Louboutin, S. and Okazaki, R.
Osaka J. Math.
36 (1999), 229-257

DETERMINATION OF ALL QUATERNION CM-FIELDS WITH IDEAL CLASS GROUPS OF EXPONENT 2

STÉPHANE LOUBOUTIN and RYOTARO OKAZAKI

(Received June 6, 1995)

1. Introduction

In [10], we determined all normal octic CM-fields with class number one and noticed that class numbers of quaternion octic CM-fields are always even. Here, quaternion octic fields, or simply, quaternion fields are number fields whose Galois groups are isomorphic to the quaternion group of order 8. Later, the first author [9] determined all quaternion CM-fields with class number two: there is exactly one such number field. Now determination of CM-fields with ideal class groups of exponent ≤ 2 is a natural extension of class number one and two problems. In this paper, we prove:

Main Theorem *There are exactly two quaternion* CM*-fields with ideal class groups of exponent* 2*. Namely, the two following quaternion CM-fields:*

$$\boldsymbol{Q}\left(\sqrt{-(2+\sqrt{2})(3+\sqrt{6})}\right)$$

with discriminant $2^{24}3^6$ *and class number* 2*, and*

$$\boldsymbol{Q}\left(\sqrt{-\frac{5+\sqrt{5}}{2}\,\frac{5+\sqrt{21}}{2}(21+2\sqrt{105})}\right)$$

with discriminant $3^6 5^6 7^6$ *and class number* 8*.*

The proof consists of algebraic discussion, analytic discussion and numerical computation. In chapter 2, we determine possible forms of quartic subfields of quaternion CM-fields whose class groups have 4-rank being zero. Then, we determine possible forms, as radical extensions, of such quaternion CM-fields. In this determination, we use Fröhlich's description of quaternion fields [2], various results on quadratic fields (e.g. Rédei-Reichardt Theorem [11] and Scholz' Theorem [12]) and Kubota's description of bicyclic biquadratic fields [5]. In chapter 3, we give upper bounds on discriminants of quaternion CM-fields whose class groups have exponent 2 by using

analytic estimate on the value of L-functions at $s = 1$ [6]. Then, we determine all such CM-fields by computing relative class numbers with an algorithm developed in [8].[1]

Let F be an arbitrary algebraic number field of finite degree. We use the following notations throughout this paper. We denote by D_F the discriminant, $\mathcal{C}(F)$ the ideal class group, $h(F)$ the class number, U_F the unit group, and U_F^+ the totally positive unit group of F. In this paper, prime numbers always mean positive rational prime numbers. A prime number p is said to be ramified in an extension F_1/F_2 of algebraic number fields if a prime ideal of F_1 above (p) is ramified in F_1/F_2. If p is ramified in $F/\boldsymbol{Q}$, p is said to be ramified in F. We denote by $t_{L/F}$ the number of finite primes of L which are ramified in L/F for an extension L/F. We abbreviate $t_L = t_{L/\boldsymbol{Q}}$. We denote by T_L the number of prime numbers ramified in L. (Note T_L counts prime ideals of $\boldsymbol{Q}$ while t_L counts prime ideals of L.) When p is a prime number, we denote by $e_F(p)$ the ramification index of p in $F/\boldsymbol{Q}$ and $f_F(p)$ the inertia degree of p in $F/\boldsymbol{Q}$. When F is a CM-field, $h^-(F)$ denotes the relative class number of F.

The letter N always denotes a quaternion field and K denotes a bicyclic biquadratic field.

2. Determination of Possible Forms of N

In this chapter, we determine possible forms of a quaternion CM-field N whose ideal class group has 4-rank being zero. We shall firstly review Fröhlich's description of quaternion fields. We shall secondly determine possible forms of the quartic subfield K of N (see Theorem 9.) We shall then determine possible forms of N as a radical extension (see Theorem 11.) We lastly give an efficient method for calculating decomposition of rational primes in $N/\boldsymbol{Q}$.

2.1. Fröhlich's description

We shall review Fröhlich's description [2] of quaternion fields that plays the central role in algebraic part of this paper. Before giving his description, we note that d_i's, which are discriminants here, slightly differ from d_i's of [2] which are square free integers. Now we quote Fröhlich's description:

Proposition 1 (Theorem 3 on [2, page 146]). *Let K be a bicyclic biquadratic field. Denote by d_1, d_2 and d_3 the discriminants of the three distinct quadratic subfields of K. Then there is a quaternion field N containing K if and only if the*

[1]The UBASIC program for computing these relative class numbers is available from the first author.

following condition is satisfied by all primes p's of $\boldsymbol{Q}$ *including the infinite prime:*

$$1 = \left(\frac{d_1, d_2}{p}\right)\left(\frac{-1, d_1}{p}\right)\left(\frac{-1, d_2}{p}\right). \tag{1}$$

Here $(\bullet, \bullet/\bullet)$ *is the Hilbert symbol.*

This condition at the infinite prime is equivalent to:

$$d_1 > 0, \quad d_2 > 0. \tag{2}$$

If p is a prime number coprime to D_K, (1) is trivial at p. If $p \mid d_2$ is a prime number coprime to d_1, (1) at p is rewritten in the Kronecker symbol and the parity of the contribution θ of p in the character $(d_2/\bullet)$:

$$\left(\frac{d_1}{p}\right) = \theta(-1) \tag{3}$$

If p divides all three of d_i's, we have $p = 2$. In this case, we pick up $d = d_i \equiv 4 \pmod 8$ and put $d' = d/4$. Then (1) reads:

$$d' \equiv 3 \pmod 8. \tag{4}$$

Proposition 1 also implies

(5) *If* 2 *does not totally ramify in* K, $d_i \not\equiv 4 \pmod 8$ *for* $i = 1, 2$ *and* 3.

The notion of pure quaternion field is useful for studying ramification in quaternion fields:

DEFINITION 2. *A quaternion field* N *is called a pure quaternion field if all prime numbers dividing* D_N *divide the discriminant of the quartic subfield of* N.

It is obvious that a quartic subfield of a quaternion field is uniquely defined. Conversely, a pure quaternion field is almost defined by the quartic subfield:

Lemma 3 (Theorem 4 on [2, page 146]). *Let* K *be bicyclic biquadratic field which satisfies the condition given in Proposition 1 and* $T = T_K$ *the number of prime numbers ramified in* K. *Then, the number of pure quaternion fields containing* K *is* 2^{T-1} *if the prime number* 2 *ramifies in* K *or* 2^{T-2} *otherwise.*

Pure quaternion fields are basis for studying all quaternion fields:

Lemma 4 (Theorem 4 on [2, page 146]). *For a quaternion field* N *and its quartic subfield* K, *we can find a pure quaternion field* $N_0 = K(\sqrt{\delta_0})$ *and a fundamental discriminant* Δ *coprime to* D_K *such that* $N = K(\sqrt{\Delta\delta_0})$.

Here, a fundamental discriminant is a discriminant of some quadratic field, i.e., it is either a square free integer congruent to 1 modulo 4 or four times a square free integer congruent to 2 or 3 modulo 4. Now, we can determine the discriminant of N as follows:

Proposition 5. *Let notations be as in Lemma 4. The discriminant D_N of N is written as $D_{N_0}\Delta^4$ in the notation of the Lemma 4 and the discriminant D_{N_0} of N_0 is given by $D_{N_0} = 16D_K^3$ if 2 has ramification index 2 in $K/\boldsymbol{Q}$ or $D_{N_0} = D_K^3$ otherwise.*

Proof. Let k be a quadratic subfield of N, χ the character associated to N/k, $\mathfrak{d}$ the conductor of χ and $\mathfrak{d}_2$ the conductor of χ^2. Set χ_Δ to be the character associated to $k(\sqrt{\Delta})/k$. Then $\chi_0 = \chi\chi_\Delta$ is associated to N_0/k. Since Δ and D_{N_0} are coprime, Conductor-Discriminant formula now implies $D_N = D_{N_0}\Delta^4$.

We factor D_{N_0} into prime powers. It is obvious that signatures and the odd components of D_{N_0} and D_K^3 or $16D_K^3$ agree. When (2) does not ramify in K, 2-components of discriminants are trivial and agree. When $e_K(2) = f_K(2) = 2$, we choose k to be the splitting field of (2) in $K/\boldsymbol{Q}$. We then look at localizations of N/k at primes above (2). It follows that 2-components of D_{N_0} and $16D_K^3$ agree.

It remains to show that 2-components of D_{N_0} and D_K^3 agree when $e_K(2) = 2$ and $f_K(2) = 1$ hold.

Let k be a subfield of K whose discriminant is not a multiple of 8. Then, $D_{N_0} = D_K D_k^2 N_{k/\boldsymbol{Q}}\mathfrak{d}^2$ and $D_K = D_k^2 N_{k/\boldsymbol{Q}}\mathfrak{d}_2$ holds. The choice of k implies (2) is either inert or ramified in $k/\boldsymbol{Q}$. When (2) is inert in $k/\boldsymbol{Q}$, (4) divides $\mathfrak{d}_2$ and our target is equivalent to $\mathfrak{d} = (2)\mathfrak{d}_2$. When (2) is ramified in $k/\boldsymbol{Q}$, (4) exactly divides $\mathfrak{d}_2$ and our target is equivalent to $\mathfrak{d} = (2)\mathfrak{d}_2$. Therefore it suffice to show the assertion that orders of the prime $\mathfrak{p}$ of k above (2) in $\mathfrak{d}$ and $(2)\mathfrak{d}_2$ agree. Obviously, we have $\chi^2(1+4\alpha) = \chi(1+8\alpha+16\alpha^2)$ for arbitrary integer α of k. With Hensel's Lemma, this implies $\chi(1+8\alpha) = 1$ for α such that $4\alpha \in \mathfrak{d}_2$. Since (4) divides $\mathfrak{d}_2$, we see $2\mathfrak{d}_2 \subset \mathfrak{d}$. Take an element $\beta \in \mathfrak{p}^{-1}\mathfrak{d}_2 - \mathfrak{d}_2$ such that $1 \neq \chi^2(1+\beta) = \chi(1+2\beta+\beta^2)$. Since we have $\beta^2 \in \mathfrak{p}^{-2}\mathfrak{d}_2^2 \subset (2)^{-1}(4)\mathfrak{d}_2 \subset \mathfrak{d}$ by $(\mathfrak{d}_2) \subset (4)$ and $2\mathfrak{d}_2 \subset \mathfrak{d}$, we see $\chi(1+2\beta) \neq 1$ while $2\beta \in \mathfrak{p}\mathfrak{d}_2$. Hence, we get $\mathfrak{p}\mathfrak{d}_2 \not\subset \mathfrak{d}$. Since $\mathfrak{p}^2\mathfrak{d}_2 = 2\mathfrak{d}_2 \subset \mathfrak{d} \subset \mathfrak{d}_2$, this implies $\mathfrak{d} = 2\mathfrak{d}_2$. ■

REMARK. It is not generally true that the conductor of χ is 2 times the conductor of χ^2, even if the conductors are even. A counterexample arises when the conductor of χ^2 is exactly divisible by (2). The choice of k in the proof is to avoid complicatedness coming from such a case. Indeed, we would have $\mathfrak{d} = 2\mathfrak{p}\mathfrak{d}_2$ if we have chosen k whose discriminant is a multiple of 8 in the case $e_K(2) = 4$.

2.2. Determination of possible forms of K

We determine possible forms of K by means of construction of appropriate ideal characters of appropriate quadratic subfields of K. We use norm residue symbols for such construction. The description obtained is however given in rational terms: it is written in term of rational congruences, the Legendre symbols and the rational quartic residue symbols $(\bullet/\bullet)_4$. Although the quartic residue symbols are defined up to inversion, we are interested in the values at quadratic residues and hence the ambiguity does not matter. We extend the rational quartic residue symbol by

$$(a/2)_4 = \begin{cases} +1 & \text{if} \quad a \equiv 1 \pmod{16} \\ -1 & \text{if} \quad a \equiv 9 \pmod{16} \end{cases} \tag{6}$$

for $a \equiv 1 \pmod 8$. We use Fröhlich's description [2] of quaternion fields, Rédei-Reichardt Theorem [11] and Scholz' Theorem [12]. We also implicitly use the theory of genera and the ambiguous ideal theory.

In this chapter, we write ε_d for the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$ which is greater than 1 in the embedding of $\boldsymbol{Q}(\sqrt{d}) \longrightarrow \boldsymbol{R}$ in which $\sqrt{d}$ becomes positive. We also write o_d for the ring of integers of $\boldsymbol{Q}(\sqrt{d})$. Let K be a real bicyclic biquadratic field, k_i $(i = 1, 2, 3)$ the three distinct quadratic subfields of K and d_i's respective discriminants of k_i's. Then, K contains square roots $\sqrt{d_1}$, $\sqrt{d_2}$ and $\sqrt{d_3}$. We choose the signature of $\sqrt{d_3}$ to be the product of the signatures of $\sqrt{d_1}$ and $\sqrt{d_2}$: $\sqrt{d_1}\sqrt{d_2} = d'\sqrt{d_3}$ for some positive integer d'. It turned out that confusion in the choice cause a delicate problem (§2.4..) The following fact is also implicitly used (see [5] for details including a numerical algorithm):

$$U_{k_1}^2 U_{k_2}^2 U_{k_3}^2 \subset U_K^2 \subset U_{k_1} U_{k_2} U_{k_3} \cap U_K^+. \tag{7}$$

We also quote the following class number formula for a real bicyclic biquadratic field (see e.g. [5]):

$$h(K) = \frac{Q_K}{4} h(k_1) h(k_2) h(k_3) \tag{8}$$

where Q_K is the unit index $Q_K = [U_K : U_{k_1} U_{k_2} U_{k_3}] \in \{1, 2, 4\}$.

Let N/k be a cyclic quartic extension. Then, construction of appropriate characters of k gives an unramified cyclic extension of degree $[N : k]$ over N when there are too many totally ramified prime ideals in N/k. For the construction of the character, we use norm residue symbols (see e.g. [4].) We denote by $k_{\mathfrak{p}}$ the localization of k at $\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ and $U_{k_{\mathfrak{p}}}$ the unit group of $k_{\mathfrak{p}}$. We use the fact that the Artin map canonically determines a character $U_{k_{\mathfrak{p}}} \to \mathrm{Gal}\,(M/k)$ for a cyclic extension M/k and a finite prime $\mathfrak{p}$. The order of the character is the ramification index of $\mathfrak{p}$. If $\mathfrak{p}$ is coprime to the order of $\mathrm{Gal}\,(M/k)$, the norm residue symbol becomes a power residue symbol modulo $\mathfrak{p}$ up to group isomorphism of

the image. In this case, we think of the norm residue symbol as the canonical power residue symbol. We sometimes identify the cyclic group $\mathrm{Gal}(U/k)$ with a suitable subgroup of $\boldsymbol{C}^1$ for convenience, in particular, elements of order 1 and 2 in $\mathrm{Gal}(U/k)$ become ± 1. (We use all values of norm residue symbols an power residue symbols in the following context. They are used in a different way from the way rational quartic residue symbols are used.) Products of norm residue symbols are then used in the following Lemma:

Lemma 6. *Let N be a quaternion field, $k = \boldsymbol{Q}(\sqrt{d})$ one of its quadratic subfields, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell$ finite primes of k, and $\chi^\sharp$ a product of odd powers of norm residue symbols of N/k at $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell$. Set $S = \{\pm 1\}$ if $N_{k/\boldsymbol{Q}}\varepsilon_d = -1$ or $S = \{1\}$ otherwise. Assume that $\chi^\sharp(\varepsilon_d) \in S$. Then, there is an ideal character χ of 2-power order of k such that $\chi((\alpha)) = \chi^\sharp(\alpha)$ for each totally positive integer α coprime to $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell$. Assume further that the 4-rank of $\mathcal{C}(N)$ is zero. Then, the extension of k associated to χ^2 is contained in N. The order of χ is 4 if one of the $\mathfrak{p}_i$'s is totally ramified in N/k.*

Proof. The assumption on $\chi^\sharp(\varepsilon_d)$ implies that $\chi^\sharp(U_k^+) = 1$ and $\chi^\sharp(U_k) \subset \{\pm 1\}$. Embed U_k/U_k^+ into $\{\pm 1\}^2$ by signature and extend $\chi^\sharp : U_k/U_k^+ \longrightarrow \{\pm 1\}$ to a character χ_∞ of $\{\pm 1\}^2$. Identify χ_∞ with the character it induces on $k^\times$ via signature. Then, the product $\chi' = \chi^\sharp\chi_\infty$ vanishes on U_k. Hence, there is an ideal character χ such that $\chi((\alpha)) = \chi'(\alpha)$ for each element α of $k^\times$. Taking a suitable odd power, we can choose χ so that the order of χ is a 2-power. This implies the first statement. Let L be the extension of k associated to χ and M the extension of k associated to χ^2. By construction of L, LN/N is unramified cyclic extension of a 2-power degree. (Note that N is totally imaginary.) If M is not contained in N, then LN/N must be an unramified cyclic extension whose relative degree is a multiple of 4. Hence, $\mathcal{C}(N)$ must have a non-trivial 4-rank, which contradicts the assumption on $\mathcal{C}(N)$. Therefore, the second statement of the Lemma holds. Assume that some $\mathfrak{p}_i$ $(1 \leq i \leq \ell)$ is totally ramified in N/k, i.e., the order of the norm residue symbol at $\mathfrak{p}_i$ is 4. Then 4 divides the order of χ and $\mathfrak{p}_i$ has the ramification index 2 in M/k associated to χ^2. Comparison of ramification indices shows that $M \subset N$ is a proper subfield of N and hence M/k is quadratic. Therefore, the order of χ^2 is 2, or equivalently, the order of χ is 4. We have proven the last statement of the Lemma. ■

The following two Lemmas are used for calculation of quadratic residue symbols at fundamental units.

Lemma 7. *Let $q_1, q_2, \ldots, q_t$ be even number of distinct prime numbers congruent to 3 modulo 4 and $d = q_1q_2\ldots q_t$. Write $\mathfrak{q}_i$ for the prime ideal of $\boldsymbol{Q}(\sqrt{d})$ above q_i for $1 \leq i \leq t$. Then, $(\varepsilon_d/\mathfrak{q}_i) = -1$ for some $1 \leq i \leq t$.*

Lemma 8. *Let $q \equiv 3 \pmod 8$ be a prime number and $\mathfrak{q}$ be the prime ideal of $\boldsymbol{Q}(\sqrt{q})$ above q. Then, $(\varepsilon_q/\mathfrak{q}) = -1$.*

These two Lemmas are proven in a similar way. Hence, we give a proof of the former and omit that of the latter.

Proof.[2] Define a and b by $\varepsilon_d = a + b\sqrt{d}$ if $\varepsilon_d \in \boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$ or $\varepsilon_d^3 = a + b\sqrt{d}$ otherwise. Then, $a + b\sqrt{d}$ becomes the fundamental unit of $\boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$.

Taking norm, we see that $a^2 - b^2 d = 1$. (The sign of the right hand side is plus since q_i's are congruent to 3 modulo 4.) This identity implies the congruence $a^2 - b^2 \equiv 1 \pmod 4$ which implies that a is odd and b is even. The identity also reads $(a-1)(a+1) = b^2 d$.

Suppose that the q_i divides $a - 1$ for each $1 \leq i \leq t$. Then, the claims of the previous paragraph implies that there is a decomposition $b = 2b_1 b_2$ such that $a - 1 = 2b_1^2 d$ and $a + 1 = 2b_2^2$. Subtracting these identities, we get $b_2^2 - b_1^2 d = 1$ where $0 < |b_1| \leq b/2 < b$. This contradicts the choice of a and b in the first paragraph of this proof. Hence, some q_i must divide $a + 1$. Therefore, we have $a + b\sqrt{d} \equiv -1 \pmod{\mathfrak{q}_i}$. Since $q_i \equiv 3 \pmod 4$, this implies $(\varepsilon_d/\mathfrak{q}_i) = (a + b\sqrt{d}/\mathfrak{q}_i) = (-1/\mathfrak{q}_i) = (-1/q_i) = -1$. ■

We recall $Q_K = [U_K : U_{k_1} U_{k_2} U_{k_3}]$ for a real bicyclic biquadratic field K with three distinct subfields k_1, k_2 and k_3.

Theorem 9. *Let N be a quaternion* CM*-field whose ideal class group has 4-rank being zero, K the quartic subfield of N. Then, the number $T = T_K$ of prime numbers ramified in K is at most 3, the number t_K of finite primes of K ramified in $K/\boldsymbol{Q}$ is at most 4, class number $h(K)$ of K is odd and the 2-rank ρ of U_K^+/U_K^2 is one. More specifically K is of one of the following forms:*

1a. *$K = \boldsymbol{Q}(\sqrt{2}, \sqrt{q})$, $t_K = 4$, $T = 2$ and $Q_K = 2$ with $q \equiv 1 \pmod 8$ such that*

$$\left(\frac{q}{2}\right)_4 \left(\frac{2}{q}\right)_4 = -1;$$

1b. *$K = \boldsymbol{Q}(\sqrt{p}, \sqrt{q})$, $t_K = 4$, $T = 2$ and $Q_K = 2$ with $p \equiv q \equiv 1 \pmod 4$ which satisfy $p < q$ and*

$$\left(\frac{p}{q}\right) = 1,$$

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = -1;$$

2a. *$K = \boldsymbol{Q}(\sqrt{2}, \sqrt{qr})$, $t_K = 4$, $T = 3$ and $Q_K = 2$ with $q \equiv r \equiv 3 \pmod 8$ such that $q < r$;*

[2] Franz Lemmermeyer kindly told us this elementary proof. The authors would like to express their gratitude to him.

2b. $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{2r})$, $t_K = 4$, $T = 3$ *and* $Q_K = 2$ *with* $p \equiv 5 \pmod 8$ *and* $r \equiv 3 \pmod 4$ *such that*

$$\left(\frac{p}{r}\right) = -1;$$

2c. $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{qr})$, $t_K = 4$, $T = 3$ *and* $Q_K = 2$ *with* $p \equiv 1 \pmod 4$ *and* $q \equiv r \equiv 3 \pmod 4$ *such that* $q < r$ *and*

$$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1;$$

3a. $K = \boldsymbol{Q}(\sqrt{2q}, \sqrt{qr})$, $t_K = T = 3$ *and* $Q_K = 4$ *with* $q \equiv 7 \pmod 8$ *and* $r \equiv 3 \pmod 8$ *such that*

$$\left(\frac{r}{q}\right) = -1;$$

3b. $K = \boldsymbol{Q}(\sqrt{pq}, \sqrt{qr})$, $t_K = T = 3$ *and* $Q_K = 4$ *with* $p \equiv q \equiv r \equiv 3 \pmod 4$ *such that*

$$\left(\frac{q}{p}\right) = \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1$$

or

4. $K = \boldsymbol{Q}(\sqrt{2}, \sqrt{q})$, $t_K = T = 2$ *and* $Q_K = 4$ *with* $q \equiv 3 \pmod 8$.

Here p, q, r *denote distinct prime numbers. The 2-rank* ρ' *of* $U_K \cap N_{N/K}N^\times / U_K^2$ *is at most* 1 *in all cases and* $\rho' = 0$ *except possibly in case 3a and 3b.*

Corollary 10. *The two numbers* t_K *and* ρ' *satisfy the following inequality:*

$$t_K + \rho' \leq 4. \tag{9}$$

Proof of Theorem 9. To avoid inessential complicatedness such as introducing notation for 2-class numbers, we assume that the odd part of $\mathcal{C}(N)$ is trivial. This assumption implies that the class numbers of quadratic subfields of K are powers of 2.

We have $e_K(p) \leq 2$ for each odd prime p. Now, we divide the proof into the following four cases, which are discussed in separate subsections:

1. Two prime numbers $p < q$ satisfy
   $e_K(p) = e_K(q) = 2$ and $f_K(p) = f_K(q) = 1$;
2. Exactly one prime number p satisfies
   $e_K(p) = 2$ and $f_K(p) = 1$;
3. All prime numbers ramified in K have inertia degree 2 in K or
4. All odd prime numbers ramified in K have inertia degree 2 in K and $e_K(2) = 4$.

2.2.1. Case 1

Let k be the splitting subfield of p in K. Write $\mathfrak{p}$ and $\mathfrak{p}'$ for the two primes of k above p. Let $\chi_{\mathfrak{p}}$ and $\chi_{\mathfrak{p}'}$ be the respective norm residue symbols of N/k at $\mathfrak{p}$ and $\mathfrak{p}'$. Then, we have $\chi_{\mathfrak{p}} \circ N_{k/Q} = \chi_{\mathfrak{p}}\chi_{\mathfrak{p}'}^3$ by commutation relation of $\mathrm{Gal}(N/\boldsymbol{Q})$. Let $\chi^{\natural}$ be the Dirichlet character induced by $\chi_{\mathfrak{p}}$. Put $\chi^{\sharp} = \chi^{\natural} \circ N_{k/Q}$ on numbers and $\chi = \chi^{\natural} \circ N_{k/Q}$ on ideals. Then, Lemma 6 implies that K is associated to χ^2. The transfer Theorem in class field theory implies that K is the composite of k and the quadratic field associated to the Dirichlet character induced by $(\chi^{\natural})^2$, i.e., $\boldsymbol{Q}(\sqrt{p}) \subset K$. The same argument proves $\boldsymbol{Q}(\sqrt{q}) \subset K$. Therefore, K is of the form $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{q})$ where p and q are prime numbers not congruent to 3 modulo 4. The assumption on p and q eliminates the possibility of $q = 2$. Now (q) splits as $(q) = \mathfrak{q}\mathfrak{q}'$ in $\boldsymbol{Q}(\sqrt{p})$. Let $\chi_{\mathfrak{q}}$ be the norm residue symbol of $N/\boldsymbol{Q}(\sqrt{p})$ at $\mathfrak{q}$. If $\chi_{\mathfrak{q}}^2(\varepsilon_p) = 1$, we would have $\chi_{\mathfrak{q}}(\varepsilon_p) = \pm 1$. Hence, application of Lemma 6 to a product of $\chi_{\mathfrak{q}}$ and a suitable character at infinity would imply that K/k would be associated to a suitable extension of $\chi_{\mathfrak{q}}^2$ to ideal classes. However, K/k is also ramified at $\mathfrak{q}'$, a contradiction. Hence, we have

$$\chi_{\mathfrak{q}}^2(\varepsilon_p) = -1. \tag{10}$$

Since q is odd, $\chi_{\mathfrak{q}}^2$ is written by the quadratic residue symbol $\chi_{\mathfrak{q}}^2 = (\bullet/\mathfrak{q})$. By Scholz' Theorem, the above identity implies that $(p/q)_4(q/p)_4 = -1$ and that $\mathcal{C}\left(\boldsymbol{Q}(\sqrt{pq})\right)$ has 4-rank being zero. The former gives the form of K stated in cases 1a and 1b. The latter implies that $K = \boldsymbol{Q}(\sqrt{\varepsilon_{pq}})$ since the 4-rank of the strict ideal class group of $\boldsymbol{Q}(\sqrt{pq})$ is 1 by the Rédei-Reichardt Theorem [11]. Thus, we have $Q_K = 2$. This implies that $h(K) = 1$ since $h(\boldsymbol{Q}(\sqrt{p}))$ and $h(\boldsymbol{Q}(\sqrt{q}))$ are one and $h(\boldsymbol{Q}(\sqrt{pq})) = 2$. Since $\varepsilon_{pq} \gg 0$, either $p\varepsilon_{pq}$ or $q\varepsilon_{pq}$ is a square of a totally positive element $\xi(p,q)$ of $\boldsymbol{Q}(\sqrt{pq})$. Let r be one of p or q chosen so that $r\varepsilon_{pq} = \xi(p,q)^2$:

$$r\varepsilon_{pq} = \xi(p,q)^2 \quad r = p \text{ or } q, \text{ and } 0 \ll \xi(p,q) \in \boldsymbol{Q}(\sqrt{pq}). \tag{11}$$

Put

$$\eta = \eta(p,q) = \xi(p,q)/\sqrt{r}\varepsilon_r \gg 0. \tag{12}$$

Then $\eta\varepsilon_r$ is a square root of ε_{pq}. Thus, we have $U_K^+ = U_K^2 \cup \eta U_K^2$ and $\rho = 1$. We now show that $\rho' = 0$. Suppose contrary $\rho' > 0$. Then, $\rho' = \rho = 1$ and η would be a norm in N/K. Taking relative norm to $\boldsymbol{Q}(\sqrt{r})$, we see ε_r^2 would be a norm in $N/\boldsymbol{Q}(\sqrt{r})$. However, an argument similar to (10) shows that ε_r^2 cannot be a norm residue in $N/\boldsymbol{Q}(\sqrt{r})$. We are led to a desired contradiction, proving $\rho' = 0$. This finishes case 1.

2.2.2. Case 2

The same argument to the one given in case 1 shows $\boldsymbol{Q}(\sqrt{p}) \subset K$. By (3), the discriminant d of the splitting subfield k of p in K is a product of coprime negative prime discriminants. Since d is positive, d is a product of an even number of prime discriminants.

We firstly investigate odd divisors of d. Let q be an odd prime divisor of d. Then (q) remains prime in $\boldsymbol{Q}(\sqrt{p})$. and the norm residue symbol of $N/\boldsymbol{Q}(\sqrt{p})$ at qo_p gives the quartic residue symbol $(\bullet/qo_p)_4$. On the other hand, $q \equiv 3 \pmod 4$ implies

$$(\varepsilon_p/qo_p)_4^2 = (\varepsilon_p/qo_p) = (N_{\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q}}(\varepsilon_p)/q) = (-1/q) = -1.$$

We secondly show that the discriminant d is a product of exactly two coprime negative prime discriminants. Suppose contrary that d has at least three prime factors. Then, two distinct odd prime numbers q and r divide d. As was shown in the previous paragraph, the respective quartic residue symbols $(\bullet/qo_p)_4$ and $(\bullet/ro_p)_4$ given by the norm residue symbols of $N/\boldsymbol{Q}(\sqrt{p})$ at qo_p and ro_p satisfy $(\varepsilon_p^2/qo_p)_4 = (\varepsilon_p^2/ro_p)_4 = -1$. Thus, $\chi^\sharp = (\bullet/qo_p)_4(\bullet/ro_p)_4$ satisfies $\chi^\sharp(\varepsilon_p^2) = 1$, i.e., $\chi^\sharp(\varepsilon_p) = \pm 1$. Since $N_{\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q}}(\varepsilon_p) = -1$, application of Lemma 6 to $\chi^\sharp$ implies that $K/\boldsymbol{Q}(\sqrt{p})$ is associated to $(\bullet/qo_p)_4^2(\bullet/ro_p)_4^2 = (\bullet/qo_p)(\bullet/ro_p)$. Hence, qo_p and ro_p are the only ramified ideals in K/k, contradicting the assumption of this paragraph. Therefore, d is a product of exactly two coprime negative prime discriminants.

Let $q < r$ be the two distinct prime divisors of d. As we saw in the first paragraph, neither q nor r is congruent to 1 $\pmod 4$. If $p = 2$, $K = \boldsymbol{Q}(\sqrt{2}, \sqrt{qr})$ is of the form 2a. If pd is odd, $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{qr})$ is of the form 2c. If d is even, (5) implies $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{2r})$ which is in the form 2b. Thus, the form of K falls into one of 2a, 2b or 2c.

Now, we investigate numeric invariants. We show that U_K is generated by $-1, \varepsilon_p, \varepsilon_{qr}$ and a square root of ε_{pqr}. The fundamental unit ε_{pqr} of k is totally positive since $r \equiv 3 \pmod 4$. Thus one of the prime ideals above p, q and r is principal. Solving congruences $x^2 - pqry^2 \equiv \pm 4p, \pm 4q$ or $\pm 4r$ modulo p if p is odd or $x^2 - pqry^2 \equiv \pm p, \pm q$ or $\pm r$ modulo 8 if $p = 2$, we see that the prime ideal above p in $\boldsymbol{Q}(\sqrt{pqr})$ is principal. Solving the same congruences modulo r, we see that the prime ideal above p in $\boldsymbol{Q}(\sqrt{pqr})$ is generated by an integer which has a negative norm. Thus, there is a totally positive integer $\xi(p;q,r)$ such that:

$$\xi(p;q,r)^2 = qr\varepsilon_{pqr} \quad 0 \ll \xi(p;q,r) \in \boldsymbol{Q}(\sqrt{pqr}). \tag{13}$$

We have $(\xi(p;q,r)/\sqrt{qr})^2 = \varepsilon_{pqr}$. The fundamental unit ε_{qr} of k is totally positive since $r \equiv 3 \pmod 4$. Thus $r\varepsilon_{qr}$ is a square in k. Since $\sqrt{r} \notin K$, ε_{qr} is non-square in K. We now see that U_K has the desired system of generators. This determination of generators implies that $Q_K = 2$, that $\rho = 1$ or more precisely $U_K^+ = U_K^2 \cup \varepsilon_{qr} U_K^2$.

The latter also uses the fact $\xi(p;q,r)/\sqrt{qr}$ has the same signature as $\sqrt{qr}$. Using Rédei-Reichardt Theorem, we see

$$h(\boldsymbol{Q}(\sqrt{p})) = h(\boldsymbol{Q}(\sqrt{qr})) = 1; \quad h(\boldsymbol{Q}(\sqrt{pqr})) = 2.$$

This together with $Q_K = 2$ implies that $h(K) = 1$.

Lastly, we show that $\rho' = 0$. Suppose contrary that $\rho' = \rho = 1$ or more specifically that ε_{qr} were a norm in N/K. Then ε_{qr}^2 would be a norm in N/k. Let $\chi_{\mathfrak{p}}$ be the norm residue symbol of N/k at a prime $\mathfrak{p}$ of k above p. Then, the hypothesis implies that $\chi_{\mathfrak{p}}^2(\varepsilon_{qr}) = \chi_{\mathfrak{p}}(\varepsilon_{qr}^2) = 1$. On the other hand, $\chi_{\mathfrak{p}}^2(-1) = \chi_{\mathfrak{p}}((-1)^2) = 1$ is clear. Thus, $\chi_{\mathfrak{p}}^2$ would be trivial on $U_{\boldsymbol{Q}(\sqrt{qr})}$. Using the fact that $\mathfrak{p}$ is totally ramified in N/k, we see that the order of $\chi_{\mathfrak{p}}^2$ is 2. Noting that $h(\boldsymbol{Q}(\sqrt{qr})) = 1$, we see that $\chi_{\mathfrak{p}}^2$ would induce an ideal character of order 2. Let L be the extension of $\boldsymbol{Q}(\sqrt{qr})$ associated to it. The normal closure of L would be a totally real dihedral octic field containing K. Thus, LK/K would be an unramified quadratic extension while $h(K) = 1$. Hence, we are led to a desired contradiction, proving $\rho' = 0$. We finish case 2.

2.2.3. Case 3

By (3), discriminants d_i's are products of coprime negative prime discriminants. We firstly show that $t_{K/k_i} \leq 2$ for $i = 1, 2$ and 3. Let k be one of the k_i's and d its discriminant. Suppose that more than two primes are ramified in K/k. Then, at least two odd primes are ramified in K/k. Remembering the assumption of this case, we pick up two odd prime numbers p_1 and p_2 such that $p_1 o_d$ and $p_2 o_d$ are ramified primes in K/k. The norm residue symbols of N/k at p_1 and p_2 define the quartic residue symbols $(\bullet/p_1 o_d)_4$ and $(\bullet/p_2 o_d)_4$ respectively. Similar argument to the second paragraph of case 2 shows that $(\varepsilon_d/p_i o_d)_4 = \pm 1$ for $i = 1$ and 2. If $(\varepsilon_d/p_i o_d)_4 = 1$ for $i = 1$ or 2, Lemma 6 applied to k and $p_i o_d$ leads to a contradiction. If $(\varepsilon_d/p_1 o_d)_4 = (\varepsilon_d/p_2 o_d)_4 = -1$, Lemma 6 applied to k, $p_1 o_d$ and $p_2 o_d$ leads to a contradiction to that three primes are ramified in K/k. Hence we must have $t_{K/k} \leq 2$ for each quadratic subfield k of K.

We secondly show that $t_{K/k} = 1$ for some quadratic subfield k of K. In fact, we shall see in the next paragraph that $t_{K/k} = 1$ for each quadratic subfield k of K. Separation of the proof of this fact in two steps is a detour to overcome the difficulty due to the behavior of prime ideal above (2). Let p be the smallest prime number ramified in K and k the inertia subfield of K at p. Then, the discriminant d of k is odd and $t_{K/k} \geq 1$. Suppose that there is a prime number $r > p \geq 2$ such that r remains inert in $k/\boldsymbol{Q}$ and ro_d ramifies in K/k. As was shown in the first paragraph, $(\varepsilon_d/ro_d)_4 = 1$ implies $t_{K/k} = 1$ contrary to the supposition. Thus, we must have $(\varepsilon_d/ro_d)_4 = -1$. By Lemma 7, there is a prime ideal $\mathfrak{q}$ of k ramified

in $k/\boldsymbol{Q}$ such that $(\varepsilon_d/\mathfrak{q}) = -1$. Now, Lemma 6 applied to k, ro_d and $\mathfrak{q}$ implies that ro_d is the only ramified prime in K/k, a contradiction. Hence we must have $t_{K/k} = 1$.

We now show that $t_{K/k_i} = 1$ for $i = 1, 2$ and 3 or equivalently that the discriminant d_i of each k_i is a product of exactly two coprime negative prime discriminants. Let p, k and d be as in the previous paragraph. We assume without loss of generality that $k = k_1$. Then d decomposes into a product $d = d'_2 d'_3$ of coprime fundamental discriminants and the field K is of the form $K = \boldsymbol{Q}(\sqrt{p^* d'_2}, \sqrt{p^* d'_3})$ where p^* is a prime discriminant divisible by p. The result of the first paragraph implies d'_2 is a product of at most two prime discriminants. As was said in the beginning of this case, the discriminant $d_2 = p^* d'_2$ is a product of coprime negative prime discriminants. On the other hand, d_2 is positive. Combining these three points, we see that d_2 is a product of exactly two coprime negative prime discriminants. The same argument proves that d_3 is also a product of exactly two coprime negative prime discriminants. These imply that d'_2 and d'_3 are prime discriminants and hence that $d = d'_2 d'_3$ is also a product of exactly two coprime negative prime discriminants. Hence each discriminant d_i is a product of exactly two coprime negative prime discriminants.

Now, using (5) if the prime number 2 ramifies in K, we see that $K = \boldsymbol{Q}(\sqrt{pq}, \sqrt{qr})$ for prime numbers p, q and r which are not congruent to 1 (mod 4) such that

$$\left(\frac{-q}{p}\right) = \left(\frac{-r}{q}\right) = \left(\frac{-p}{r}\right) = 1.$$

Here, we assume without loss of generality that $p < q, r$; $d'_2 = -r$ and $d'_3 = -q$. The forms of K in case 3a and 3b follow easily.

We now proceed to numeric invariants. For simplicity we write

$$p_1 = p, \quad p_2 = q, \quad p_3 = r. \tag{14}$$

Here the numbering (mod 3) is chosen so that p_i and d_i are coprime: $k_i = \boldsymbol{Q}(\sqrt{p_{i+1}p_{i+2}})$. It is easily verified that

$$h(\boldsymbol{Q}(\sqrt{pq})) = h(\boldsymbol{Q}(\sqrt{qr})) = h(\boldsymbol{Q}(\sqrt{rp})) = 1. \tag{15}$$

In particular, we have that $p_i \varepsilon_{p_i p_{i+2}}$ is a square in $\boldsymbol{Q}(\sqrt{p_i p_{i+2}})$. Recall that

$$d_{i+1} = \begin{cases} 4p_i p_{i+2} & 2 \mid p_i p_{i+2}, \\ p_i p_{i+2} & 2 \nmid p_i p_{i+2}. \end{cases} \tag{16}$$

Using congruence, we see that the equation

$$x^2 - d_{i+1} y^2 = -4p_i \tag{17}$$

has positive rational integral solutions in x and y. We set

$$\pi(p_i, p_{i+2}) = (x + y\sqrt{d_{i+1}})/2 \tag{18}$$

or equivalently let $\pi(p_i, p_{i+2})$ be an integer in $\boldsymbol{Q}(\sqrt{p_i p_{i+2}})$ of norm $-p_i$. Then,

$$\eta(p_i, p_{i+1}, p_{i+2}) = \pi(p_{i+1}, p_i)\pi(p_{i+2}, p_{i+1})/\sqrt{p_{i+1}p_{i+2}} \tag{19}$$

is a unit such that

$$\eta(p_i, p_{i+1}, p_{i+2})^2 = \varepsilon_{d_i}\varepsilon_{d_{i+1}} \quad \text{and} \quad \eta(p_i, p_{i+1}, p_{i+2})\sqrt{p_i p_{i+1}} \gg 0. \tag{20}$$

On the other hand, $\varepsilon_{d_{i+1}}$ is non-square in K since $p_i\varepsilon_{d_{i+1}}$ is a square in K while $\sqrt{p_i} \notin K$. Therefore, we have $Q_K = 4$, $\rho = 1$ and $h(K)$ is odd. Unfortunately, we cannot determine ρ' without specifying N in this case.

2.2.4. Case 4

Similar argument to case 2 and case 3 shows that the number of odd ramified primes in the relative extension K over each quadratic subfield of K is at most 1. Inspecting the signature of prime discriminants and using (4), we see that K is of the form given in case 4 of the Theorem or

$$K = \boldsymbol{Q}(\sqrt{2r}, \sqrt{q})$$

with $q \equiv 3 \pmod 8$, $r \equiv 3 \pmod 4$ and $(q/r) = -1$. The latter possibility is eliminated by a similar argument to the third paragraph of case 3 with Lemma 8. Thus, K must be of the form given in case 4 of the Theorem.

Numeric invariants are determined in [9]. ■

2.3. Determination of possible forms of N's as radical extensions

We shall determine possible forms of quaternion fields containing K's described in the previous section as follows:

Theorem 11. *Let N be a quaternion* CM*-field whose class group has 4-rank being zero and K its quartic subfield. Then, N is written as a radical extension $N = K(\sqrt{-\delta(N)})$ with a totally positive element $\delta(N) = -\Delta\delta_0$ of K. Here δ_0 is a product of quadratic integers in appropriate quadratic subfields and Δ is a fundamental discriminant coprime to D_K. Moreover, the norm of δ_0 divides D_K and $N_0 = K(\sqrt{\delta_0})$ is a pure quaternion field.*

We only need to determine all pure quaternion fields containing K and to appeal to Lemma 4. However, we must not forget to determine real pure quaternion fields, since Δ can be negative in Lemma 4. Therefore, we determine all pure quaternion fields containing K which is of one of the forms listed in Theorem 9.

Lemma 3 and the following Lemmas are essential for this determination and are used without mention:

Lemma 12. *Let δ be an integer of K. Then $K(\sqrt{\delta})$ is a quaternion field if and only if $N_{K/k_i}\delta \in (K^\times)^2 \setminus (k_i^\times)^2$ for $i = 1, 2$ and 3.*

We also use the following Lemma for studying the behavior of 2.

Lemma 13. *Let $d \equiv 1 \pmod 4$ be a fundamental discriminant, α an integer in $\boldsymbol{Q}(\sqrt{d})$ and a the norm of α. Assume that $a \equiv 1 \pmod 4$ and that $\alpha^2 = |a|\,\varepsilon_d$. Then, α or $-\alpha$ is a square modulo $4o_d$.*

Proof. The following facts are easily verified:

1. $\alpha^2 \notin \boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$. if $\alpha \notin \boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$;
2. $d \equiv 5 \pmod 8$ if $\varepsilon_d \notin \boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$;
3. $\alpha^3 \in \boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$ if $d \equiv 5 \pmod 8$.

In the situation of the Lemma, these three points imply that $\alpha\varepsilon_d = \alpha^3/|a|$ resides in $\boldsymbol{Z} + \boldsymbol{Z}\sqrt{d}$. Write $\alpha\varepsilon_d = b + c\sqrt{d}$. The condition on the norm implies the congruence $b^2 - c^2 \equiv 1 \pmod 4$. Hence, b is odd and c is even. We now have the following congruence:

$$\alpha\varepsilon_d = b + c\sqrt{d} = b - c + 2c \cdot (1 + \sqrt{d})/2 \equiv b - c \equiv \pm 1 \pmod{4o_d}. \tag{21}$$

The condition on α^2 and that on the norm a imply

$$\alpha^2 = |a|\,\varepsilon_d \equiv \pm\varepsilon_d \pmod{4o_d}. \tag{22}$$

These two congruences imply the desired statement. ■

Put

$$\pi = \pi(p) = \begin{cases} +\sqrt{p}\varepsilon_p & \text{if} \quad p \equiv 1 \pmod 8 \quad \text{or} \quad p = 2, \\ -\sqrt{p}\varepsilon_p & \text{if} \quad p \equiv 5 \pmod 8. \end{cases} \tag{23}$$

Then, $\sqrt{\pi}$ generates a cyclic quartic field whose conductor is a power of p.

Proof of Theorem 11. The possible forms of N are determined in the following cases according to the cases listed in Theorem 9. (The radicand δ_0 is a radicand in one of "Lemma RE"'s that apply to the given K.)

2.3.1. Case 1

Let r be one of p or q satisfying

$$\xi(p,q)^2 = r\varepsilon_{pq}, \quad \text{for some } 0 \ll \xi(p,q) \in \boldsymbol{Q}(\sqrt{pq}). \tag{24}$$

Put

$$\eta(p,q) = \xi(p,q)/\pi(r) \tag{25}$$

where $\pi(r)$ is defined by (23). Put,

$$\delta(p,q) = \pi(p)\pi(q)\eta(p,q). \tag{26}$$

Then, $K\left(\sqrt{\pm\delta(p,q)}\right)$ are quaternion fields. Counting pure quaternion fields, we see

Lemma RE1a. *In case 1a, $K\left(\sqrt{\pm\delta(p,q)}\right)$ are all of pure quaternion fields containing K.*

We must take care of the behavior of 2 if D_K is odd. The field $K\left(\sqrt{\pi(p)\pi(q)}\right)$ is an abelian octic field of conductor pq. On the other hand, the strict class field of K is $K\left(\sqrt{-\eta(p,q)}\right)$. Therefore

Lemma RE1b. *In case 1b, $K\left(\sqrt{-\delta(p,q)}\right)$ is the only pure quaternion field containing K.*

This finishes case 1.

2.3.2. Case 2

Let $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{qr})$ allowing one of p or q to be 2. We already know that $qr\varepsilon_{pqr}$ is a square of a totally positive integer $\xi(p;q,r)$ in $\boldsymbol{Q}(\sqrt{pqr})$. Set

$$\delta(p;q,r) = \pi(p)\xi(p;q,r). \tag{27}$$

Then, $K(\sqrt{\pm\delta(p;q,r)})$ and $K(\sqrt{\pm\delta(p;q,r)\varepsilon_{qr}})$ are quaternion fields. Counting pure quaternion fields, we see

Lemma RE2a + RE2b. *Write $\delta = \delta(p;q,r)$. Then, $K(\sqrt{\pm\delta})$ and $K(\sqrt{\pm\delta\varepsilon_{qr}})$ are all of pure quaternion fields containing K in case 2a or 2b.*

Now we proceed to the case of D_K being odd. We must take care of the behavior of 2 in this case. By Lemma 13, we have

(28) *We can choose the sign $s = s(p;q,r) = \pm 1$ such that $s\xi(p;q,r)$ is a square modulo 4 in $\boldsymbol{Q}(\sqrt{pqr})$.*

Recalling that $q\varepsilon_{qr}$ is a square in $\boldsymbol{Q}(\sqrt{qr})$ and that $\boldsymbol{Q}(\sqrt{qr},\sqrt{-q})/\boldsymbol{Q}(\sqrt{pqr})$ is unramified at finite primes, we see

Lemma RE2c. *Write $\delta=\delta(p;q,r)$ and $s=s(p;q,r)$. Then, $K\left(\sqrt{s\delta}\right)$ and $K\left(\sqrt{-s\delta\varepsilon_{qr}}\right)$ are all of pure quaternion fields containing K in case 2c.*

This finishes case 2.

2.3.3. Case 3

In this case, it is convenient to number everything according to the numbering $p_1=p$, $p_2=q$ and $p_3=r$. Here, $p=p_1$ may be 2. Thus, we follow the convention in the proof of Theorem 9. Moreover, we write

$$\epsilon_i=\varepsilon_{p_{i+1}p_{i+2}} \tag{29}$$

for the fundamental units of k_i's. We know that there is an integer π_i in k_{i+1} such that

$$\pi_i^2=p_i\epsilon_{i+1}\quad \pi_i\sqrt{p_{i-1}p_i}\in k_{i+1}^+. \tag{30}$$

Put

$$\delta(p_1,p_2,p_3)=\pi_1\pi_2\pi_3. \tag{31}$$

Then, $K\left(\sqrt{\pm\delta(p_1,p_2,p_3)}\right)$ and$K\left(\sqrt{\pm\delta(p_1,p_2,p_3)\varepsilon_{qr}}\right)$are quaternion fields: Counting pure quaternion fields, we see that

Lemma RE3a. *Write $\delta=\delta(p,q,r)$. Then, $K\left(\sqrt{\pm\delta}\right)$ and $K\left(\sqrt{\pm\delta\varepsilon_{qr}}\right)$ are all of pure quaternion fields containing K in case 3a.*

Now assume that $p_1\neq 2$ or equivalently $2\not| \ D_K$. By Lemma 13, we have

(32) *We can choose $s_i=\pm 1$ so that $s_i\pi_i$ is a square modulo 4 in k_{i+1}.*

(33) *Put $s(p,q,r)=s_1s_2s_3$.*

Then, we have the following Lemma:

Lemma RE3b. *Write $\delta=\delta(p,q,r)$ and $s=s(p,q,r)$. Then, $K\left(\sqrt{s\delta}\right)$ and $K\left(\sqrt{-s\delta\varepsilon_{qr}}\right)$ are the all two pure quaternion fields containing K in case 3b.*

We finished case 3.

2.3.4. Case 4

Let $\mathfrak{q}$ be the prime ideal of $\boldsymbol{Q}(\sqrt{2q})$ above q. Then, it is easily verified by congruence that $\mathfrak{q}$ has a totally positive generator $\xi(q)$:

$$\xi(q)^2 = q\varepsilon_{2q} \quad 0 \ll \xi(q) \in \boldsymbol{Q}(\sqrt{2q}). \tag{34}$$

We have

Lemma RE4. *Write $\delta = \delta(q) = (2+\sqrt{2})\xi(q)$. Then, $K(\sqrt{\pm\delta})$ are all two pure quaternion* CM*-fields containing K in case 4.*

We finished case 4 and hence all cases.■

2.4. Character associated to N/K

We shall give here an efficient method for calculating the decomposition law of a quaternion field N which is determined in Theorem 11 through "Lemma RE"'s in §2.3.. This enables us to compute the multiplicative functions $n \mapsto \phi_n$ in the notation of [8] and to compute the relative class number $h^-(N)$ when N is a CM-field. Let K, Δ and δ_0 as in Theorem 11. Further let d_1, d_2 and d_3 be discriminants of the three distinct quadratic subfields of K. Let l be a prime number and $\mathfrak{L}$ a prime ideal of K above l. We discuss the behavior of $\mathfrak{L}$ in N/K according to the behavior of l in $K/\boldsymbol{Q}$. The following three cases are easy (with j denoting a natural number):

(35) *If l ramifies in $K/\boldsymbol{Q}$, $\mathfrak{L}$ ramifies in N/K and $\phi_{l^j} = 0$,*

(36) *If l divides Δ, $\mathfrak{L}$ ramifies in N/K and $\phi_{l^j} = 0$,*

(37) *If l does not ramify in $K/\boldsymbol{Q}$, divide Δ nor split completely in $K/\boldsymbol{Q}$, $\mathfrak{L}$ remains inert in N/K. Further, $\phi_{l^j} = (j/2+1)(-1)^{j/2}$ if j is even or $\phi_{l^j} = 0$ if j is odd.*

We look at N over a quadratic subfield of K containing the inertia subfield of l in $K/\boldsymbol{Q}$ for the first point. The second point follows from the definition of a pure quaternion field and Theorem 11. For the third point, we merely look at N over the splitting subfield of l in $K/\boldsymbol{Q}$.

Hereafter, we assume that l splits completely in $K/\boldsymbol{Q}$ and that l does not divide Δ. Then $\phi_{l^j} = \frac{1}{2}(k+1)(k+2)(k+3)\sigma_l^j$ with $\sigma_l = +1$ or -1 according as $\mathfrak{L}$ splits or remains inert in N/K. Since l splits completely in $K/\boldsymbol{Q}$, the completion $K_{\mathfrak{L}}$ of K at $\mathfrak{L}$ is isomorphic to the l-adic field $\boldsymbol{Q}_l$. The image of $\Delta\delta_0$ under this isomorphism is a square if and only if $\mathfrak{L}$ splits in N/K or $\sigma_l = +1$. Now, we make this procedures explicit. By Theorem 11, we can write δ_0 as a product of three quadratic integers, say $(a_i + b_i\sqrt{d_i})/2$ for $i = 1, 2$ and 3. Let δ_1 and δ_2 be respective square roots of d_1 and d_2 in $\boldsymbol{Q}_l$. Define δ_3 by $\delta_1\delta_2 = d'\delta_3$ in $\boldsymbol{Q}_l$ with d' being the

positive integer such that $\sqrt{d_1}\sqrt{d_2} = d'\sqrt{d_3}$. Then, the image of $\Delta\delta_0$ under the isomorphism $K_{\mathfrak{L}} \tilde{\to} \boldsymbol{Q}_l$ equals $\Delta\prod_{i=1}^{3}(a_i + b_i s_i \delta_i)/2$ for some triple of signs s_1, s_2 and s_3 from ± 1. The choice of $\sqrt{d_3}$ in K and that of δ_3 in $\boldsymbol{Q}_l$ forces $s_3 = s_1 s_2$. On the other hand, four choices for a pair (s_1, s_2) corresponds to four conjugates of $\mathfrak{L}$. Noting that $N_{K/\boldsymbol{Q}}(\Delta\delta_0)$ is coprime to l, that $U_{\boldsymbol{Q}_l}/U_{\boldsymbol{Q}_l}^2 \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ and that N and K are normal, we see that the class of $\Delta\prod_{i=1}^{3}(a_i + b_i s_i \delta_i)/2$ modulo $U_{\boldsymbol{Q}_l}^2$ is independent of the choice of a pair (s_1, s_2). This means that the "signs" of respective square roots δ_1 and δ_2 of d_1 and d_2 need not be determined while the square root δ_3 of d_3 need be calculated from δ_1 and δ_2.

For an odd prime l, the class modulo $U_{\boldsymbol{Q}_l}^2$ is determined by the Legendre symbol $\sigma_l = (\Delta\delta_0/\mathfrak{L}) = (2\Delta\prod_{i=1}^{3}(a_i + b_i\delta_i)/l)$ which is calculated in $\boldsymbol{F}_l$.

For $l = 2$, the procedure becomes slightly complicated. In this case, all d_i's are congruent to 1 modulo 8. Further, each norm $(a_i^2 - b_i^2 d_i)/4$ is odd by Theorem 11. Then, a_i and b_i are even. Put $A_i = a_i/2$ and $B_i = b_i/2$. Then, $\sigma_2 = +1$ or -1 according as $\Delta\prod_{i=1}^{3}(A_i + B_i\delta_i) \equiv 1$ or 5 modulo 8. Here, δ_1 and δ_2 are chosen so that $\delta_i \equiv 1$ or 3 modulo 8 according as $d_i \equiv 1$ or 9 modulo 16 while $\delta_3 = \delta_1\delta_2/d'$.

3. Proof of Main Theorem

3.1. Analytic lower bounds

Let N be a quaternion CM-field and K its quartic subfield. Then numeric invariants $Q_N = 1$ and $w_N = 2$ are known [10] where Q_N is the Hasse's unit index of N and w_N is the number of roots of unity in N. There is no confusion between notations Q_N and Q_K: the former is defined for CM-fields and the latter is defined for real bicyclic biquadratic fields. We proved in [9] that the quotient ζ_N/ζ_K of Dedekind zeta functions of N and K is non-negative in the interval $]0, 1[$. Hence, we have:

Proposition 14 (see [6, Theorem 1 and 2(a)]). *Let N be a quaternion CM-field such that the Dedekind zeta function of its quartic subfield K satisfies*

$$\zeta_K\left(1 - \frac{2}{\log(D_N)}\right) \leq 0. \tag{H}$$

Then, we have:

$$h^-(N) \geq \left(1 - \frac{8\pi e^{1/4}}{D_N^{1/8}}\right)\frac{1}{4e\pi^4}\frac{1}{\mathrm{Res}_{s=1}(\zeta_K)}\frac{\sqrt{D_N/D_K}}{\log(D_N)}. \tag{38}$$

Moreover, the hypothesis (H) *is satisfied provided that we have*

$$h^-(N) \leq \frac{1}{16e}\sqrt{\frac{D_N}{D_K^2}}. \tag{39}$$

We point out that for any real bicyclic biquadratic field K we have:

$$\mathrm{Res}_{s=1}(\zeta_K) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_3) = \frac{8\log(\epsilon_1)\log(\epsilon_2)\log(\epsilon_3)}{\sqrt{d_1d_2d_3}}h_1h_2h_3,$$

i.e.

$$\mathrm{Res}_{s=1}(\zeta_K) = \frac{32\log(\epsilon_1)\log(\epsilon_2)\log(\epsilon_3)}{Q_K\sqrt{d_1d_2d_3}}h(K) \tag{40}$$

where χ_i, ϵ_i, d_i and h_i stand for the characters, the fundamental units, the discriminants and the class numbers of the three real quadratic subfields k_i of K. Hence, $d_1d_2d_3 = D_K$ and (38) may be written

$$h(N) \geq \left(1 - \frac{8\pi e^{1/4}}{D_N^{1/8}}\right)\frac{Q_K}{128e\pi^4\log(\epsilon_1)\log(\epsilon_2)\log(\epsilon_3)}\frac{\sqrt{D_N}}{\log(D_N)}. \tag{41}$$

Lemma 15. *Set $c = 2 + \gamma - \log(4\pi)$ and $c' = 2 + \gamma - \log(\pi)$, where $\gamma = 0.577215\cdots$ is the Euler's constant, so that we have $3c \leq 0.14$ and $3c' \leq 4.3$. Let K be a bicyclic biquadratic field. Then,*

$$\mathrm{Res}_{s=1}(\zeta_K) \leq \frac{1}{216}\big(\log(D_K) + 3c\big)^3. \tag{42}$$

Moreover, if 2 is ramified in K then

$$\mathrm{Res}_{s=1}(\zeta_K) \leq \frac{1}{864}\big(\log(D_K) + 3c'\big)^3. \tag{43}$$

Moreover, if 2 is totally ramified in K, then the inequality above is valid with 1728 instead of 864.

Proof. From [7] we know that we have $L(1,\chi_i) \leq \frac{1}{2}\big(\log(d_i) + c\big)$ in general or $L(1,\chi_i) \leq \frac{1}{4}\big(\log(d_j) + c'\big)$ if 2 is ramified in k_i. Let us note that if 2 is ramified in K then 2 is ramified in at least two of its quadratic subfields. Now, the Lemma follows from the arithmetic-geometric mean inequality $XYZ \leq \frac{1}{27}(X+Y+Z)^3$ applied to $\sum_{i=1}^{3}\log d_i = \log D_K$.■

Now our strategy is as follows.

Firstly, using the ambiguous class number formula, we show that if a quaternion CM-field has an ideal class group of exponent 2 then (39) is satisfied, except for a finite number of K's for which we use a trick that shows that the hypothesis (H) is satisfied.

Secondly, using (38) and (42) we thus get an upper bound on the discriminants of quaternion CM-fields that have ideal class groups of exponent 2.

Thirdly, using the method developed in [8], we compute the relative class numbers of the quaternion CM-fields of discriminants less than or equal to this upper bound.

Lemma 16. *If N is a quaternion* CM*-field with ideal class group of exponent* 2, *then $h(K) = 1$ and $h^-(N) \leq 2^{4m+3}$ where m is the number of prime integers that divide D_N and do not divide D_K, i.e. m is the number of distinct prime divisors of Δ in Theorem 11.*

Proof. Firstly, we remind the reader of the ambiguous class number formula. An ideal class of N is said to be *ambiguous* (in N/K) if it remains invariant under the complex conjugation. We let $A(N/K)$ be the subgroup of the ideal class group of N consisting of ambiguous ideal classes. Let $t_{N/K}$ be the number of prime ideals of K that ramify in N/K. Then, using the ambiguous class number formula by Chevalley (see [1] or [3]), noticing that the $[K : \boldsymbol{Q}]$ infinite primes of K ramify in N/K and noticing that the index $[U_K : U_K^2]$ is equal to $2^{[K:\boldsymbol{Q}]}$, we have:

$$\#A(N/K) = 2^{t_{N/K}-1}[U_K \cap N_{N/K}(N^\times) : U_K^2]h(K).$$

By Theorem 9, $h(K)$ is 1 in our situation. Therefore, this ambiguous class number formula implies that the 2-rank of $\mathcal{C}(N)$ is $t_{N/K}-1+\rho'$ with ρ' defined in Theorem 9. Indeed, every ideal class of $\mathcal{C}(N)$ is ambiguous since every ideal class in $\mathcal{C}(N)$ has order 2 . Thus, $h(K) = \#A(N/K)$.

Since there are at most four prime ideals of K above any finite prime that divides D_N and does not divide D_K, we have $t_{N/K} \leq 4m+t_K$ where t_K is the number of prime ideals in K that ramify in $K/\boldsymbol{Q}$. The result follows from Corollary 10.■

For $m \geq 0$, set $\Delta_0 = 1$ and $\Delta_m = l_1 l_2 \cdots l_m$ with $3 = l_1 < 4 = l_2 < 5 = l_3 < \cdots < l_m$ where the l_i's $i \geq 3$ is the increasing sequence of odd primes greater than 3. Proposition 5 implies $D_N \geq D_K^3 \Delta_m^4$ with m being as in Lemma 16.

Lemma 17. *If the ideal class group of a quaternion* CM*-field N has exponent* 2, *then the hypothesis* (H) *of Proposition 14 is satisfied if $D_K \geq 382617$ or if $D_K \geq 23914$ and 2 has ramification index 2 in $K/\boldsymbol{Q}$.*

Proof. Noticing that $h^-(N) \leq 8 \cdot 4^{2m}$ (see Lemma 16) and $\sqrt{D_N/D_K^2} \geq \Delta_m^2\sqrt{D_K}$, it suffices to show that we have

$$\left(\frac{\Delta_m}{4^m}\right)^2 = \left(\frac{l_1}{4}\frac{l_2}{4}\cdots\frac{l_m}{4}\right)^2 \geq \frac{128e}{\sqrt{D_K}}. \tag{44}$$

But one can easily check that $(9/16) \geq (128e/\sqrt{D_K})$ implies (44), so that (44) is satisfied if $D_K \geq 382617$. Moreover, if 2 has ramification index 2 in $K/\boldsymbol{Q}$, then we have $\sqrt{D_N/D_K^2} \geq 4\Delta_m^2\sqrt{D_K}$ by Proposition 5, which implies the second result.■

Using the fact that the Dedekind zeta function of a bicyclic biquadratic field is the product of the Riemann zeta function and the three L-functions of Dirichlet characters associated to the three quadratic subfields of K, we have the following result which enables us to show that the hypothesis (H) is satisfied when we have $D_K \leq 382616$.

Lemma 18. *Let k be a real quadratic field of conductor d and quadratic character χ. Then, the Dedekind zeta function of k is negative on $]0,1[$ provided that $S(n) = \sum_{a=1}^{n}\sum_{b=1}^{a}\chi(b)$ satisfies $S(n) \geq 0,\ 1 \leq n \leq d$.*

3.2. Upper bounds on D_K

Let us assume that K is a quartic subfield of a quaternion CM-field N with ideal class group of exponent 2 such that the hypothesis (H) is satisfied. Then, we have:

$$f_K(m) := \left(1 - \frac{8\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K \Delta_m^2 16^{-m}}{\left(\log(D_K) + 0.14\right)^3 \log(D_K^3 \Delta_m^4)} \leq \frac{4e\pi^4}{27}. \tag{45}$$

Indeed, $D_N \geq D_K^3 \Delta_m^4$ and $h^-(N) \leq 2^{4m+3}$ by Proposition 5 and from (38) and (40) we get

$$\left(1 - \frac{8\pi e^{1/4}}{(D_N)^{1/8}}\right) \frac{\sqrt{D_N/D_K}}{\left(\log(D_K) + 3c\right)^3 \log(D_N)} \leq \frac{e\pi^4}{54} h^-(N). \tag{46}$$

Now, one can easily see that we have $f_K(m) \geq f_K(2)$, $m \geq 0$ (simply look at $f_K(m+1)/f_K(m)$). Hence (45) implies

$$\left(1 - \frac{8\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K}{\left(\log(D_K) + 0.14\right)^3 \log(12^4 D_K^3)} \leq \frac{64e\pi^4}{243}. \tag{47}$$

One can easily check that (47) implies

$$D_K \leq 25 \cdot 10^6.$$

Moreover, instead of using (42), for a fixed K that satisfies hypothesis (H) let us use (40). We get a more restrictive inequality than (47), namely:

$$\left(1 - \frac{8\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K}{\log(12^4 D_K^3)} \leq \frac{512e\pi^4}{9} \mathrm{Res}_{s=1}(\zeta_K). \tag{48}$$

Moreover, if we assume that 2 has ramification index 2 in K, then Δ is odd. Hence, for $m \geq 0$ we set $f_0 = 1$ and $\Delta'_m = l_1 l_2 \cdots l_m$ with $3 = l_1 < 5 = l_2 < 7 = l_3 < \cdots < l_m$ where the l_i's $i \geq 1$ is the increasing sequence of odd primes greater than 1 (This sequence $\{\Delta'_m\}$ is slightly different from the previous sequence $\{\Delta_m\}$ which contains 4.) Then, Proposition 5 implies $D_N \geq 16 D_K^3 {\Delta'_m}^4$. Following the same line of reasoning as above and using (43) instead of (42), we have:

$$f_K(m) := \left(1 - \frac{4\sqrt{2}\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K {\Delta'_m}^2 16^{-m}}{\left(\log(D_K) + 4.3\right)^3 \log(16 D_K^3 {\Delta'_m}^4)} \leq \frac{e\pi^4}{108}. \tag{49}$$

Indeed, $D_N \geq 16 D_K^3 {\Delta'_m}^4$ and $h^-(N) \leq 2^{4m+3}$ and from (38) and (43) we get

$$\left(1 - \frac{4\sqrt{2}\pi e^{1/4}}{(D_N)^{1/8}}\right) \frac{\sqrt{D_N/D_K}}{\left(\log(D_K) + 3c'\right)^3 \log(D_N)} \leq \frac{e\pi^4}{216} h^-(N). \tag{50}$$

Now, one can easily see that we have $f_K(m) \geq f_K(1)$, $m \geq 0$. Hence (49) implies

$$\left(1 - \frac{4\sqrt{2}\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K}{\left(\log(D_K) + 4.3\right)^3 \log(1296 D_K^3)} \leq \frac{4e\pi^4}{243}. \tag{51}$$

One can easily check that (51) implies

$$D_K \leq 2 \cdot 10^6.$$

Moreover, instead of using (43), for a fixed K that satisfies hypothesis (H) let us use (40). We get a more restrictive inequality than (47), namely:

$$\left(1 - \frac{4\sqrt{2}\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K}{\log(1296 D_K^3)} \leq \frac{128 e\pi^4}{9} \mathrm{Res}_{s=1}(\zeta_K). \tag{52}$$

Finally, if 2 is totally ramified in K, then $D_N \geq D_K^3 \Delta_m^4$ and we get

$$\left(1 - \frac{8\pi e^{1/4}}{D_K^{3/8}}\right) \frac{D_K}{\log(81 D_K^3)} \leq \frac{512 e\pi^4}{9} \mathrm{Res}_{s=1}(\zeta_K). \tag{53}$$

All Lemmas labeled **Lemma DK**... in the rest of this paper are obtained by using (48), (52) or (53).

3.3. An upper bound D_N

Now, for each given K we use (45) and (49) to put an upper bound $m_{\max}$ on m, and then we use (46) and (50) with $h^-(N) = 2^{4m_{\max}+3}$ to put a very reasonable upper bound on D_N. Finally, using this upper bound on D_N, we list D_N for each K, compute the exact value of $t_{N/K}$ for each D_N then use the upper bound $h^-(N) \leq 2^{t_{N/K}-1}$ in (38) to get rid of many N's, i.e. we use

$$\left(1 - \frac{8\pi e^{1/4}}{(D_N)^{1/8}}\right) \frac{\sqrt{D_N/D_K}}{\log(D_N)} \leq 2e\pi^4 2^{t_{N/K}+\rho'} \mathrm{Res}_{s=1}(\zeta_K). \tag{54}$$

All Lemmas labeled **Lemma DN**... in the rest of this paper are obtained by using (54).

3.4. Successive examination according to the eight possibility of forms for K

Examination in cases of eight possible forms for K in Theorem 9 proves Main Theorem. We explain on one of the eight possible forms for K, how we get upper bounds on discriminants of quaternion CM-fields with ideal class groups of exponent 2.

Now, we assume that the ideal class group of a quaternion CM-field N of the form 3c in Theorem 9 has exponent 2. Hence $K = K_{(p,qr)} = \boldsymbol{Q}(\sqrt{p}, \sqrt{qr})$, with

$$p \equiv 1 \pmod 4 \text{ and } q \equiv r \equiv 3 \pmod 4 \text{ three distinct primes such that } \left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1.$$

Then, $\rho' = 0$ and $h(K_{(p,qr)})$ is odd, so that the 2-rank of $\mathcal{C}(N)$ is $t_{N/K_{(p,qr)}} - 1$. Moreover, $D_{K_{(p,qr)}} = (pqr)^2$ and $D_N = (pqr)^6\Delta^4$ where Δ is a possibly negative fundamental discriminant coprime to pqr. Moreover, we have

$$\begin{aligned} pqr &= 5 \cdot 3 \cdot 7 = 105 \\ &= 5 \cdot 3 \cdot 23 = 345 \\ &= 17 \cdot 3 \cdot 7 = 357 \\ &= 17 \cdot 3 \cdot 11 = 561 \end{aligned}$$

or $pqr \geq 5 \cdot 3 \cdot 43 = 645$, hence we have $D_{K_{(p,qr)}} \geq 382617$. Using Lemmas (17) and (18), we get that the hypothesis (H) is satisfied whenever $K_{(p,qr)}$ is a quartic subfield of a quaternion CM-field with ideal class group of exponent 2. Now, we lower our previous upper bound on D_K. Indeed, for the 65 fields $K_{(p,qr)}$'s such that $D_{K_{(p,qr)}} \leq 25 \cdot 10^6$, we use (48) instead of (47). We thus get that only 8 out of these 65 quartic fields could be quartic subfields of quaternion CM-fields with ideal class groups of exponent 2, i.e., we have proved:

Lemma DK2c. *If $K_{(p,qr)}$ is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $(p,q,r) \in \{ (5,3,7); (5,3,23); (17,3,7); (17,3,11); (5,3,47); (5,7,23); (41,3,7); (41,3,11)\}$.

We note that these eight real quartic fields satisfy $h(K_{(p,qr)}) = 1$. Using (54), we get:

Lemma DN2c. *If N is a quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of some $K_{(p,qr)}$, then we have:*

(p,qr)	$D_N \in$	2-rank of $\mathcal{C}(N) =$
$(5, 3\cdot 7)$	$\{(5\cdot 3\cdot 7)^6,\ (5\cdot 3\cdot 7)^6 4^4,\ (5\cdot 3\cdot 7)^6 8^4\}$	3, 5, 5
$(5, 3\cdot 23)$	$\{(5\cdot 3\cdot 23)^6\}$	3
$(17, 3\cdot 11)$	$\{(17\cdot 3\cdot 11)^6,\ (17\cdot 3\cdot 11)^6 4^4,\ (17\cdot 3\cdot 11)^6 8^4\}$	3, 7, 7.

Now, we compute the relative class numbers of these 9 possible CM-fields N using the decomposition law described in section 2.4. and the method developed in [8]. By Theorem 11 we know that $N \subset N_0(\sqrt{\Delta})$ where N_0 is one of the two pure quaternion fields with discriminants $(pqr)^6$, namely N_0 is the real one if $\Delta < 0$ and N_0 the imaginary one if $\Delta > 0$. The relative class numbers are as in the next table. (Let us point out that there are two occurrences of non-isomorphic quaternion CM-fields with same discriminants and same real quartic subfields.) Hence, there exists exactly one quaternion CM-field N containing some $K_{(p,qr)}$ that has an ideal class group of exponent 2, namely the pure quaternion field

$$N = N_0 = \boldsymbol{Q}\left(\sqrt{-\frac{5+\sqrt{5}}{2}(21+2\sqrt{105})\frac{5+\sqrt{21}}{2}}\right).$$

The ideal class group $\mathcal{C}(N_0)$ is isomorphic to $(\boldsymbol{Z}/2\boldsymbol{Z})^3$.

$\delta(N)$	$h^-(N)$
$\frac{5+\sqrt{5}}{2}(21+2\sqrt{105})\frac{5+\sqrt{21}}{2}$	2^3
$4\cdot\frac{5+\sqrt{5}}{2}(21+2\sqrt{105})$	$2^5\cdot 3^2$
$8\cdot\frac{5+\sqrt{5}}{2}(21+2\sqrt{105})\frac{5+\sqrt{21}}{2}$	$2^5\cdot 5^2$
$8\cdot\frac{5+\sqrt{5}}{2}(21+2\sqrt{105})$	$2^5\cdot 5^2$
$\frac{5+\sqrt{5}}{2}(483+26\sqrt{345})$	$2^3\cdot 3^2$
$(17+4\sqrt{17})(2937+124\sqrt{561})(23+4\sqrt{33})$	$2^3\cdot 3^2$
$4\cdot(17+4\sqrt{17})(2937+124\sqrt{561})$	$2^9\cdot 3^2$
$8\cdot(17+4\sqrt{17})(2937+124\sqrt{561})(23+4\sqrt{33})$	$2^7\cdot 13^2$
$8\cdot(17+4\sqrt{17})(2937+124\sqrt{561})$	$2^9\cdot 7^2$

Lemma DK1a. *In case 1a, if K is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $q \in \{17, 73, 89, 97\}$.

Lemma DN1a. *If N is a quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the K's of Lemma above, then we have* $d(N) = 2^{22}17^6$ *and the* 2*-rank of* $\mathcal{C}(N)$ *is* 3.

Hence, the only candidate and its relative class number are as follows.

$\delta(N)$	$h^-(N)$
$(17+4\sqrt{17})(6+\sqrt{34})$	$2^3 \cdot 3^2$

Lemma DK1b. *In case 1b, if K is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $(p,q) \in \{ (5,29); (5,41); (13,17); (5,61); (13,29); (5,89); (5,101); (5,109); (5,149); (13,61); (17,89)\}$.

Moreover, $(p/q)_4(q/p)_4 = +1$ for $(p,q) \in \{(5,29); (5,89); (5,101); (13,61)\}$ so that we can get rid of these four pairs.

Lemma DN1b. *If N is a quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the K's of Lemma above, then we have:*

(p,q)	$D_N \in$	2-rank of $\mathcal{C}(N) =$
$(5,41)$	$\{(5\cdot 41)^6,\ (5\cdot 41)^6 3^4,\ (5\cdot 41)^6 4^4\}$	3, 5, 5
$(13,17)$	$\{(13\cdot 17)^6,\ (13\cdot 17)^6 3^4,\ (13\cdot 17)^6 4^4\}$	3, 5, 5
$(5,61)$	$\{(5\cdot 61)^6,\ (5\cdot 61)^6 3^4\}$	3, 5
$(13,29)$	$\{(13\cdot 29)^6\}$	3

Moreover, the quaternion fields with discriminants $(5\cdot 41)^6$, $(13\cdot 17)^6$, and $(5\cdot 61)^6 3^4$ are real, so that we can get rid of these three discriminants. Hence, surviving

candidates and their relative class numbers are as follows.

$\delta(N)$	$h^-(N)$
$3\cdot(205+32\sqrt{41})\,\dfrac{15+\sqrt{205}}{2}$	$2^5\cdot 3^2$
$4\cdot(205+32\sqrt{41})\,\dfrac{15+\sqrt{205}}{2}$	$2^5\cdot 5^2$
$3\cdot\dfrac{13+3\sqrt{13}}{2}\,\dfrac{17+\sqrt{221}}{2}$	$2^5\cdot 3^2$
$4\cdot\dfrac{13+3\sqrt{13}}{2}\,\dfrac{17+\sqrt{221}}{2}$	$2^5\cdot 5^2$
$\dfrac{305+39\sqrt{61}}{2}\,(35+2\sqrt{305})$	$2^3\cdot 3^2$
$\dfrac{29+5\sqrt{29}}{2}\,(39+2\sqrt{377})$	$2^3\cdot 3^2$

Lemma DK2a. *In case 2a, if K is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $(q,r,qr)\in\{(3,11,33);(3,19,57)\}$.

Lemma DN2a. *If N is a quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the K's of Lemma above, then we have:*

$$(q,r)=(3,11),\ D_N=16\cdot(8\cdot 3\cdot 11)^6,\ \text{2-rank of}\ \mathcal{C}(N)\le 3.$$

Hence, surviving candidates are the following two non-isomorphic pair of pure quaternion CM-fields with the same discriminant and their relative class numbers are as follows.

$\delta(N)$	$h^-(N)$
$(2+\sqrt{2})\,(33+4\sqrt{66})$	$2^3\cdot 5^2$
$(2+\sqrt{2})\,(33+4\sqrt{66})\,(23+4\sqrt{33})$	$2^3\cdot 7^2$

Lemma DK2b. *In case 2b, if K is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $(p,r)\in\{(5,7);(5,11)\}$.

Lemma DN2b. *There is no quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the* K*'s of Lemma above.*

Lemma DK3a. *In case* 3a*, if* K *is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $(q,r) \in \{(7,11);(7,23)\}$.

Lemma DN3a. *There is no quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the* K*'s of Lemma above.*

Lemma DK3b. *In case* 3b*, if* K *is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*,*
then we have $(p,q,r) \in \{(3,7,11);(3,7,23);(3,11,19)\}$.

Noticing that in that case we can have $\rho' = 1$, using (54) we get:

Lemma DN3b. *If* N *is a quaternion* CM*-field with ideal class group of exponent* 2 *that is a quadratic extension of one of the* K*'s of Lemma above, then we have:*

(p,q,r)	$D_N \in$	2-rank of $\mathcal{C}(N) \leq$
$(3,11,7)$	$\{(3\cdot 7\cdot 11)^6\}$	2
$(3,23,7)$	$\{(3\cdot 7\cdot 23)^6\}$	2
$(3,11,19)$	$\{(3\cdot 11\cdot 19)^6,\ (3\cdot 11\cdot 19)^6 4^4\}$	2, 6.

Hence, surviving candidates and their relative class numbers are as follows.

$\delta(N)$	$h^-(N)$
$\frac{3+\sqrt{21}}{2}(11+2\sqrt{33})(35+4\sqrt{77})$	$2^3\cdot 3^2$
$\frac{3+\sqrt{21}}{2}\ \frac{23+3\sqrt{69}}{2}(203+16\sqrt{161})$	$2^3\cdot 3^2$
$(11+2\sqrt{33})(665+46\sqrt{209})(15+2\sqrt{57})$	$2^3\cdot 3^6$
$4\cdot(517+90\sqrt{33})(665+46\sqrt{209})(15+2\sqrt{57})$	$2^7\cdot 7^2$

Lemma DK4. *In case* 4*, if* K *is a quartic subfield of a quaternion* CM*-field with ideal class group of exponent* 2*, then* $q \in \{3,11,19,43\}$.

Lemma DN4. *If N is a quaternion CM-field with ideal class group of exponent 2 that is a quadratic extension of one of the K's of Lemma above, then we have:*

q	$D_N \in$	2-rank of $\mathcal{C}(N) =$
3	$\{2^{24}\cdot 3^6,\ 2^{24}\cdot 3^6\cdot 5^4,\ 2^{24}\cdot 3^6\cdot 7^4\}$	1, 3, 3
11	$\{2^{24}\cdot 11^4, 2^{24}\cdot 11^6\cdot 3^4\}$	1, 3.

Hence, surviving candidates and their relative class numbers are as follows.

$\delta(N)$	$h^-(N)$
$(2+\sqrt{2})(3+\sqrt{6})$	2
$5\cdot(2+\sqrt{2})(3+\sqrt{6})$	$2^3\cdot 3^2$
$7\cdot(2+\sqrt{2})(3+\sqrt{6})$	$2^3\cdot 5^2$
$(2+\sqrt{2})(33+7\sqrt{22})$	$2\cdot 3^2$
$3\cdot(2+\sqrt{2})(33+7\sqrt{22})$	$2^3\cdot 3^4$

The proof of Main Theorem is completed.■

References

[1] C. Chevalley: *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Univ. Tokyo **2** (1933), Part 9.

[2] A. Fröhlich: *Artin-Root Numbers and Normal Integral Bases for Quaternion Fields*, Inventiones Math. **17** (1972), 143-166.

[3] G. Gras: *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier, Grenoble **23** (1973), 1-48, Chapter IV A.

[4] H. Hasse: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II:Reziprozitätsgesetz, Physica-Verlag, Würzburg-Wien (1970), 25-40, Chapter II.

[5] T. Kubota: *Über den bizyklischen biquadratischen Zahlkörper,* Nagoya Math J. **10** (1956), 65-84.

[6] S. Louboutin: *Lower bounds for relative class numbers of* CM*-fields,* Proc. Amer. Math. Soc. **120** (1994), 425-434.

[7] S. Louboutin: *Majorations explicites de* $|L(1,\chi)|$, C. R. Acad. Sci. Paris, t. **316**, Série I (1993), 11-14.
[8] S. Louboutin: *Calculs des nombres de classes relatifs: application aux corps quaternioniques à multiplication complexe*, C. R. Acad. Sci. Paris, t. **317**, Série I (1993), 643-646.
[9] S. Louboutin: *Determination of all quaternion octic* CM*-fields with class number* 2, J. London Math. Soc. **54** (1996), 227-238.
[10] S. Louboutin and R. Okazaki: *Determination of all non-normal quartic* CM*-fields and of all non-abelian normal octic* CM*-fields with class number one*, Acta Arith. **67** (1994), 47-62.
[11] L. Rédei and H. Reichardt: *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1934), 69-74.
[12] A. Scholz: *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39** (1935), 95-111.

S. Louboutin
Université de Caen, U.F.R. Sciences
Département de Mathématiques
Esplanade de la Paix
14032 Caen Cedex, France
e-mail: loubouti@univ-caen.fr

R. Okazaki
Doshisha University
Department of Mathematics
Kyotanabe, Kyoto
610-0321, Japan
e-mail: rokazaki@mail.doshisha.ac.jp