TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 349, Number 9, September 1997, Pages 3657–3678
S 0002-9947(97)01768-6

THE CLASS NUMBER ONE PROBLEM FOR SOME NON-ABELIAN NORMAL CM-FIELDS

STÉPHANE LOUBOUTIN, RYOTARO OKAZAKI, AND MICHEL OLIVIER

Abstract. Let $\mathbf{N}$ be a non-abelian normal CM-field of degree $4p$, p any odd prime. Note that the Galois group of $\mathbf{N}$ is either the dicyclic group of order $4p$, or the dihedral group of order $4p$. We prove that the (relative) class number of a dicyclic CM-field of degree $4p$ is always greater then one. Then, we determine all the dihedral CM-fields of degree 12 with class number one: there are exactly nine such CM-fields.

Introduction

A.M. Odlyzko proved that there are only finitely many normal CM-fields with class number one (see [Odl]), J. Hoffstein proved that they have degree less than or equal to 436 (see [Hof]), and K. Yamamura determined all the abelian CM-fields with class number one (see [Yam]). We will note that there is no non-abelian normal CM-field of degree 4, 6 or 10. Then, S. Louboutin and R. Okazaki determined all the non-abelian normal CM-fields of degree 8 with class number one (see [Lou-Oka]). Here, thanks to good upper bounds on residues of Dedekind zeta-functions at $s = 1$ and a technique for computing relative class numbers of non-abelian CM-fields, we will determine all the non-abelian normal CM-fields of degree 12 with class number one:

Theorem 1. *There are exactly* 16 *non-abelian normal* CM*-fields* $\mathbf{N}$ *of degree* 12 *with relative class number one, namely the* 16 *dihedral* CM*-fields* $\mathbf{N} = \mathbf{K}M$ *of degree* 12 *with relative class number equal to* 1 *which are listed in Table 1, where* $\mathbf{K} = \mathbf{Q}(\alpha_{\mathbf{K}})$ *(with* $P_{\mathbf{K}}(\alpha_{\mathbf{K}}) = 0$*) is a totally real non-normal cubic number field with discriminant* $d_{\mathbf{K}}$ *and* $\mathbf{M} = \mathbf{Q}(\sqrt{-D_0}, \sqrt{-D_1})$ *(with* $D_0 \geq 1$ *and* $D_1 \geq 1$ *square-free) is an imaginary bicyclic biquadratic number field with relative class number equal to* 1 *and such that* $\mathbf{Q}(\sqrt{d_{\mathbf{K}}}) \subseteq \mathbf{M}$*. Exactly* 9 *out of these fields* $\mathbf{N}$ *have class number one: those which appear in Table 1 and are such that the class number* $h_{\mathbf{N}^+}$ *of their maximal totally real subfields* $\mathbf{N}^+$ *is equal to* 1.

Throughout this paper we let p denote any odd prime.

The proof of this theorem will be divided into four steps:

In section 1, we prove some useful results on CM-fields. We will make use of some of them in a forthcoming paper when we solve the class number one problem for non-abelian normal CM-fields of degree 20. We also prove that the Galois group $\mathbf{G}$ of a normal CM-field of degree $4p$ is isomorphic to either the dicyclic group T_{4p} or the dihedral group D_{4p}.

Received by the editors July 16, 1995 and, in revised form, March 21, 1996.

1991 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R21, 11R42, 11M20, 11Y40.

Key words and phrases. CM-field, dihedral field, relative class number.

TABLE 1

$(d_{\mathbf{K}}, P_{\mathbf{K}}(X))$	(D_0, D_1)	$h_{\mathbf{N}^+}$
$(148, X^3 + X^2 - 3X - 1)$	$(1, 37)$	1
$(469, X^3 + X^2 - 5X - 4)$	$(7, 67)$	1
$(473, X^3 - 5X - 1)$	$(11, 43)$	1
$(756, X^3 - 6X - 2)$	$(3, 7)$	1
$(940, X^3 - 7X - 4)$	$(1, 235)$	2
$(1304, X^3 - X^2 - 11X - 1)$	$(2, 163)$	1
$(1425, X^3 - X^2 - 8X - 3)$	$(3, 19)$	1
$(1620, X^3 - 12X - 14)$	$(3, 15$	1
$(1708, X^3 - X^2 - 8X - 2)$	$(1, 427)$	2
$(1944, X^3 - 9X - 6)$	$(2, 3)$	1
$(2700, X^3 - 15X - 20)$	$(1, 3)$	1
$(4104, X^3 - 18X - 16)$	$(6, 19)$	2
$(4312, X^3 + X^2 - 16X - 8)$	$(2, 11)$	3
$(4860, X^3 - 18X - 12)$	$(3, 5)$	2
$(8505, X^3 - 27X - 51)$	$(7, 35)$	2
$(14520, X^3 - 33X - 22)$	$(3, 10)$	2

In section 2, we prove that dicyclic CM-fields of degree $4p$ with $p \equiv 3 \pmod 4$ have even relative class numbers, and therefore even class numbers (see Theorem 6). Moreover, we wil prove that for any odd prime p the relative class number of a dicyclic CM-field of degree $4p$ is always greater than one (see Theorem 7). Hence, for the remainder of the paper we will focus on dihedral CM-fields of degree $4p$.

In section 3, we quote results from the first author which yield very good lower bounds on relative class numbers $h_{\mathbf{N}}^-$ of CM-fields $\mathbf{N}$ of fixed degree provided that their Dedekind zeta-functions $\zeta_{\mathbf{N}}$ satisfy $\zeta_{\mathbf{N}}(s_0) \leq 0$, where $s_0 = 1 - (2/\log d_{\mathbf{N}})$. Such lower bounds on $h_{\mathbf{N}}^-$ yield upper bounds on the absolute values of the discriminants $d_{\mathbf{N}}$ of $\mathbf{N}$ when $h_{\mathbf{N}}^- = 1$. We note that by using Stark and Hoffstein's results instead of the ones we developed in this section, we would not get as good an upper bound (on discriminants of dihedral CM-fields of degree 12 with relative class numbers equal to one) as the one we get in section 4.3. Indeed, our techniques yield a better lower bound on the residue of the Dedekind zeta-function of $\mathbf{N}$ at $s = 1$, and a better upper bound on the residue of the Dedekind zeta-function at $s = 1$ of its maximal totally real subfield $\mathbf{N}^+$.

In section 4, we finally solve the relative class number one and class number one problems for dihedral CM-fields $\mathbf{N}$ of degree $4p = 12$. This section will be divided into seven steps. First, in section 4.1 we draw a lattice of subfields of $\mathbf{N}$ and notice that $\mathbf{N}$ contains an imaginary bicyclic biquadratic subfield $\mathbf{M}$ whose relative class number $h_{\mathbf{M}}^-$ divides $h_{\mathbf{N}}^-$ (we use section 1). Hence $h_{\mathbf{N}}^- = 1$ yields $h_{\mathbf{M}}^- = 1$. Second, in section 4.2 we thus determine all the imaginary bicyclic biquadratic number fields with relative class number one: there are 147 such number fields. We notice that the Dedekind zeta-functions $\zeta_{\mathbf{M}}$ of these 147 numbers fields satisfy $\zeta_{\mathbf{M}}(s) \leq 0$, $s \in]0, 1[$. This will enable us to prove that if $h_{\mathbf{N}}^- = 1$ then $\zeta_{\mathbf{N}}(s) \leq 0$, $s \in]0, 1[$. Hence, in the third place, according to section 3, we manage to get in section 4.3 the upper bound $d_{\mathbf{N}} \leq 4 \cdot 10^{44}$ on the discriminants of the dihedral CM-fields $\mathbf{N}$ of degree 12 with relative class number one. Moreover, with the notations of the previous Theorem 1, we prove that $h_{\mathbf{N}}^- = 1$ implies $d_{\mathbf{K}} \leq 5 \cdot 10^8$. Fourthly, in section 4.4 we remind the reader of the results of the first author which enable us to compute the relative class number of any CM-field. Here, we note that it would require too much computation to complete the determination of all the dihedral CM-fields $\mathbf{N}$ with relative class numbers equal to 1, but working with CM-fields of smaller degree would drastically alleviate the computations. Hence, in the fifth place, we give in section 4.5 a factorization of $h_{\mathbf{N}}^-$ which shows that $h_{\mathbf{N}}^- = 1$ if and only if $h_{\mathbf{M}}^- = h_{\mathbf{N}_0}^- = 1$, where $\mathbf{N}_0$ is some non-normal sextic CM-subfield of $\mathbf{N}$. Moreover, in order to drastically reduce the amount of relative class number computation, in the sixth place, we provide in section 4.6 necessary conditions for the relative class number of $\mathbf{N}$ to be odd. These necessary conditions enable us to get rid of many of the occurrences of $\mathbf{N}$ and $\mathbf{N}_0$. Finally, in the seventh place, by using computers, we determine in section 4.7 all the dihedral CM-fields of degree 12 such that $d_{\mathbf{K}} \leq 5 \cdot 10^8$ with $\mathbf{L} = \mathbf{Q}(\sqrt{d_{\mathbf{K}}})$ a real quadratic subfield of any one of the 147 imaginary bicyclic biquadratic number fields $\mathbf{M}$ with $h_{\mathbf{M}}^- = 1$, and such that the previous necessary conditions for $h_{\mathbf{N}}^-$ to be odd are fulfilled. In this way, we get a table of 11761 pairs $(\mathbf{K}, \mathbf{M})$. The computation of the relative class numbers of the corresponding 11761 sextic CM-fields $\mathbf{N}_0$ yields the first part of Theorem 1. Its second part is an easy consequence.

1. Some useful results on CM-fields

We assume that all the number fields we will be looking at lie in the field of complex numbers. We let c denote the complex conjugation. If $\mathbf{N}$ is normal, we may think of c as being in its Galois group. When $\mathbf{E}$ is a number field, we let $U_{\mathbf{E}}$ be the unit group of the ring of algebraic integers of $\mathbf{E}$, $W_{\mathbf{E}}$ be the group of roots of unity in $\mathbf{E}$, $w_{\mathbf{E}}$ be the order of $W_{\mathbf{E}}$ and $d_{\mathbf{E}}$ be the absolute value of the discriminant of $\mathbf{E}$. When $\mathbf{E}/\mathbf{F}$ is an extension of number fields we let $j_{\mathbf{E}/\mathbf{F}}$ be the canonical map from the group of fractional ideals of $\mathbf{F}$ to that of $\mathbf{E}$ and $N_{\mathbf{E}/\mathbf{F}}$ be the norm map from the group of fractional ideals of $\mathbf{E}$ to that of $\mathbf{F}$. When $\mathbf{K}$ is a CM-field, we let $\mathbf{K}^+$ be its maximal totally real subfield (hence $\mathbf{K}$ is a quadratic extension of $\mathbf{K}^+$), $Q_{\mathbf{K}} = [U_{\mathbf{K}} : W_{\mathbf{K}} U_{\mathbf{K}^+}]$ be Hasse's unit index of $\mathbf{K}$ and $\kappa_{\mathbf{K}}$ be the order of the kernel of $j_{\mathbf{K}/\mathbf{K}^+}$. Note that $Q_{\mathbf{K}} = [U_{\mathbf{K}} : W_{\mathbf{K}} U_{\mathbf{K}^+}] = [U_{\mathbf{K}}^{c-1} : W_{\mathbf{K}}^2] = 2/[W_{\mathbf{K}} : U_{\mathbf{K}}^{c-1}]$. Since $W_{\mathbf{K}}^2 = W_{\mathbf{K}}^{c-1} \subseteq U_{\mathbf{K}}^{c-1}$ and since $W_{\mathbf{K}}$ is a cyclic group, we get $\kappa_{\mathbf{K}} \in \{1, 2\}$. We have an injective homomorphism

$$\phi_{\mathbf{K}} : \ \ker(j_{\mathbf{K}/\mathbf{K}^+}) \mapsto W_{\mathbf{K}}/U_{\mathbf{K}}^{c-1}$$

which maps an ideal class $\mathcal{C}$ in this kernel to the image of $\bar{\alpha}/\alpha$ in the factor group $W_{\mathbf{K}}/U_{\mathbf{K}}^{c-1}$, where $(\alpha) = j_{\mathbf{K}/\mathbf{K}^+}(\mathcal{C})$. Moreover, we have $W_{\mathbf{K}}^2 = W_{\mathbf{K}}^{c-1} \subseteq U_{\mathbf{K}}^{c-1}$. Hence, we get $\kappa_{\mathbf{K}} \in \{1, 2\}$ (note a slight mistake in the proof of [Wa, Th. 10.3]). Note also that $Q_{\mathbf{K}} = 2$ implies $[W_{\mathbf{K}} : U_{\mathbf{K}}^{c-1}] = 1$ and $\kappa_{\mathbf{K}} = 1$. Finally, if $\mathbf{K}/\mathbf{k}$ is an extension of CM-fields, note that $N_{\mathbf{K}/\mathbf{k}} \circ j_{\mathbf{K}/\mathbf{K}^+} = j_{\mathbf{k}/\mathbf{k}^+} \circ N_{\mathbf{K}^+/\mathbf{k}^+}$ on fractional ideals and on ideal classes (use the finitness of the class groups to reduce the proof to the case of principal ideals).

Lemma 2. (i). *Let* $\mathbf{K}$ *be a totally imaginary number field and let* $\mathbf{N}$ *be any normal closure of* $\mathbf{K}$. *Then,* $\mathbf{K}$ *is a* CM-*field if and only if for all* $g \in \mathrm{Gal}(\mathbf{N}/\mathbf{Q})$ *the commutators* $[c, g] = c^{-1}g^{-1}cg$ *lie in* $\mathrm{Gal}(\mathbf{N}/\mathbf{K})$.

(ii). *Hence, a totally imaginary normal number field is a* CM-*field if and only if the complex conjugation lies in the center of its Galois group.*

(iii). *Any subfield of a* CM*-field is either a* CM*-field or a totally real number field.*

(iv). *There is no non-abelian normal* CM*-field of degree* $2p$ *or* $2p^2$, p *any odd prime.*

Proof. We notice that point (i) readily implies points (ii) and (iii), and we now prove point (i). Set $\mathbf{G} = \mathrm{Gal}(\mathbf{N}/\mathbf{Q})$, $\mathbf{H} = \mathrm{Gal}(\mathbf{N}/\mathbf{K})$, and for any subfield $\mathbf{K}^+$ of $\mathbf{N}$ set $\mathbf{H}_+ = \mathrm{Gal}(\mathbf{N}/\mathbf{K}^+)$. Since for any $g \in \mathbf{G}$ we have $\mathrm{Gal}(\mathbf{N}/g(\mathbf{K}^+)) = g\mathrm{Gal}(\mathbf{N}/\mathbf{K}^+)g^{-1} = g\mathbf{H}_+g^{-1}$, then $\mathbf{K}^+$ is totally real if and only if for all $g \in \mathbf{G}$ we have $c \in g\mathbf{H}_+g^{-1}$. Moreover, as $\mathbf{K}$ is totally imaginary then for any $g \in \mathbf{G}$ we have $c \notin \mathrm{Gal}(\mathbf{N}/g(\mathbf{K})) = g\mathrm{Gal}(\mathbf{N}/\mathbf{K})g^{-1} = g\mathbf{H}g^{-1}$ and $g^{-1}cg \notin \mathbf{H}$. Therefore, as $\mathbf{K}$ is a CM-field if and only if we can find a totally real subfield $\mathbf{K}^+$ of $\mathbf{N}$ with $\mathbf{K}^+ \subseteq \mathbf{K}$ and $[\mathbf{K} : \mathbf{K}^+] = 2$, then $\mathbf{K}$ is a CM-field if and only if there exists a subgroup $\mathbf{H}_+$ of $\mathbf{G}$ such that

1) $\mathbf{H} \subseteq \mathbf{H}_+$,
2) $[\mathbf{H}_+ : \mathbf{H}] = 2$,
3) $g \in \mathbf{G}$ implies $g^{-1}cg \in \mathbf{H}^+ \setminus \mathbf{H}$.

Now, 1), 2) and 3) imply $[c, g] \in \mathbf{H}$ for all $g \in \mathbf{G}$. Conversely, if $[c, g] \in \mathbf{H}$ for all $g \in \mathbf{G}$ then $\mathbf{H}_+ = \langle \mathbf{H}, c\rangle$, the subgroup of $\mathbf{G}$ generated by $\mathbf{H}$ and c, satisfies 1), 2) and 3).

Finally, point (iv) follows from the fact that $\mathbf{G} = \mathbf{S}_2\mathbf{S}_p$, where $\mathbf{S}_2 = \{\mathrm{Id}, c\}$ is a subgroup of the center of $\mathbf{G}$ and $\mathbf{S}_p$ is any p-Sylow subgroup of $\mathbf{G}$, and from the fact that any group of order p or p^2 is abelian. □

Hence, the smallest possible degrees for non-abelian normal CM-fields are 8, 12, 16 and 20. Recently S. Louboutin and R. Okazaki solved the class number one problem for the non-abelian normal octic CM-fields (see [Lou-Oka]). Now, we prove that the Galois group of a non-abelian normal CM-field of degree $4p$ (which will cope with normal CM-fields of degree 12 and 20) is isomorphic either to the dihedral group D_{4p} or the dicyclic group T_{4p}:

Lemma 3. *Let* $\mathbf{G}$ *be a non-abelian group of order* $4p$. *If the center* $Z(\mathbf{G})$ *of* $\mathbf{G}$ *has even order, then* $\mathbf{G}$ *is isomorphic either to the dihedral group* D_{4p} *or to the dicyclic group* T_{4p}. *Here, we set*

$$D_{4p} = \langle a, b : \ a^{2p} = b^2 = 1, b^{-1}ab = a^{-1}\rangle \text{ (dihedral group of order } 4p\text{)},$$
$$T_{4p} = \langle a, b : \ a^{2p} = 1, a^p = b^2, b^{-1}ab = a^{-1}\rangle \text{ (dicyclic group of order } 4p\text{)}.$$

Note that in both cases $Z(\mathbf{G}) = \{1, a^p\}$ *and* $\mathbf{G}/Z(\mathbf{G})$ *is the dihedral group of order* $2p$.

Proof. Since the product of an element of order p and of an element of order 2 which lies in $Z(\mathbf{G})$ has order $2p$, there exists an element a of order $2p$ in $\mathbf{G}$. Then, the subgroup $\langle a\rangle$ of order $2p$ which has index two in $\mathbf{G}$ is a normal subgroup of $\mathbf{G}$. We let S_2 be a 2-Sylow subgroup of $\mathbf{G}$ which contains a^p, which has order 2. Then S_2 has order 4.

First, assume that $S_2 = \langle b\rangle$ is cyclic, where $b^4 = 1$. Then, there exists an integer k such that $b^{-1}ab = a^k$. We get $a = a^{-p}aa^p = b^{-2}ab^2 = b^{-1}a^kb = a^{k^2}$. Hence, $k^2 \equiv 1 \pmod{2p}$, which implies $k \equiv \pm 1 \pmod{2p}$ and $b^{-1}ab = a$ or $b^{-1}ab = a^{-1}$. In the first case, we would have $ab = ba$ and $\mathbf{G}$ would be abelian, a contradiction. Hence, $b^{-1}ab = a^{-1}$ and $\mathbf{G}$ is somorphic to T_{4p}. Second, assume that $S_2 = \langle 1, a^p, b, a^pb\rangle$

is bicyclic, where $b^2 = 1$. As in the previous case we get $b^{-1}ab = a^{-1}$ and $\mathbf{G}$ is isomorphic to D_{4p}. $\square$

Lemma 4. (i). (*See* [Lou-Oka] *and* [Lou 7]) *Let* $\mathbf{N}$ *be a* CM-*field and let* t *be the number of distinct prime ideals of* $\mathbf{N}$ *which are ramified in* $\mathbf{N}/\mathbf{N}^+$. *Then* 2^{t-1} *divides* $h_{\mathbf{N}}^-$.

(ii). (*See* [Mar]) *Let* $\mathbf{N}^+$ *be a dihedral number field of degree* $2p$ *(*p *any odd prime), let* $\mathbf{L}$ *be the only quadratic subfield of* $\mathbf{N}^+$, *and let* q *be any prime positive rational integer which is ramified in* $\mathbf{L}/\mathbf{Q}$, *i.e.* $(q) = \mathcal{Q}_{\mathbf{L}}^2$ *in* $\mathbf{L}$. *Then, either* $\mathcal{Q}_{\mathbf{L}}$ *splits completely in* $\mathbf{N}^+/\mathbf{L}$, *or* $\mathcal{Q}_{\mathbf{L}}$ *is totally ramified in* $\mathbf{N}^+/\mathbf{L}$. *In the latter case, we also have* $q = p$. *Moreover, the conductor of the extension* $\mathbf{N}^+/\mathbf{L}$ *is a positive integer* f *such that for any prime* q *which divides* f *we have* $q \equiv \chi_{\mathbf{L}}(q) \pmod{p}$, *where* $\chi_{\mathbf{L}}$ *denotes the quadratic Dirichlet character associated with* $\mathbf{L}$. *In particular, if* $\mathbf{L} = \mathbf{Q}(\sqrt{p})$ *with* $p \equiv 1 \pmod 4$ *prime, then* $q \neq p$ *and* q *divides* f *imply* $q \equiv 1 \pmod{p}$.

(iii). *Let* $\mathbf{K}$ *be any subfield of degree* p *of a dihedral number field* $\mathbf{N}^+$ *of degree* $2p$. *Then,* $\mathbf{N}^+ = \mathbf{KL}$, $d_{\mathbf{N}^+} = d_{\mathbf{L}}d_{\mathbf{K}}^2$, *and there exists a rational integer* $f \geq 1$ *such that* $d_{\mathbf{N}^+} = d_{\mathbf{L}}^p f^{2(p-1)}$ *and* $d_{\mathbf{K}} = d_{\mathbf{L}}^{(p-1)/2} f^{p-1}$. *Hence,* $\mathbf{L} = \mathbf{Q}(\sqrt{d_{\mathbf{L}}}) = \mathbf{Q}(\sqrt[p-1]{d_{\mathbf{K}}})$ *is well determined by* $d_{\mathbf{K}}$.

The last assertion of Lemma 4(ii) will be proved at the begining of the proof of Proposition 8. We note that by using point (ii) of the following Theorem 5 and [Hor, Corollary on page 519] we could prove point (iii) of Theorem 5. However, we will give a different proof of this point (iii).

Theorem 5. *Let* $\mathbf{k} \subseteq \mathbf{K}$ *be two* CM-*fields. Assume that* $[\mathbf{K} : \mathbf{k}] = m$ *is odd. Then,*

(i). $Q_{\mathbf{k}} = Q_{\mathbf{K}}$.

(ii). $j_{\mathbf{K}^+/\mathbf{k}^+} : \ \ker(j_{\mathbf{k}/\mathbf{k}^+}) \longrightarrow \ker(j_{\mathbf{K}/\mathbf{K}^+})$ *is an isomorphism. Hence,* $\kappa_{\mathbf{k}} = \kappa_{\mathbf{K}}$.

(iii). $h_{\mathbf{k}}^-$ *divides* $h_{\mathbf{K}}^-$.

Proof. To start with, we notice that both the factor groups $W_{\mathbf{K}}/W_{\mathbf{K}}^2$ and $W_{\mathbf{k}}/W_{\mathbf{k}}^2$ have order 2. Moreover, since $W_{\mathbf{k}}^m = N_{\mathbf{K}/\mathbf{k}}(W_{\mathbf{k}}) \subseteq N_{\mathbf{K}/\mathbf{k}}(W_{\mathbf{K}})$ and since m is odd, then $N_{\mathbf{K}/\mathbf{k}}$ induces an isomorphism from the factor group $W_{\mathbf{K}}/W_{\mathbf{K}}^2$ onto the factor group $W_{\mathbf{k}}/W_{\mathbf{k}}^2$. In particular, if $\zeta \in W_{\mathbf{K}}$, then $N_{\mathbf{K}/\mathbf{k}}(\zeta) \in W_{\mathbf{k}}^2$ if and only if $\zeta \in W_{\mathbf{K}}^2$.

We prove point (i). Since $Q_{\mathbf{K}}$ and $Q_{\mathbf{k}}$ are equal to 1 or 2, it is sufficient to prove that $Q_{\mathbf{K}} = 2$ if and only if $Q_{\mathbf{k}} = 2$. Assume that $[U_{\mathbf{K}}^{c-1} : W_{\mathbf{K}}^2] = Q_{\mathbf{K}} = 2$. Then, there exists $\epsilon \in U_{\mathbf{K}}$ such that $\zeta = \bar{\epsilon}/\epsilon \in W_{\mathbf{K}} \setminus W_{\mathbf{K}}^2$. Set $\eta = N_{\mathbf{K}/\mathbf{k}}(\epsilon)$. As the complex conjugation commutes with all the embeddings of $\mathbf{K}$ (Lemma 1(i)), then η is a unit in $\mathbf{k}$ such that $\bar{\eta}/\eta = N_{\mathbf{K}/\mathbf{k}}(\bar{\epsilon}/\epsilon) = N_{\mathbf{K}/\mathbf{k}}(\zeta) \notin W_{\mathbf{K}}^2$. Hence, $Q_{\mathbf{k}} = [U_{\mathbf{k}}^{c-1} : W_{\mathbf{k}}^2] = 2$. Assume conversely that $Q_{\mathbf{k}} = [U_{\mathbf{k}}^{c-1} : W_{\mathbf{k}}^2] = 2$. Then, there exists $\eta \in U_{\mathbf{k}}$ such that $\bar{\eta}/\eta \notin W_{\mathbf{k}}$. Now, $W_{\mathbf{k}} \cap W_{\mathbf{K}}^2 = W_{\mathbf{k}}^2$ for $w = \zeta^2 \in W_{\mathbf{k}} \cap W_{\mathbf{K}}^2$ implies $w^m = N_{\mathbf{K}/\mathbf{k}}(w) = (N_{\mathbf{K}/\mathbf{k}}(\zeta))^2 \in W_{\mathbf{k}}^2$ and $w \in W_{\mathbf{k}}^2$. Thus, η is a unit of $\mathbf{K}$ such that $\bar{\eta}/\eta \notin W_{\mathbf{K}}^2$. Hence, $Q_{\mathbf{K}} = [U_{\mathbf{K}}^{c-1} : W_{\mathbf{K}}^2] = 2$.

We prove point (ii). Since $N_{\mathbf{K}^+/\mathbf{k}^+} \circ j_{\mathbf{K}^+/\mathbf{k}^+}(\mathcal{C}) = \mathcal{C}^m$ on ideal classes $\mathcal{C}$ of $\mathbf{k}^+$, since $\ker j_{\mathbf{k}/\mathbf{k}^+}$ has order $\kappa_{\mathbf{k}} \leq 2$ and since m is odd, then $j_{\mathbf{K}^+/\mathbf{k}^+}$ induces a well defined injective homomorphism

$$j : \ \ker j_{\mathbf{k}/\mathbf{k}^+} \longrightarrow \ker j_{\mathbf{K}/\mathbf{K}^+}. \tag{1}$$

Hence, if $\kappa_{\mathbf{k}} = 2$ then $\kappa_{\mathbf{K}} = 2$ and j of (1) is an isomorphism. Conversely, assume that $\kappa_{\mathbf{K}} = 2$ and let $\mathbf{I}$ be an ideal of $\mathbf{K}^+$ such that $j_{\mathbf{K}/\mathbf{K}^+}(\mathbf{I}) = (\alpha)$ with $\zeta =$

$\bar{\alpha}/\alpha \in W_{\mathbf{K}} \setminus U_{\mathbf{K}}^{c-1}$. Since $\kappa_{\mathbf{K}} = 2$, then $[W_{\mathbf{K}} : U_{\mathbf{K}}^{c-1}] = 2$ and $Q_{\mathbf{K}} = 1$. According to point (i) we get $Q_{\mathbf{k}} = [U_{\mathbf{k}}^{c-1} : W_{\mathbf{k}}^2] = 1$. Therefore, $U_{\mathbf{K}}^{c-1} = W_{\mathbf{K}}^2$ and $U_{\mathbf{k}}^{c-1} = W_{\mathbf{k}}^2$. Then, $j_{\mathbf{k}/\mathbf{k}^+} \circ N_{\mathbf{K}^+/\mathbf{k}^+}(\mathbf{I}) = N_{\mathbf{K}/\mathbf{k}} \circ j_{\mathbf{K}/\mathbf{K}^+}(\mathbf{I}) = (\beta)$ with $\beta = N_{\mathbf{K}/\mathbf{k}}(\alpha)$. Hence, the ideal class of $\mathbf{J} = N_{\mathbf{K}^+/\mathbf{k}^+}(\mathbf{I})$ is in the kernel of $j_{\mathbf{k}/\mathbf{k}^+}$. Since $\bar{\beta}/\beta = N_{\mathbf{K}/\mathbf{k}}(\bar{\alpha}/\alpha) = N_{\mathbf{K}/\mathbf{k}}(\zeta) \in W_{\mathbf{k}} \setminus W_{\mathbf{k}}^2 = W_{\mathbf{k}} \setminus U_{\mathbf{k}}^{c-1}$, then $\kappa_{\mathbf{k}} = 2$ and j of (1) is an isomorphism.

We prove point (iii). We have

$$h_{\mathbf{K}}^- = \frac{|\ker N_{\mathbf{K}/\mathbf{k}}|}{|\ker N_{\mathbf{K}^+/\mathbf{k}^+}|}\frac{|\mathrm{coker} N_{\mathbf{K}^+/\mathbf{k}^+}|}{|\mathrm{coker} N_{\mathbf{K}/\mathbf{k}}| h_{\mathbf{k}}^-}. \tag{2}$$

Let $\mathbf{H}_k$ and $\mathbf{H}_{\mathbf{k}^+}$ be the Hilbert class fields of $\mathbf{k}$ and $\mathbf{k}^+$, and let $\mathbf{A}_k/\mathbf{k}$ and $\mathbf{A}_{\mathbf{k}^+}/\mathbf{k}^+$ be the maximal unramified abelian sub-extensions of $\mathbf{K}/\mathbf{k}$ and $\mathbf{K}^+/\mathbf{k}^+$. According to class field theory we have

$$\frac{|\mathrm{coker} N_{\mathbf{K}^+/\mathbf{k}^+}|}{|\mathrm{coker} N_{\mathbf{K}/\mathbf{k}}|} = \frac{[\mathbf{K}^+ \cap \mathbf{H}_{\mathbf{k}^+} : \mathbf{k}^+]}{[\mathbf{K} \cap \mathbf{H}_k : \mathbf{k}]} = \frac{[\mathbf{A}_{\mathbf{k}^+} : \mathbf{k}^+]}{[\mathbf{A}_k : \mathbf{k}]}. \tag{3}$$

Since $\mathbf{A}_{\mathbf{k}^+}/\mathbf{k}^+$ is an unramified abelian sub-extension of $\mathbf{K}^+/\mathbf{k}^+$, then $\mathbf{A}_{\mathbf{k}^+}\mathbf{k}/\mathbf{k}$ is an unramified abelian sub-extension of $\mathbf{K}/\mathbf{k}$, which yields $\mathbf{A}_{\mathbf{k}^+} \subseteq \mathbf{A}_k$, which in turn yields $\mathbf{A}_{\mathbf{k}^+} \subseteq \mathbf{A}_{\mathbf{k}}^+$. Conversely, since $\mathbf{A}_k/\mathbf{k}$ is an unramified abelian sub-extension of $\mathbf{K}/\mathbf{k}$ and since $\mathbf{A}_k$ is a CM-field (Lemma 2(iii)), then $\mathbf{A}_{\mathbf{k}}^+/\mathbf{k}^+$ is an abelian sub-extension of $\mathbf{K}^+/\mathbf{k}^+$ which is clearly unramified if $m = [\mathbf{K} : \mathbf{k}]$ is odd. Hence, we get $\mathbf{A}_{\mathbf{k}}^+ \subseteq \mathbf{A}_{\mathbf{k}^+}$. Therefore, we have $\mathbf{A}_{\mathbf{k}}^+ = \mathbf{A}_{\mathbf{k}^+}$ and $[\mathbf{A}_{\mathbf{k}^+} : \mathbf{k}^+] = [\mathbf{A}_k : \mathbf{k}]$. Hence, (2) and (3) yield

$$h_{\mathbf{K}}^-/h_{\mathbf{k}}^- = |\ker N_{\mathbf{K}/\mathbf{k}}|/|\ker N_{\mathbf{K}^+/\mathbf{k}^+}|. \tag{4}$$

Since $N_{\mathbf{K}/\mathbf{k}} \circ j_{\mathbf{K}/\mathbf{K}^+} = j_{\mathbf{k}/\mathbf{k}^+} \circ N_{\mathbf{K}^+/\mathbf{k}^+}$, then $j_{\mathbf{K}/\mathbf{K}^+}$ induces a well defined homomorphism

$$J: \ \ker N_{\mathbf{K}^+/\mathbf{k}^+} \longrightarrow \ker N_{\mathbf{K}/\mathbf{k}}. \tag{5}$$

According to point (ii), if $\mathcal{C}$ is in $\ker J$ then $\mathcal{C} = j_{\mathbf{K}^+/\mathbf{k}^+}(\mathcal{C}')$ with $\mathcal{C}' \in \ker j_{\mathbf{k}/\mathbf{k}^+}$. Hence, we have $1 = N_{\mathbf{K}^+/\mathbf{k}^+}(\mathcal{C}) = \mathcal{C}'^m$. Since m is odd and $\mathcal{C}'$ has order ≤ 2 (since $\kappa_{\mathbf{k}} \in \{1, 2\}$), we get $\mathcal{C}' = 1$, which implies $\mathcal{C} = 1$. Thus, J of (5) is injective, $|\ker N_{\mathbf{K}^+/\mathbf{k}^+}|$ divides $|\ker N_{\mathbf{K}/\mathbf{k}}|$, and (4) provides us with the desired result. □

2. Class number problems for dicyclic CM-fields of degree $4p$

Let $\mathbf{N}$ be a normal CM-field with Galois group T_{4p}, p any odd prime. With the notations of Lemma 3, we let $\mathbf{N}^+$ be the fixed field of the group $Z(T_{4p}) = \{1, a^p\}$, and $\mathbf{M}$ be the fixed field of the cyclic subgroup $\langle a^2 \rangle = \{1, a^2, \cdots, a^{2(p-1)}\}$. According to Lemma 2(ii) and Lemma 3, we have that a^p is the complex conjugation. Hence, $\mathbf{N}^+$ is the maximal totally real subfield of $\mathbf{N}$ and $\mathbf{M}$ is an imaginary cyclic quartic field. We let $\mathbf{L}$ be the real quadratic subfield of $\mathbf{M}$. Then $\mathbf{N}^+/\mathbf{Q}$ is dihedral of degree $2p$, and $\mathbf{N}/\mathbf{L}$ is cyclic of degree $2p$. We have the following lattice of subfields:

$$\begin{tikzcd}
\mathbf{N} \arrow[d, dash, "2"'] \arrow[ddr, dash, "p"] & \\
\mathbf{N}^+ \arrow[dd, dash, "p"'] & \\
& \mathbf{M} \arrow[ddl, dash, "2"] \\
\mathbf{L} \arrow[d, dash, "2"'] & \\
\mathbf{Q} &
\end{tikzcd}$$

Now, assume that $h^-_{\mathbf{N}}$ is odd. Thus, there exists at most one prime ideal of $\mathbf{N}^+$ which is ramified in the quadratic extension $\mathbf{N}/\mathbf{N}^+$ (Lemma 4(i)), thus at most one prime ideal of $\mathbf{M}$ which is ramified in $\mathbf{M}/\mathbf{L}$. Since $\mathbf{M}/\mathbf{Q}$ is cyclic quartic, then there exists exactly one rational prime q which is ramified in $\mathbf{M}/\mathbf{Q}$, and that prime q is totally ramified in this extension $\mathbf{M}/\mathbf{Q}$. Now, according to Lemma 4(ii), if $q \neq p$ or $q = p$ but p is not ramified in $\mathbf{N}^+/\mathbf{L}$, then the prime ideal $\mathcal{Q}_{\mathbf{L}}$ of $\mathbf{L}$ lying above q splits completely in $\mathbf{N}^+/\mathbf{L}$. Since $\mathbf{M}/\mathbf{Q}$ is totally ramified at p, these p prime ideals of $\mathbf{N}^+$ lying above $\mathcal{Q}_{\mathbf{L}}$ are ramified in $\mathbf{N}/\mathbf{N}^+$, and 2^{p-1} divides $h^-_{\mathbf{N}}$. A contradiction. Thus, $q = p$ and p is totally ramified in $\mathbf{N}^+/\mathbf{Q}$. Finally, as $\mathbf{L}$ is ramified only at p, we must have $p \equiv 1 \pmod 4$, and $\mathbf{L} = \mathbf{Q}(\sqrt{p})$. Thus, we have proved point (ii) of the following Theorem

Theorem 6. *Let $\mathbf{N}$ be a dicyclic* CM*-field of degree $4p$, p any odd prime.*

(i). *If $p \equiv 3 \pmod 4$ then 2^{p-1} divides $h^-_{\mathbf{N}}$.*

(ii). *If $h^-_{\mathbf{N}}$ is odd then $p \equiv 1 \pmod 4$, $\mathbf{M}$ has conductor p and p is totally ramified in $\mathbf{N}^+/\mathbf{Q}$.*

(iii). *If $h^-_{\mathbf{N}} = 1$ then $p \in \{5,\ 13,\ 29,\ 37,\ 53\}$.*

Proof. (i). In that case $(2) = \mathcal{P}^2_{\mathbf{L}}$ is ramified in $\mathbf{L}/\mathbf{Q}$, and the previous discussion shows that $\mathcal{P}_{\mathbf{L}}$ splits completely in $\mathbf{N}^+/\mathbf{Q}$ and is ramified in $\mathbf{M}/\mathbf{L}$. Thus, at least p prime ideals of $\mathbf{N}$ are ramified in $\mathbf{N}/\mathbf{N}^+$ and Lemma 4(i) yields the desired result.

(iii). If $h^-_{\mathbf{N}} = 1$, then $h^-_{\mathbf{M}} = 1$ (Theorem 5(iii)), and $\mathbf{M}$ has conductor p. But it is well known that there are only finitely many imaginary cyclic quartic number fields $\mathbf{M}$ with relative class number equal to one, and B. Setzer determined all these fields. According to [Set], we get the desired result. □

The remainder of this section is devoted to proving the following result:

Theorem 7. *There does not exist any dicyclic* CM*-field of degree $4p$, p any odd prime, with relative class number equal to one.*

To get this result we will first prove in Proposition 8 that if $\mathbf{M}$ has conductor p and $p \equiv 1 \pmod 4$ and $h^-_{\mathbf{N}}$ is not divisible by p, then $\mathbf{N}^+$ must be a so-called *pure real dihedral number field of degree* $2p$, which means that p is totally ramified in $\mathbf{N}^+/\mathbf{Q}$ and no other rational prime is ramified in $\mathbf{N}^+/\mathbf{Q}$. We will then provide in Proposition 9 a powerful necessary condition for the existence of a pure real dihedral number field of degree $2p$. Hence, we will easily get that there is no pure real dihedral number field of degree $2p$ with $p \in \{5,\ 13,\ 29,\ 37,\ 53\}$. According to Theorem 6, we will have proved Theorem 7.

Proposition 8. *Let p be any odd prime. Let $\mathbf{N}/\mathbf{M}$ be a cyclic extension of degree p of* CM*-fields Assume that $\mathbf{N}^+/\mathbf{M}^+$ also is a cyclic extension of degree p. Let T be the number of prime ideals of $\mathbf{M}^+$ which split in $\mathbf{M}/\mathbf{M}^+$ and are ramified in $\mathbf{N}^+/\mathbf{M}^+$. Then, $p^{T-1}h_{\mathbf{M}}^-$ divides $h_{\mathbf{N}}^-$, and $p^T h_{\mathbf{M}}^-$ divides $h_{\mathbf{N}}^-$ if p does not divide $w_{\mathbf{M}}$, the order of the finite group of roots of unity in $\mathbf{M}$. In particular, if $\mathbf{N}$ is a dicyclic* CM*-field of degree $4p$, $p \equiv 1 \pmod 4$ an odd prime, if $\mathbf{M}$ has conductor p, and if $\mathbf{N}^+$ is not a pure real dihedral number field of degree $2p$, then p divides $h_{\mathbf{N}}^-$.*

Proof. The last assertion follows from the previous ones when we notice that any rational prime $q \neq p$ which divides the conductor f of the extension $\mathbf{N}^+/\mathbf{L}$ must satisfy $q \equiv \chi_{\mathbf{L}}(q) \equiv \pm 1 \pmod p$, where $\chi_{\mathbf{L}}$ denotes the quadratic Dirichlet character associated with $\mathbf{L}$ (see Lemma 4(ii)). Here we have $\chi_{\mathbf{L}}(q) = (q/p)$ (Legendre's symbol). If we had $q \equiv -1 \pmod p$ then we would get $\chi_{\mathbf{L}}(q) = (q/p) = (-1/p) = 1 \not\equiv q \pmod p$. Hence $q \equiv 1 \pmod p$. Since $\mathbf{M}$ has conductor p, then q splits completely in $\mathbf{M}/\mathbf{Q}$. Hence, if $\mathbf{N}^+$ is not pure then we get $T \geq 2$, and p divides $h_{\mathbf{N}}^-$.

Now, let us prove the first part of Proposition 8. Let $a_{\mathbf{N}/\mathbf{M}}$ be the ambiguous class number of the cyclic of extension $\mathbf{N}/\mathbf{M}$ of degree p, let $t_{\mathbf{N}/\mathbf{M}}$ be the number of prime ideals of $\mathbf{M}$ which are ramified in the cyclic extension $\mathbf{N}/\mathbf{M}$ of degree p, and let $U_{\mathbf{M}}$ be the unit group of the ring of algebraic integers of $\mathbf{N}$. Let $a_{\mathbf{N}^+/\mathbf{M}^+}$, $t_{\mathbf{N}^+/\mathbf{M}^+}$ and $U_{\mathbf{N}^+}$ be defined accordingly. We thus have $t_{\mathbf{N}/\mathbf{M}} = (t_{\mathbf{N}^+/\mathbf{M}^+} - T) + 2T = t_{\mathbf{N}^+/\mathbf{M}^+} + T$. The ambiguous class number formula yields

$$
\begin{aligned}
\frac{a_{\mathbf{N}/\mathbf{M}}}{a_{\mathbf{N}^+/\mathbf{M}^+}} &= \frac{[U_{\mathbf{M}^+} : U_{\mathbf{M}^+} \cap N_{\mathbf{N}^+/\mathbf{M}^+}(\mathbf{N}^+)]}{[U_{\mathbf{M}} : U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]} \frac{h_{\mathbf{M}}}{h_{\mathbf{M}^+}} p^{t_{\mathbf{N}/\mathbf{M}} - t_{\mathbf{N}^+/\mathbf{M}^+}} \\
&= \frac{[U_{\mathbf{M}^+} : U_{\mathbf{M}^+} \cap N_{\mathbf{N}^+/\mathbf{M}^+}(\mathbf{N}^+)]}{[U_{\mathbf{M}} : U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]} h_{\mathbf{M}}^- p^T.
\end{aligned}
$$

To get the desired results, we prove the two following assertions :

1). $[U_{\mathbf{M}} : U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]$ divides $\epsilon_p [U_{\mathbf{M}^+} : U_{\mathbf{M}^+} \cap N_{\mathbf{N}^+/\mathbf{M}^+}(\mathbf{N}^+)]$ with $\epsilon_p = 1$ if p does not divide $w_{\mathbf{M}}$, and $\epsilon_p = p$ if p divides $w_{\mathbf{M}}$.

2). $a_{\mathbf{N}/\mathbf{M}}/a_{\mathbf{N}^+/\mathbf{M}^+}$ divides $h_{\mathbf{N}}^-$.

Proof of assertion 1). We set $\tilde{U}_{\mathbf{M}} = W_{\mathbf{M}} U_{\mathbf{M}^+}$. Since $\mathbf{M}$ is a CM-field, then the Hasse index $Q_{\mathbf{M}} = [U_{\mathbf{M}} : \tilde{U}_{\mathbf{M}}]$ is equal to 1 or 2 (see [Has], [Wa]). We first note that

$$
\begin{aligned}
[U_{\mathbf{M}} : U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})] &= \frac{[U_{\mathbf{M}} : \tilde{U}_{\mathbf{M}}][\tilde{U}_{\mathbf{M}} : \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]}{[U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}) : \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]} \\
&= [\tilde{U}_{\mathbf{M}} : \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})].
\end{aligned}
$$

Indeed, if $Q_{\mathbf{M}} = 1$, then $\tilde{U}_{\mathbf{M}} = U_{\mathbf{M}}$ and

$$[U_{\mathbf{M}} : \tilde{U}_{\mathbf{M}}] = [U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}) : \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})].$$

If $Q_{\mathbf{M}} = 2$, then we have a one-to-one canonical morphism from the quotient group $U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}) \ / \ \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})$ into the quotient group $U_{\mathbf{M}} \ / \ \tilde{U}_{\mathbf{M}}$ of order 2, and this morphism is onto, for $\epsilon \in U_{\mathbf{M}} \setminus \tilde{U}_{\mathbf{M}}$ implies

$$\epsilon^p \in U_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}) \setminus \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}).$$

Now,

$$\begin{aligned}\tilde{U}_{\mathbf{M}} \cap W_{\mathbf{N}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+}) &= W_{\mathbf{M}} U_{\mathbf{M}^+} \cap W_{\mathbf{N}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})\\ &\subseteq W_{\mathbf{M}} U_{\mathbf{M}^+} \cap N_{\mathbf{N}/\mathbf{M}}(W_{\mathbf{N}}) N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})\\ &= \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\tilde{U}_{\mathbf{N}}) \subseteq \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N}).\end{aligned}$$

Thus, $[\tilde{U}_{\mathbf{M}} : \tilde{U}_{\mathbf{M}} \cap N_{\mathbf{N}/\mathbf{M}}(\mathbf{N})]$ divides $[\tilde{U}_{\mathbf{M}} : \tilde{U}_{\mathbf{M}} \cap W_{\mathbf{N}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})]$, and

$$\begin{aligned}[\tilde{U}_{\mathbf{M}} : \tilde{U}_{\mathbf{M}} \cap W_{\mathbf{N}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})] &= [W_{\mathbf{M}} U_{\mathbf{M}^+} : W_{\mathbf{M}} U_{\mathbf{M}^+} \cap W_{\mathbf{M}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})]\\ &= [W_{\mathbf{M}} U_{\mathbf{M}^+} : W_{\mathbf{M}}^p U_{\mathbf{M}^+} \cap W_{\mathbf{M}}^p N_{\mathbf{N}^+/\mathbf{M}^+}(U_{\mathbf{N}^+})]\\ &= [W_{\mathbf{M}} : W_{\mathbf{M}}^p][U_{\mathbf{M}^+} : U_{\mathbf{M}^+} \cap N_{\mathbf{N}^+/\mathbf{M}^+}(\mathbf{N}^+)]\\ &= \epsilon_p [U_{\mathbf{M}^+} : U_{\mathbf{M}^+} \cap N_{\mathbf{N}^+/\mathbf{M}^+}(\mathbf{N}^+)].\end{aligned}$$

Proof of assertion 2). Let $\mathcal{A}_{\mathbf{N}/\mathbf{M}}$ denote the group of ambiguous classes of the cyclic extension $\mathbf{N}/\mathbf{M}$ of degree p, and define $\mathcal{A}_{\mathbf{N}^+/\mathbf{M}^+}$ accordingly. Let $j_{\mathbf{N}/\mathbf{N}^+}$ be the canonical map from the group $\mathcal{C}_{\mathbf{N}^+}$ of fractional ideals of $\mathbf{N}^+$ to $\mathcal{C}_{\mathbf{N}}$, which is the same for $\mathbf{N}$. Let σ be of order p in the Galois group of the cyclic extension $\mathbf{N}/\mathbf{M}$ of degree p. Then σ_+, the restriction of σ to $\mathbf{N}^+$, has order p in the Galois group of the cyclic extension $\mathbf{N}^+/\mathbf{M}^+$ of degree p. Now, it is easily seen that we have $j_{\mathbf{N}/\mathbf{N}^+}(\mathcal{A}_{\mathbf{N}^+/\mathbf{M}^+}) \subseteq \mathcal{A}_{\mathbf{N}/\mathbf{M}}$. Hence, we have a morphism between quotient groups

$$\tilde{j} : \mathcal{C}_{\mathbf{N}^+}/\mathcal{A}_{\mathbf{N}^+/\mathbf{M}^+} \longrightarrow \mathcal{C}_{\mathbf{N}}/\mathcal{A}_{\mathbf{N}/\mathbf{M}}.$$

If we prove that $\tilde{j}$ is injective then we have the desired result. Now, let $\mathcal{C}_+ \in \mathcal{C}_{\mathbf{N}^+}$ be in the kernel of $\tilde{j}$. Then we have $j_{\mathbf{N}/\mathbf{N}^+}(\mathcal{C}_+) \in \mathcal{A}_{\mathbf{N}/\mathbf{M}}$, which yields $j_{\mathbf{N}/\mathbf{N}^+}(\mathcal{C}_+) = \sigma(j_{\mathbf{N}/\mathbf{N}^+}(\mathcal{C}_+)) = j_{\mathbf{N}/\mathbf{N}^+}(\sigma(\mathcal{C}_+)) = j_{\mathbf{N}/\mathbf{N}^+}(\sigma_+(\mathcal{C}_+))$. Hence, we get $\mathcal{C}_0 \stackrel{def}{=} \mathcal{C}_+^{1-\sigma_+} \in \ker j_{\mathbf{N}/\mathbf{N}^+}$, which obviously implies $\sigma_+(\mathcal{C}_0) \in \ker j_{\mathbf{N}/\mathbf{N}^+}$. Since this kernel has order ≤ 2, we get $\sigma_+(\mathcal{C}_0) = \mathcal{C}_0$. Hence, we have

$$\mathcal{C}_0 = \mathcal{C}_0^p = \mathcal{C}_0^{1+\sigma_+ + \cdots + \sigma_+^{p-1}} = \mathcal{C}_+^{1-\sigma_+^p} = 1,$$

which amounts to saying that $\mathcal{C}_+ = \sigma_+(\mathcal{C}_+)$, i.e., that $\mathcal{C}_+$ is in $\mathcal{A}_{\mathbf{N}^+/\mathbf{M}^+}$. □

Proposition 9. *Let $p \equiv 1 \pmod 4$ be a prime and let $\epsilon_p = (u_p + v_p\sqrt{p})/2 > 1$ be the fundamental unit of $\mathbf{L}_p = \mathbf{Q}(\sqrt{p})$. If p does not divides v_p, then there does not exist any real dihedral number field $\mathbf{N}^+$ of degree $2p$ such that p is totally ramified in $\mathbf{N}^+/\mathbf{Q}$ and p is the only rational prime which is ramified in $\mathbf{N}^+/\mathbf{Q}$.*

Proof. Assume that such a number field $\mathbf{N}^+$ exists. Then the extension $\mathbf{N}^+/\mathbf{L}_p$ has conductor (p) (see [Mar, Prop. III.4 and Lemma III.1]). According to class field theory $\mathbf{N}^+$ is a subfield of $\mathbf{L}_p^1$, where $\mathbf{L}_p^1$ denotes the unit ray class field of conductor (p) of $\mathbf{L}_p$. Hence, p divides the degree $[\mathbf{L}_p^1 : \mathbf{L}_p]$. Since p is ramified in $\mathbf{L}_p/\mathbf{Q}$, then

$$[\mathbf{L}_p^1 : \mathbf{L}_p] = p(p-1)h_p/(U_p : U_p^1),$$

where h_p is the class number of $\mathbf{L}_p$, where U_p is the unit group of the ring of algebraic integers $\mathbf{R}_p$ of $\mathbf{L}_p$ and where

$$U_p^1 = \{\alpha;\ \alpha \in U_p \text{ and } \alpha \equiv 1 \pmod{(p)}\}.$$

Since $h_p < p$, then p does not divide the index $(U_p : U_p^1)$. Since $(U_p : U_p^1)$ divides $p(p-1) = |\mathbf{R}_p/(p)|^*$, then $(U_p : U_p^1)$ divides $p-1$, hence $\epsilon_p^{p-1} \equiv 1 \pmod{(p)}$. Finally, since

$$\begin{aligned}\epsilon_p^{p-1} &\equiv 2^{p-1}\epsilon_p^{p-1}\\ &\equiv (u_p + v_p\sqrt{p})^{p-1}\\ &\equiv u_p^{p-1} + (p-1)u_p^{p-2}v_p\sqrt{p}\\ &\equiv 1 - u_p^{p-2}v_p\sqrt{p} \pmod{(p)}\end{aligned}$$

and since u_p is prime to p, we get that p divides v_p. □

Remark. Proposition 9 is stronger than the following result in [JY, Theorem I.2.2]: *If* $p \equiv 1 \pmod 4$ *is regular then the discriminant of a real dihedral field of degree* $2p$ *is not a power of* p. Indeed, p is regular if and only if p does not divides B_j for $j \in \{2, 4, \cdots, p-3\}$, while p divides $B_{\frac{p-1}{2}}$ if and only if p divides v_p (see [Wa, Th. 5.37]).

3. Explicit lower bounds for relative class numbers of CM-number fields

We set up some of the notation we will use and remind the reader of a number of results of the first author we will use. We let $\mathbf{N}$ be a totally imaginary number field of degree $2n$ that is a quadratic extension of a totally real subfield $\mathbf{N}^+$ of degree n, i.e., $\mathbf{N}$ is a CM-field with maximal totally real subfield $\mathbf{N}^+$. In that situation, it is well known that the class number $h_{\mathbf{N}^+}$ of $\mathbf{N}^+$ divides the class number $h_{\mathbf{N}}$ of $\mathbf{N}$. We set $h_{\mathbf{N}}^- = h_{\mathbf{N}}/h_{\mathbf{N}^+}$, which is a positive integer called the relative class number of $\mathbf{N}$. We have

$$h_{\mathbf{N}}^- = \frac{Q_{\mathbf{N}} w_{\mathbf{N}}}{(2\pi)^n}\sqrt{\frac{d_{\mathbf{N}}}{d_{\mathbf{N}^+}}}\frac{\mathrm{Res}_{s=1}(\zeta_{\mathbf{N}})}{\mathrm{Res}_{s=1}(\zeta_{\mathbf{N}^+})}, \tag{6}$$

where $Q_{\mathbf{N}} \in \{1, 2\}$ is the Hasse unit index of $\mathbf{N}$, $w_{\mathbf{N}} \geq 2$ is the number of roots of unity in $\mathbf{N}$, $d_{\mathbf{N}}$, $\zeta_{\mathbf{N}}$, $d_{\mathbf{N}^+}$ and $\zeta_{\mathbf{N}^+}$ are the absolute value of the discriminant and the Dedekind zeta-function of $\mathbf{N}$ and $\mathbf{N}^+$, respectively (see [Wa, Chapter 4]). We now provide lower bounds on relative class numbers.

Theorem 10. (*See* [Lou 5, Th. 2]) *Let* $\mathbf{N}$ *be a totally imaginary number field of degree* $2n \geq 2$, *and set* $\epsilon_{\mathbf{N}} = 2\pi n e^{1/n}/d_{\mathbf{N}}^{1/2n}$. *Assume that* $\zeta_{\mathbf{N}}\big(1 - (2/\log d_{\mathbf{N}})\big) \leq 0$. *Then,*

$$h_{\mathbf{N}}^- \geq \frac{1-\epsilon_{\mathbf{N}}}{\mathrm{Res}_{s=1}(\zeta_{\mathbf{N}^+})}\frac{2Q_{\mathbf{N}}w_{\mathbf{N}}}{e(2\pi)^n}\frac{\sqrt{d_{\mathbf{N}}/d_{\mathbf{N}^+}}}{\log d_{\mathbf{N}}}. \tag{7}$$

Theorem 11. (*See* [Lou 6]) *Let* $\mathbf{L}$ *be a real quadratic number field,* $\mathbf{K}$ *be a totally real number field, and assume that* $\mathbf{K}/\mathbf{L}$ *is an abelian extension. Then, there exists an explicit constant* $\mu_{\mathbf{L}}$ *such that for any Artin character* $\chi \neq 1$ *(of conductor* $\mathcal{F}$*) of such an extension we have*

$$|L(1, \chi, \mathbf{K}/\mathbf{L})| \leq \mathrm{Res}_{s=1}(\zeta_{\mathbf{L}})\left(\big(1 - \frac{1}{f}\big)\log f + \big(1 + \frac{1}{f}\big)\mu_{\mathbf{L}}\right) \tag{8}$$

(with $f=\sqrt{N_{\mathbf{L}/\mathbf{Q}}(\mathcal{F})}$). In particular, let $\mathbf{N}^+$ be a totally real sextic number field which is a cyclic cubic extension of a real quadratic number field $\mathbf{L}$. Then, we have

$$\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{N}^+}\big) \leq \frac{1}{128}(\log d_{\mathbf{L}}+0.05)^3\log^2(d_{\mathbf{N}^+}/d_{\mathbf{L}}), \tag{9}$$

and if $d_{\mathbf{N}^+}\geq d_{\mathbf{L}}^4$ then we have the better upper bound

$$\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{N}^+}\big) \leq \frac{1}{128}(\log d_{\mathbf{L}}+0.05)^3\log^2(d_{\mathbf{N}^+}/d_{\mathbf{L}}^2). \tag{10}$$

Proof. We only have to prove (10). Set $f^4=d_{\mathbf{N}^+}/d_{\mathbf{L}}^3$. We have (see [Lou 6]) :

$$\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{L}}\big)\leq(\log d_{\mathbf{L}}+0.05)/2 \text{ and } \mu_{\mathbf{L}}\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{L}}\big)\leq\frac{1}{4}\log^2 d_{\mathbf{L}}.$$

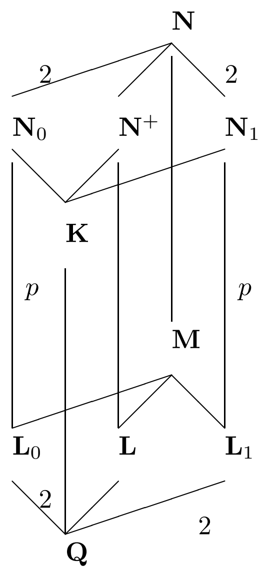
Hence, according to (8) we get (10) from

$$\begin{aligned}\frac{\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{N}^+}\big)}{\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{L}}\big)} &\leq \Big((1-\frac{1}{f})\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{L}}\big)\log f+(1+\frac{1}{f})\mu_{\mathbf{L}}\mathrm{Res}_{s=1}\big(\zeta_{\mathbf{L}}\big)\Big)^2\\ &\leq \Big((1-\frac{1}{f})\frac{\log d_{\mathbf{L}}+0.05}{2}\log f+(1+\frac{1}{f})\frac{\log^2 d_{\mathbf{L}}}{4}\Big)^2\\ &\leq \Big(\frac{\log d_{\mathbf{L}}+0.05}{2}\Big(\log f+\frac{\log d_{\mathbf{L}}}{4}-\frac{1}{f}\big(\log f-\frac{\log d_{\mathbf{L}}}{4}\big)\Big)\Big)^2.\end{aligned}$$

□

4. The class number one problem for dihedral CM-fields of degree $4p$

4.1. **Notations and a lattice of subfields.** For the remainder of this paper we let $\mathbf{N}$ be a dihedral CM-field of degree $4p$, p an odd prime. With the notations of Lemma 3, we let $\mathbf{N}^+$ be the fixed field of the group $Z(D_{4p})=\{1,a^p\}$, $\mathbf{M}$ be the fixed field of the group $\langle a^2\rangle=\{1,a^2,a^4,\cdots,a^{2(p-1)}\}$, and $\mathbf{K}$ be the fixed field of the group $\{1,b,a^p,a^pb\}$. Note that according to Lemma 2(ii) and Lemma 3, we have that a^p is the complex conjugation. Hence, $\mathbf{N}^+$ is the maximal totally real subfield of $\mathbf{N}$ and $\mathbf{M}$ is an imaginary bicyclic biquadratic number field. Note that $\mathbf{K}/\mathbf{Q}$ is not normal. We let $\mathbf{L}_0$ and $\mathbf{L}_1$ denote the two imaginary quadratic subfields of $\mathbf{M}$, and $\mathbf{L}$ its real quadratic subfield. Finally, we set $\mathbf{N}_0=\mathbf{KL}_0$ and $\mathbf{N}_1=\mathbf{KL}_1$. Then $\mathbf{N}^+/\mathbf{Q}$, $\mathbf{N}/\mathbf{L}_0$ and $\mathbf{N}/\mathbf{L}_1$ are dihedral of degree $2p$, and $\mathbf{N}/\mathbf{L}$ is cyclic of degree $2p$. Note that $\mathbf{N}_0$ and $\mathbf{N}_1$ are both CM-fields, with $\mathbf{N}_0^+=\mathbf{N}_1^+=\mathbf{K}$. We have the following lattice of subfields:



Conversely, let $\mathbf{N}^+$ be a totally real dihedral field of degree $2p$, let $\mathbf{L}$ be its real quadratic subfield, and let $\mathbf{M}$ be an imaginary bicyclic biquadratic field whose real quadratic subfield is $\mathbf{L}$. Then, $\mathbf{N} = \mathbf{N}^+\mathbf{M}$ is a dihedral CM-field of degree $4p$.

Proposition 12. *Let* $\mathbf{N}$ *be a dihedral* CM*-field of degree* $4p$. *Then,*
(i). $Q_{\mathbf{N}} = Q_{\mathbf{M}}$ *and* $Q_{\mathbf{N}_0} = Q_{\mathbf{N}_1} = 1$.
(ii). $W_{\mathbf{N}} = W_{\mathbf{M}}$, $W_{\mathbf{N}_0} = W_{\mathbf{L}_0}$ *and* $W_{\mathbf{N}_1} = W_{\mathbf{L}_1}$.
(iii). $h^-_{\mathbf{M}}$ *divides* $h^-_{\mathbf{N}}$, $h^-_{\mathbf{L}_0}$ *divides* $h^-_{\mathbf{N}_0}$ *and* $h^-_{\mathbf{L}_1}$ *divides* $h^-_{\mathbf{N}_1}$.

Proof. Since Hasse unit indices of imaginary quadratic number fields are clearly equal to 1, point (i) follows from Theorem 5(i). Point (ii) follows from the fact that $\mathbf{M}$ is the maximal abelian subfield of $\mathbf{N}$, that $\mathbf{L}_0$ is the maximal abelian subfield of $\mathbf{N}_0$ and that $\mathbf{L}_1$ is the maximal abelian subfield of $\mathbf{N}_1$. Point (iii) follows from Theorem 5(iii). □

4.2. **Determination of all imaginary bicyclic biquadratic number fields with relative class number one.** According to Proposition 12(iii), if $\mathbf{N}$ is a dihedral CM-field of degree $4p$ such that $h^-_{\mathbf{N}} = 1$, then $h^-_{\mathbf{M}} = 1$. Hence, it is worth determining all imaginary bicyclic biquadratic number fields $\mathbf{M}$ with relative class number one. Let $\mathbf{M} = \mathbf{L}_0\mathbf{L}_1$ be an imaginary bicyclic biquadratic number field, where $\mathbf{L}_0$ and $\mathbf{L}_1$ are the two distinct imaginary quadratic subfields of $\mathbf{M}$. Then

$$h^-_{\mathbf{M}} = \begin{cases} h_{\mathbf{L}_0}h_{\mathbf{L}_1} = 1 & \text{if } \mathbf{M} = \mathbf{Q}(\sqrt{-1}, \sqrt{-2}) = \mathbf{Q}(\zeta_8), \\ (Q_{\mathbf{M}}/2)h_{\mathbf{L}_0}h_{\mathbf{L}_1} & \text{if } \mathbf{M} \neq \mathbf{Q}(\sqrt{-1}, \sqrt{-2}) = \mathbf{Q}(\zeta_8) \end{cases} \tag{11}$$

(see [BP]), and $Q_{\mathbf{M}}$ can easily be determined according to the following Lemma 13. Now, all the imaginary quadratic number fields with class number ≤ 2 are known (see [MW], [Sta 1] and [Sta 2]). Hence, we easily get there are 147 imaginary bicyclic biquadratic number fields $\mathbf{M}$ with relative class number one.

Lemma 13. (*See* [Lou 1], [Lou 2] *and* [BWW]) *Let* $\mathbf{M} = \mathbf{L}_0\mathbf{L}_1 \neq \mathbf{Q}(\zeta_8)$ *be an imaginary bicyclic biquadratic number field which is a compositum of two distinct imaginary quadratic fields* $\mathbf{L}_0 = \mathbf{Q}(\sqrt{-D_0})$ *and* $\mathbf{L}_1 = \mathbf{Q}(\sqrt{-D_1})$. *Let* $\mathbf{M}^+ = \mathbf{L} =$

$\mathbf{Q}(\sqrt{D_+})$ *be the real quadratic subfield of* $\mathbf{M}$. *Here,* D_0, D_1 *and* D_+ *are positive square-fee integers. Let* d_0, d_1 *and* d_+ *be the discriminants of* $\mathbf{L}_0, \mathbf{L}_1$ *and* $\mathbf{L}$, *respectively. Then,*

(i). $w_{\mathbf{M}} = w_{\mathbf{L}_0} w_{\mathbf{L}_1}/2$.

(ii). *If* $\mathbf{L}_0 = \mathbf{Q}(i)$ *then* $Q_{\mathbf{M}} = 2$ *if and only if the principal ideal* (2) *of* $\mathbf{L}$ *is the square of a principal ideal of* $\mathbf{L}$, *i.e. if and only if* 2 *divides* d_+ *and the only ideal of* $\mathbf{L}$ *of norm* 2 *is principal in* $\mathbf{L}$, *which amounts to saying that* 2 *is one of the* Q_i*'s which appear in the periodic continued fractional expansion* $x_i = (P_i + \sqrt{d_+})/(2Q_i)$ *of* $x_0 = (d_+ + \sqrt{d_+})/2$.

(iii). *If* $\mathbf{L}_0 \neq \mathbf{Q}(i)$ *then* $Q_{\mathbf{M}} = 2$ *if and only if the principal ideal* (D_1) *of* $\mathbf{L}$ *is the square of a principal ideal of* $\mathbf{L}$, *i.e. if and only if* D_1 *divides* d_+ *and the only ideal of* $\mathbf{L}$ *of norm* D_1 *is principal in* $\mathbf{L}$, *which amounts to saying that* D_1 *or* $\tilde{D}_1$ *is one of the* Q_i*'s which appear in the periodic continued fractional expansion* $x_i = (P_i + \sqrt{d_+})/(2Q_i)$ *of* $x_0 = (d_+ + \sqrt{d_+})/2$. *Here,* $\tilde{D}_1$ *is the norm of the dual ideal of the ramified ideal of norm* D_1, *i.e.*

$$\tilde{D}_1 = \begin{cases} D_+/D_1 & \text{if } D_+ \text{ is even,} \\ D_+/D_1 & \text{if } D_+ \text{ and } D_1 \text{ are odd,} \\ 2D_+/D_1 & \text{if } D_+ \text{ is odd and } D_1 \text{ is even.} \end{cases}$$

4.3. **Upper bounds on discriminants of subfields of dihedral CM-fields of degree 12 with relative class number one.** Let $\mathbf{K}$ be a totally real cubic number field of positive discriminant $d_{\mathbf{K}}$ and assume that $d_{\mathbf{K}}$ is not a square, which amounts to saying that $\mathbf{K}$ is not normal. Set $\mathbf{L} = \mathbf{Q}(\sqrt{d_{\mathbf{K}}})$. Let $\mathbf{M}$ be an imaginary bicyclic biquadratic number field with real quadratic subfield $\mathbf{L}$. Then, the compositum $\mathbf{N} = \mathbf{KM}$ is a dihedral CM-field of degree 12, and any dihedral CM-field of degree 12 is such a compositum.

First, if $h_{\mathbf{N}}^- = 1$ then $h_{\mathbf{M}}^- = 1$ (Proposition 12(iii)), and we note that the Dedekind zeta-functions of the 147 imaginary bicyclic biquadratic fields $\mathbf{M}$ with relative class number satisfy $\zeta_{\mathbf{M}}(s) < 0$, $s \in]0,1[$ (see [Yam]).

Second, since $\mathbf{N}/\mathbf{L}$ is cyclic of degree 6, then $\zeta_{\mathbf{N}}(s) = \zeta_{\mathbf{M}}(s) \prod_\chi L(s,\chi)$, where the product is taken over the four non-quadratic characters of degree 1 of $\mathrm{Gal}(\mathbf{N}/\mathbf{L})$. Since these four characters come in conjugate pairs, and since $\zeta_{\mathbf{M}}$ is negative on $]0,1[$ when $\mathbf{M}$ has relative class number one, we get that $h_{\mathbf{M}}^- = 1$ implies $\zeta_{\mathbf{N}}(s) \leq 0$, $s \in]0,1[$.

Third, according to (9) of Theorem 11, we have $\mathrm{Res}_{s=1}(\zeta_{\mathbf{N}^+}) \leq 11 \log^2(d_{\mathbf{N}^+}/d_{\mathbf{L}})$ when $\mathbf{L}$ is the real quadratic subfield of one of the 147 bicyclic biquadratic imaginary number fields $\mathbf{M}$ with relative class number one. Indeed, if $h_{\mathbf{M}}^- = 1$, then $d_{\mathbf{L}} \leq 65689$ (when $\mathbf{M} = \mathbf{Q}(\sqrt{-403}, \sqrt{-163})$). Hence, according to the previous paragraph and Theorem 10, if $h_{\mathbf{M}}^- = 1$, then we have:

$$h_{\mathbf{N}}^- \geq \frac{2(1-\epsilon_{\mathbf{N}^+})}{11e(2\pi)^6} \frac{\sqrt{d_{\mathbf{N}^+}}}{\log^3 d_{\mathbf{N}^+}},$$

so that $h_{\mathbf{N}}^- = 1$ implies $d_{\mathbf{N}^+} \leq 2 \cdot 10^{22}$. Here, we set

$$\epsilon_{\mathbf{N}} \stackrel{def}{=} 12\pi e^{1/6}/d_{\mathbf{N}}^{1/12} \leq \epsilon_{\mathbf{N}^+} \stackrel{def}{=} 12\pi e^{1/6}/d_{\mathbf{N}^+}^{1/6} \leq \epsilon_{\mathbf{K}} \stackrel{def}{=} 12\pi/d_{\mathbf{K}}^{1/3}$$

(since $d_{\mathbf{N}} \geq d_{\mathbf{N}^+}^2$ and $d_{\mathbf{N}^+} = d_{\mathbf{L}} d_{\mathbf{K}}^2 \geq 5 d_{\mathbf{K}}^2$).

Fourth, we would like to have a good upper bound on $d_{\mathbf{K}}$ when $h_{\mathbf{N}}^- = 1$. Hence, we give a lower bound on $h_{\mathbf{N}}^-$ which depends on $d_{\mathbf{L}}$ and $d_{\mathbf{K}}$. According to the next-to-previous paragraph, to Theorem 10 and to (10) of Theorem 11 we get that $h_{\mathbf{M}}^- = 1$ implies

$$h_{\mathbf{N}}^- \geq \frac{4\sqrt{d_{\mathbf{L}}}}{e\pi^6(\log d_{\mathbf{L}} + 0.05)^3} \frac{(1-\epsilon_{\mathbf{K}})d_{\mathbf{K}}}{\log(d_{\mathbf{L}}d_{\mathbf{K}}^2)\log^2(d_{\mathbf{K}}^2/d_{\mathbf{L}})} \geq \frac{\sqrt{d_{\mathbf{L}}}}{(\log d_{\mathbf{L}} + 0.05)^3} \frac{(1-\epsilon_{\mathbf{K}})d_{\mathbf{K}}}{2e\pi^6 \log^3 d_{\mathbf{K}}}$$

provided that $d_{\mathbf{K}} \geq d_{\mathbf{L}}^{3/2}$. Note that if $h_{\mathbf{M}}^- = 1$ and $\mathbf{L} \subseteq \mathbf{M}$, then $d_{\mathbf{L}}^{3/2} < 2 \cdot 10^7$. Assuming $d_{\mathbf{K}} \geq 5 \cdot 10^8$, we get

$$h_{\mathbf{N}}^- \geq (1 - 12\pi \cdot (5 \cdot 10^8)^{-1/3}) \frac{\sqrt{d_{\mathbf{L}}}}{(\log d_{\mathbf{L}} + 0.05)^3} \frac{5 \cdot 10^8}{2e\pi^6 \log^3(5 \cdot 10^8)} \geq 1.028$$

(the right hand term of this inequality is minimal for $d_{\mathbf{L}}$ a positive integer when $d_{\mathbf{L}} = 384$). We have thus proved

Theorem 14. *Let* $\mathbf{N}$ *be a dihedral* CM*-field of degree* 12 *and maximal totally real subfield* $\mathbf{N}^+$. *Let* $\mathbf{K}$ *be any of the three totally real cubic subfields of* $\mathbf{N}^+$. *If* $h_{\mathbf{N}}^- = 1$, *then* $d_{\mathbf{K}} \leq 5 \cdot 10^8$, $d_{\mathbf{N}^+} \leq 2 \cdot 10^{22}$ *and* $d_{\mathbf{N}} \leq 4 \cdot 10^{44}$.

4.4. **Computation of relative class numbers of CM-fields.** It was well known that it is easy to compute relative class numbers of abelian CM-fields by using generalized Bernoulli numbers (see [Wa, Th. 4.17]). Now, the first author developed the following technique for computing the relative class number of any CM-field:

Theorem 15. (*See* [Lou 3] *and* [Lou 4]). *Let* $\mathbf{N}$ *be a totally imaginary number field of degree* $2n$ *which is a quadratic extension of a totally real number field* $\mathbf{N}^+$ *of degree* n, *i.e.* $\mathbf{N}$ *is a* CM*-field. Let* ϕ_k *be the coefficients of the Dirichlet series* $(\zeta_{\mathbf{N}}/\zeta_{\mathbf{N}^+})(s) = \sum_{k\geq 1} \phi_k k^{-s}$. *Set* $A_{\mathbf{N}/\mathbf{N}^+} = \sqrt{d_{\mathbf{N}}/\pi^n d_{\mathbf{N}^+}}$. *We have*

$$h_{\mathbf{N}}^- = \frac{Q_{\mathbf{N}} w_{\mathbf{N}}}{(2\pi)^n} \sqrt{\frac{d_{\mathbf{N}}}{d_{\mathbf{N}^+}}} \sum_{k\geq 1} \frac{\phi_k}{k} K_n(k/A_{\mathbf{N}/\mathbf{N}^+}) \tag{12}$$

where

$$K_n(A) = \frac{A^2}{2i\pi} \int_{a-i\infty}^{a+i\infty} 2f_n(s)ds \quad \textit{with} \quad f_n(s) = \Gamma^n(s)A^{-2s}\left(\frac{1}{2s-1} + \frac{1}{2s-2}\right).$$

Moreover, $0 \leq K_n(A) \leq n2^n \exp(-A^{2/n})$.

Hence (see [Lou 4]), if $\lambda > 1$ and N are given, then the limit of $|h_{\mathbf{N}}^- - h_{approx,\mathbf{N}}^-|$ as $d_{\mathbf{N}}$ approaches infinity is equal to 0, where $h_{approx,\mathbf{N}}^-$ is the approximation of the relative class number obtained by truncating the series occurring in (12) after

$$k \leq B(\mathbf{N}) \stackrel{def}{=} A_{\mathbf{N}/\mathbf{N}^+}\left(\lambda \log A_{\mathbf{N}/\mathbf{N}^+}\right)^{n/2}.$$

Finally, the following Lemma 16 explains how we compute the numerical values of the function $A \mapsto K_n(A)$ according to its series expansion:

Lemma 16. (*See* [Lou 3]). *Take* $A > 0$. *Then*

$$K_n(A) = 1 + \pi^{n/2}A + 2A^2 \sum_{m\geq 0} \mathrm{Res}_{s=-m}(f_n)$$

and [1]

$$\mathrm{Res}_{s=-m}(f_n) = -(-1)^{nm} \frac{A^{2m}}{(m!)^n} \sum_{i=-n}^{-1} 2^{-1-i} h_i(m)((2m+1)^i + (2m+2)^i),$$

[1]Note the misprint in the formula given in [Lou 3].

where the $h_i(m)$'s are computed recursively from the $h_i(0)$'s by using

$$h_i(m+1) = \sum_{j=-n}^{i} h_j(m) \frac{b_{i-j}}{(m+1)^{i-j}},$$

where $b_k = ((k+n-1)!/k!(n-1)!)$ and

$$\sum_{j=0}^{n-1} h_{j-n}(0)s^j \ + O(s^n) = \Gamma^n(s+1)A^{-2s}.$$

Since the computation of the relative class numbers of all the dihedral CM-fields $\mathbf{N}$ of degree 12 with $d_{\mathbf{N}} \leq 4 \cdot 10^{44}$ would take too much time on a computer, we now develop a techniques that will enable us to solve efficiently the relative class number one problem for dihedral CM-fields $\mathbf{N}$ of degree 12. The idea is to deal with CM-fields $\mathbf{N}_0$ of degree smaller than 12, hence such that $B(\mathbf{N}_0)$ is much smaller than $B(\mathbf{N})$, because the computation of the relative class numbers of the $\mathbf{N}_0$'s is then likely to be much more efficient than that for the $\mathbf{N}$'s.

4.5. **Relative class number factorizations.** Let $\mathbf{N}$ be a dihedral CM-field of degree $4p$. As $\mathbf{N}/\mathbf{L}_0$, $\mathbf{N}/\mathbf{L}_1$ and $\mathbf{N}^+/\mathbf{Q}$ are dihedral, we get

$$(13) \qquad \left(\zeta_{\mathbf{N}_0}/\zeta_{\mathbf{L}_0}\right)^2 = \zeta_{\mathbf{N}}/\zeta_{\mathbf{M}} = \left(\zeta_{\mathbf{N}_1}/\zeta_{\mathbf{L}_1}\right)^2 \quad \text{and} \quad \zeta_{\mathbf{N}^+}/\zeta_{\mathbf{L}} = \left(\zeta_{\mathbf{K}}/\zeta_{\mathbf{Q}}\right)^2,$$

which yields

$$(14) \qquad \left(\zeta_{\mathbf{N}_0}/\zeta_{\mathbf{K}}\right)/\left(\zeta_{\mathbf{L}_0}/\zeta_{\mathbf{Q}}\right) = \left(\zeta_{\mathbf{N}_1}/\zeta_{\mathbf{K}}\right)/\left(\zeta_{\mathbf{L}_1}/\zeta_{\mathbf{Q}}\right)$$

and

$$(15) \qquad \left(\zeta_{\mathbf{N}}/\zeta_{\mathbf{N}^+}\right)/\left(\zeta_{\mathbf{M}}/\zeta_{\mathbf{L}}\right) = \left(\left(\zeta_{\mathbf{N}_0}/\zeta_{\mathbf{K}}\right)/\left(\zeta_{\mathbf{L}_0}/\zeta_{\mathbf{Q}}\right)\right)^2.$$

We recall that the functional equation of a Dedekind zeta-function $\zeta_{\mathbf{E}}$ contains a factor $d_{\mathbf{E}}^{s/2}$. Applying the functional equation to each of the Dedekind zeta-functions of (13), (14) and (15), one can derive the relations

$$(16) \qquad \left(d_{\mathbf{N}_0}/d_{\mathbf{L}_0}\right)^2 = d_{\mathbf{N}}/d_{\mathbf{M}} = \left(d_{\mathbf{N}_1}/d_{\mathbf{L}_1}\right)^2 \quad \text{and} \quad d_{\mathbf{N}^+}/d_{\mathbf{L}} = d_{\mathbf{K}}^2,$$

$$(17) \qquad \left(d_{\mathbf{N}_0}/d_{\mathbf{N}_0^+}\right) \,/\, \left(d_{\mathbf{L}_0}/d_{\mathbf{L}_0^+}\right) = \left(d_{\mathbf{N}_1}/d_{\mathbf{N}_1^+}\right) \,/\, \left(d_{\mathbf{L}_1}/d_{\mathbf{L}_1^+}\right),$$

$$(18) \qquad \left(d_{\mathbf{N}}/d_{\mathbf{N}^+}\right) \,/\, \left(d_{\mathbf{M}}/d_{\mathbf{M}^+}\right) = \left(d_{\mathbf{N}_0}/d_{\mathbf{N}_0^+}\right) \,/\, \left(d_{\mathbf{L}_0}/d_{\mathbf{L}_0^+}\right),$$

and

$$(19) \qquad \left(A_{\mathbf{N}/\mathbf{N}^+}\right) \,/\, \left(A_{\mathbf{M}/\mathbf{M}^+}\right) = \left(A_{\mathbf{N}_0/\mathbf{N}_0^+} \,/\, A_{\mathbf{L}_0/\mathbf{L}_0^+}\right)^2.$$

As in [Lou 7], by using (6) and (17) we get

$$\frac{h^-_{\mathbf{N}_0}}{Q_{\mathbf{N}_0}w_{\mathbf{N}_0}} \Big/ \frac{h^-_{\mathbf{L}_0}}{Q_{\mathbf{L}_0}w_{\mathbf{L}_0}} = \frac{h^-_{\mathbf{N}_1}}{Q_{\mathbf{N}_1}w_{\mathbf{N}_1}} \Big/ \frac{h^-_{\mathbf{L}_1}}{Q_{\mathbf{L}_1}w_{\mathbf{L}_1}},$$

and by using (6) and (18) we get

$$\frac{h^-_{\mathbf{N}}}{Q_{\mathbf{N}}w_{\mathbf{N}}} \Big/ \frac{h^-_{\mathbf{M}}}{Q_{\mathbf{M}}w_{\mathbf{M}}} = \left(\frac{h^-_{\mathbf{N}_0}}{Q_{\mathbf{N}_0}w_{\mathbf{N}_0}} \Big/ \frac{h^-_{\mathbf{L}_0}}{Q_{\mathbf{L}_0}w_{\mathbf{L}_0}}\right)^2.$$

According to Proposition 12 we thus get

Proposition 17. *Let* $\mathbf{N}$ *be a dihedral* CM*-field of degree* $4p$*. Then,*

$$h_{\mathbf{N}}^- = \left(h_{\mathbf{N}_0}^-/h_{\mathbf{L}_0}^-\right)^2 h_{\mathbf{M}}^- = \left(h_{\mathbf{N}_1}^-/h_{\mathbf{L}_1}^-\right)^2 h_{\mathbf{M}}^-. \tag{20}$$

Now, according to (11), Proposition 12(iii) and Proposition 17 we get

Corollary 18. (i). *Let* $\mathbf{M} = \mathbf{L}_0\mathbf{L}_1$ *be an imaginary bicyclic biquadratic number field which is a compositum of two distinct imaginary quadratic fields* $\mathbf{L}_0$ *and* $\mathbf{L}_1$*. If* $h_{\mathbf{M}}^-$ *is odd then* $h_{\mathbf{L}_0}^-$ *or* $h_{\mathbf{L}_1}^-$ *is odd, and if* $h_{\mathbf{M}}^- = 1$ *then* $h_{\mathbf{L}_0}^-$ *or* $h_{\mathbf{L}_1}^-$ *is equal to one (and for the rest of this paper we choose notations so that these conclusions hold with* $\mathbf{L}_0$*).*

(ii). *Let* $\mathbf{N}$ *be a dihedral* CM*-field of degree* $4p$*. Then* $h_{\mathbf{N}}^-$ *is odd if and only if* $h_{\mathbf{M}}^-$ *and* $h_{\mathbf{N}_0}^-$ *are odd, and* $h_{\mathbf{N}}^- = 1$ *if and only if* $h_{\mathbf{M}}^- = h_{\mathbf{N}_0}^- = 1$*.*

Remark. Proposition 17 is very useful when doing explicit computations, because it reduces computation of relative class numbers of dihedral CM-fields of degree $4p$ to that of CM-fields of degree 4 and $2p$. Indeed, let us make more precise our conclusion of section 4.4. According to (19) and by using $d_{\mathbf{M}} = d_{\mathbf{L}}d_{\mathbf{L}_0}d_{\mathbf{L}_1}$, we get

$$A_{\mathbf{N}_0/\mathbf{N}_0^+} = \sqrt{\frac{d_{\mathbf{L}_0}}{d_{\mathbf{L}_1}}}\sqrt{A_{\mathbf{N}/\mathbf{N}^+}}.$$

Hence, if we content ourselves with imaginary bicyclic biquadratic number fields $\mathbf{M}$ with relative class numbers equal to one (see Corollary 18(i)), then $d_{\mathbf{L}_0}$ and $d_{\mathbf{L}_1}$ take on only finitely many values, and we get

$$B(\mathbf{N}_0) = O\left(\sqrt{B(\mathbf{N})}\right).$$

Therefore, the computation of $h_{\mathbf{N}_0}^-$ is indeed much faster than that of $h_{\mathbf{N}}^-$.

4.6. **Restrictions on dihedral CM-fields N of degree** $4p$ **with odd relative class numbers.** If $h_{\mathbf{N}}^-$ is odd then the number t of prime ideals of $\mathbf{N}^+$ which ramify in the quadratic extension $\mathbf{N}/\mathbf{N}^+$ is ≤ 1 (Lemma 4(i)). Hence, we get

Theorem 19. *Let* $\mathbf{N}$ *be a dihedral* CM*-field of degree* $4p$ *(*p *any odd prime). If the relative class number* $h_{\mathbf{N}}^-$ *of* $\mathbf{N}$ *is odd then* $\mathbf{L}_0/\mathbf{Q}$ *is ramified at only one positive prime rational integer* p_0 *which divides* $d_{\mathbf{K}}$*, and if* $p_0 = 2$ *then* 2 *is not totally ramified in* $\mathbf{M}/\mathbf{Q}$*.*

Proof. First, if $h_{\mathbf{N}}^-$ is odd then $h_{\mathbf{L}_0} = h_{\mathbf{L}_0}^-$ is odd. According to genus theory, we get that $\mathbf{L}_0/\mathbf{Q}$ is ramified at exactly one finite prime, to be denoted by p_0.

Second, if 2 is totally ramified in $\mathbf{M}/\mathbf{Q}$, then 2 is ramified in $\mathbf{L}/\mathbf{Q}$, i.e., $(2) = \mathcal{P}^2$. According to Lemma 3, this prime ideal $\mathcal{P}$ splits completely in $\mathbf{N}^+/\mathbf{L}$, the p prime ideals of $\mathbf{N}^+$ which lie above $\mathcal{P}$ are ramified in $\mathbf{N}/\mathbf{N}^+$, and 2^{p-1} divides $h_{\mathbf{N}}^-$, which is thus even.

Third, if p_0 does not divide $d_{\mathbf{K}}$, then p_0 divides neither $d_{\mathbf{L}}$ nor $d_{\mathbf{N}^+}$ (since $d_{\mathbf{K}} = d_{\mathbf{L}}^{\frac{p-1}{2}} f^{p-1}$ and $d_{\mathbf{N}^+} = d_{\mathbf{L}}d_{\mathbf{K}}^2$). Hence, p_0 is unramified in $\mathbf{N}^+/\mathbf{Q}$. First, assume that p_0 is inert in $\mathbf{L}/\mathbf{Q}$. Since $\mathbf{N}^+/\mathbf{Q}$ is dihedral, hence is not cyclic, then p_0 is not inert in $\mathbf{N}^+/\mathbf{Q}$. Thus, p_0 splits completely in $\mathbf{N}^+/\mathbf{L}$. Now, the p prime ideals of $\mathbf{N}^+$ which lie above p_0 are ramified in $\mathbf{N}/\mathbf{N}^+$, and here again 2^{p-1} divides $h_{\mathbf{N}}^-$, which is thus even. Second, if p_0 splits completely in $\mathbf{L}_0/\mathbf{Q}$, i.e. $(p_0) = \mathcal{P}_1\mathcal{P}_2$, then each $\mathcal{P}_i$ is ramified in $\mathbf{M}/\mathbf{L}$. Hence, the prime ideals of $\mathbf{N}^+$ which lie above $\mathcal{P}_1$ and $\mathcal{P}_2$ are ramified in $\mathbf{N}/\mathbf{N}^+$. Since there are at least 2 such prime ideals, then 2 divides $h_{\mathbf{N}}^-$ which is thus even. □

Remark. Exactly 6 out of the 147 imaginary bicyclic biquadratic number fields $\mathbf{M}$ with $h_{\mathbf{M}}^- = 1$ are such that 2 is totally ramified in $\mathbf{M}/\mathbf{Q}$, namely

$$\mathbf{Q}(\sqrt{-1}, \sqrt{-2}), \qquad \mathbf{Q}(\sqrt{-1}, \sqrt{-10}), \qquad \mathbf{Q}(\sqrt{-1}, \sqrt{-58}),$$
$$\mathbf{Q}(\sqrt{-2}, \sqrt{-5}), \qquad \mathbf{Q}(\sqrt{-2}, \sqrt{-13}), \qquad \mathbf{Q}(\sqrt{-2}, \sqrt{-37}).$$

4.7. **The required computations.** Let $\mathbf{K}$ be a non-normal cubic number field with discriminant $d_{\mathbf{K}} = d_{\mathbf{L}} f^2$, where $d_{\mathbf{L}}$ is the discriminant of the quadratic subfield $\mathbf{L}$ of the normal closure of $\mathbf{K}$. Let q be a positive prime integer. Then q satisfies one of the following conditions :
1k). If q does not divide $d_{\mathbf{K}}$ and $(d_{\mathbf{K}}/q) = -1$ (Kronecker's symbol), then $(q) = \mathcal{Q}_1\mathcal{Q}_2$ in $\mathbf{K}$, where $\mathcal{Q}_1$ has inertia degree equal to 1 and $\mathcal{Q}_2$ has inertia degree equal to 2.
2k). If q does not divide $d_{\mathbf{K}}$ and $(d_{\mathbf{K}}/p) = +1$, then $(q) = \mathcal{Q}$ or $(q) = \mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3$ in $\mathbf{K}$, in which cases we respectively set $\eta_q = -1$ or $+1$. If q does not divides the index $i_{\mathbf{K}}$ of $\mathbf{Z}[\alpha_{\mathbf{K}}]$ in the ring of the algebraic integers of $\mathbf{K}$ where $\mathbf{K} = \mathbf{Q}(\alpha_{\mathbf{K}})$ for some algebraic integer $\alpha_{\mathbf{K}}$, then the two cases are distinguished by the splitting modulo q of the minimal polynomial $P_{\mathbf{K}}(X)$ of $\alpha_{\mathbf{K}}$. We note that that in all the cases considered in Table 2, on page 3676, if q divides $i_{\mathbf{K}}$ then q is ramified in $\mathbf{K}/\mathbf{Q}$.
3k). If q divides f, then $(q) = \mathcal{Q}^3$ in $\mathbf{K}$.
4k). If q divides $d_{\mathbf{L}}$ and q does not divide f, then $(q) = \mathcal{Q}_1\mathcal{Q}_2^2$ in $\mathbf{K}$.

Then, let $\mathbf{L}_0$ be a quadratic number field, set $\mathbf{N}_0 = \mathbf{K}\mathbf{L}_0$ and $\mathbf{M} = \mathbf{L}_0\mathbf{L}$, and let $\mathbf{L}_1$ be the third quadratic subfield of $\mathbf{M}$. Thus, $\mathbf{N} = \mathbf{K}\mathbf{M}$ is a dihedral number field of degree 12. We want to compute $\phi(k) = \sum_{\mathbf{I}} \chi_{\mathbf{N}_0/\mathbf{K}}(\mathbf{I})$, where this sum is over the integral ideals $\mathbf{I}$ of $\mathbf{K}$ with norms equal to $k \geq 1$. Here, $\chi_{\mathbf{N}_0/\mathbf{K}}$ is the quadratic character associated to the quadratic extension $\mathbf{N}_0/\mathbf{K}$, which is well determined once we know that it is a completely multiplicative function defined on the non-zero integral ideals of $\mathbf{K}$ which satisfies $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}) = -1$, 0 or $+1$ according as the prime ideal $\mathcal{Q}$ of $\mathbf{K}$ is inert, is ramified or splits in $\mathbf{N}_0/\mathbf{K}$. Since $k \mapsto \phi(k)$ is multiplicative, we only have to explain how we compute $\phi(q^m)$ when q is prime and $m \geq 1$. Let e be the ramification index of a prime ideal $\mathcal{Q}$ of $\mathbf{K}$ lying above some prime q. We have:
1l). If q is inert in $\mathbf{L}_0/\mathbf{Q}$, we set $\epsilon_0 = -1$. Then $\mathcal{Q}$ is inert or splits in $\mathbf{N}_0/\mathbf{K}$ according as the inertia degree of $\mathcal{Q}$ is odd or even.
2l). If q is ramified in $\mathbf{L}_0/\mathbf{Q}$, we set $\epsilon_0 = 0$. Then, if $e = 1$ or $e = 3$ then $\mathcal{Q}$ is ramified in $\mathbf{N}_0/\mathbf{K}$, while if $e = 2$ then $\mathcal{Q}$ is inert, is ramified or splits in $\mathbf{N}_0/\mathbf{K}$ according as the prime ideals of $\mathbf{L}$ lying above q are inert, are ramified or split in $\mathbf{M}/\mathbf{L}$ (which amounts to saying that q is inert, is ramified or splits in $\mathbf{L}_1/\mathbf{Q}$), in which cases we respectively set $\epsilon_1 = -1$, 0 or $+1$.
3l). If q splits in $\mathbf{L}_0/\mathbf{Q}$, we set $\epsilon_0 = +1$. Then $\mathcal{Q}$ splits in $\mathbf{N}_0/\mathbf{K}$.

Note that $\epsilon_0 = (-d_{\mathbf{L}_0}/q)$ and $\epsilon_1 = (-d_{\mathbf{L}_1}/q)$ (Kronecker's symbols). From these two points we get the following rules, which enable us to compute $\phi(q^m)$:
1n). We assume that 1k) holds. Then $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1) = \epsilon_0$ and $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2) = 1$ if $\epsilon_0 \neq 0$, and $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2) = 0$ if $\epsilon_0 = 0$. Hence, $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2) = \epsilon_0^2$ and

$$\phi(q^m) = \sum_{a+2b=m} \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1^a\mathcal{Q}_2^b) = \sum_{a+2b=m} \epsilon_0^m = \left[\frac{m+2}{2}\right]\epsilon_0^m,$$

where $[x]$ stands for the greatest relative integer less than or equal to x.

2n). We assume that 2k) holds. If $\eta_q = -1$, then $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}) = \epsilon_0$ and

$$\phi(q^m) = \begin{cases} 0 & \text{if 3 does not divide } m, \\ \epsilon_0^{m/3} = \epsilon_0^m & \text{if 3 divides } m. \end{cases}$$

If $\eta_q = +1$, then $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_i) = \epsilon_0$, $1 \le i \le 3$, and

$$\phi(q^m) = \sum_{a+b+c=m} \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1^a \mathcal{Q}_2^b \mathcal{Q}_3^c) = \sum_{a+b+c=m} \epsilon_0^m = \frac{(m+1)(m+2)}{2} \epsilon_0^m.$$

3n). We assume that 3k) holds. Then $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}) = \epsilon_0$. Hence,

$$\phi(q^m) = \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}^m) = \epsilon_0^m.$$

4n). We assume that 4k) holds. Then $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1) = \epsilon_0$. Now, $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2) = \epsilon_0$ if $\epsilon_0 \neq 0$, in which case we get

$$\phi(q^m) = \sum_{a+b=m} \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1^a \mathcal{Q}_2^b) = \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2^m) = \epsilon_0^{a+b} = (m+1)\epsilon_0^m,$$

while $\chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_2) = \epsilon_1$ if $\epsilon_0 = 0$, in which case we get

$$\phi(q^m) = \sum_{a+b=m} \chi_{\mathbf{N}_0/\mathbf{K}}(\mathcal{Q}_1^a \mathcal{Q}_2^b) = \sum_{a+b=m} 0^a \epsilon_1^b = \epsilon_1^m.$$

Since $\epsilon_0 \neq 0$ implies $\epsilon_1 = 0$ (for q is ramified in $\mathbf{L}/\mathbf{Q}$, hence ramified in at least two of the quadratic subfields of $\mathbf{M}$), we may collect these two subcases of case 4n) in the following convenient formula:

$$\phi(q^m) = (m+1)\epsilon_0^m + \epsilon_1^m.$$

The following Lemma 20 then makes it easy to apply Theorem 15 and Lemma 16 in order to compute the relative class numbers of such $\mathbf{N}_0$'s:

Lemma 20. *Let $\mathbf{K}$ be a non-normal cubic number field and $\mathbf{L}_0$ be a quadratic number field. Assume that $\mathbf{L}_0$ is not equal to the quadratic subfield $\mathbf{L}$ of the normal closure $\mathbf{N}$ of $\mathbf{K}$, let $\mathbf{L}_1$ be the third quadratic subfield of the bicyclic biquadratic number field $\mathbf{M} = \mathbf{L}\mathbf{L}_0$, and set $\mathbf{N}_0 = \mathbf{K}\mathbf{L}_0$. Then, $d_{\mathbf{N}_0} = f_0 d_{\mathbf{L}_0} d_{\mathbf{K}}^2$, with $f_0 = d_{\mathbf{L}_0} d_{\mathbf{L}_1} / \gcd(d_{\mathbf{K}}, d_{\mathbf{L}_0} d_{\mathbf{L}_1})$.*

Proof. We note that $\mathbf{N} = \mathbf{K}M$ is dihedral of degree 12. Hence, $\mathbf{N}/\mathbf{L}$ is cyclic sextic. We set $\mathbf{N}^+ = \mathbf{K}L$. We let χ be a character of order 6 associated to this extension, and $\mathcal{F}_i$ be the conductor of χ^i. Hence, we have $\mathcal{F}_1 = \operatorname{lcm}(\mathcal{F}_2, \mathcal{F}_3)$. Set $f_i = N_{\mathbf{L}/\mathbf{Q}}(\mathcal{F}_i)$, $1 \le i \le 3$. We claim that $f_1 = \operatorname{lcm}(f_2, f_3)$. Indeed, when $\mathbf{K}/\mathbf{k}$ is an extension of number fields, let $\mathcal{D}_{\mathbf{K}/\mathbf{k}}$ be its different and $d_{\mathbf{K}/\mathbf{k}} = N_{\mathbf{K}/\mathbf{k}}(\mathcal{D}_{\mathbf{K}/\mathbf{k}})$ be its relative discriminant. Then, $d_{\mathbf{N}^+/\mathbf{L}} = \mathcal{F}_2^2$ and $d_{\mathbf{M}/\mathbf{L}} = \mathcal{F}_3$. Since $\mathbf{N}^+/\mathbf{Q}$, $\mathbf{N}^+/\mathbf{L}$, $\mathbf{M}/\mathbf{Q}$, and $\mathbf{M}/\mathbf{L}$ are normal, then $\mathcal{D}_{\mathbf{N}^+/\mathbf{L}}$ and $d_{\mathbf{N}^+/\mathbf{L}}$ are invariant under the action of $\operatorname{Gal}(\mathbf{N}^+/\mathbf{Q})$, and $\mathcal{D}_{\mathbf{M}/\mathbf{L}}$ and $d_{\mathbf{M}/\mathbf{L}}$ are invariant under the action of $\operatorname{Gal}(\mathbf{M}/\mathbf{Q})$. Hence, $\mathcal{F}_2$ and $\mathcal{F}_3$ are invariant under the action of $\operatorname{Gal}(\mathbf{L}/\mathbf{Q})$. Thus, $\mathcal{F}_1 = \operatorname{lcm}(\mathcal{F}_2, \mathcal{F}_3)$ implies $f_1 = \operatorname{lcm}(f_2, f_3)$. Now, we have $d_{\mathbf{N}} = d_{\mathbf{L}}^6 f_1^2 f_2^2 f_3$, $d_{\mathbf{N}^+} = d_{\mathbf{L}}^3 f_2^2$ and $d_{\mathbf{M}} = d_L^2 f_3$. According to (16) we have $d_{\mathbf{N}^+} = d_{\mathbf{L}} d_{\mathbf{K}}^2$ and $d_{\mathbf{N}}/d_{\mathbf{M}} = (d_{\mathbf{N}_0}/d_{\mathbf{L}_0})^2$. Moreover, as $\mathbf{M}/\mathbf{Q}$ is bicyclic biquadratic we also have $d_{\mathbf{M}} = d_{\mathbf{L}} d_{\mathbf{L}_0} d_{\mathbf{L}_1}$.

Thus, $f_2 = d_{\mathbf{K}}/d_{\mathbf{L}}$, $f_3 = d_{\mathbf{M}}/d_{\mathbf{L}}^2 = d_{\mathbf{L}_0}d_{\mathbf{L}_1}/d_{\mathbf{L}}$ and $f_1 = \mathrm{lcm}(d_{\mathbf{K}}/d_{\mathbf{L}}, d_{\mathbf{L}_0}d_{\mathbf{L}_1}/d_{\mathbf{L}})$. Hence,

$$\begin{aligned} d_{\mathbf{N}_0}/d_{\mathbf{L}_0} = \sqrt{d_{\mathbf{N}}/d_{\mathbf{M}}} = d_{\mathbf{L}}^2 f_1 f_2 &= d_{\mathbf{K}}d_{\mathbf{L}}\mathrm{lcm}(d_{\mathbf{K}}/d_{\mathbf{L}}, d_{\mathbf{L}_0}d_{\mathbf{L}_1}/d_{\mathbf{L}}) \\ &= d_{\mathbf{K}}\mathrm{lcm}(d_{\mathbf{K}}, d_{\mathbf{L}_0}d_{\mathbf{L}_1}) = f_0 d_{\mathbf{K}}^2. \end{aligned}$$

□

Thanks to [Coh] and [Ol] we get Table 2, which provides all the non-normal totally real cubic number fields $\mathbf{K}$ with $d_{\mathbf{K}} \leq 15000$ such that (see Theorem 19)
(i): there exists at least one of the 141 imaginary bicyclic biquadratic number field $\mathbf{M}$ with $h_{\mathbf{M}}^- = 1$ in which 2 is not totally ramified which satisfies $\mathbf{L} = \mathbf{Q}(\sqrt{d_{\mathbf{K}}}) \subseteq \mathbf{M}$;
(ii): and $p_0 \mid d_{\mathbf{K}}$.

Then, for each $\mathbf{K}$ that occurs it provides all the possible choices for $\mathbf{M} = \mathbf{L}\mathbf{L}_0$. We set $\mathbf{L}_0 = \mathbf{Q}(\sqrt{-D_0})$ and $\mathbf{L} = \mathbf{Q}(\sqrt{D_{\mathbf{L}}})$ with $1 \leq D_0$ and $1 < D_{\mathbf{L}}$ square-free. Finally, if $\mathbf{K} = \mathbf{Q}(\alpha_{\mathbf{K}})$ where $\alpha_{\mathbf{K}}$ is an algebraic integer which is a root of some unitary cubic polynomial with integral coefficients $P_{\mathbf{K}}(X)$, we let $i_{\mathbf{K}}$ denote the index of the ring $\mathbf{Z}[\alpha_{\mathbf{K}}]$ in the ring of algebraic integers of $\mathbf{K}$. Finally, we wrote a UBASIC program[2] which, with D_0, $D_{\mathbf{L}}$ and $P_{\mathbf{K}}(X)$ as inputs, outputs the relative number of $\mathbf{N}_0$. Moreover, when $h_{\mathbf{N}_0}^- = 1$ we give the value $h_{\mathbf{N}^+}$ of the class number of $\mathbf{N}^+$. Note that there are 16 sextic CM-fields $\mathbf{N}_0$ with relative class number one in Table 2.

Finally, according to the more extensive similar calculations up to $d_{\mathbf{K}} \leq 5 \cdot 10^8$ done by M. Olivier[3] and according to Theorem 14, there is no other dihedral CM-field $\mathbf{N}$ of degree 12 with relative class number one. Therefore, and according to Lemma 2 and Theorem 6, we have solved the relative class number one and class number one problems for non-abelian normal CM-fields of degree 12, and Theorem 1 is proved.

Final remark. When we wrote the first version of this paper, we had not come up with Proposition 8, which explains why most of the relative class numbers of dihedral CM-fields of degree 12 we had computed are divisible by 3. Hence, using Proposition 8 would now drastically reduce the amount of relative class number computation required to solve the class number one problem for non-abelian normal CM-fields of degree 12. Indeed, we get:

Corollary 21. *Let $\mathbf{N}$ be a dihedral* CM-*field of degree $4p$, p any odd prime. Let $\mathbf{M}$ be the imaginary biquadratic bicyclic subfield of $\mathbf{N}$ and let $\mathbf{L} = \mathbf{M}^+$ be the real quadratic subfield of $\mathbf{N}$. Assume $p > 3$, or $p = 3$ but $\mathbf{Q}(\sqrt{-3}) \not\subset \mathbf{M}$. If there exists some rational prime which is unramified in $\mathbf{M}/\mathbf{Q}$, inert in $\mathbf{L}/\mathbf{Q}$ and ramified in $\mathbf{N}^+/\mathbf{L}$, then p divides $h_{\mathbf{N}}^-$. Assume $p = 3$ and $\mathbf{Q}(\sqrt{-3}) \subset \mathbf{M}$. If there exist at least*

[2]This program is available from the first author.

[3]First, he found that there are 10283 non-normal totally real cubic number fields $\mathbf{K}$ with $d_{\mathbf{K}} \leq 5 \cdot 10^8$ such that $\mathbf{L} = \mathbf{Q}(\sqrt{d_{\mathbf{K}}})$ is the real quadratic subfield of one of the 141 imaginary biquadratic number fields $\mathbf{M}$ with $h_{\mathbf{M}}^- = 1$, with 2 not totally ramified in $\mathbf{M}/\mathbf{Q}$ and with p_0 dividing $d_{\mathbf{K}}$ (see Theorem 19). Second, he found that there are 11761 possible non-normal sextic CM-fields $\mathbf{N}_0$. Third, he computed the relative class numbers of these 11761 CM-fields. Roughly speaking, it took only 2 days to get these 11761 CM-fields but 40 days to complete the calculation of their relative class numbers. Finally, by using unconditional Minkowski upper bounds, he computed the class numbers of the maximal real subfields $\mathbf{N}^+$ of the 16 dihedral CM-fields of degree 12 with relative class number one.

TABLE 2

$(d_{\mathbf{K}}, D_{\mathbf{L}}, D_0)$	$(i_{\mathbf{K}}, P_{\mathbf{K}}(X))$	$(h^-_{\mathbf{N}_0}, h_{\mathbf{N}^+})$
$(148, 37, 1)$	$(1, X^3 + X^2 - 3X - 1)$	$(1, 1)$
$(469, 469, 7)$	$(1, X^3 + X^2 - 5X - 4)$	$(1, 1)$
$(473, 473, 11)$	$(1, X^3 - 5X - 1)$	$(1, 1)$
$(756, 21, 3)$	$(1, X^3 - 6X - 2)$	$(1, 1)$
$(940, 235, 1)$	$(1, X^3 - 7X - 4)$	$(1, 2)$
$(1300, 13, 1)$	$(1, X^3 - 10X - 10)$	3
$(1304, 326, 2)$	$(2, X^3 - X^2 - 11X - 1)$	$(1, 1)$
$(1425, 57, 3)$	$(1, X^3 - X^2 - 8X - 3)$	$(1, 1)$
$(1620, 5, 1)$	$(1, X^3 - 12X - 14)$	3
$(1620, 5, 2)$	$(1, X^3 - 12X - 14)$	3
$(1620, 5, 3)$	$(1, X^3 - 12X - 14)$	$(1, 1)$
$(1708, 427, 1)$	$(1, X^3 - X^2 - 8X - 2)$	$(1, 2)$
$(1944, 6, 2)$	$(1, X^3 - 9X - 6)$	$(1, 1)$
$(2057, 17, 11)$	$(1, X^3 - 11X - 11)$	2
$(2673, 33, 3)$	$(1, X^3 - 9X - 3)$	2
$(2700, 3, 1)$	$(1, X^3 - 15X - 20)$	$(1, 1)$
$(3325, 133, 7)$	$(1, X^3 - 10X - 5)$	3
$(4104, 114, 19)$	$(2, X^3 - 18X - 16)$	$(1, 2)$
$(4212, 13, 1)$	$(1, X^3 - 12X - 10)$	4
$(4312, 22, 2)$	$(2, X^3 + X^2 - 16X - 8)$	$(1, 3)$
$(4860, 15, 1)$	$(2, X^3 - 18X - 12)$	5
$(4860, 15, 3)$	$(2, X^3 - 18X - 12)$	$(1, 2)$
$(5073, 5073, 19)$	$(1, X^3 + X^2 - 18X - 33)$	2
$(5684, 29, 2)$	$(1, X^3 - 14X - 14)$	11
$(5780, 5, 1)$	$(1, X^3 + X^2 - 11X - 5)$	6
$(5780, 5, 2)$	$(1, X^3 + X^2 - 11X - 5)$	6
$(6237, 77, 7)$	$(1, X^3 - 12X - 5)$	3
$(7220, 5, 1)$	$(2, X^3 + X^2 - 25X - 45)$	7
$(7220, 5, 2)$	$(2, X^3 + X^2 - 25X - 45)$	9
$(7425, 33, 3)$	$(1, X^3 - 15X - 15)$	3
$(7700, 77, 7)$	$(1, X^3 - 20X - 30)$	3
$(8092, 7, 1)$	$(1, X^3 - X^2 - 28X - 46)$	6
$(8505, 105, 3)$	$(1, X^3 - 27X - 51)$	3
$(8505, 105, 7)$	$(1, X^3 - 27X - 51)$	$(1, 2)$
$(9045, 1005, 67)$	$(1, X^3 - 18X - 23)$	4
$(10164, 21, 3)$	$(2, X^3 + X^2 - 29X - 57)$	3
$(10580, 5, 1)$	$(1, X^3 + X^2 - 15X - 17)$	9
$(10580, 5, 2)$	$(1, X^3 + X^2 - 15X - 17)$	9
$(11109, 21, 3)$	$(1, X^3 - X^2 - 15X - 6)$	4
$(12177, 1353, 11)$	$(1, X^3 - 15X - 7)$	3
$(12852, 357, 7)$	$(2, X^3 - 24X - 12)$	3
$(13932, 43, 1)$	$(2, X^3 - 39X - 82)$	2
$(14036, 29, 2)$	$(2, X^3 - X^2 - 29X - 31)$	12
$(14520, 30, 2)$	$(3, X^3 - 33X - 22)$	9
$(14520, 30, 3)$	$(3, X^3 - 33X - 22)$	$(1, 2)$

two rational primes which are unramified in $\mathbf{M}/\mathbf{Q}$, *inert in* $\mathbf{L}/\mathbf{Q}$ *and ramified in* $\mathbf{N}^+/\mathbf{L}$, *then* p *divides* $h_{\mathbf{N}}^-$.

Examples. Let us explain why some of the relative class numbers of the table are divisible by 3. First, take $d_{\mathbf{K}} = 1300$ and $\mathbf{M} = \mathbf{Q}(\sqrt{-1}, \sqrt{-13})$. The table yields $h_{\mathbf{N}}^- = 3^2$. Since $l = 5$ is unramified in $\mathbf{M}/\mathbf{Q}$, inert in $\mathbf{L}/\mathbf{Q}$ and ramified in $\mathbf{N}^+/\mathbf{L}$, we understand why 3 divides $h_{\mathbf{N}}^-$. Second, take $d_{\mathbf{K}} = 1620$ and $\mathbf{M} = \mathbf{Q}(\sqrt{-3}, \sqrt{-15})$. The table yields $h_{\mathbf{N}}^- = 1$. Here $l = 2$ is unramified in $\mathbf{M}/\mathbf{Q}$, inert in $\mathbf{L}/\mathbf{Q}$ and ramified in $\mathbf{N}^+/\mathbf{L}$. But since $w_{\mathbf{M}} = 6$, then Proposition 8 does not yield that 3 divides $h_{\mathbf{N}}^-$ and we do not meet with any contradiction.

References

[BP] E. Brown and C.J. Parry. The imaginary bicyclic biquadratic fields with class number 1. *J. Reine Angew. Math.* **266** (1974), 118-120. MR **49:**4974

[BWW] D.A. Buell, H.C. Williams and K.S. Williams. On the imaginary bicyclic biquadratic fields with class number 2. *Math. Comp.* **31** (1977), 1034-1042. MR **56:**305

[Coh] H. Cohen. *A course in computational algebraic number theory.* Springer-Verlag, Grad. Texts Math. **138**, 1993. MR **94i:**11105

[Has] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper.* Akademie-Verlag, Berlin 1952. MR **14:**141a

[Hof] J. Hoffstein. Some analytic bounds for zeta functions and class numbers. *Inventiones Math.* **55** (1979), 37-47. MR **80k:**12019

[Hor] K. Horie. On a ratio between relative class number. *Math. Z.* **211** (1992), 505-521. MR **94a:**11171

[JY] C.U. Jensen and N. Yui. Polynomials with D_p as Galois group. *J. Number Th.* **15** (1982), 347-375. MR **84g:**12011

[Lou 1] S. Louboutin. Continued fractions and real quadratic fields. *J. Number Theory* **30** (1988), 167-176. MR **90a:**11119

[Lou 2] S. Louboutin. Norme relative de l'unité fondamentale et 2-rang du groupe des classes d'idéaux de certains corps biquadratiques. *Acta Arith.* **58** (1991), 273-288. MR **93a:**11090

[Lou 3] S. Louboutin. Calcul des nombres de classes relatifs de certains corps de classes de Hilbert. *C. R. Acad. Sci. Paris Sér. I Math.* **319** I (1994), 321-325. MR **95g:**11111

[Lou 4] S. Louboutin. Calcul du nombre de classes des corps de nombres. *Pacific J. Math.* **17** (1995), 455-467. MR **97a:**11176

[Lou 5] S. Louboutin. Lower bounds for relative class numbers of CM-fields. *Proc. Amer. Math. Soc.* **120** (1994), 425-434. MR **94d:**11089

[Lou 6] S. Louboutin. Majorations explicites du résidu au point 1 des fonctions zêta des corps de nombres. to appear in the *Journal of the Mathematical Society of Japan.*

[Lou 7] S. Louboutin. Determination of all quaternion octic CM-fields with class number 2. *J. London Math. Soc.* (2) 54 (1996), 227–238. CMP 96:17.

[Lou-Oka] 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. MR **95g:**11107

[Mar] J. Martinet. Sur l'arithmétique des extensions galoisiennes à groupe de galois diédral d'ordre $2p$. *Ann. Inst. Fourier, Grenoble* **19** (1969), 1-80. MR **41:**6820

[MW] H.L. Montgomery and P.J. Weinberger. Notes on small class number. *Acta Arith.* **24** (1974), 529-542. MR **50:**9841

[Odl] A.M. Odlyzko. Some analytic estimates of class numbers and discriminants. *Inventiones Math.* **29** (1975), 279-286. MR **51:**12788

[Ol] M. Olivier. Table des corps cubiques réels de discriminant inférieur à 50000, avec base d'entiers, nombre de classes, régulateur et unités fondamentales. (January 1992), private communication.

[Set] B. Setzer. The determination of all imaginary quartic abelian number fields with class number 1. *Math. Comp.* **35** (1980), 1383-1386. MR **81k:**12005

[Sta 1] H.M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.* **14** (1967), 1-27. MR **36:**5102

[Sta 2] H.M. Stark. On complex quadratic fields with class-number two. *Math. Comp.* **29** (1975), 289-302. MR **51:**5548

[Sta 3] H.M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.* **23** (1974), 135-152. MR **49:**7218

[Sun] J.S. Sunley. Class numbers of totally imaginary quadratic extensions of totally real fields. *Trans. Amer. Math. Soc.* **175** (1973), 209-232. MR **47:**184

[Wa] L.C. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, Grad.Texts Math. **83**, 1982. MR **85g:**11001

[Yam] K. Yamamura. The determination of the imaginary abelian number fields with class-number one. *Math. Comp.* **62** (1994), 899-921. MR **94g:**11096

Université de Caen, UFR Sciences, Département de Mathématiques, Esplanade de la paix, 14032 Caen Cedex, France

E-mail address: `louboutî@math.unicaen.fr`

Doshisha University, Department of Mathematics, Tanabe, Kyoto, 610-03, Japan

E-mail address: `rokazaki@doshisha.ac.jp`

Laboratoire A2X, UMR 99 36, Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France

E-mail address: `olivier@math.u-bordeaux.fr`