COLLOQUIUM MATHEMATICUM

VOL. 80 1999 NO. 2

THE CLASS NUMBER ONE PROBLEM FOR THE DIHEDRAL AND DICYCLIC CM-FIELDS

BY

STÉPHANE LOUBOUTIN (CAEN)

Abstract. We recall the determination of all the dihedral CM-fields with relative class number one, and prove that dicyclic CM-fields have relative class numbers greater than one.

1. Introduction. Whenever $\mathbf{N}$ is a CM-field, we let $\mathbf{N}^+$ and $h_{\mathbf{N}}^-$ denote its maximal totally real subfield and its relative class number (see [Wa, Chapter 4]). A. Odlyzko [Odl] proved that there are only finitely many normal CM-fields with class number one, and J. Hoffstein [Hof] made this result more precise by proving that the degree of a normal CM-field with class number one is less than 436. (Note that K. Yamamura [Yam] solved the class number one problem for the abelian CM-fields.)

The aim of this paper is to provide the reader with the determination of all the non-abelian normal CM-fields with Galois group isomorphic either to any dihedral group (which we call a *dihedral CM-field*) or any dicyclic group (which we call a *dicyclic CM-field*) which have class number one.

Let us first recall the definition of these two non-abelian groups: the *dihedral group* of order $2m > 4$ is

$$D_{2m} = \langle a, b : a^m = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle,$$

for which $(a^i b)^2 = 1$, and the *dicyclic group* of order $4n > 4$ is

$$Q_{4n} = \langle a, b : a^{2n} = 1, a^n = b^2, b^{-1}ab = a^{-1}\rangle,$$

for which $(a^i b)^2 = a^n$. Since the centre $Z(D_{2m})$ of a dihedral group of order $2m$ with m odd is trivial, the degree of a dihedral CM-field must be divisible by 4 (Proposition 2(i)) and its Galois group will be denoted by D_{4n}. Since $Z(D_{4n}) = Z(Q_{4n}) = \{1, a^n\}$ and since both the quotient groups $D_{4n}/Z(D_{4n})$ and $Q_{4n}/Z(Q_{4n})$ are isomorphic to D_{2n}, the dihedral group of order $2n$, for any dihedral or dicyclic CM-field $\mathbf{N}$ of degree $4n$ its maximal totally real subfield $\mathbf{N}^+$ is normal with Galois group D_{2n}.

1991 *Mathematics Subject Classification*: Primary 11R29, 11R21.

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

The determination of all the dihedral CM-fields with relative class number and class number one has just been completed by a student of ours, Y. Lefeuvre, and his determination stems from the previous determination in [LO2] of all the dihedral CM-fields of 2-power degrees with relative class number one. Let us gather up all these results in the following Theorem:

THEOREM 1. (i) (see [LO2]) *There are* 24 *dihedral CM-fields of* 2*-power degrees* $4n = 2^r \geq 8$ *with relative class number one. More precisely*,

• *There are* 19 *dihedral CM-fields of degree* 8 *with relative class number one*: *the narrow Hilbert* 2*-class fields of the* 19 *real quadratic number fields* $\mathbb{Q}(\sqrt{pq})$ *with* $pq \in \{2\cdot 17, 2\cdot 73, 2\cdot 89, 2\cdot 233, 2\cdot 281, 5\cdot 41, 5\cdot 61, 5\cdot 109, 5\cdot 149, 5\cdot 269, 5\cdot 389, 13\cdot 17, 13\cdot 29, 13\cdot 157, 13\cdot 181, 17\cdot 137, 17\cdot 257, 29\cdot 53, 73\cdot 97\}$. *Moreover*, *the narrow Hilbert* 2*-class fields of* $\mathbb{Q}(\sqrt{5\cdot 269})$ *and* $\mathbb{Q}(\sqrt{17\cdot 257})$ *have class number* 3, *and the* 17 *remaining narrow Hilbert* 2*-class fields have class number one.*

• *There are* 5 *dihedral CM-fields of degree* 16 *with relative class number one*: *the narrow Hilbert* 2*-class fields of the* 5 *real quadratic number fields* $\mathbb{Q}(\sqrt{pq})$ *with* $pq \in \{2\cdot 257, 5\cdot 101, 5\cdot 181, 13\cdot 53, 13\cdot 61\}$. *Moreover*, *the narrow Hilbert* 2*-class field of* $\mathbb{Q}(\sqrt{2\cdot 257})$ *has class number* 3, *and the* 4 *remaining narrow Hilbert* 2*-class fields have class number one.*

• *Dihedral CM-fields of degree* $2^r > 16$ *have relative class numbers greater than one.*

(ii) (see [LOO]) *There are* 16 *non-abelian normal CM-fields of degree* 12 *with relative class number one. Moreover*, *nine of these fields have class number one.*

(iii) (see [Lef] and [LL]) *There are only* 2 *dihedral CM-fields of degree* $4p \geq 20$, $p \geq 5$ *a prime*, *with relative class number one. Only one of these has class number one. There is only one dihedral CM-field of degree* $2^r p$, $r \geq 3$, *with relative class number one*, *namely the narrow Hilbert class field of the real quadratic field* $\mathbb{Q}(\sqrt{5\cdot 269})$, *and it has degree* 24 *and class number one.*

(iv) *Apart from these* $43 = 19 + 5 + 16 + 2 + 1$ *fields* (*respectively*, *these* $32 = 17 + 4 + 9 + 1 + 1$ *fields*), *there is no other dihedral CM-field of degree* $4n > 4$ *with relative class number one* (*respectively*, *with class number one*).

2. Prerequisites. Let p be an odd prime. *A pure real dihedral field* is a normal field $\mathbf{F}$ of degree $2p$ and Galois group D_{2p} such that p is totally ramified in $\mathbf{F}/\mathbb{Q}$ and such that p is the only rational prime which is ramified in $\mathbf{F}/\mathbb{Q}$. Note that we must have $p \equiv 1 \pmod 4$ and $\mathbb{Q}(\sqrt{p})$ must be the quadratic subfield of $\mathbf{F}$.

We now collect known results we will use to prove that there is no dicyclic CM-field with relative class number one:

PROPOSITION 2. (i) (see [LOO, Lemma 2]) *Let* $\mathbf{N}$ *be a normal CM-field with Galois group* $\mathbf{G}$. *Then the complex conjugation is in the centre* $Z(\mathbf{G})$ *of* $\mathbf{G}$ (*and* $\mathbf{N}^+/\mathbb{Q}$ *is therefore normal*).

(ii) (see [LOO, Th. 5]) *Let* $\mathbf{k} \subseteq \mathbf{K}$ *be two CM-fields. If the degree* $[\mathbf{K} : \mathbf{k}]$ *of the extension* $\mathbf{K}/\mathbf{k}$ *is odd*, *then* $h_{\mathbf{k}}^-$ *divides* $h_{\mathbf{K}}^-$.

(iii) (see [LO1]) *If* t *prime ideals of* $\mathbf{N}$ *are ramified in the quadratic extension* $\mathbf{N}/\mathbf{N}^+$ *then* 2^{t-1} *divides* $h_{\mathbf{N}}^-$.

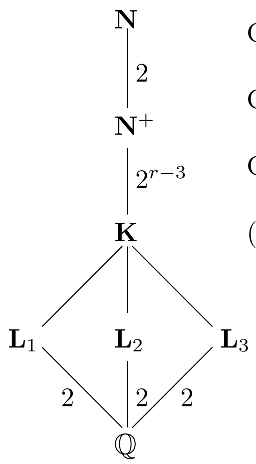
(iv) (see [LOO, Prop. 8]) *Let* p *be any odd prime and* $\mathbf{N}/\mathbf{M}$ *be a cyclic extension of degree* p *of CM-fields. Assume that* $\mathbf{N}^+/\mathbf{M}^+$ *is a cyclic extension of degree* p. *Let* T *be the number of prime ideals of* $\mathbf{M}^+$ *which split in* $\mathbf{M}/\mathbf{M}^+$ *and are ramified in* $\mathbf{N}^+/\mathbf{M}^+$. *Then* $p^{T-1}h_{\mathbf{M}}^-$ *divides* $h_{\mathbf{N}}^-$.

(v) (see [LOO, Prop. 9]) *Let* $p \equiv 1 \pmod 4$ *be a prime and let* $\varepsilon_p = (u_p + v_p\sqrt{p})/2 > 1$ *be the fundamental unit of* $\mathbb{Q}(\sqrt{p})$. *If* p *does not divide* v_p, *then there does not exist any pure real dihedral number field* $\mathbf{F}$ *of degree* $2p$.

(vi) (see [Mar]) *Let* $\mathbf{F}$ *be a dihedral field of degree* $2p$. *Let* $\mathbf{L}$ *denote its quadratic subfield*, *let* $\chi_{\mathbf{L}}$ *denote the primitive quadratic Dirichlet character associated with* $\mathbf{L}$ *and let* q *denote a rational prime. If* q *is ramified in* $\mathbf{L}/\mathbb{Q}$, *say* $(q) = \mathcal{Q}^2$ *in* $\mathbf{L}$, *then either* $\mathcal{Q}$ *splits completely in* $\mathbf{F}/\mathbf{L}$ *or* $\mathcal{Q}$ *is totally ramified in* $\mathbf{F}/\mathbf{L}$. *In the latter case*, $q = p$. *Moreover*, *if the prime ideals of* $\mathbf{L}$ *above a rational prime* q *different from* p (1) *are ramified in* $\mathbf{F}/\mathbf{L}$ *then* $q \equiv \chi_{\mathbf{L}}(q) \pmod p$.

3. Relative class numbers of dicyclic CM-fields

Diagram 1



$\mathrm{Gal}(\mathbf{N}/\mathbb{Q}) = Q_{2^r}$

$\mathrm{Gal}(\mathbf{N}/\mathbf{K}) = C_{2^{r-2}}$

$\mathrm{Gal}(\mathbf{K}/\mathbb{Q}) = C_2^2$

(where C_m denotes a cyclic group of order m)

(1) Note that we forgot to mention this restriction in [LOO, Lemma 4(ii)].

THEOREM 3. *Let* $\mathbf{N}$ *be a dicyclic CM-field of degree* $4n = 2^r \geq 8$. *Then at least two distinct rational primes are ramified in* $\mathbf{N}/\mathbf{N}^+$. *Hence,* $h_{\mathbf{N}}^-$ *is even* (use Proposition 2(iii)).

Proof. Let $\mathbf{K}$ denote the subfield of $\mathbf{N}$ fixed by the cyclic subgroup $\mathbf{H} = \langle a^2\rangle$ of $\mathbf{G} = \mathrm{Gal}(\mathbf{N}/\mathbb{Q}) = Q_{2^r} = \langle a, b : a^{2^{r-1}} = 1,\ a^{2^{r-2}} = b^2,\ b^{-1}ab = a^{-1}\rangle$ (see the incomplete lattice of subfields in Diagram 1). Since $\mathrm{Gal}(\mathbf{N}/\mathbf{N}^+) = \{1, a^{2^{r-2}}\} = Z(\mathbf{G})$ is the only subgroup of order two of $\mathbf{G}$, any non-trivial subgroup of $\mathbf{G}$ contains $\mathrm{Gal}(\mathbf{N}/\mathbf{N}^+)$. Therefore, using inertia groups, we find that if a rational prime p is ramified in $\mathbf{N}/\mathbb{Q}$ then all the prime ideals of $\mathbf{N}^+$ above p are ramified in $\mathbf{N}/\mathbf{N}^+$. Since $\mathbf{K}$ is a real biquadratic bicyclic field, at least two distinct rational primes are ramified in $\mathbf{K}/\mathbb{Q}$, and hence at least two distinct prime ideals of $\mathbf{N}^+$ are ramified in $\mathbf{N}/\mathbf{N}^+$. ■

COROLLARY 4 (Use Theorem 3 and Proposition 2(ii)). *If* $\mathbf{N}$ *is a normal CM-field of degree* 24 *with Galois group isomorphic either to* $Q_8 \times C_3$ *or to* Q_{24}, *then* $h_{\mathbf{N}}^-$ *is always even.*

The following result is more general than [LOO, Th. 6] and its statement and proof correct several slight mistakes made in [LOO, p. 3663]:

THEOREM 5. *Let* p *be an odd prime and let* $\mathbf{N} = \mathbf{FM}$ *denote a non-abelian normal CM-field of degree* $2^r p$, $r \geq 2$, *which is a compositum of a real dihedral field* $\mathbf{F}$ *of degree* $2p$ *and of an imaginary cyclic field* $\mathbf{M}$ *of degree* $2^r \geq 4$ *and conductor* $f_{\mathbf{M}}$, *both* $\mathbf{F}$ *and* $\mathbf{M}$ *having the same real quadratic subfield* $\mathbf{L}$ (see the incomplete lattice of subfields in Diagram 2).

(i) *If* 2^{p-1} *does not divide* $h_{\mathbf{N}}^-$ *then* $p \equiv 1 \pmod 4$, $\mathbf{L} = \mathbb{Q}(\sqrt{p})$ *and* p *is totally ramified in* $\mathbf{F}/\mathbb{Q}$ (2).

(ii) *If* $h_{\mathbf{N}}^-$ *is odd then* $f_{\mathbf{M}} = p$. *Hence,* $p \equiv 1 + 2^r \pmod{2^{r+1}} \equiv 1 \pmod 4$.

(iii) *If* $f_{\mathbf{M}} = p$ *and if* $p \equiv 1 \pmod 4$, *then any rational prime* $q \neq p$ *which is ramified in* $\mathbf{F}/\mathbf{L}$ *satisfies* $q \equiv 1 \pmod p$ *and splits completely in* $\mathbf{M}/\mathbb{Q}$.

(iv) *If* $h_{\mathbf{N}}^- = 1$ *then* $\mathbf{F}$ *is a pure real dihedral field of degree* $2p$ *and* $p \in \{5, 13, 17, 29, 37, 41, 53, 61\}$ (3).

(v) *We always have* $h_{\mathbf{N}}^- > 1$.

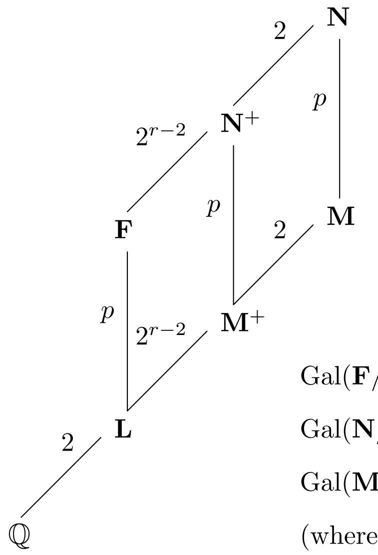
Proof. (i) If $p \equiv 1 \pmod 4$ and $\mathbf{L} \neq \mathbb{Q}(\sqrt{p})$, or if $p \not\equiv 1 \pmod 4$ and $\mathbf{L} = \mathbb{Q}(\sqrt{p})$, then there exists a prime q different from p which is ramified in $\mathbf{L}/\mathbb{Q}$, say $(q) = \mathcal{Q}^2$ in $\mathbf{L}$. According to Proposition 2(vi), this ideal $\mathcal{Q}$ splits completely in $\mathbf{F}/\mathbf{L}$. Since $\mathbf{M}/\mathbb{Q}$ is cyclic of 2-power degree, q is totally ramified in $\mathbf{M}/\mathbb{Q}$. Therefore, there are at least p prime ideals of $\mathbf{N}^+ = \mathbf{FM}^+$

(2) Note that [LOO, Th. 6(i)] should have been so stated, and our proof of [LOO, Th. 6(i)] was incorrect.

(3) Note that the possibility $p = 61$ for which $\mathbf{M}$ is cyclic quartic was not taken care of in [LOO, Th. 6(iii)].

above q and they are all ramified in the quadratic extension $\mathbf{N}/\mathbf{N}^+$, and according to Proposition 2(iii), we find that 2^{p-1} divides $h^-_{\mathbf{N}}$.

Diagram 2



$\mathrm{Gal}(\mathbf{F}/\mathbb{Q}) = D_{2p}$

$\mathrm{Gal}(\mathbf{N}/\mathbf{F}) = C_{2^r}$

$\mathrm{Gal}(\mathbf{M}/\mathbb{Q}) = C_{2^r}$

(where C_m denotes a cyclic group of order m)

(ii) If $h^-_{\mathbf{N}}$ is odd then $h^-_{\mathbf{M}}$ is odd (Proposition 2(ii)) and at most one prime ideal of $\mathbf{M}^+$ is ramified in $\mathbf{M}/\mathbf{M}^+$ (Proposition 2(iii)). Since $\mathbf{M}/\mathbb{Q}$ is cyclic of 2-power degree, at most one rational prime q is ramified in $\mathbf{M}/\mathbb{Q}$, hence $f_{\mathbf{M}} = q$ and according to the previous point, $q = p$.

(iii) According to Proposition 2(vi), we have $q \equiv \chi_{\mathbf{L}}(q) \pmod p$. Since our assumptions yield $\mathbf{L} = \mathbb{Q}(\sqrt{p})$ we have $\chi_{\mathbf{L}}(q) = \left(\frac{q}{p}\right) = \left(\frac{\pm 1}{p}\right) = +1$ and so $q \equiv 1 \pmod p$. Since $\mathbf{M}$ is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$ and since $q \equiv 1 \pmod p$ implies that q splits completely in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, it follows that q splits completely in $\mathbf{M}/\mathbb{Q}$.

(iv) According to points (ii) and (iii) and to Proposition 2(iv), if $\mathbf{F}$ were not a pure real dihedral field then p^{T-1} with $T \geq [\mathbf{M}^+ : \mathbb{Q}] = 2^{r-1} \geq 2$ would divide $h^-_{\mathbf{N}}$. Now, according to Proposition 2(ii), if $h^-_{\mathbf{N}} = 1$ then $h^-_{\mathbf{M}} = 1$. But according to [Lou2] we have $h^-_{\mathbf{M}} = 1$ if and only if $f_{\mathbf{M}} \in \{16, 32, 5, 13, 17, 29, 37, 41, 53, 61\}$.

(v) According to Proposition 2(v), there does not exist any pure real dihedral field of degree $2p$ with $p \in \{5, 13, 17, 29, 37, 41, 53, 61\}$. ∎

Corollary 6. *The relative class numbers of dicyclic CM-fields of degree* $4p$ (*p any odd prime*) *are greater than one*, *as are the relative class numbers of non-abelian normal CM-fields of degree* 24 *with Galois group* $C_3 \rtimes C_8 = \langle a, b : a^3 = b^8 = 1,\ b^{-1}ab = a^{-1} \rangle$.

THEOREM 7. *Let* $\mathbf{N}$ *be a dicyclic CM-field of degree* $4n > 4$. *If* n *is even then* $h_{\mathbf{N}}^-$ *is even and if* n *is odd then* $h_{\mathbf{N}}^- > 1$.

Proof. Assume that n is even, write $4n = 2^r f$ with $f \geq 1$ odd and $r \geq 3$, and let $\mathbf{M}$ be the subfield of $\mathbf{N}$ fixed by the cyclic group $\langle a^{2n/f} \rangle$ of order f. Then $\mathbf{M}$ is a normal CM-subfield of $\mathbf{N}$. Since $[\mathbf{N} : \mathbf{M}] = f$ is odd, $h_{\mathbf{M}}^-$ divides $h_{\mathbf{N}}^-$ (Proposition 2(ii)) and since $\mathbf{M}$ is a normal dicyclic CM-field of degree $2^r \geq 8$, we see that $h_{\mathbf{M}}^-$ is even (Theorem 3).

Now, assume that m is odd, let p denote any prime divisor of m, write $4m = 4pf$ with $f \geq 1$ odd and let $\mathbf{M}$ be the subfield of $\mathbf{N}$ fixed by the cyclic group $\langle a^{2n/f} \rangle$ of order f. Then $\mathbf{M}$ is a normal CM-subfield of $\mathbf{N}$ and $[\mathbf{N} : \mathbf{M}] = f$ is odd. Hence, $h_{\mathbf{M}}^-$ divides $h_{\mathbf{N}}^-$ and since $\mathbf{M}$ is a normal dicyclic CM-field of degree $4p$, we have $h_{\mathbf{M}}^- > 1$ (Corollary 6). ■

4. Remarks. There are 12 non-abelian groups of order 24, and 11 out of them have an element of order two in their centre (those different from the symmetric group S_4) and we have proved that any normal CM-field of degree 24 with Galois groups isomorphic to three out of these 11 groups, namely the groups $C_3 \rtimes C_8$, $C_3 \times Q_8$ and Q_{24}, has relative class number greater than one. Since we have also noticed that the relative class number one problem is solved for the dihedral CM-fields of degree 24, there remain seven Galois groups to look at. In this respect, we refer the reader to [LLO] for the determination of all the normal CM-fields of degree 24 with Galois groups $\mathrm{SL}_2(F_3)$ and $A_4 \times C_2$ with class number one.

REFERENCES

[Hof] J. Hoffstein, *Some analytic bounds for zeta functions and class numbers*, Invent. Math. 55 (1979), 37–47.

[Lef] Y. Lefeuvre, *Corps diédraux à multiplication complexe principaux*, preprint, Univ. Caen, 1998.

[LL] Y. Lefeuvre and S. Louboutin, *The class number one problem for the dihedral CM-fields*, in: Proc. Conf. on Algebraic Number Theory and Diophantine Analysis, Graz, August–September 1998, to appear.

[LLO] F. Lemmermeyer, S. Louboutin and R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of degree 24*, J. Théor. Nombres Bordeaux, to appear.

[Lou1] S. Louboutin, *Determination of all quaternion octic CM-fields with class number 2*, J. London Math. Soc. 54 (1996), 227–238.

[Lou2] —, *CM-fields with cyclic ideal class groups of* 2*-power orders*, J. Number Theory 67 (1997), 1–10.

[LO1] 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.

[LO2] S. Louboutin and R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of 2-power degrees*, Proc. London Math. Soc. (3) 76 (1998), 523–548.

[LOO] S. Louboutin, R. Okazaki and M. Olivier, *The class number one problem for some non-abelian normal CM-fields*, Trans. Amer. Math. Soc. 349 (1997), 3657–3678.

[Mar] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier (Grenoble) 19 (1969), no. 1, 1–80.

[Odl] A. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. 29 (1975), 275–286.

[TW] A. D. Thomas and G. V. Wood, *Group Tables*, Shiva Publ. Kent, 1980.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1982; 2nd ed., 1997.

[Yam] K. Yamamura, *The determination of the imaginary abelian number fields with class-number one*, Math. Comp. 206 (1994), 899–921.

Département de Mathématiques
Université de Caen, Campus 2
BP 5186
14032 Caen Cedex, France
E-mail: loubouti@math.unicaen.fr

Received 14 December 1998