.3. *Let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. For $0 \le n \le f-1$, the submodules V_n and Q_n depend only on n and not on individual L_0's. Further, for $f \le n \le e$, $\dim_{\mathbb{F}_2} V_n$ depends only on n.*

Proof. The first assertion on V_n follows from Lemma 4.2(I). The assertion on Q_n holds because $\omega_n = N_{f/n}\omega$ for $0 \le n \le f-1$ and the element ω defined in (4.6) does not depend on L_0's. For $f \le n \le e$, $\omega_n = \omega_f$ depends on L_0. However, the last assertion on $\dim_{\mathbb{F}_2} V_n$ holds because $\omega_f = \omega$ or $\omega\ell^*$ and $\ell^* = \ell$ is positive. □

5 Class field corresponding to $\tilde{A}_n/\tilde{A}_n^2$

In this section, we construct the class fields of $\mathcal{F}_n$ corresponding to $\tilde{A}_n/\tilde{A}_n^2$ and A_n/A_n^2 ($0 \le n \le e-1$), respectively, and show Lemma 1.1 and Propositions 1.1, 1.2. We begin with showing Lemma 1.1. Let J be the nontrivial automorphism of $\mathcal{F}_n/k_n$.

Proof of Lemma 1.1. Via the identification (1.2), the automorphism J corresponds to $(1+T)^{2^n} \in \Lambda$. Since the narrow class number $\tilde{h}_{k_n}$ of k_n is odd, the norm $N_{\mathcal{F}_n/k_n} = 1 + J$ annihilates $\tilde{A}_n$ and its quotient A_n. From this we obtain the assertion. □

Next, let us show Proposition 1.1 on the 2-rank $r_2(\tilde{A}_n)$. Let L/K be a quadratic extension over a totally real number field K with $G = \mathrm{Gal}(L/K)$. When the narrow class number $\tilde{h}_K$ is odd, we have the following invariant class number formula on the narrow class group $\tilde{Cl}_L$:

$$|\tilde{Cl}_L^G| = \frac{|\tilde{Cl}_K| \times \prod_\wp e_\wp}{[L:K]}. \tag{5.1}$$

Here, $\wp$ runs over the prime ideals of K and $e_\wp$ is the ramification index of $\wp$ in L. This is a special case of a general invariant class number formula due to Gras [4, II, Proposition 6.2.4].

Proof of Proposition 1.1. We show the assertion for the case $L_0 = \mathbb{Q}(\sqrt{2\ell})$. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{2})$. Let g_n be the number of invariant classes in $\tilde{A}_n$; namely g_n is the 2-part of $|\tilde{Cl}_{\mathcal{F}_n}^G|$ with $G = \mathrm{Gal}(\mathcal{F}_n/k_n) = \langle J \rangle$. Let r be the 2-rank of $\tilde{A}_n$. For a class $c \in \tilde{A}_n$, we see from Lemma 1.1 that $c^J = c$ if and only if $c^2 = 1$. It follows that $g_n = 2^r$. Further, the prime ideals of k_n ramified in $\mathcal{F}_n$ are those over the prime numbers p, ℓ and 2. The number of such prime ideals of k_n are

$$1 + 1 + 2^n \quad \text{or} \quad 1 + 1 + 2^f$$

according as $0 \leq n \leq f-1$ or $f \leq n \leq e-1$. Accordingly, we see from (5.1) and $2 \nmid \tilde{h}_{k_n}$ that $g_n = 2^{1+2^n}$ or 2^{1+2^f}. Thus, we obtain the assertion. $\square$

The prime ideals $\mathfrak{p}_n$ and $\mathfrak{q}_n^\sigma$ of k_n are ramified in $\mathcal{F}_n$, where $\sigma \in G_n$ for $0 \leq n \leq f-1$ and $\sigma \in G_f$ for $f \leq n \leq e-1$. We denote the prime ideals of $\mathcal{F}_n$ over $\mathfrak{p}_n$ and $\mathfrak{q}_n^\sigma$ by $\mathfrak{P}_n$ and $\mathfrak{Q}_n^\sigma$, respectively, so that we have $\mathfrak{p}_n = \mathfrak{P}_n^2$ and $\mathfrak{q}_n^\sigma = (\mathfrak{Q}_n^\sigma)^2$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$, the prime number ℓ remains prime in k_n by (1.1) and the prime ideal of k_n over ℓ ramifies in $\mathcal{F}_n$. Let $\mathfrak{L}_n$ be the prime ideal of $\mathcal{F}_n$ over ℓ; $(\ell) = \mathfrak{L}_n^2$.

Lemma 5.1. *When $L_0 = \mathbb{Q}(\sqrt{2})$, ${}_2\tilde{A}_n$ is generated by the narrow classes $[\mathfrak{Q}_n^h]$ and $[(x)]$ with all $x \in \mathcal{F}_n^\times$ over the group ring $\mathbb{F}_2[G_n]$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$, ${}_2\tilde{A}_n$ is generated by the narrow classes $[\mathfrak{P}_n^h]$, $[\mathfrak{Q}_n^h]$ and $[(x)]$ with all $x \in \mathcal{F}_n^\times$ over $\mathbb{F}_2[G_n]$.*

Proof. We show the assertion when $L_0 = \mathbb{Q}(\sqrt{2\ell})$. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{2})$. We see that the narrow classes $[\mathfrak{P}_n^h]$ and $[\mathfrak{Q}_n^h]$ are elements of ${}_2\tilde{A}_n$ because $\mathfrak{P}_n^{2h} = \mathfrak{p}_n^h$ and $\mathfrak{Q}_n^{2h} = \mathfrak{q}_n^h$ are principal ideals of k_n and the narrow class number $\tilde{h}_{k_n}$ of k_n is odd. Conversely, let c be an arbitrary class in ${}_2\tilde{A}_n$. Then, by Lemma 1.1, we have $c^J = c^{-1} = c$. For an ideal $\mathfrak{A} \in c$, it follows that $\mathfrak{A}^J = \rho\mathfrak{A}$ for some $\rho \in \mathcal{F}_n^\times$ with $\rho \gg 0$. Then, we see that $\eta = N_{\mathcal{F}_n/k_n}\rho \in E_n = E_{k_n}$. We have $\eta \gg 0$ as $\rho \gg 0$, and hence we see that $\eta = \epsilon^2$ for some unit $\epsilon \in E_n$ as $\tilde{h}_{k_n}$ is odd. Using $\rho\epsilon^{-1}$ in place of ρ, we observe that $\mathfrak{A}^J = \rho\mathfrak{A}$ and $N_{\mathcal{F}_n/k_n}\rho = 1$. Then, we can write $\rho = x^{1-J}$ for some $x \in \mathcal{F}_n^\times$, and we have $(x\mathfrak{A})^J = x\mathfrak{A}$. Therefore, it follows that $x\mathfrak{A}$ is a product of some powers of invariant prime ideals $\mathfrak{P}_n$, $\mathfrak{Q}_n^\sigma$ $(\sigma \in G_n)$, $\mathfrak{L}_n$ of $\mathcal{F}_n/k_n$ and an ideal of k_n. As $\tilde{h}_{k_n}$ is odd, it follows that the narrow class $c = c^h = [\mathfrak{A}^h]$ is a product of some powers of the narrow classes $[\mathfrak{P}_n^h]$, $[(\mathfrak{Q}_n^\sigma)^h]$, $[\mathfrak{L}_n^h]$ and $[(x)]$ with some $x \in \mathcal{F}_n^\times$. Further, we have

$$(\sqrt{2\ell\delta_n}) = \mathfrak{P}_n^h \mathfrak{L}_n \prod_{\sigma \in G_n} (\mathfrak{Q}_n^\sigma)^h$$

in $\mathcal{F}_n = k_n(\sqrt{2\ell\delta_n})$ (see (4.4)). Therefore, we can express the class c as a product of some powers of $[\mathfrak{P}_n^h]$, $[(\mathfrak{Q}_n^\sigma)^h]$ and $[(x)]$ with some $x \in \mathcal{F}_n^\times$. □

For $0 \leq n \leq e-1$, we put

$$\tilde{M}_n^1 = \mathcal{F}_n(\sqrt{\alpha} \mid [\alpha] \in \tilde{V}_n)$$

for every L_0. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$, we put

$$\tilde{M}_n^0 = \mathcal{F}_n(\sqrt{\ell^*}) \quad \text{and} \quad \tilde{M}_n^2 = \tilde{M}_n^0 \tilde{M}_n^1 = \mathcal{F}_n(\sqrt{\alpha} \mid [\alpha] \in \tilde{W}_n).$$

Further, when $\ell \in \mathbb{P}_+$ (and hence $\ell^* = \ell$), we put

$$M_n^1 = \mathcal{F}_n(\sqrt{\alpha} \mid [\alpha] \in V_n) \quad \text{and} \quad M_n^2 = \tilde{M}_n^0 M_n^1 = \mathcal{F}_n(\sqrt{\ell}, \sqrt{\alpha} \mid [\alpha] \in V_n).$$

Lemma 5.2. (I) *The case $L_0 = \mathbb{Q}(\sqrt{2})$. The extensions $\tilde{M}_n^1/\mathcal{F}_n$ and $M_n^1/\mathcal{F}_n$ are the class fields of $\mathcal{F}_n$ corresponding to $\tilde{A}_n/\tilde{A}_n^2$ and A_n/A_n^2, respectively.*

(II) *The case $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$. The extension $\tilde{M}_n^2/\mathcal{F}_n$ is the class field of $\mathcal{F}_n$ corresponding to $\tilde{A}_n/\tilde{A}_n^2$, and $\tilde{M}_n^1/\mathcal{F}_n$ is the maximal subextension of $\tilde{M}_n^2/\mathcal{F}_n$ in which the prime ideal $\mathfrak{P}_n$ splits completely. When $\ell \in \mathbb{P}_+$, the extension $M_n^2/\mathcal{F}_n$ is the class field of $\mathcal{F}_n$ corresponding to A_n/A_n^2.*

Proof. We show the assertion (II) for the case $L_0 = \mathbb{Q}(\sqrt{2\ell})$. The assertion (I) is shown similarly and more easily. We see from Lemma 4.2(II) that the Galois group $\mathrm{Gal}(\tilde{M}_n^2/\mathcal{F}_n)$ is isomorphic to $1+2^n$ or $1+2^f$ copies of C_2 according as $0 \leq n \leq f-1$ or $f \leq n \leq e-1$. On the other hand, by Proposition 1.1, the quotient $\tilde{A}_n/\tilde{A}_n^2$ is also isomorphic to $1+2^n$ or $1+2^f$ copies of C_2. Therefore, for showing the first assertion of (II), it suffices to show that $\tilde{M}_n^2/\mathcal{F}_n$ is narrowly unramified. To show that it is narrowly unramified, it suffices to show that the quadratic subextensions $\mathcal{F}_n(\sqrt{\ell^*})/\mathcal{F}_n$ and $\mathcal{F}_n(\sqrt{\omega_n^\sigma})/\mathcal{F}_n$ with $\sigma \in G_n$ are narrowly unramified. As $\mathcal{F}_n/\mathbb{Q}$ is Galois, the extension $\mathcal{F}_n(\sqrt{\omega_n^\sigma})/\mathcal{F}_n$ is narrowly unramified if and only if so is $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$. The extension $\mathcal{F}_n(\sqrt{\ell^*})/\mathcal{F}_n$ is narrowly unramified outside ℓ because of $\ell^* \equiv 1 \bmod 8$ and Lemma 3.2. It is unramified also at ℓ because in the $(2,2)$-extension $\mathcal{F}_n(\sqrt{\ell^*})/k_n$, ℓ is ramified in the quadratic subextension $\mathcal{F}_n/k_n$. From this, we also see that $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$ is unramified at ℓ even when ($f \leq n \leq e-1$ and) $\omega_n = \omega\ell^*$. Therefore, as $(\omega) = \mathfrak{q}_n^h$, $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$ is narrowly unramified outside 2. We have $\mathcal{F}_n = k_n(\sqrt{2^*\ell^*\delta_n})$ by (4.4) and (4.5), and hence

$$\mathcal{F}_n(\sqrt{\omega_n}) = \mathcal{F}_n(\sqrt{x}) \quad \text{with} \quad x = \frac{\omega_n}{(2^*)^h} \times (\ell^*\delta_n)^{-1}.$$

Therefore, it follows from the congruences (4.1), (4.5), (4.7) and Lemma 3.2(i) that $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$ is unramified also at 2. Thus, we have shown that $\tilde{M}_n^2/\mathcal{F}_n$ is the class field corresponding to $\tilde{A}_n/\tilde{A}_n^2$. The element ℓ^* is a quadratic non-residue modulo $\mathfrak{P}_n$ by (4.5), and ω_n is a quadratic residue modulo $\mathfrak{P}_n$ by

Lemma 4.1. Therefore, $\tilde{M}_n^1/\mathcal{F}_n$ is the maximal subextension of $\tilde{M}_n^2/\mathcal{F}_n$ in which the prime ideal $\mathfrak{P}_n$ splits completely. When $\ell \in \mathbb{P}_+$, we see that M_n^2 is the maximal totally real subextension of $\tilde{M}_n^2/\mathcal{F}_n$ from the definition of V_n and $\ell^* = \ell$. This implies that $M_n^2/\mathcal{F}_n$ is the class field corresponding to A_n/A_n^2. □

Proof of Proposition 1.2. We show the assertion (II) for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$. The assertion (I) is shown similarly. Let $\tilde{\mathcal{M}}_n/\mathcal{F}_n$ and $\mathcal{M}_n/\mathcal{F}_n$ be the class fields of $\mathcal{F}_n$ corresponding to the class groups $\tilde{A}_n$ and A_n, respectively. The Galois groups $\mathrm{Gal}(\tilde{\mathcal{M}}_n/\mathcal{F}_n)$ and $\mathrm{Gal}(\mathcal{M}_n/\mathcal{F}_n)$ are naturally regarded as modules over $\Gamma_n = \mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$, and hence as modules over Λ by (1.2). We have identifications of Λ-modules:

$$\mathrm{Gal}(\tilde{\mathcal{M}}_n/\mathcal{F}_n) = \tilde{A}_n \quad \text{and} \quad \mathrm{Gal}(\mathcal{M}_n/\mathcal{F}_n) = A_n$$

via the reciprocity law map. We put

$$\tilde{B}_n = \mathrm{Gal}(\tilde{\mathcal{M}}_n/\tilde{M}_n^0), \quad \text{and} \quad B_n = \mathrm{Gal}(\mathcal{M}_n/\tilde{M}_n^0).$$

The group B_n is defined only when $\ell \in \mathbb{P}_+$ (and hence $\tilde{M}_n^0 = \mathcal{F}_n(\sqrt{\ell})$). By Lemma 5.1, the narrow (resp. ordinary) class containing $\mathfrak{P}_n^h$ is an element of ${}_2\tilde{A}_n$ (resp. ${}_2A_n$). Let $\tilde{C}_n$ (resp. C_n) be the subgroup of $\tilde{A}_n$ (resp. A_n) generated by this narrow (resp. ordinary) class.

Let us deal with the narrow class group $\tilde{A}_n$. We see that $\tilde{B}_n$ is a Λ-submodule of $\tilde{A}_n$ because $\tilde{M}_n^0$ is Galois over $\mathbb{Q}$. We see that $\tilde{C}_n$ is a Λ-submodule of $\tilde{A}_n$ since the prime ideal $\mathfrak{P}_n$ is invariant under the action of $\Gamma_n = \mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$. Further, as the narrow class $[\mathfrak{P}_n^h]^2$ is trivial, we see that $\tilde{C}_n$ is trivial or isomorphic to $\Lambda/(2,T)$. By Lemma 5.2(II), the prime ideal $\mathfrak{P}_n$ remains prime in the quadratic extension $\tilde{M}_n^0/\mathcal{F}_n$. This implies that $[\mathfrak{P}_n^h] \notin \tilde{B}_n = \mathrm{Gal}(\tilde{\mathcal{M}}_n/\tilde{M}_n^0)$. It follows that $\tilde{C}_n \cong \Lambda/(2,T)$ as $|\tilde{C}_n| \le 2$ and that $\tilde{B}_n \cap \tilde{C}_n = \{0\}$. Therefore, we see that $\tilde{A}_n = \tilde{B}_n \oplus \tilde{C}_n$ since $[\tilde{A}_n : \tilde{B}_n] = [\tilde{M}^0 : \mathcal{F}_n] = 2$. Hence, $\tilde{A}_n^2 = \tilde{B}_n^2$. Therefore, we see from Lemma 5.2(II) that the subextension of $\tilde{\mathcal{M}}_n/\tilde{M}_n^0$ corresponding to $\tilde{B}_n^2$ by Galois theory equals $\tilde{M}_n^2 = \tilde{M}_0\tilde{M}_n^1$. Hence, we obtain an isomorphism

$$\tilde{B}_n/\tilde{B}_n^2 = \mathrm{Gal}(\tilde{M}_n^2/\tilde{M}_n^0) \cong \mathrm{Gal}(\tilde{M}_n^1/\mathcal{F}_n), \tag{5.2}$$

which is compatible with the action of Γ_n. As we mentioned after showing Lemma 4.2, we may regard $\tilde{V}_n$ as a submodule of $\mathcal{F}_n^\times/(\mathcal{F}_n^\times)^2$. Then, we can regard $\tilde{V}_n$ as a module over $R_n = \mathbb{Z}_2[\Gamma_n]$ through the surjection $\Gamma_n \to G_n$, and hence as a module over Λ by (1.2). The module $\tilde{V}_n$ is cyclic over Λ since it is cyclic over $\mathbb{F}_2[G_n]$. The Kummer pairing

$$\mathrm{Gal}(\tilde{M}_n^1/\mathcal{F}_n) \times \tilde{V}_n \longrightarrow \{\pm 1\};\ (g, [v]) \to \langle b, v \rangle = (\sqrt{v})^{g-1}$$

is nondegenerate and satisfies $\langle b^\gamma, v^\gamma \rangle = \langle b, v \rangle$ for $\gamma \in \Gamma_n$. Thus we obtain an isomorphism

$$\mathrm{Gal}(\tilde{M}_n^1/\mathcal{F}_n) \cong H = \mathrm{Hom}(\tilde{V}_n, \{\pm 1\}), \tag{5.3}$$

which is compatible with the action of Γ_n. Here, $\gamma \in \Gamma_n$ acts on $f \in H$ by $f^{\gamma}([v]) = f([v]^{\gamma^{-1}})$. From this, we see that $\mathrm{Gal}(\tilde{M}_n^1/\mathcal{F}_n)$ is cyclic over Λ as $\tilde{V}_n$ is cyclic over Λ. Hence, so is $\tilde{B}_n/\tilde{B}_n^2$ by (5.2). Now we see that $\tilde{B}_n$ is cyclic over Λ by Nakayama's lemma. Thus, we have shown the assertion (II) of Proposition 1.2 for the narrow class group $\tilde{A}_n$.

Let us show the assertion for A_n. Similarly to $\tilde{A}_n$, we can show that $A_n = B_n \oplus C_n$ and $C_n \cong \Lambda/(2,T)$. Further, $B_n = \mathrm{Gal}(\mathcal{M}_n/\tilde{M}_n^0)$ is a quotient of $\tilde{B}_n = \mathrm{Gal}(\tilde{\mathcal{M}}_n/\tilde{M}_n^0)$ as a Λ-module since $\mathcal{M}_n$ is Galois over $\mathbb{Q}$. Hence, B_n is cyclic over Λ since so is $\tilde{B}_n$. □

Corollary 5.1. (I) *We have* $\dim_{\mathbb{F}_2} \tilde{V}_n = r_2(\tilde{A}_n)$ *or* $r_2(\tilde{B}_n)$ *according as* $L_0 = \mathbb{Q}(\sqrt{2})$ *or* $\mathbb{Q}(\sqrt{2\ell})$.

(II) *We have* $\dim_{\mathbb{F}_2} V_n = r_2(A_n)$ *or* $r_2(B_n)$ *according as* $L_0 = \mathbb{Q}(\sqrt{2})$ *or* $\mathbb{Q}(\sqrt{2\ell})$ *with* $\ell \in \mathbb{P}_+$.

(III) *The 2-rank* $r_2(A_n)$ *for* $L_0 = \mathbb{Q}(\sqrt{2})$ *and* $r_2(B_n)$ *for* $L_0 = \mathbb{Q}(\sqrt{2\ell})$ *with* $\ell \in \mathbb{P}_+$ *depend only on n and not individual* L_0*'s.*

Proof. The assertions (I) and (II) for $L_0 = \mathbb{Q}(\sqrt{2})$ are immediate consequences of Lemma 5.2(I). The assertion (I) for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ follows from (5.2) and (5.3). We can show the assertion (II) for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ by a similar way replacing $\tilde{X}$ to X for every object $\tilde{X}$ in the Kummer theory argument in the proof of Proposition 1.2. The assertion (III) follows from (II) and Lemma 4.3. □

6 Proofs of Theorems

In this section, we prove Theorems 1.1, 1.2 and Propositions 1.4–1.8. We use the same notation as in the previous sections. First, we show Proposition 1.7.

Proof of Proposition 1.7. Let $\ell \in \mathbb{P}_-$ and $L_0 = \mathbb{Q}(\sqrt{2\ell})$. Let $0 \leq n \leq e-1$. By genus theory, the assumption $\ell \in \mathbb{P}_-$ implies that the ordinary class number of L_0 is odd. The prime number p remains prime in L_0 by (1.1), and the $C_{2^{n+1}}$-extension L_{n+1}/L_0 is ramified only at the prime ideal over p. It follows that the ordinary class number of L_{n+1} is odd by [13, Theorem 10.2]. On the other hand, we observe that $L_{n+1}/\mathcal{F}_n$ is unramified because L_n/k_n is unramified outside 2ℓ and k_{n+1}/k_n is unramified outside p. Therefore, we obtain $A_n \cong \mathbb{Z}/2$. □

For $s \geq 2$, let $\tilde{L}_{n,2^s}$ be the composite of all narrowly unramified quadratic extensions over $\mathcal{F}_n$ which extends to a narrowly unramified C_{2^s}-extension, and let $L_{n,2^s}$ be the composite of all unramified quadratic extensions over $\mathcal{F}_n$ which extends to an unramified C_{2^s}-extension. We easily see that a narrowly unramified (resp. an unramified) quadratic extension $N/\mathcal{F}_n$ extends to a narrowly unramified (resp. an unramified) C_{2^s}-extension if and only if N is contained in $\tilde{L}_{n,2^s}$ (resp. $L_{n,2^s}$), and that $\tilde{L}_{n,2^s}$ (resp. $L_{n,2^s}$) is Galois over $\mathbb{Q}$.

Lemma 6.1. *Let $L_0 = \mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}$, and let $[\alpha] \in \tilde{W}_n$. We have $[\alpha] \in \tilde{V}_n$ if $\mathcal{F}_n(\sqrt{\alpha}) \subseteq \tilde{L}_{n,4}$.*

Proof. Assume that $\mathcal{F}_n(\sqrt{\alpha})/\mathcal{F}_n$ extends to a narrowly unramified C_4-extension. Then, by Lemma 3.3 (with Remark 3.1) and Lemma 5.1, we see that the prime ideal $\mathfrak{P}_n$ of $\mathcal{F}_n$ splits in $\mathcal{F}_n(\sqrt{\alpha})$. Hence, we see from Lemma 5.2(II) that $[\alpha]$ is an element of $\tilde{V}_n$. □

In view of Lemma 6.1, let $\tilde{V}_{n,2^s}$ (resp. $V_{n,2^s}$) be the submodule of $\tilde{V}_n$ (resp. V_n) consisting of elements $[\alpha]$ for which $\mathcal{F}_n(\sqrt{\alpha}) \subseteq \tilde{L}_{n,2^s}$ (resp. $\mathcal{F}_n(\sqrt{\alpha}) \subseteq L_{n,2^s}$).

Lemma 6.2. *We have $r_{2^s}(\tilde{A}_n) \geq 1$ if and only if $\mathcal{F}_n(\sqrt{2^*}) \subseteq \tilde{L}_{n,2^s}$, and $r_{2^s}(A_n) \geq 1$ if and only if $\mathcal{F}_n(\sqrt{2^*}) \subseteq L_{n,2^s}$.*

Proof. Since $\tilde{L}_{n,2^s}$ is Galois over $\mathbb{Q}$, $\tilde{V}_{n,2^s}$ is a submodule of $\tilde{V}_n$ over $\mathbb{F}_2[G_n]$. This implies that the image $\iota(\tilde{V}_{n,2^s})$ is an ideal of $\mathcal{R} = \mathbb{F}_2[G_f]$. By Lemma 3.6(II), the smallest nontrivial ideal of $\mathcal{R}$ is $J_0 = (N_{f/0})$. Therefore, we observe that $r_{2^s}(\tilde{A}_n) \geq 1$ if and only if $J_0 \subseteq \iota(\tilde{V}_{n,2^s})$. By (4.9), the last condition is equivalent to $[N_{f/0}\omega_f] = [2^*] \in \tilde{V}_{n,2^s}$. Thus we obtain the assertion for $\tilde{A}_n$. The assertion for A_n is shown similarly. □

Proof of Proposition 1.4. As $\ell \in \mathbb{P}_-$, we have $\mathcal{F}_n(\sqrt{2^*}) = \mathcal{F}_n(\sqrt{-2})$. Since the narrowly unramified quadratic extension $\mathcal{F}_n(\sqrt{-2})/\mathcal{F}_n$ is totally imaginary, we see from Lemma 3.3 and Remark 3.1 that it does not extends to a narrowly unramified C_4-extension. Now, the assertion follows from Lemma 6.2 with $s = 2$. □

Proof of Proposition 1.5. We have $\mathcal{F}_n(\sqrt{2^*}) = \mathcal{F}_n(\sqrt{2})$ and $\ell^* = \ell$ in this case. Further, by (4.4), we have

$$\mathcal{F}_n(\sqrt{2}) = \mathcal{F}_n(\sqrt{\delta_n}) \quad \text{or} \quad \mathcal{F}_n(\sqrt{\ell\delta_n})$$

according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. Then, it follows from the congruences (4.2), (4.3) and Lemma 3.2(ii) that the prime ideals $\mathfrak{Q}_n^\sigma$ $(\sigma \in G_n)$ of $\mathcal{F}_n$ split in $\mathcal{F}_n(\sqrt{2})$ if and only if $0 \leq n \leq f-1$. When $L_0 = \mathbb{Q}(\sqrt{2\ell})$, we see that the prime ideal $\mathfrak{P}_n$ of $\mathcal{F}_n$ splits in $\mathcal{F}_n(\sqrt{2})$ because $p \equiv 1 \bmod 8$. Therefore, for $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$, we observe that $\mathcal{F}_n(\sqrt{2}) \subseteq \tilde{L}_{n,4}$ if and only if $0 \leq n \leq f-1$ from Lemma 3.3 (with Remark 3.1) and Lemma 5.1. Thus, we obtain the assertion from Lemma 6.2. □

Lemma 6.3. *Let $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$ with $\ell \in \mathbb{P}_+$. Then, for $0 \leq n \leq f-1$, we have*

$$\tilde{V}_{n,4} = Q_n \quad \text{and} \quad r_4(\tilde{A}_n) = \dim_{\mathbb{F}_2} Q_n$$

In particular, the module $\tilde{V}_{n,4}$ and the 4-rank $r_4(\tilde{A}_n)$ depend only on n.

Proof. Let $0 \leq n \leq f-1$. We begin with a simple remark. Let x be an element of k_n relatively prime to the prime ideal $\mathfrak{q}_n^\sigma$ of k_n over 2 with $\sigma \in G_n$. Then, we easily see that the prime ideal $\mathfrak{Q}_n^\sigma$ of $\mathcal{F}_n$ over $\mathfrak{q}_n^\sigma$ splits in $\mathcal{F}_n(\sqrt{x})/\mathcal{F}_n$ if and only if $\mathfrak{q}_n^\sigma$ splits in $k_n(\sqrt{x})/k_n$. Since 2 splits completely in k_n, we obtain the following equivalence from Lemma 3.2(ii'):

$$\mathfrak{Q}_n^\sigma \text{ splits in } \mathcal{F}_n(\sqrt{x})/\mathcal{F}_n \Longleftrightarrow x \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^3. \tag{6.1}$$

Let

$$\alpha = \prod_{\sigma \in G_n} (\omega_n^\sigma)^{a_\sigma}$$

be an element of $k_n^\times$ with $a_\sigma = 0,\, 1$. Then, α satisfies the congruence (4.11), and $\mathcal{F}_n(\sqrt{\alpha})/\mathcal{F}_n$ is narrowly unramified by Lemma 5.2. By Lemma 3.3 (with Remark 3.1) and Lemma 5.1, we observe that $[\alpha] \in \tilde{V}_{n,4}$ if and only if $\alpha \gg 0$ and the prime ideals $\mathfrak{Q}_n^\sigma$ with $\sigma \in G_n$ (and $\mathfrak{P}_n$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$) split in $\mathcal{F}_n(\sqrt{\alpha})$. As $[\alpha] \in \tilde{V}_n$, we see from Lemma 5.2(II) that $\mathfrak{P}_n$ splits in $\mathcal{F}_n(\sqrt{\alpha})$ when $L_0 = \mathbb{Q}(\sqrt{2\ell})$. By (4.4), we have

$$\mathcal{F}_n(\sqrt{\alpha}) = \mathcal{F}_n(\sqrt{\beta}) \quad \text{with} \quad \beta = \frac{\alpha}{2^h} \times (\delta_n \ell)^{-1}.$$

Further, $\delta_n \ell \equiv 1 \bmod 8$ by (4.2). Now, we see from (4.11) and (6.1) that the prime ideals $\mathfrak{Q}_n^\sigma$ over 2 split in $\mathcal{F}_n(\sqrt{\alpha})/\mathcal{F}_n$ if and only if α satisfies the congruence in (4.12). Therefore, we have shown that $[\alpha] \in \tilde{V}_{n,4}$ if and only if α satisfies the two conditions in (4.12). Thus, we obtain $\tilde{V}_{n,4} = Q_n$, and hence $r_4(\tilde{A}_n) = \dim_{\mathbb{F}_2} Q_n$. The last assertion follows from Lemma 4.3. □

For a while, let $L_0 = \mathbb{Q}(\sqrt{2})$, and let $0 \leq n \leq f-1$. Then, the unramified quadratic extension $L_{n+1} = \mathcal{F}_n(\sqrt{2})$ over $\mathcal{F}_n$ extends to a narrowly unramified C_4-extension by Proposition 1.5 and Lemma 6.2. Let us give a generator of such a C_4-extension. Let ρ be a generator of the cyclic Galois group $G_f = \mathrm{Gal}(k_f/\mathbb{Q})$ of order 2^f. For each $0 \leq n \leq f-1$, we put

$$a_n = \sum_{j=0}^{2^n-1} \rho^j \in \mathcal{R} = \mathbb{F}_2[G_f] \quad \text{and} \quad \pi_n = (\omega_{n+1})^{a_n} \in k_{n+1}^\times,$$

so that we have

$$[\pi_n] \in \tilde{V}_{n+1}.$$

We can easily show that

$$a_n = (1+\rho)^{2^n-1}$$

by induction on n. Then, because of (3.1) and (4.8), we see that

$$\iota([\pi_n]) = \iota([\omega_f]^{a_n N_{f/n+1}}) = a_n N_{f/n+1} = (1+\rho)^{2^f-(2^n+1)} \in \mathcal{R}. \tag{6.2}$$

Lemma 6.4. *Let $L_0 = \mathbb{Q}(\sqrt{2})$, and let $0 \le n \le f-1$. Under the above notation, $L_{n+1}(\sqrt{\pi_n})/\mathcal{F}_n$ is a narrowly unramified C_4-extension.*

Proof. We see that the element $a_n(1+\rho^{2^n}) \in \mathcal{R}$ acts on k_{n+1} as the norm $N_{n+1/0}$ from k_{n+1} to $k_0 = \mathbb{Q}$. Let σ be the nontrivial automorphism of $L_{n+1}/\mathcal{F}_n$. Since σ coincides with ρ^{2^n} on k_{n+1}, we observe from (4.9) that

$$\pi_n^{1+\sigma} = (\omega_{n+1})^{a_n(1+\rho^{2^n})} = N_{n+1/0}(\omega_{n+1}) \equiv 2^h \bmod (\mathbb{Q}^\times)^2.$$

As $\sqrt{2}^\sigma = -\sqrt{2}$, we see from Lemma 3.4 that $L_{n+1}(\sqrt{\pi_n})/\mathcal{F}_n$ is a C_4-extension. Further, we see from $(\omega_{n+1}) = \mathfrak{q}_{n+1}^h$ and the congruence (4.7) that the extension $L_{n+1}(\sqrt{\pi_n})/L_{n+1}$ is narrowly unramified because of Lemma 3.2(i). Thus we obtain the assertion. □

Proof of Proposition 1.6. Let $L_0 = \mathbb{Q}(\sqrt{2})$ and let $0 \le n \le f-2$. By Lemma 6.2, we have $r_8(\tilde{A}_n) \ge 1$ if and only if the unramified quadratic extension $L_{n+1} = \mathcal{F}_n(\sqrt{2})/\mathcal{F}_n$ extends to a narrowly unramified C_8-extension. By Lemma 6.4, $L_{n+1}(\sqrt{\pi_n})/\mathcal{F}_n$ is a narrowly unramified C_4-extension containing L_{n+1}. By Lemma 3.5, other such C_4-extensions are of the form $L_{n+1}(\sqrt{\pi_n\alpha})/\mathcal{F}_n$ with $[\alpha] \in \tilde{V}_n$. Therefore, we see that $r_8(\tilde{A}_n) \ge 1$ if and only if there exists some $[\alpha] \in \tilde{V}_n$ such that $(*)$ the narrowly unramified C_4-extension $L_{n+1}(\sqrt{\pi_n\alpha})/\mathcal{F}_n$ extends to a narrowly unramified C_8-extension. As $L_{n+1}(\sqrt{\pi_n\alpha})/\mathcal{F}_n$ is a narrowly unramified C_4-extension, the primes over 2 split in the quadratic subextension $L_{n+1}/\mathcal{F}_n$ by Lemma 3.3 (with Remark 3.1) and Lemma 5.1. Then, by the same two lemmas, we see that the condition $(*)$ on $[\alpha] \in \tilde{V}_n$ is equivalent to saying that $\pi_n\alpha \gg 0$ and the prime ideals of L_{n+1} over 2 split in $L_{n+1}(\sqrt{\pi_n\alpha})/L_{n+1}$.

As $n+2 \le f$, the primes over 2 split in k_{n+2}/k_{n+1}, and hence in L_{n+2}/L_{n+1}. Therefore, we see that the primes over 2 split in $L_{n+1}(\sqrt{\pi_n\alpha})/L_{n+1}$ if and only if they split in $L_{n+2}(\sqrt{\pi_n\alpha})/L_{n+2}$. As $n+1 \le f-1$, we have $r_4(\tilde{A}_{n+1}) \ge 1$ by Proposition 1.5, and hence we see that $L_{n+2} = \mathcal{F}_{n+1}(\sqrt{2}) \subseteq \tilde{L}_{n+1,4}$ by Lemma 6.2. Thus, the primes over 2 split in $L_{n+2}/\mathcal{F}_{n+1}$ by Lemma 3.3 (with Remark 3.1) and Lemma 5.1. It follows that the primes over 2 split in $L_{n+2}(\sqrt{\pi_n\alpha})/L_{n+2}$ if and only if they split in $\mathcal{F}_{n+1}(\sqrt{\pi_n\alpha})/\mathcal{F}_{n+1}$. Thus, we have shown that $r_8(\tilde{A}_n) \ge 1$ if and only if $\pi_n\alpha \gg 0$ and the prime ideals $\mathfrak{Q}_{n+1}^\sigma$ $(\sigma \in G_{n+1})$ of $\mathcal{F}_{n+1}$ split in $\mathcal{F}_{n+1}(\sqrt{\pi_n\alpha})/\mathcal{F}_{n+1}$ for some $[\alpha] \in \tilde{V}_n$. Again, by the same two lemmas, we see that $r_8(\tilde{A}_n) \ge 1$ if and only if $[\pi_n\alpha] \in \tilde{V}_{n+1,4}$ for some $[\alpha] \in \tilde{V}_n$; namely if and only if $[\pi_n\alpha] \in Q_{n+1}$ for some $[\alpha] \in \tilde{V}_n$ by Lemma 6.3.

As $[\alpha] \in \tilde{V}_n$, we have $\iota([\alpha]) \in J_n = (N_{f/n})$ by (4.10). Hence, we observe from (3.1) and (6.2) that

$$\begin{aligned} \iota([\pi_n\alpha]) &= \iota([\pi_n]) + \iota([\alpha]) = (1+\rho)^{2^f-(2^n+1)} + r_\alpha(1+\rho)^{2^f-2^n} \\ &= (1+\rho)^{2^f-(2^n+1)} \times u = \iota([\pi_n]) \times u \end{aligned} \tag{6.3}$$

with

$$u = 1 + r_\alpha(1+\rho).$$

Here, r_α is an element of $\mathcal{R}$ depending on α. As u is a unit of $\mathcal{R}$, we see that $r_8(\tilde{A}_n) \geq 1$ if and only if $[\pi_n] \in Q_{n+1}$. The ideal $(\iota([\pi_n]))$ of $\mathcal{R}$ coincides with $U_{2^f-(2^n+1)}$ by (6.2), and $\iota(Q_n) = \mathcal{Q}_n$ by definition. Therefore, we see from Lemma 3.6 that the condition $[\pi_n] \in Q_{n+1}$ is equivalent to

$$2^n + 1 = \dim_{\mathbb{F}_2} U_{2^f-(2^n+1)} \leq \dim_{\mathbb{F}_2} \mathcal{Q}_{n+1} = r_4(\tilde{A}_{n+1}).$$

Here, the last equality holds by Lemma 6.3. Therefore, we obtain the assertion. □

Proof of Proposition 1.8. Let $L_0 = \mathbb{Q}(\sqrt{2})$ and let $0 \leq n \leq f-1$. By Lemma 6.2, we have $r_4(A_n) \geq 1$ if and only if there is an unramified C_4-extension of $\mathcal{F}_n$ containing $L_{n+1} = \mathcal{F}_n(\sqrt{2})$. By Lemma 6.4 combined with Lemma 3.5, the last condition holds if and only if $\pi_n\alpha \gg 0$ for some $[\alpha] \in \tilde{V}_n$, namely if and only if $[\pi_n\alpha] \in V_{n+1}$ for some $[\alpha] \in \tilde{V}_n$. By (6.3), this is equivalent to $[\pi_n] \in V_{n+1}$. Thus, we have seen that $r_4(A_n) \geq 1$ if and only if $[\pi_n] \in V_{n+1}$. By (6.2), we have $(\iota([\pi_n])) = U_{2^f-(2^n+1)}$. Therefore, we observe from Lemma 3.6 that $[\pi_n] \in V_{n+1}$ if and only if

$$2^n + 1 = \dim_{\mathbb{F}_2} U_{2^f-(2^n+1)} \leq \dim_{\mathbb{F}_2} \iota(V_{n+1}).$$

Thus, we obtain the equivalence

$$r_4(A_n) \geq 1 \iff \dim_{\mathbb{F}_2} V_{n+1} \geq 2^n + 1. \tag{6.4}$$

(This holds even when $f = e$ and $n = f-1$ as we have defined V_n also for the case $n = e$.) First, assume that $n_p < \infty$ (so that $0 \leq n_p \leq f-1$). By Corollary 5.1(II), the 2-rank $c_p = r_2(A_{n_p})$ equals $\dim_{\mathbb{F}_2} V_{n_p}$ ($\leq 2^{n_p}$). When $n_p \geq 1$, we see that $\dim_{\mathbb{F}_2} V_{n_p} \geq 2^{n_p-1}+1$ from $r_4(A_{n_p-1}) \geq 1$ and (6.4). Thus, we obtain (1.5) in this case. When $n_p = 0$, $c_p = r_2(A_0) = 1$ by genus theory. Assume that $n_p = \infty$ and $f \leq e-1$. Then we have

$$2^{f-1} + 1 \leq \dim_{\mathbb{F}_2} V_f \ (< 2^f)$$

from $r_4(A_{f-1}) \geq 1$ and (6.4). Therefore, we obtain (1.6) from Corollary 5.1(II). □

Proof of Theorem 1.1. The assertion (I) is contained in Lemma 6.3.

Let us show (II-i). Let $0 \leq n \leq m_p - 1$. First, let $L_0 = \mathbb{Q}(\sqrt{2})$. Then, from the very definition of m_p, we have $r_8(\tilde{A}_n) \geq 1$ for each $0 \leq n \leq m_p - 1$. This implies that $r_4(\tilde{A}_n) = 2^n$ by Proposition 1.3 and (1.3). Here, the Λ-module $\tilde{A}_n$ satisfies the assumptions of Proposition 1.3 by Lemma 1.1 and Proposition 1.2. Then, we see from the assertion (I) that $r_4(\tilde{A}_n) = 2^n$ also for $L_0 = \mathbb{Q}(\sqrt{2\ell})$

with $\ell \in \mathbb{P}_+$.

Let us show (II-ii). Let $m_p \leq n \leq f-1$. For $L_0 = \mathbb{Q}(\sqrt{2})$, we have $r_8(\tilde{A}_{m_p}) = 0$ and $r_4(\tilde{A}_{m_p}) = b_p \leq 2^{m_p}$. Recall that $2^{m_p} = \dim_{\mathbb{F}_2} \tilde{V}_{m_p} = \dim_{\mathbb{F}_2} J_{m_p}$ by Lemma 4.2(II) and (4.10), and that $b_p = r_4(\tilde{A}_{m_p}) = \dim_{\mathbb{F}_2} \mathcal{Q}_{m_p}$ by Lemma 6.3.

First, assume that $b_p < 2^{m_p}$. Then, we observe that $\mathcal{Q}_{m_p} = \mathcal{Q} \cap J_{m_p} \subsetneq J_{m_p}$ by (4.13) and Lemma 3.6. This implies that $\mathcal{Q} \subsetneq J_{m_p}$ by Remark 3.2. Hence, $\mathcal{Q}_n = \mathcal{Q} \cap J_n = \mathcal{Q}_{m_p}$ for every $m_p \leq n \leq f-1$. Therefore, we see from Lemma 6.3 that

$$r_4(\tilde{A}_n) = \dim_{\mathbb{F}_2} \mathcal{Q}_n = b_p \ (< 2^n) \tag{6.5}$$

for $m_p \leq n \leq f-1$ and every L_0. We have

$$\Lambda/\Theta_n \cong (\mathbb{Z}/2)^{\oplus(2^n - b_p)} \oplus (\mathbb{Z}/4)^{\oplus b_p}$$

as abelian groups. Therefore, we see from Proposition 1.3 and (1.3) that (6.5) implies that $\tilde{A}_n$ or $\tilde{B}_n$ is isomorphic to Λ/Θ_n for each n according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$.

Next, assume that $b_p = 2^{m_p}$ and $m_p \leq f-2$. For $L_0 = \mathbb{Q}(\sqrt{2})$, we already know that $r_4(\tilde{A}_{m_p+1}) \leq 2^{m_p}$ by $r_8(\tilde{A}_{m_p}) = 0$ and Proposition 1.6. On the other hand, since $Q_{m_p} \subseteq Q_{m_p+1}$, we see from Lemma 6.3 that

$$b_p = 2^{m_p} = r_4(\tilde{A}_{m_p}) = \dim_{\mathbb{F}_2} Q_{m_p} \leq \dim_{\mathbb{F}_2} Q_{m_p+1} = r_4(\tilde{A}_{m_p+1}).$$

Therefore, we have $r_4(\tilde{A}_{m_p+1}) = b_p = 2^{m_p} < 2^{m_p+1}$ for $L_0 = \mathbb{Q}(\sqrt{2})$. Then, similarly to the case $r_4(\tilde{A}_{m_p}) = b_p < 2^{m_p}$, we can show that $r_4(\tilde{A}_n) = b_p \ (< 2^n)$ for every $m_p + 1 \leq n \leq f-1$ and every L_0. Therefore, for these n, we see from Proposition 1.3 and (1.3) that $\tilde{A}_n$ or $\tilde{B}_n$ is isomorphic to Λ/Θ_n according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $L_0 = \mathbb{Q}(\sqrt{2\ell})$. Let us deal with the case where ($b_p = 2^{m_p}$ and) $n = m_p \leq f-2$. For $L_0 = \mathbb{Q}(\sqrt{2})$, we have $\tilde{A}_{m_p} \cong (\mathbb{Z}/4)^{\oplus 2^{m_p}}$ as abelian groups from the definition of m_p. It follows from Proposition 1.3 and (1.3) that the Λ-module $\tilde{A}_{m_p}$ is isomorphic to Λ/Θ_{m_p} because

$$\Theta_{m_p} = (4, 2T^{b_p}, (1+T)^{2^{m_p}} + 1) = (4, (1+T)^{2^{m_p}} + 1)$$

as $b_p = 2^{m_p}$. For $L_0 = \mathbb{Q}(\sqrt{2\ell})$, we have $r_4(\tilde{A}_{m_p}) = 2^{m_p}$ by the assertion (I).

Let $b_p = 2^{m_p}$ and $m_p = f-1$. Then, the assertion is shown similarly to the above case where $b_p = 2^{m_p}$ and $n = m_p \leq f-2$. Thus, we have shown the assertion (II-ii).

Finally, we show (III). The assertion for $L_0 = \mathbb{Q}(\sqrt{2})$ follows from the definition of m_p, Proposition 1.3 and (1.3). Then, the assertion for $L_0 = \mathbb{Q}(\sqrt{2\ell})$ follows from (I). □

Proof of Theorem 1.2. The assertion (I) is contained in Corollary 5.1(III).

Let us show (II-i). Let $0 \leq n \leq n_p - 1$. For a while, let $L_0 = \mathbb{Q}(\sqrt{2})$. Then, from the definition of n_p, we have $r_4(A_n) \geq 1$ for these n. Therefore, we obtain $r_2(A_n) = 2^n$ by Propositions 1.2(I) and 1.3. Then, by the assertion (I), we see that $r_2(B_n) = 2^n$ for $L_0 = \mathbb{Q}(\sqrt{2\ell})$.

Let us show (II-ii). Let $n_p \leq n \leq e-1$. For a while, we let $L_0 = \mathbb{Q}(\sqrt{2})$. By the definition of n_p and Proposition 1.1, we have $r_4(A_{n_p}) = 0$ and $c_p = r_2(A_{n_p}) \leq 2^{n_p}$. By Proposition 1.3, we have $A_{n_p} \cong \Lambda/(2, T^{c_p})$ for $L_0 = \mathbb{Q}(\sqrt{2})$. It also follows that $\dim_{\mathbb{F}_2} V_{n_p} = c_p \leq 2^{n_p}$ by Corollary 5.1(II).

First, assume that $c_p < 2^{n_p}$. Then, we observe from Lemma 4.2 that $V_{n_p} \subsetneq \tilde{V}_{n_p}$ or equivalently $\iota(V_{n_p}) \subsetneq \iota(\tilde{V}_{n_p}) = J_{n_p}$. Since $V_{n_p} = V \cap \tilde{V}_{n_p}$, it follows that $\iota(V) \subsetneq J_{n_p}$ from Remark 3.2. This implies that $V \subsetneq \tilde{V}_{n_p}$. Therefore, we see that $V_{n_p} = V$ and that $V_n = V \cap \tilde{V}_n = V_{n_p}$ for every $n_p \leq n \leq e-1$. For these n, we see from Corollary 5.1(II) that when $L_0 = \mathbb{Q}(\sqrt{2})$,

$$r_2(A_n) = \dim_{\mathbb{F}_2} V_n = \dim_{\mathbb{F}_2} V_{n_p} = c_p < 2^n$$

and that when $L_0 = \mathbb{Q}(\sqrt{2\ell})$, $r_2(B_n) = c_p < 2^n$. Then, for these n, we observe from Proposition 1.3 that A_n or B_n is isomorphic to $\Lambda/(2, T^{c_p})$ according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$.

Next, assume that $c_p = 2^{n_p}$ and $n_p \leq e-2$. For a while, let $L_0 = \mathbb{Q}(\sqrt{2})$. Then, as $r_4(A_{n_p}) = 0$, we have $r_2(V_{n_p+1}) \leq 2^{n_p} < 2^{n_p+1}$ by (6.4). Further, as $V_n \subseteq V_{n+1}$, we see that

$$\dim_{\mathbb{F}_2} V_{n_p+1} \geq \dim_{\mathbb{F}_2} V_{n_p} = c_p = 2^{n_p}.$$

Hence, $\dim_{\mathbb{F}_2} V_{n_p+1} = 2^{n_p} < 2^{n_p+1}$. As $n_p+1 \leq e-1$, it follows from Corollary 5.1(II) that

$$r_2(A_{n_p+1}) = r_2(V_{n_p+1}) = c_p = 2^{n_p} < 2^{n_p+1}$$

for $L_0 = \mathbb{Q}(\sqrt{2})$. Then, for $n_p+1 \leq n \leq e-1$, we can show that A_n or B_n is isomorphic to $\Lambda/(2, T^{c_p})$ exactly similarly to the case $c_p = r_2(A_{n_p}) < 2^{n_p}$. Let us deal with the case $n = n_p$. We already remarked that $A_{n_p} \cong \Lambda/(2, T^{c_p})$ for $L_0 = \mathbb{Q}(\sqrt{2})$ at the beginning of the proof of (II-ii). Then, by the assertion (I), we obtain $r_2(B_{n_p}) = c_p$ for $L_0 = \mathbb{Q}(\sqrt{2\ell})$.

Finally, assume that $c_p = 2^{n_p}$ and $n_p = e-1$. (This case happens only when $f = e$). The assertion is shown exactly similarly to the above case for $n = n_p$. Thus, we have shown the assertion (II-ii).

Let us show (III). The assertion (III-i) is shown similarly to the assertion (II-i). Let us show (III-ii). As $r_2(A_f) = d_p$ for $L_0 = \mathbb{Q}(\sqrt{2})$, we have $\dim_{\mathbb{F}_2} V_f = d_p$ from Corollary 5.1(II). Let $f \leq n \leq e-1$. Then, as $V_n = V_f$, we see from Corollary 5.1(II) that $r_2(A_n)$ or $r_2(B_n)$ equals d_p according as $L_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{2\ell})$. On the other hand, $r_4(A_n) = 0$ for these n by Proposition 1.5 and Remark 1.1. Therefore, we obtain the assertion from Proposition 1.3. $\square$

7 Numerical data

In the previous sections, we were working with a fixed $e \geq 2$ and prime numbers p of the form $p = 2^{e+1}q + 1$. In this section, we deal with various e and various prime numbers $p < 10^4$, and we put

$$e_p = \mathrm{ord}_2(p-1) - 1 \quad \text{and} \quad f_p = \min\{e_p - \kappa_p + 1, e_p\},$$

so that we have $p = 2^{e_p+1}q + 1$ with $2 \nmid q$.

In Table 1 (resp. Table 2), we give the number of prime numbers $p < 10^4$ with $(e_p, \kappa_p) = (e, \kappa)$ (resp. $f_p = f$).

Table 1. The number of prime numbers with $(e_p, \kappa_p) = (e, \kappa)$.

$e \setminus \kappa$	0	1	2	3	4	5	6	7	8	total
0	308	311	0	0	0	0	0	0	0	619
1	0	0	314	0	0	0	0	0	0	314
2	35	39	77	0	0	0	0	0	0	151
3	5	12	18	36	0	0	0	0	0	71
4	2	1	3	10	19	0	0	0	0	35
5	0	0	2	2	6	11	0	0	0	21
6	0	1	0	0	2	3	5	0	0	11
7	0	0	0	0	1	0	1	3	0	5
8	0	0	0	0	0	0	0	0	1	1
total	350	364	414	48	28	14	6	3	1	1228

Table 2. The number of prime numbers with $f_p = f$.

f	0	1	2	3	4	5	6	total
	933	152	112	24	6	0	1	1228

Table 3 deals with prime numbers $p < 10^4$ with $f_p > 3$, Table 4 those with $f_p = 3$, and Table 5 those with $f_p = 2$ and $e_p \geq 3$. By Proposition 2.1, these are the prime numbers satisfying $r_8(\tilde{A}_0) = 1$ (or equivalently $m_p \geq 1$). In these tables, we give the data on the abelian groups $\tilde{A}_n$ and A_n for $n = 0$, 1 and 2. In the column $\tilde{A}_n$ (resp. A_n), the sequence of integers $\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_{\tilde{r}}$ (resp. $e_1, e_2, \ldots, e_r$) indicates that

$$\tilde{A}_n \cong \bigoplus_{i=1}^{\tilde{r}} \mathbb{Z}/2^{\tilde{e}_i} \qquad (\text{resp. } A_n \cong \bigoplus_{i=1}^{r} \mathbb{Z}/2^{e_i})$$

as abelian groups. The structures of the abelian groups $\tilde{A}_n$ and A_n can be computed by Magma [9] for $n = 0$, 1, 2 under the generalized Riemann hypothesis. It seems to be difficult to compute $\tilde{A}_3$ and A_3 by ordinary commands of Magma, because the extension degree $[\mathcal{F}_3 : \mathbb{Q}] = 16$ is large. However, we can determine the values of m_p, b_p, n_p, c_p and d_p from these data, except for d_{4993}. For $p = 4993$, we have $e_p = 6$, $f_p = 3$, $n_p = \infty$ in Table 4, and hence $d_p = r_2(A_3)$. We compute d_{4993} with another method, which we explain later. Note that in Table 4, $n_p = \infty$ but d_p is not defined for $p = 1553$, 4273 and 6481 since $e_p = f_p = 3$ for these p. (We are dealing with those n with $0 \le n \le e_p - 1$.)

On the other hand, Tables 6–8 list the prime numbers $p < 10^4$ with $e_p \ge 2$ and $r_8(\tilde{A}_0) = 0$ (or equivalently $m_p = 0$). These three tables correspond to the cases (ii), (iii) and (iv) in Proposition 2.1, respectively.

Table 3. $\tilde{A}_n$, A_n and invariants for prime numbers p with $f_p > 3$.

p	f_p	e_p	κ_p	$\tilde{A}_0$	$\tilde{A}_1$	$\tilde{A}_2$	m_p	b_p	A_0	A_1	A_2	n_p	c_p	d_p
6529	6	6	1	3	2,3	2,2,2,2	2	4	2	1,2	1,1,1,1	2	4	
257	4	7	4	3	2,3	1,2,2,2	2	3	2	2,2	1,1,1	2	3	
2113	4	5	2	3	2,2	1,1,2,2	1	2	3	1,2	1,1,1	2	3	
2593	4	4	0	4	2,2	1,1,2,2	1	2	3	1,1	1,1	1	2	
2657	4	4	1	3	2,3	1,2,2,2	2	3	2	2,2	1,1,1	2	3	
4513	4	4	0	4	2,2	1,1,2,2	1	2	4	1,1	1,1	1	2	
7489	4	5	2	3	2,2	1,1,2,2	1	2	3	1,1	1,1	1	2	

Table 4. $\tilde{A}_n$, A_n and invariants for prime numbers p with $f_p = 3$.

p	f_p	e_p	κ_p	$\tilde{A}_0$	$\tilde{A}_1$	$\tilde{A}_2$	m_p	b_p	A_0	A_1	A_2	n_p	c_p	d_p
337	3	3	0	3	2,2	1,1,2,2	1	2	2	2,2	1,1,1	2	3	
881	3	3	0	3	2,2	1,1,2,2	1	2	2	2,2	1,1,1	2	3	
1217	3	5	3	4	2,3	1,2,2,2	2	3	3	1,2	1,1,1	2	3	
1249	3	4	2	3	2,2	1,1,2,2	1	2	2	2,2	1,1,1	2	3	
1553	3	3	1	3	2,3	2,2,2,2	2	4	2	1,2	1,2,2,2	∞		–
1777	3	3	1	3	2,2	1,1,2,2	1	2	3	1,2	1,1,1	2	3	
2833	3	3	1	3	2,2	1,1,2,2	1	2	2	1,1	1,1	1	2	
4049	3	3	1	3	2,2	1,1,2,2	1	2	2	2,2	1,1,1	2	3	
4177	3	3	0	3	2,2	1,1,2,2	1	2	3	2,2	1,1,1,1	2	4	
4273	3	3	1	3	2,3	2,2,2,2	2	4	2	1,2	1,1,1,2	∞		–
4481	3	6	4	4	2,3	1,2,2,2	2	3	3	1,2	1,1,1	2	3	
4721	3	3	0	3	2,2	1,1,2,2	1	2	3	2,2	1,1,1,1	2	4	
4993	3	6	4	3	2,3	2,2,2,3	∞		2	1,2	1,1,1,2	∞		$*6$
5297	3	3	1	4	2,3	1,2,2,2	2	3	3	1,2	1,1,1	2	3	
6353	3	3	0	3	2,2	1,1,2,2	1	2	3	1,2	1,1,1	2	3	
6449	3	3	1	3	2,2	1,1,2,2	1	2	2	1,1	1,1	1	2	
6481	3	3	1	3	2,2	1,1,2,2	1	2	3	2,2	1,1,1,2	∞		–
6689	3	4	2	3	2,2	1,1,2,2	1	2	2	1,1	1,1	1	2	
7121	3	3	1	3	2,2	1,1,2,2	1	2	2	1,2	1,1,1,1	2	4	
8081	3	3	1	3	2,2	1,1,2,2	1	2	2	1,1	1,1	1	2	
8609	3	4	2	4	3,3	2,2,2,2	2	4	3	3,3	1,1,1,1	2	4	
9137	3	3	1	3	2,2	1,1,2,2	1	2	2	1,2	1,1,1,1	2	4	
9281	3	5	3	4	2,3	1,2,2,2	2	3	3	1,2	1,1,1	2	3	
9649	3	3	1	3	2,2	1,1,2,2	1	2	3	1,2	1,1,1	2	3	

Table 5. $\tilde{A}_n$, A_n and invariants for prime numbers p with $f_p = 2$ and $e_p \geq 3$.

p	f_p	e_p	κ_p	$\tilde{A}_0$	$\tilde{A}_1$	$\tilde{A}_2$	m_p	b_p	A_0	A_1	A_2	n_p	c_p	d_p
113	2	3	2	3	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
353	2	4	3	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
577	2	5	4	3	2,3	1,1,1,1	∞		2	2,2	1,1,1	∞		3
593	2	3	2	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
1153	2	6	5	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
1201	2	3	2	3	2,3	1,1,1,1	∞		3	1,2	1,1,1	∞		3
1601	2	5	4	3	3,3	1,1,1,1	∞		3	2,3	1,1,1,1	∞		4
1889	2	4	3	3	2,3	1,1,1,1	∞		2	1,2	1,1,1,1	∞		4
2129	2	3	2	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
2273	2	4	3	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
2689	2	6	5	3	2,2	1,1,1,1	1	2	2	2,2	1,1,1	∞		3
3089	2	3	2	4	2,2	1,1,1,1	1	2	4	1,1	1,1	1	2	
3121	2	3	2	3	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
3137	2	5	4	3	4,4	1,1,1,1	∞		3	3,4	1,1,1,1	∞		4
3217	2	3	2	3	2,3	1,1,1,1	∞		2	1,2	1,1,1,1	∞		4
3313	2	3	2	4	2,2	1,1,1,1	1	2	4	1,1	1,1	1	2	
3361	2	4	3	4	2,2	1,1,1,1	1	2	3	1,2	1,1,1	∞		3
3761	2	3	2	3	2,3	1,1,1,1	∞		3	1,2	1,1,1	∞		3
4001	2	4	3	3	2,3	1,1,1,1	∞		2	2,2	1,1,1	∞		3
4289	2	5	4	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
4657	2	3	2	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
4801	2	5	4	3	2,3	1,1,1,1	∞		2	1,2	1,1,1,1	∞		4
4817	2	3	2	3	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
5233	2	3	2	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
5393	2	3	2	4	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
5569	2	5	4	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
7393	2	4	3	3	2,2	1,1,1,1	1	2	2	1,1	1,1	1	2	
7793	2	3	2	3	2,3	1,1,1,1	∞		3	1,2	1,1,1	∞		3
7841	2	4	3	4	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
8161	2	4	3	3	2,2	1,1,1,1	1	2	2	1,2	1,1,1,1	∞		4
8209	2	3	2	3	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
8273	2	3	2	3	3,3	1,1,1,1	∞		3	2,2	1,1,1,1	∞		4
8369	2	3	2	3	2,2	1,1,1,1	1	2	2	2,2	1,1,1	∞		3
9377	2	4	3	3	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
9473	2	7	6	4	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
9521	2	3	2	4	2,2	1,1,1,1	1	2	3	1,2	1,1,1	∞		3
9601	2	6	5	4	2,2	1,1,1,1	1	2	3	1,1	1,1	1	2	
9697	2	4	3	3	2,2	1,1,1,1	1	2	2	1,2	1,1,1,1	∞		4

Table 6. Prime numbers p with $f_p = 2$ and $e_p = 2$.

p	$m_p = 0$, $b_p = 1$, $n_p = 0$ and $c_p = 1$
73,89,233,281,601,617,937,1033,1049,1097,1193,1289,1433,1481,1609,1721,1753,1801,1913, 2089,2281,2393,2441,2473,2857,2969,3049,3257,3449,3529,3673,3833,4057,4153,4201,4217, 4297,4409,4457,4937,5081,5113,5209,5689,5737,5881,6089,6121,6361,6521,6553,6569,6761, 6793,6841,6857,7129,7481,7529,7577,7753,7817,7993,8233,8537,8713,8761,8969,9001,9209, 9241,9337,9721,9769	

Table 7. Prime numbers p with $f_p = 1$ and $e_p = 2$.

p	$m_p = 0$, $b_p = 1$, $n_p = \infty$ and $d_p = 2$
41,137,313,409,457,521,569,761,809,857,953,1129,1321,1657,1993,2137,2153,2297,2377, 2521,2617,2633,2713,2729,2777,2953,3001,3209,3433,3593,3769,3881,3929,4073,4441,4649, 4729,4793,4889,4969,5273,5417,5449,5641,5657,5801,5849,5897,6073,6217,6329,6473,7001, 7177,7193,7321,7369,7417,7433,7561,7673,8009,8089,8297,8329,8377,8521,8681,9049,9161, 9257,9433,9497,9689,9817,9833,9929	

Table 8. Prime numbers p with $f_p = 1$ and $e_p \geq 3$.

p	$m_p = 0$, $b_p = 1$, $n_p = 0$ and $c_p = 1$
17,97,193,241,401,433,449,641,673,769,929,977,1009,1297,1361,1409,1489,1697,1873,2017, 2081,2161,2417,2609,2753,2801,2897,3041,3169,3329,3457,3617,3697,3793,3889,4129,4241, 4337,4561,4673,5009,5153,5281,5441,5521,5857,5953,6113,6257,6337,6577,6673,6737,6833, 6961,6977,7057,7297,7457,7537,7649,7681,7873,7937,8017,8353,8513,8641,8689,8737,8753, 8849,8929,9041,9857	

Let us look back our results using the data in the tables. In the following, we denote the groups $\tilde{B}_n$ and B_n in Theorems 1.1 and 1.2 for $L_0 = \mathbb{Q}(\sqrt{2l})$ with $l \in \mathbb{P}_+$ by $\tilde{B}_n(l)$ and $B_n(l)$. We use the symbols $\tilde{A}_n$ and A_n only for the case $L_0 = \mathbb{Q}(\sqrt{2})$.

First, let us look at $p = 6529$ in Table 3. As $f_p = e_p = 6$, our targets are the class groups of $\mathcal{F}_n$ with $0 \leq n \leq 5$. By Theorem 1.1 and the data in Table 3, we observe that

$$\begin{aligned}
\tilde{A}_0 &\cong \mathbb{Z}/8, \\
\tilde{A}_1 &\cong \mathbb{Z}/4 \oplus \mathbb{Z}/8, \\
\tilde{A}_2 &\cong (\mathbb{Z}/4)^{\oplus 4}, \\
\tilde{A}_n &\cong (\mathbb{Z}/2)^{\oplus(2^n-4)} \oplus (\mathbb{Z}/4)^{\oplus 4} \quad \cong \tilde{B}_n(l) \qquad \text{for} \quad 3 \leq n \leq 5.
\end{aligned}$$

Further, by Theorem 1.2 and the data in Table 3, we observe that

$$\begin{aligned}
A_0 &\cong \mathbb{Z}/4, \\
A_1 &\cong \mathbb{Z}/2 \oplus \mathbb{Z}/4, \\
A_2 &\cong (\mathbb{Z}/2)^{\oplus 4}, \\
A_n &\cong (\mathbb{Z}/2)^{\oplus 4} \qquad \cong B_n(l) \qquad \text{for} \quad 3 \leq n \leq 5.
\end{aligned}$$

The groups $\tilde{B}_n(\ell)$ and $B_n(\ell)$ are independent of ℓ for $3 \leq n \leq 5$. However, as Table 9 shows, the structures of $\tilde{B}_n(l)$ and $B_n(l)$ depend on l for $n = 0$, 1 and 2. This is caused by the data $m_p = 2$, $b_p = 2^{m_p}$, $n_p = 2$ and $c_p = 2^{n_p}$ in Table 3. Recall here that the assertion of Theorem 1.1(II-i) (resp. Theorem 1.2(II-i)) is divided into two cases according as $(n, b_p) = (m_p, 2^{m_p})$ (resp. $(n, c_p) = (n_p, 2^{n_p})$) or not.

Table 9. $\tilde{B}_n(l)$ and $B_n(l)$ for $p = 6529$ and $L_0 = \mathbb{Q}(\sqrt{2l})$.

l	$\tilde{B}_0(l)$	$\tilde{B}_1(l)$	$\tilde{B}_2(l)$	$B_0(l)$	$B_1(l)$	$B_2(l)$
97	2	2,2	2,2,2,2	1	1,1	1,2,2,2
137	2	2,2	2,2,2,2	2	2,2	1,1,1,1
193	2	2,2	2,2,2,2	1	1,1	1,1,1,2
233	2	2,2	2,2,2,3	1	1,1	1,1,2,2
241	2	2,2	2,2,2,2	1	1,1	2,2,2,2
353	3	2,3	2,2,2,2	2	2,3	1,1,1,1
449	2	2,2	2,2,2,2	1	1,1	2,2,2,2
521	2	2,2	2,2,2,2	2	1,2	1,1,1,1
569	2	2,2	2,2,2,2	2	1,2	1,1,1,1
593	3	2,3	2,2,2,2	3	1,2	1,1,1,1

Next, let us look at $p = 257$ in Table 3. As $f_p = 4$ and $e_p = 7$, our targets are the class groups of $\mathcal{F}_n$ with $0 \le n \le 6$. By Theorem 1.1, Corollary 1.2 and the data in Table 3, we see that

$$\begin{aligned}
\tilde{A}_0 &\cong \mathbb{Z}/8, \\
\tilde{A}_1 &\cong \mathbb{Z}/4 \oplus \mathbb{Z}/8, \\
\tilde{A}_2 &\cong \mathbb{Z}/2 \oplus (\mathbb{Z}/4)^{\oplus 3} && \cong \tilde{B}_2(l), \\
\tilde{A}_3 &\cong (\mathbb{Z}/2)^{\oplus 5} \oplus (\mathbb{Z}/4)^{\oplus 3} && \cong \tilde{B}_3(l), \\
\tilde{A}_n &\cong (\mathbb{Z}/2)^{\oplus 16} && \cong \tilde{B}_n(l) \qquad \text{for} \quad 4 \le n \le 6.
\end{aligned}$$

Further, by Theorem 1.2 and the data in Table 3, we see that

$$\begin{aligned}
A_0 &\cong \mathbb{Z}/4, \\
A_1 &\cong (\mathbb{Z}/4)^{\oplus 2}, \\
A_n &\cong (\mathbb{Z}/2)^{\oplus 3} && \cong B_n(l) \qquad \text{for} \quad 2 \le n \le 6.
\end{aligned}$$

The groups $\tilde{B}_n(\ell)$ and $B_n(\ell)$ are independent of ℓ for $2 \le n \le 6$. However, as Table 10 shows, the structures of $\tilde{B}_n(l)$ and $B_n(l)$ depend on l for $n = 0$ and 1. This is caused by the data $m_p = 2$, $b_p \ne 2^{m_p}$, $n_p = 2$ and $c_p \ne 2^{n_p}$ in Table 3.

Table 10. $\tilde{B}_n(l)$ and $B_n(l)$ for $p = 257$ and $L_0 = \mathbb{Q}(\sqrt{2l})$.

l	$\tilde{B}_0(l)$	$\tilde{B}_1(l)$	$\tilde{B}_2(l)$	$B_0(l)$	$B_1(l)$	$B_2(l)$
41	2	2,2	1,2,2,2	2	1,2	1,1,1
97	2	2,2	1,2,2,2	1	1,1	1,1,1
233	2	2,2	1,2,2,2	1	1,1	1,1,1
281	2	2,2	1,2,2,2	1	1,1	1,1,1
313	2	2,2	1,2,2,2	2	1,2	1,1,1
337	3	2,3	1,2,2,2	3	2,2	1,1,1
353	3	2,3	1,2,2,2	2	1,2	1,1,1
409	2	2,2	1,2,2,2	2	2,2	1,1,1
449	2	2,2	1,2,2,2	1	1,1	1,1,1
521	2	2,2	1,2,2,2	2	1,2	1,1,1

Let $p = 4993$, and let us briefly explain how to compute the value d_p in Table 4. Since $f_p = 3$ and $[k_3 : \mathbb{Q}] = 8$ is small, we can use Magma for computing d_p under the generalized Riemann hypothesis. We have $\dim_{\mathbb{F}_2} V_f = r_2(A_f) = d_p$ by Corollary 5.1(II). First, we explicitly compute the integer $\omega \in k_3$ defined by (4.6). Then, we have $\tilde{V} = \tilde{V}_f = \mathbb{F}_2[G_f] \cdot [\omega]$ and

$$V = V_f = \{[\alpha] \in \tilde{V}_f \mid \alpha \gg 0\} = (1+\rho)^{2^f - d_p} \tilde{V}_f \ (\cong (\mathbb{Z}/2)^{\oplus d_p}).$$

Here, the third equality for V_f holds by $\dim_{\mathbb{F}_2} V_f = d_p$ and Lemma 3.6(I). Next, we check using Magma that $\omega^{1+\rho}$ is not totally positive and $\omega^{(1+\rho)^2}$ is totally positive. This implies that $2^f - d_p = 2$ and hence $d_p = 6$.

References

[1] H. Cohn and J. C. Lagarias, On the existence of fields governing the 2-invariants of the classgroup of $\mathbb{Q}(\sqrt{dp})$ as p varies, Math. Comp. **41** (1983) 711–730.

[2] P. E. Conner and J. Hurrelbrink, Class Number Parity, (World Scientific, Singapore, 1988).

[3] F. Gerth, III, The 4-class ranks of quadratic fields, Invent. Math. **77**(3) (1984) 489–515.

[4] G. Gras, Class Field Theory: From Theory to Practice, (Springer, Berlin, 2003).

[5] H. Ichimura and H. Sumida-Takahashi, On the class group of an imaginary cyclic field of conductor $8p$ and 2-power degree, Tokyo J. Math. **44**(1) (2021) 157–174.

[6] H. Ichimura and H. Sumida-Takahashi, On the class groups of certain imaginary cyclic fields of 2-power degree, J. Math. Soc. Japan **74**(3) (2022), 945–972.

[7] P. Koymans, The 16-rank of $\mathbb{Q}(\sqrt{-p})$, Algebra Number Theory **14**(1) (2020) 37–65.

[8] D. Z. Milovic, On the 8-rank of narrow class groups of $\mathbb{Q}(\sqrt{-4pq})$, $\mathbb{Q}(\sqrt{-8pq})$, and $\mathbb{Q}(\sqrt{2pq})$, Int. J. Number Theory **14**(8) (2018) 2165–2193.

[9] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symb. Comput. **24**(3–4) (1997) 235–265.

[10] P. Morton, The quadratic number fields with cyclic 2-class groups, Pacific J. Math. **108**(1) (1983) 165–175.

[11] L. Rédei and H. Reichardt, Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math. **170** (1934) 69–74.

[12] H. Wada, A Table of Ideal Class Numbers of Real Quadratic Fields, (Sophia Kokyuroku in Mathematics, No. 10, 1981).

[13] L. C. Washington, Introduction to Cyclotomic Fields, 2nd. ed., (Springer, New York, 1997).

[14] Y. Yamamoto, Divisibility by 16 of class numbers of quadratic fields whose 2-class groups are cyclic, Osaka J. Math. **21** (1984) 1–22.

[15] L. Zhang and Q. Yue, Another case of a Scholz's theorem on class groups, Int. J. Number Theory **4**(3) (2008) 495–501.