ACTA ARITHMETICA
LXXXIX.3 (1999)

Construction of the real dihedral number fields of degree $2p$. Applications

by

Stéphane Louboutin (Caen), Young-Ho Park (Seoul)
and Yann Lefeuvre (Caen)

1. Introduction. We use class field theory to construct the real dihedral fields. This construction is reduced to that of primitive characters on the ring class groups of real quadratic fields which are then used to compute the relative class numbers of dihedral CM-fields of degree $4p$, p any odd prime.

We first fix some notation. Let K be a normal real number field (considered as a subfield of the field of complex numbers) of degree $2n$ with Galois group $D_{2n} = \langle a, b : a^n = b^2 = 1,\ bab^{-1} = a^{-1}\rangle$, the dihedral group of order $2n$. Let L denote the real quadratic subfield of K fixed by the cyclic subgroup of order n generated by a, and let E denote any one of the n non-normal subfields of degree n of K fixed by the n non-normal subgroups of order two $\{1, a^k b\}$ of G, $0 \le k \le n-1$. We let A_L, d_L, $\varepsilon_L > 1$ and χ_L denote the ring of algebraic integers, the discriminant, the fundamental unit and the primitive quadratic character modulo d_L associated with L, respectively. In order to use continued fraction expansions to compute ε_L, we specify a generator of A_L: let g_L denote the unique rational integer with the same parity as d_L such that $\sqrt{d_L} - 2 < g_L < \sqrt{d_L}$ and set $\omega_L = (g_L + \sqrt{d_L})/2$, whose continued fraction expansion is purely periodic. Finally, d_F denotes the absolute value of the discriminant of a number field F.

Let $\mathcal{M}$ be an integral ideal of L, let $I_L(\mathcal{M})$ denote the subgroup of the group I_L of fractional ideals of L generated by the integral ideals relatively prime to $\mathcal{M}$, and let $P_L(\mathcal{M})$ denote the subgroup of $I_L(\mathcal{M})$ generated by

1991 *Mathematics Subject Classification*: Primary 11R29, 11R21, 11Y35.

Key words and phrases: dihedral field, dihedral group, CM-field.

This paper was written while the second author was visiting Caen University and he was supported by grants from the Embassy of France in Korea and from the Korean Research Foundation.

the principal ideals of the form (α) where $\alpha \in A_L$ satisfies $\alpha \equiv 1 \pmod{\mathcal{M}}$. The *ray class group* for the modulus $\mathcal{M}$ is the quotient group $Cl_L(\mathcal{M}) = I_L(\mathcal{M})/P_L(\mathcal{M})$. According to class field theory, for any abelian extension K/L of conductor dividing $\mathcal{M}$ the kernel $H = \ker \Phi_{K/L}$ of the surjective Artin map $\Phi_{K/L} : I_L(\mathcal{M}) \to \mathrm{Gal}(K/L)$ is a congruence subgroup for the modulus $\mathcal{M}$, that is, $P_L(\mathcal{M}) \subseteq H \subseteq I_L(\mathcal{M})$. Conversely, according to the Existence Theorem of class field theory, for any congruence subgroup H for the modulus $\mathcal{M}$ there exists a unique abelian extension K/L, all whose ramified primes are finite and divide $\mathcal{M}$, such that $H = \ker \Phi_{K/L}$. This field K is called the *class field* of L for the congruence subgroup H. Of particular importance is the case where $H = P_{L,\mathbb{Z}}(\mathcal{M})$ is the group generated by the principal ideals of the form (α) where $\alpha \in A_L$ satisfies $\alpha \equiv a \pmod{\mathcal{M}}$ for some integer a relatively prime to $\mathcal{M}$, in which case Existence Theorem provides us with the so-called *ring class field* $H_L(\mathcal{M})$ of L for the modulus $\mathcal{M}$. Let $Cl_{L,\mathbb{Z}}(\mathcal{M})$, the *ring class group* for the modulus $\mathcal{M}$, be the quotient group $Cl_{L,\mathbb{Z}}(\mathcal{M}) = I_L(\mathcal{M})/P_{L,\mathbb{Z}}(\mathcal{M})$.

2. Real dihedral fields and ring class fields

PROPOSITION 1. *Let L be a real quadratic field. If K is a real dihedral field of degree $2n$ cyclic over L, then the conductor $\mathcal{F}_{K/L}$ of the cyclic extension K/L is invariant under the action of* $\mathrm{Gal}(L/\mathbb{Q})$ *and* $\ker \Phi_{K/L}$ *is a subgroup of $I_L(\mathcal{F}_{K/L})$ containing $P_{L,\mathbb{Z}}(\mathcal{F}_{K/L})$ such that the quotient group $I_L(\mathcal{F}_{K/L})/\ker \Phi_{K/L}$ is cyclic of order n. Conversely, if the modulus $\mathcal{F}$ is invariant under the action of* $\mathrm{Gal}(L/\mathbb{Q})$ *and if H is a congruence subgroup of $I_L(\mathcal{F})$ containing $P_{L,\mathbb{Z}}(\mathcal{F})$ such that the quotient group $I_L(\mathcal{F})/H$ is cyclic of order n, then its associated class field K is a real dihedral field of degree $2n$ and the conductor $\mathcal{F}_{K/L}$ of the extension K/L divides $\mathcal{F}$.*

Proof. For any prime ideal $\mathcal{Q}_F$ of a normal field F which is unramified in $F/\mathbb{Q}$ we let $[F/\mathbb{Q}, \mathcal{Q}_F]$ denote the Frobenius automorphism of $\mathcal{Q}_F$ (see [Jan]). Assume that K is dihedral and let q be a rational prime not in $\mathcal{F}_{K/L}$. We must prove that $\Phi_{K/L}((q)) = 1$. First, if $(q) = \mathcal{Q}_L^2$ is ramified in L then $(\Phi_{K/L}(\mathcal{Q}_L))^{-1} = b\Phi_{K/L}(\mathcal{Q}_L)b^{-1} = \Phi_{K/L}(b(\mathcal{Q}_L)) = \Phi_{K/L}(\mathcal{Q}_L)$ and $\Phi_{K/L}((q)) = \Phi_{K/L}(\mathcal{Q}_L)\Phi_{K/L}(\mathcal{Q}_L) = \Phi_{K/L}(\mathcal{Q}_L)(\Phi_{K/L}(\mathcal{Q}_L))^{-1} = 1$. Second, if $(q) = \mathcal{Q}_L\mathcal{Q}_L'$ splits in L then since the restriction of b to L is non-trivial we get $(\Phi_{K/L}(\mathcal{Q}_L))^{-1} = b\Phi_{K/L}(\mathcal{Q}_L)b^{-1} = \Phi_{K/L}(b(\mathcal{Q}_L)) = \Phi_{K/L}(\mathcal{Q}_L')$ and we get $\Phi_{K/L}((q)) = \Phi_{K/L}(\mathcal{Q}_L)\Phi_{K/L}(\mathcal{Q}_L') = \Phi_{K/L}(\mathcal{Q}_L)(\Phi_{K/L}(\mathcal{Q}_L))^{-1} = 1$. Finally, if $(q) = \mathcal{Q}_L$ is inert in L and if $\mathcal{Q}_K$ is any prime ideal of K lying above $\mathcal{Q}_L$, then $\Phi_{K/L}((q)) = \Phi_{K/L}(\mathcal{Q}_L) = [K/L, \mathcal{Q}_L] = [K/L, \mathcal{Q}_K] = [K/\mathbb{Q}, \mathcal{Q}_K]^2$ and since q is inert in L it follows that $[K/\mathbb{Q}, \mathcal{Q}_K] = a^k b$ is not in the cyclic group $\langle a \rangle = \mathrm{Gal}(K/L)$, which implies $[K/\mathbb{Q}, \mathcal{Q}_K]^2 = (a^k b)^2 = 1$ and $\Phi_{K/L}((q)) = 1$.

Conversely, the trickiest step for proving the last assertion is to prove that for any $\sigma \in \mathrm{Gal}(H_L(\mathcal{F})/\mathbb{Q})$ such that the restriction $\sigma_{/L}$ is not trivial we have $\sigma^2 = 1$ (the remainder of the proof being similar to that of [Cox, Lemma 9.3]). Set $H = H_L(\mathcal{F})$. To prove this assertion we use the Chebotarev Density Theorem (see [Jan, Theorem 10.4]) according to which $\sigma = [H/\mathbb{Q}, \mathcal{Q}_H]$ for some prime ideal $\mathcal{Q}_H$ of H unramified in $H/\mathbb{Q}$. Since $\sigma_{/L} = [H/\mathbb{Q}, \mathcal{Q}_H]_{/L} = [L/\mathbb{Q}, \mathcal{Q}_L]$ is not trivial (where $\mathcal{Q}_L = \mathcal{Q}_H \cap A_L$), $\mathcal{Q}_L = (q)$ is inert in L and we get $\sigma^2 = [H/\mathbb{Q}, \mathcal{Q}_H]^2 = [H/L, \mathcal{Q}_H] = [H/L, \mathcal{Q}_L] = [H/L, (q)] = \Phi_{H/L}((q)) = 1$ (for we have $(q) \in P_{L,\mathbb{Z}}(\mathcal{F}) = \ker \Phi_{H/L}$). ∎

If $\mathcal{M}'$ divides $\mathcal{M}$ then the canonical map $s : Cl_L(\mathcal{M}) \to Cl_L(\mathcal{M}')$ is surjective and any character χ' on $Cl_L(\mathcal{M}')$ may be construed as a character on $Cl_L(\mathcal{M})$. A character χ on a ray class group $Cl_L(\mathcal{M})$ is *primitive* if it is not induced by any character χ' on the ray class group $Cl_L(\mathcal{M}')$ for any proper divisor $\mathcal{M}'$ of $\mathcal{M}$. Noticing that there is a bijective correspondence between the characters of order n on an abelian group G and the subgroups H of index n of G such that the quotient group G/H is cyclic of order n, according to Proposition 1 and Galois and Class Field theories we obtain:

THEOREM 2. *Let $\mathcal{M}$ be a modulus of a real quadratic field L which is invariant under the action of* $\mathrm{Gal}(L/\mathbb{Q})$. *Then there is a bijective correspondence between the real dihedral fields K of degree $2n$ containing L and such that the conductor $\mathcal{F}_{K/L}$ of the extension K/L is equal to $\mathcal{M}$ and the groups of order n generated by the primitive characters of order n on $Cl_L(\mathcal{M})$ which are trivial on the image of $P_{L,\mathbb{Z}}(\mathcal{M})$ in this group.*

Let χ be a character on $Cl_{L,\mathbb{Z}}(\mathcal{M})$. Then $\alpha \mapsto \chi((\alpha))$ defines a character χ_0 on $(A_L/\mathcal{M})^*$ which is called the *modular character associated with* χ. Notice that this modular character must be trivial on ε_L and on the image of $\mathbb{Z}$ in $(A_L/\mathcal{M})^*$. If $\mathcal{M}'$ divides $\mathcal{M}$ then the canonical map $s : (A_L/\mathcal{M})^* \to (A_L/\mathcal{M}')^*$ is surjective and any modular character χ_0' on $(A_L/\mathcal{M}')^*$ may be construed as a modular character on $(A_L/\mathcal{M})^*$.

We say that a modular character χ_0 on $(A_L/\mathcal{M})^*$ is *primitive* if it is not induced by any modular character χ_0' on $(A_L/\mathcal{M}')^*$ for any proper divisor $\mathcal{M}'$ of $\mathcal{M}$. One can easily check that a modular character χ_0 on $(A_L/\mathcal{M})^*$ is primitive if and only if for any proper divisor $\mathcal{M}'$ of $\mathcal{M}$ there exists $\alpha \in A_L$ coprime with $\mathcal{M}$ such that $\alpha \equiv 1 \pmod{\mathcal{M}'}$ but $\chi_0(\alpha) \neq 1$. Moreover, if $\mathcal{M} = \prod \mathcal{Q}^{e_{\mathcal{Q}}}$ is the prime ideal factorization of $\mathcal{M}$, then according to the Chinese Remainder Theorem we may factorize χ_0 canonically as a product of modular characters $\chi_{\mathcal{Q}}$ on $(A_L/\mathcal{Q}^{e_{\mathcal{Q}}})^*$, and χ_0 is primitive if and only if each component $\chi_{\mathcal{Q}}$ is primitive. For the remainder of this paper we let χ, χ_0 and ϕ denote a character on $Cl_{L,\mathbb{Z}}(\mathcal{M})$, its associated modular character on

$(A_L/\mathcal{M})^*$ and any component of χ_0, respectively. Notice that χ is primitive if and only if χ_0 is primitive. In particular, we have

LEMMA 3. *If there exists a real dihedral field K of degree $2n$ cyclic over a real quadratic field L and such that the conductor of the extension K/L is equal to $\mathcal{F}$, then there exists a primitive modular character χ_0 of order dividing n on $(A_L/\mathcal{F})^*$ which is trivial on the ε_L and on the image $\operatorname{Im}\mathbb{Z}$ of $\mathbb{Z}$ in this group.*

THEOREM 4. *If K is a real dihedral field containing L then there exists a positive rational integer $f_{K/L}$ such that the conductor of the cyclic extension K/L is given by $\mathcal{F}_{K/L} = (f_{K/L})$.*

Proof. If $(q) = \mathcal{Q}^2$ is ramified in $L/\mathbb{Q}$ and ϕ is a character on $(A_L/\mathcal{Q}^{2f+1})^*$ which is trivial on $\operatorname{Im}\mathbb{Z}$ then ϕ is not primitive. Indeed, if $\alpha \equiv 1 \pmod{\mathcal{Q}^{2f}}$, then $\alpha = 1 + q^f\beta$ for some $\beta \in A_L$. Since the canonical map $\mathbb{Z}/q\mathbb{Z} \to A_L/\mathcal{Q}$ is bijective, there exists $a \in \mathbb{Z}$ such that $\beta \equiv a \pmod{\mathcal{Q}}$, which yields $\alpha \equiv 1 + q^f a \pmod{\mathcal{Q}^{2f+1}}$ and $\phi(\alpha) = \phi(1 + q^f a) = +1$ for ϕ is trivial on $\operatorname{Im}\mathbb{Z}$. Hence, according to Lemma 3, $\mathcal{F}_{K/L}$ is invariant under the action of $\operatorname{Gal}(L/\mathbb{Q})$ and the exponents in the prime ideal factorization of $\mathcal{F}_{K/L}$ of the prime ideals $\mathcal{Q}$ of L which are ramified in $L/\mathbb{Q}$ are even. ∎

3. Conductors of real dihedral fields of degree $2p^s$

LEMMA 5. *Let p be an odd prime. Let q be a prime. Set*

$$G_{q^e} = (A_L/(q^e))^*/\operatorname{Im}((\mathbb{Z}/q^e\mathbb{Z})^*)$$

and notice that the order of the group G_{q^e} is $q^{e-1}(q - \chi_L(q))$.

(i) *If $q \neq p$ and there exists a primitive character ϕ of order p^s on $(A_L/(q^e))^*$ which is trivial on the image of $(\mathbb{Z}/q^e\mathbb{Z})^*$ in this group then $e = 1$ and $q \equiv \chi_L(q) \pmod{p^s}$.*

(ii) *If there exists a primitive character ϕ of order p^s on $(A_L/(p^e))^*$ which is trivial on the image of $(\mathbb{Z}/p^e\mathbb{Z})^*$ in this group then $e \in \{s, s+1\}$. Moreover, if p does not divide d_L then $e = s+1$.*

(iii) (a) *If $p \geq 5$ divides d_L, then the group G_{p^e} of order p^e is cyclic and generated by $1 + \sqrt{d_L}$.*

(b) *If $d_L \equiv 3 \pmod 9$ then the group G_{3^e} of order 3^e is cyclic and generated by $1 + \sqrt{d_L}$.*

(c) *If $d_L \equiv 6 \pmod 9$ and $e \geq 2$ then the group G_{3^e} of order 3^e is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3^{e-1}\mathbb{Z})$ and generated by $1 + a_e\sqrt{d_L}$ of order 3 and $1 + 3\sqrt{d_L}$ of order 3^{e-1}. Here, a_e is any solution of the equation $a_e^2 d_L \equiv -3 \pmod{3^e}$. Hence, we may choose $a_2 = 1$.*

(iv) *If $p \geq 3$ divides d_L, then there exists a primitive character of order p^s on $(A_L/(p^e))^*$ which is trivial on the image of $\mathbb{Z}$ if and only if*

(a) $p \geq 5$ *and* $e = s$,
(b) $p = 3$, $d_L \equiv 3 \pmod 9$ *and* $e = s$,
(c) $p = 3$, $d_L \equiv 6 \pmod 9$, $s \geq 2$ *and* $e = s+1$,
(d) $p = 3$, $d_L \equiv 6 \pmod 9$, $s = 1$, *and* $e = 1$ *or* $e = 2$.

Proof. If p divides d_L, we let $\mathcal{P}$ denote the prime ideal of A_L above p. We let also $\nu_{\mathcal{P}}$ and ν_p denote the $\mathcal{P}$-adic and p-adic valuations on A_L and $\mathbb{Z}$, respectively.

(i) If $e > 1$ and $\alpha = 1 + q^{e-1}\beta \equiv 1 \pmod{(q^{e-1})}$ then $\alpha \equiv (1+\gamma q^{e-1})^{p^s} \pmod{(q^e)}$ for any γ satisfying $p^s\gamma \equiv \beta \pmod{(q)}$, which yields $\phi(\alpha) = +1$ and proves that ϕ is not primitive. Now, if there exists a primitive character ϕ of order p^s on $(A_L/(q))^*$ which is trivial on the image of $(\mathbb{Z}/q\mathbb{Z})^*$ then p^s divides the order $q - \chi_L(q)$ of G_q, which yields the desired second result.

(ii) If $e \geq s+2$ then for any $\alpha = 1 + p^{e-1}\beta \equiv 1 \pmod{(p^{e-1})}$ we have $\alpha \equiv (1 + \beta p^{e-s-1})^{p^s} \pmod{(p^e)}$ and $\phi(\alpha) = +1$. Therefore, ϕ is not primitive. Indeed, for $k \geq 2$ and $p \geq 3$ we have $k \geq 2 + \nu_p(k)$, and we obtain $\nu_p(C_{p^s}^k p^{k(e-s-1)}) = s - \nu_p(k) + k(e-s-1) = (k-1)(e-s) - k - \nu_p(k) + e \geq 2(k-1) - k - \nu_p(k) + e = k - 2\nu_p(k) - 2 + e \geq e$. Now, if there exists a primitive character ϕ of order p^s on $(A_L/(p^e))^*$ which is trivial on the image of $(\mathbb{Z}/p^e\mathbb{Z})^*$ then p^s divides the order $p^{e-1}(p - \chi_L(p))$ of G_{p^e}, which yields the desired second result.

(iii) (a) As $(1+\sqrt{d_L})^{p^k} \equiv 1 + p^k\sqrt{d_L} \pmod{(p^{k+1})}$, it follows that $1+\sqrt{d_L}$ has order p^e in the group G_{p^e} of order p^e.

(b) If $d_L \equiv 3 \pmod 9$ then $(1+\sqrt{d_L})^3 \equiv 1 + 6\sqrt{d_L} \pmod 9$. Hence $(1+\sqrt{d_L})^{3^k} \equiv 1 + 2\cdot 3^k\sqrt{d_L} \pmod{3^{k+1}}$ for $k \geq 1$, and $1+\sqrt{d_L}$ has order 3^e in G_{3^e}.

(c) Since $(1+3\sqrt{d_L})^{3^k} \equiv 1 + 3^{k+1}\sqrt{d_L} \pmod{(3^{k+2})}$ for $k \geq 0$, it follows that $1+3\sqrt{d_L}$ has order 3^{e-1} in G_{3^e}. Moreover, if $d_L \equiv 6 \pmod 9$ then there exists a_s such that $a_s^2 d_L \equiv -3 \pmod{3^{s+1}}$ and for such an a_s the element $1 + a_s\sqrt{d_L}$ has order three in G_{3^e} and does not lie in the cyclic subgroup generated by $1+3\sqrt{d_L}$. Hence, we get the desired result.

(iv) $\ker((A_L/\mathcal{P}^{2e})^* \to (A_L/\mathcal{P}^{2e-1})^*) = \{1 + p^{e-1}y\sqrt{d_L} : 0 \leq y \leq p-1\}$. According to the proof of the previous point, if $p \geq 5$, or if $p = 3$ and $d_L \equiv 3 \pmod 9$ then this kernel is the cyclic subgroup of order p generated by $(1+\sqrt{d_L})^{p^{e-1}}$. Hence, if there exists a primitive character ϕ of order p^s on $(A_L/(p^e))^*$ then $(\phi(1+\sqrt{d_L}))^{p^{e-1}} \neq 1$ and $s \geq e$, which according to (ii) yields $e = s$. If $p = 3$, $d_L \equiv 6 \pmod 9$ and $s \geq 2$ then according to (ii) and (iii) we have $s+1 \geq e \geq s \geq 2$ and $e - 1 \geq s$, and get $e = s+1$. The proof of the last point is easy. ∎

THEOREM 6 (see also [Has], [Mar], [Por]). *If K is a real dihedral field of degree $2p^s$ (p any odd prime) then $f_{K/L} = p^a \prod_{i=1}^r q_i$ where the q_i's are distinct primes $\neq p$ satisfying $q_i \equiv \chi_L(q_i) \pmod{p}$ and where $0 \le a \le s+1$. Moreover, if $s = 1$ then either $a = 0$ or*

$$a = \begin{cases} 2 & \text{if } p \text{ does not divide } d_L, \\ 1 & \text{if } p \ge 5 \text{ divides } d_L, \\ 1 & \text{if } p = 3 \text{ and } d_L \equiv 3 \pmod{9}, \\ 1 \text{ or } 2 & \text{if } p = 3 \text{ and } d_L \equiv 6 \pmod{9} \end{cases}$$

(*if $d_L \equiv 6 \pmod{9}$ and $a = 2$ we call $f_{K/L}$ an* exceptional conductor). *Conversely, let $f > 1$ be a given positive rational integer. Set*

$$\phi_L(f) = f \prod_{q \mid f} \left(1 - \frac{\chi_L(q)}{q}\right),$$

$$n_L(f) = \min\{k \ge 1 : \exists a \in \mathbb{Z},\ \varepsilon_L^k \equiv a \pmod{(f)}\} \quad \text{and} \quad i_L(f) = \phi_L(f)/n_L(f).$$

Then $i_L(f)$ is a positive integer and if there exists a real dihedral field K_{p^s} of degree $2p^s$, cyclic over L and such that $\mathcal{F}_{K_{p^s}/L} = (f)$ then p divides $i_L(f)$. Moreover, if the cyclic subextension K_p/L of degree p of K_{p^s}/L is ramified at at least one finite prime then p^s divides $i_L(f)$. Notice that $Cl_{L,\mathbb{Z}}(f)$ has order $h_L i_L(f)$ (see [Cox]).

Proof. For the first part, use Lemma 3, Theorem 4 and Lemma 5. Let us now prove the second part. The canonical map $i : H = (\mathbb{Z}/f\mathbb{Z})^* \to (A_L/(f))^* = G$ is injective. Hence, the factor group $G/i(H)$ has order $\phi_L(f)$ and $n_L(f)$ is the order of ε_L in this group. Hence, $i_L(f)$ is a positive integer. Now, as any character on $(A_L/(f))^*$ which is trivial on the image of $\mathbb{Z}$ may be construed as a character on $G/i(H)$, if there exists a character of order p on $(A_L/(f))^*$ which is trivial on the image of $\mathbb{Z}$ and on ε_L then p divides $i_L(f)$, and we finally use Lemma 3. ∎

4. Primitive modular characters of order p. The Chinese Remainder Theorem reduces the construction of primitive modular characters χ_0 of order p on $(A_L/(f))^*$ which are trivial on the image of $\mathbb{Z}$ to the construction of primitive modular characters ϕ of order p on $(A_L/(q^e))^*$ which are trivial on the image of $\mathbb{Z}$, and we may assume $1 \le e \le 2$ and $e = 1$ if $q \neq p$ (see Theorem 6). Since in Section 6 we will use such characters to perform practical computations of the relative class numbers of dihedral CM-fields of degree $4p$, we want to present fully explicit constructions.

PROPOSITION 7. *Let ϕ be a primitive character of order p on $(A_L/(f))^*$, trivial on the image of $\mathbb{Z}$ in this group. Let α' be the conjugate of $\alpha \in L$.*

(i) *If $f = q \equiv 1 \pmod{p}$ splits in L, say $(q) = \mathcal{Q}\mathcal{Q}'$, then there exists a character ψ of order p on the cyclic group $(A_L/\mathcal{Q})^*$ of order $q-1$ such that $\phi(\alpha) = \psi(\alpha/\alpha') = \psi(\alpha)\overline{\psi(\alpha')}$ for any $\alpha \in A_L$ prime to (q).*

(ii) *If* $f=q\equiv -1 \pmod p$ *is inert in* L, *then any primitive character* ϕ *of order* p *on the cyclic group* $(A_L/(q))^*$ *is trivial on* $\operatorname{Im}\mathbb{Z}$ *and is viewed as a character of order* p *on the cyclic group* $(A_L/(q))^*/\operatorname{Im}\mathbb{Z}$ *of order* $q+1$.

(iii) *If* $f=p^2$ *and* $(p)=\mathcal{P}\mathcal{P}'$ *splits in* L, *then there exists a character* ψ *of order* p *on the group* $(A_L/\mathcal{P}^2)^*$ *of order* $p(p-1)$ *such that for any* $\alpha\in A_L$ *relatively prime to* (p) *we have* $\phi(\alpha)=\psi(\alpha/\alpha')=\psi(\alpha)\overline{\psi(\alpha')}$.

(iv) *If* $f=p^2$ *and* p *is inert in* L, *then* ϕ *may be viewed as a character of order* p *on the group* $(A_L/(p^2))^*/\operatorname{Im}\mathbb{Z}$ *of order* $p(p+1)$.

(v) *If* $f=p$ *divides* d_L, *then any primitive character of order* p *on the group* $(A_L/(p))^*$ *of order* $p(p-1)$ *is trivial on* $\operatorname{Im}\mathbb{Z}$ *and is viewed as a character of order* p *on the cyclic group* $(A_L/(p))^*/\operatorname{Im}\mathbb{Z}$ *of order* p.

(vi) *Assume that* $d_L\equiv 6 \pmod 9$, *let* $\phi_{(3)}$ *be the primitive cubic character on* $(A_L/(3))^*$ *which is trivial on the image of* $\mathbb{Z}$ *and such that* $\phi_{(3)}(1+\sqrt{d_L})=\zeta_3$, *and let* $\phi_{(9)}$ *be the primitive cubic character on* $(A_L/(9))^*$ *which is trivial on the image of* $\mathbb{Z}$ *and such that* $\phi_{(9)}(1+\sqrt{d_L})=1$ *and* $\phi_{(9)}(1+3\sqrt{d_L})=\zeta_3$. *Then the six* $\phi_{(9)}^i\phi_{(3)}^j$ *with* $i\in\{1,2\}$ *and* $j\in\{0,1,2\}$ *are the only primitive cubic characters on* $(A_L/(9))^*$ *which are trivial on the image of* $\mathbb{Z}$, *and we have*:

k	1	2	3	4	5	6	7	8
$\phi_{(9)}^i\phi_{(3)}^j(1+k\sqrt{d_L})$	ζ_3^j	ζ_3^{i+2j}	ζ_3^i	ζ_3^{i+j}	ζ_3^{2i+2j}	ζ_3^{2i}	ζ_3^{2i+j}	ζ_3^{2j}

Proof. Let us, for example, prove (i). Let $\chi=\psi\psi'$ be the factorization of χ, where ψ and ψ' are characters modulo $\mathcal{Q}$ and $\mathcal{Q}'$, respectively. Let $\lambda\in A_L$ satisfy $\lambda\equiv 1 \pmod{\mathcal{Q}}$ and $\lambda\equiv 0 \pmod{\mathcal{Q}'}$, which implies $\psi(\alpha)=\chi(\lambda\alpha+\lambda')$, and $\lambda'\equiv 0 \pmod{\mathcal{Q}}$ and $\lambda'\equiv 1 \pmod{\mathcal{Q}'}$, which implies $\psi'(\alpha)=\chi(\lambda+\lambda'\alpha)=\chi((\lambda\alpha'+\lambda')')$. Since χ is trivial on $\operatorname{Im}\mathbb{Z}$, we have $\chi((\lambda\alpha'+\lambda')')=\overline{\chi(\lambda\alpha'+\lambda')}=\overline{\psi(\alpha')}$ and $\chi(\alpha)=\psi(\alpha)\psi'(\alpha)=\psi(\alpha)\overline{\psi(\alpha')}$, as desired. ■

In these five cases, we are reduced to the construction of all the characters of order p on some abelian groups whose p-Sylow subgroups are cyclic. So, let G be a multiplicative abelian group of order n and assume that p divides n and the p-Sylow subgroup of G is cyclic. Then $\{\chi_G^k : 1\le k\le p-1\}$ are the $p-1$ characters of order p on G where χ_G is the only character of order p on G such that $\chi_G(\alpha_G)=\zeta_p=\exp(2\pi i/p)$ where α_G is any fixed element in G satisfying $\beta_G=\alpha_G^{n/p}\ne 1$. Since $\{x\in G : x^{n/p}=1\}=\ker\chi_G$ is the only subgroup of order p in G, for any $\alpha\in G$ we have

$$\chi_G(\alpha)=\zeta_p^{k_\alpha} \quad \text{where} \quad k_\alpha=\min\{k\ge 0 : \alpha^{n/p}=\beta_G^k\}\in\{0,\dots,p-1\}$$

(indeed, $\chi_G(\alpha)=\zeta_p^k$ if and only if $\alpha/\alpha_G^k\in\ker\chi_G$, hence if and only if

$(\alpha/\alpha_G^k)^{n/p} = \alpha^{n/p}/\beta_G^k = 1)$. To compute efficiently $\alpha^{n/p}$ we use the binary expansion of exponent $e = n/p$ which can be quite large. This enables us to determine efficiently some α_G such that $\alpha_G^{n/p} \neq 1$, to compute fast β_G and store in some table of size p all the β_G^k, $0 \le k < p$. For any given $\alpha \in G$, we then compute efficiently $\alpha^{n/p}$ and look up in our previously computed table to which β_G^k it is equal, which yields $\chi_G(\alpha) = \zeta_p^k$.

Now, in the five cases listed in Proposition 7, we explain in detail how we use these χ_G to specify characters $\phi_{(q_i)}$ of order p on $(A_L/(q_i))^*$ trivial on $\operatorname{Im}\mathbb{Z}$ such that, in the simpler case where f is not an exceptional character,

$$X_{p,L,f} = \Big\{\chi_0^{(n)} = \prod_{i=1}^{r} \phi_{(q_i)}^{a_i(n)+1} : 0 \le n \le (p-1)^r - 1\Big\},$$

is the set of all the primitive modular characters of order p on $(A_L/(f))^*$ which are trivial on $\operatorname{Im}\mathbb{Z}$ when $f = \prod_{i=1}^r q_i$ is as in Theorem 6. Here with each $n \in \{0,\dots,(p-1)^r - 1\}$ we associated its $(p-1)$-adic development $n = \sum_{i=1}^r a_i(n)(p-1)^{i-1}$, $a_i(n) \in \{0,1,\dots,p-2\}$. In particular, for any given finite set E (containing ε_L), it is easy to compute numerically the number $n_{p,L,f,E}$ of primitive modular characters which are trivial on the image of $\mathbb{Z}$ and on some finite set E (see Proposition 8 for an application).

(i) In case (i) of Proposition 7 where $G = (A_L/\mathcal{Q})^*$ has order $q-1$, we determine P_q such that $4q$ divides $d_L - P_q^2$ and choose $\mathcal{Q} = q\mathbb{Z} + \frac{P_q+\sqrt{d_L}}{2}\mathbb{Z}$. Since G is canonically isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$, we may view χ_G as a character of order p on the cyclic group $(\mathbb{Z}/q\mathbb{Z})^*$ of order $q-1$, and if $\alpha = (x_\alpha + y_\alpha\sqrt{d_L})/2$ then $\alpha \equiv x_\alpha - y_\alpha P_q \pmod{\mathcal{Q}}$ and $\alpha' \equiv x_\alpha + y_\alpha P_q \pmod{\mathcal{Q}}$. Therefore, ϕ is a power of the character

$$\alpha \mapsto \phi_{(q)}(\alpha) = \chi_G(n_\alpha) \quad \text{where} \quad n_\alpha = \frac{x_\alpha - y_\alpha P_q}{x_\alpha + y_\alpha P_q} \quad \text{in } (\mathbb{Z}/q\mathbb{Z})^*.$$

In that case, we determine $\alpha_G \in (\mathbb{Z}/q\mathbb{Z})^*$ such that $\beta_G = \alpha_G^{(q-1)/p} \neq 1$ in $(\mathbb{Z}/q\mathbb{Z})^*$, we precompute a table defined by $\mathrm{Table}(k) = \beta_G^k$ in $(\mathbb{Z}/q\mathbb{Z})^*$, $0 \le k \le p-1$, and find that $\phi_{(q)}(\alpha) = \zeta_p^k$ if and only if $n_\alpha^{(q-1)/p} = \mathrm{Table}(k)$.

(ii) In case (ii) of Proposition 7 where $G = (A_L/(q))^*/\operatorname{Im}\mathbb{Z}$ has order $q+1$, we may assume that $\alpha_G = x_G + \omega_L$ and we determine the least $x_G \ge 0$ such that $X_G + Y_G\omega_L = \beta_G = \alpha_G^{(q+1)/p} = (x_G + \omega_L)^{(q+1)/p} \not\equiv a \pmod{(q)}$ for any rational integer a (i.e. such that $Y_G \not\equiv 0 \pmod{q}$), and we get that ϕ is a power of the character $\alpha \mapsto \phi_{(q)}(\alpha) = \chi_G(\alpha)$. Since $\beta_G^k = X_G(k) + Y_G(k)\omega_L$ with $Y_G(k) \not\equiv 0 \pmod{q}$ for $1 \le k \le p-1$, we can set $\mathrm{Table}(k) = X_G(k)/Y_G(k)$ (computed modulo q), and for any $\alpha = x_\alpha + y_\alpha\omega_L$ we compute $\alpha^{(q+1)/p} \equiv X_\alpha + Y_\alpha\omega_L \pmod{(q)}$ to conclude that ϕ is a power of the character $\alpha \mapsto \phi_{(q)}(\alpha) = \chi_G(\alpha)$ where

$$\phi_{(q)}(\alpha) = \chi_G(\alpha)$$
$$= \begin{cases} 1 & \text{if } Y_\alpha \equiv 0 \pmod{q}, \\ \zeta_p^k & \text{if } Y_\alpha \not\equiv 0 \pmod{q} \text{ and } X_\alpha/Y_\alpha = X_G(k)/Y_G(k) = \text{Table}(k). \end{cases}$$

(iii) In case (iii) of Proposition 7 where $G = (A_L/\mathcal{P}^2)^*$ has order $p(p-1)$, we determine P_p such that $4p^2$ divides $d_L - P_p^2$ and choose $\mathcal{P} = p\mathbb{Z} + \frac{P_p+\sqrt{d_L}}{2}\mathbb{Z}$, which yields $\mathcal{P}^2 = p^2\mathbb{Z} + \frac{P_p+\sqrt{d_L}}{2}\mathbb{Z}$. Since G is canonically isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})^*$, we may view χ_G as a character of order p on the cyclic group $(\mathbb{Z}/p^2\mathbb{Z})^*$ of order $p(p-1)$. Since $\alpha = (x_\alpha + y_\alpha\sqrt{d_L})/2$ implies $\alpha \equiv x_\alpha - y_\alpha P_p \pmod{\mathcal{P}^2}$ and $\alpha' \equiv x_\alpha + y_\alpha P_p \pmod{\mathcal{P}^2}$, we infer that ϕ is a power of the character

$$\alpha \mapsto \phi_{(p^2)}(\alpha) = \chi_G(n_\alpha) \quad \text{where} \quad n_\alpha = \frac{x_\alpha - y_\alpha P_p}{x_\alpha + y_\alpha P_p} \quad \text{in } (\mathbb{Z}/p^2\mathbb{Z})^*.$$

In that case, we determine $\alpha_G \in (\mathbb{Z}/p^2\mathbb{Z})^*$ such that $\beta_G = \alpha_G^{p-1} \neq 1$ in $(\mathbb{Z}/p^2\mathbb{Z})^*$, we precompute a table defined by $\text{Table}(k) = \beta_G^k$ in $(\mathbb{Z}/p^2\mathbb{Z})^*$, $0 \le k \le p-1$, and conclude that $\phi_{(p^2)}(\alpha) = \zeta_p^k$ if and only if $n_\alpha^{p-1} = \text{Table}(k)$.

(iv) In case (iv) of Proposition 7 where $G = (A_L/(p^2))^*/\text{Im}\,\mathbb{Z}$ has order $p(p+1)$, we may choose $\alpha_G = 1 + p\omega_L$ for which $\beta_G = \alpha_G^{p+1} = \alpha_G$. If $\alpha = x_\alpha + y_\alpha\omega_L$ and $\alpha^{p+1} \equiv X_\alpha + Y_\alpha\omega_L \pmod{(p^2)}$, then using $\alpha^{p+1} \equiv N_{L/\mathbb{Q}}(\alpha) \pmod{(p)}$ we get $X_\alpha \not\equiv 0 \pmod{p}$, $Y_\alpha \equiv 0 \pmod{p}$ and $\chi_G(\alpha) = \zeta_p^{(Y_\alpha/p)/X_\alpha}$. That is, ϕ is a power of the character

$$\alpha \mapsto \phi_{(p^2)}(\alpha) = \zeta_p^{(Y_\alpha/p)/X_\alpha}.$$

(v) In case (v) of Proposition 7 where $G = (A_L/(p))^*/\text{Im}\,\mathbb{Z}$ has order p, we may choose $\alpha_G = 1 + \sqrt{d_L}$ for which $\beta_G = \alpha_G$ and $\beta_G^k = 1 + k\sqrt{d_L}$. If $\alpha = (x_\alpha + y_\alpha\sqrt{d_L})/2$ then $\chi_G(\alpha) = \chi_G(1 + (y_\alpha/x_\alpha)\sqrt{d_L}) = \zeta_p^{y_\alpha/x_\alpha}$. That is, ϕ is a power of the character

$$\alpha \mapsto \phi_{(p)}(\alpha) = \zeta_p^{y_\alpha/x_\alpha}.$$

Notice that in cases (iv) and (v) we do not precompute any table. Notice also that

$$(x_\alpha + y_\alpha\sqrt{d_L}) = (x_\alpha - g_L y_\alpha)/2 + y_\alpha\omega_L$$

and

$$x_\alpha + y_\alpha\omega_L = ((2x_\alpha + g_L y_\alpha) + y_\alpha\sqrt{d_L})/2.$$

5. Primitive characters on ring class groups. Since in Section 6 we will use such characters to perform practical computations of the relative class numbers of dihedral CM-fields of degree $4p$, here again we shall be dwelling upon a completely explicit construction of all the primitive characters χ of order p on $Cl_{L,\mathbb{Z}}(f)$. To begin with, write $h_L = p^{s_L(p)}h$ with $\gcd(p,h) = 1$, let $r_L(p)$ denote the p-rank of Cl_L, let

$$Cl_L^{(p)} = \prod_{i=1}^{r_L(p)} C_{p^{e_i}}$$

with $\sum_{i=1}^{r_L(p)} e_i = s_L(p)$ be the p-Sylow subgroup of Cl_L and let J_i, $1 \le i \le r_L(p)$, be $r_L(p)$ integral ideals of A_L of norms relatively prime to f, whose ideal classes have order p^{e_i}, respectively, and such that the subgroup of Cl_L generated by the $r_L(p)$ ideal classes of these J_i is equal to $Cl_L^{(p)}$ (here, C_n denotes the cyclic group of order $n > 1$). We let $\alpha_i \in A_L$ be such that

$$J_i^{p^{e_i}} = (\alpha_i). \tag{1}$$

From a practical point of view, and since as explained in the introduction we will first fix L and p and then determine all the real dihedral fields K containing L such that $f_{K/L}$ is less than or equal to some prescribed upper bound, we compute $r_L(p)$ generators of the p-Sylow subgroup $Cl_L^{(p)}$ which are ideal classes of prime ideals J_i above rational primes l_i which split in L and satisfy $l_i \not\equiv 1 \pmod{p}$. In that case, the norms l_i of these generators are relatively prime to any possible $f_{K/L}$ (see Theorem 6). Now, for any integral ideal I of A_L of norm relatively prime to f there exists only one

$$\vec{k}_I = (k_1, \dots, k_{r_L(p)}) \in \prod_{i=1}^{r_L(p)} \{0, \dots, p^{e_i} - 1\}$$

such that

$$I^h \prod_{i=1}^{r_L(p)} J_i^{k_i} = (\beta_I) \tag{2}$$

is principal. Finally, let $h' \ge 1$ satisfy $hh' \equiv 1 \pmod{p}$.

Let now χ be a primitive character of order p on $Cl_{L,\mathbb{Z}}(f)$ and $\alpha \mapsto \chi_0(\alpha) = \chi((\alpha))$ be its associated primitive modular character of order p on $(A_L/(f))^*$. Setting $\psi_0 = \chi_0^{h'}$, we get

$$\chi(I) = \chi^{hh'}(I) = \chi^{h'}(I^h) = \psi_0(\beta_I)\chi_{\vec{\zeta}}(\vec{k}_I) \tag{3}$$

where $\vec{\zeta} = (\zeta_1, \dots, \zeta_{r_L(p)})$, where each $\zeta_i = \overline{\chi^{h'}(J_i)}$ is a pth complex root of unity and where

$$\chi_{\vec{\zeta}}(\vec{k}_I) = \prod_{i=1}^{r_L(p)} \zeta_i^{k_i}.$$

Since $J_i^{p^{e_i}} = (\alpha_i)$, we must have $\chi((\alpha_i)) = \chi_0(\alpha_i) = +1$. Conversely, let χ_0 be a given primitive character on $(A_L/(f))^*$ which is trivial on ε_L and the image of $\mathbb{Z}$, assume that $\chi_0(\alpha_i) = +1$ for $1 \le i \le r_L(p)$, set $\psi_0 = \chi_0^{h'}$, and let $\vec{\zeta} = (\zeta_1, \ldots, \zeta_{r_L(p)})$ be given, where each ζ_i is a pth complex root of unity. Then

$$\chi(I) = \psi_0(\beta_I)\chi_{\vec{\zeta}}(\vec{k}_I)$$

clearly defines a primitive character on $Cl_{L,\mathbb{Z}}(f)$ whose associated modular character ψ_0^h is equal to χ_0. We have proved:

Proposition 8. *Fix some primitive character χ_0 of order p on $(A_L/(f))^*$ which is trivial on ε_L and the image of $\mathbb{Z}$.*

(i) *If some $\chi_0(\alpha_i)$ is not equal to $+1$ for some $1 \le i \le r_L(p)$, then there is no primitive character χ on $Cl_{L,\mathbb{Z}}(f)$ of order p whose associated modular character is equal to χ_0.*

(ii) *If all the $\chi_0(\alpha_i)$ are equal to $+1$ for $1 \le i \le r_L(p)$, then there are precisely $p^{r_L(p)}$ primitive characters χ on $Cl_{L,\mathbb{Z}}(f)$ of order p whose associated modular characters are equal to χ_0.*

Corollary 9. *For $f > 1$ let $N(p, L, f)$ denote the number of primitive modular characters of order p on $(A_L/(f))^*$ which are trivial on the image of $\mathbb{Z}$, on ε_L and on all the α_i, $1 \le i \le r_L(p)$. If $N(p, L, f) > 0$ then $p - 1$ divides $N(p, L, f)$. Moreover, the number $Nd(p, L, f)$ of real dihedral fields K of degree $2p$ containing L and such that $\mathcal{F}_{K/L} = (f)$ is given by*

$$Nd(p, L, f) = \begin{cases} N(p, L, f)p^{r_L(p)}/(p-1) & \text{if } f > 1, \\ (p^{r_L(p)} - 1)/(p-1) & \text{if } f = 1. \end{cases}$$

6. Actual computations. Let $p \ge 3$ be a given odd prime and let L be a given real quadratic field. For a given $f \ge 1$ as in Theorem 6, we explain how we construct all the real dihedral fields K of degree $2p$ which contain L and for which $f_{K/L} = f$.

First, we recall that $\varepsilon_L = q_{l-1}\omega_L + q_{l-2}$ where $l \ge 1$ is the length of the purely periodic continued fraction expansion $\omega_L = [\overline{a_0, a_1, \ldots, a_{l-1}}]$ of ω_L and where $q_{-2} = 1$, $q_{-1} = 0$ and $q_k = a_k q_{k-1} + q_{k-2}$, $k \ge 0$. This enables us to compute easily ε_L modulo f and $n_L(f)$, and then compute $i_L(f)$ and check whether p divides $i_L(f)$ (see Theorem 6).

Second, in order to use (1), (2), (3) or Proposition 8, we must be able to compute an explicit generator of a given principal ideal, and we explained how to do it in [Lou].

Third, let us give one example. Choose $p = 3$ and $L = \mathbb{Q}(\sqrt{229})$ for which $h_L = 3$. The least f's such that $Nd(3, L, f) > 0$ are $f = 1, 118, 194, 197, 207, 226, 251, 281, 302, \ldots$ Moreover, $f = 23246, 24426, 29618, \ldots$ are the least f's such that $Nd(3, L, f) > 3$ (and in these three cases $Nd(3, L, f) = 6$). Finally, $f = 18, 19, 29, \ldots$ are the least f's as in Theorem 6 such that $p = 3$ divides $i_L(f)$ but for which $Nd(3, L, f) = 0$.

Finally, we explain how to use the technique developed above to compute the relative class number h_N^- of any dihedral CM-field N of degree $4p$. We let M denote the imaginary biquadratic bicyclic subfield of N, let L_0 and L_1 denote the two imaginary quadratic subfields of M and keep the notation as above: L is the real quadratic subfield of M, and the maximal totally real subfield $K = N^+$ of N is a real dihedral field of degree $2p$ cyclic over L. We let ∞_1 and ∞_2 denote the infinite places of L.

Proposition 10 (see [LOO], [LP]). *Let N be a dihedral CM-field of degree $4p$. Then h_M^- divides h_N^- and $h_N^-/h_M^- = (h_{N/M}^-)^2$ is a perfect square. Moreover, $f_{M/L} = \sqrt{d_{L_0}d_{L_1}/d_L}$ is a positive integer, and the conductor of the quadratic extension M/L is equal to $\mathcal{F}_{M/L} = \infty_1\infty_2(f_{M/L})$. If we let $\mathcal{F}_{N/L} = \mathrm{lcm}(\mathcal{F}_{N^+/L}, \mathcal{F}_{M/L}) = \infty_1\infty_2\mathrm{lcm}((f_{K/L}), (f_{M/L})) = \infty_1\infty_2(f_{N/L})$ denote the conductor of the extension N/L and set $A_N = \sqrt{d_L f_{N/L}^2}$, then*

$$h_{N/M}^- = \prod_{j=0}^{(p-3)/2} \frac{A_N}{4\pi^2} L(1, \chi_{N/L}^{2j+1}) \tag{4}$$

where $\chi_{N/L}$ denotes any of the $p-1$ Hecke characters of degree one and order $2p$ associated with the cyclic extension N/L of degree $2p$.

We explained in [Lou] how to compute numerical approximations as good as desired of $L(1,\chi)$ for Hecke L-functions $L(s,\chi) = \sum_{n\ge1} a_n(\chi)n^{-s}$ associated with primitive Hecke characters χ on ray class groups of real quadratic number fields L: letting W_χ denote the Artin root number which appears in the functional equation of this L-function we have the following absolutely convergent series expansion:

$$L(1,\chi) = \sum_{n\ge1} \frac{a_n(\chi)}{n} K_1(n/A_\chi) + W_\chi \sum_{n\ge1} \frac{\overline{a_n(\chi)}}{n} K_2(n/A_\chi) \tag{5}$$

where $B \mapsto K_1(B)$ and $B \mapsto K_2(B)$ are defined for $B > 0$ and satisfy $0 \le K_2(B) \le K_1(B) \le 2e^{-B}$. Moreover, if we let $S_{M,\chi}$ denote the value obtained by disregarding the indices $n > M$ in (5), then

$$|L(1,\chi) - S_{M,\chi}| \le 4(\log(Me) + 2)^2 e^{-M/A_\chi}. \tag{6}$$

Hence, (4)–(6) enable us to compute the relative class numbers of dihedral CM-fields of degree $4p$. Indeed, the Artin root numbers W_χ of dihedral CM-fields N of degree $4p$ are equal to $+1$ (see [FQ]) and we explained in [Lou] how to compute the coefficients $a_n(\chi)$.

In [Lef], [LL] and [Lou] we gave examples of relative class number computations for dihedral CM-fields N of degree $4p$. Here, we give more tricky examples for which we have had to use all the machinery developed in this paper.

1. There are ten imaginary biquadratic bicyclic number fields $M = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with relative class number one such that the class numbers h_L of their real quadratic subfields $L = \mathbb{Q}(\sqrt{D_1 D_2})$ are divisible by some odd prime p. For each of the ten possible triplets (M, L, p), we give in Table 1 the least $f > 1$ such $Nd(p, L, f) = pN(p, L, f)/(p - 1) > 0$. In these ten cases $Nd(p, L, f) = p$, there are p fields K to consider, we set $N = KM$, notice that these p composita are dihedral CM-fields of degree $4p$ and for each of the ten triplets (M, L, p) we give in Table 1 the values of $h^-_{N/M}$ for these p dihedral CM-fields N.

2. Choose $M = \mathbb{Q}(\sqrt{-1}, \sqrt{-32009})$, for which $h^-_M = 166$, and notice that $L = \mathbb{Q}(\sqrt{32009})$ is the real quadratic field with the least discriminant for which the 3-rank $r_3(L)$ of its ideal class group is ≥ 2. We have $d_L = 32009$, $h_L = 9$ and $r_L(3) = 2$. Therefore, $Nd(3, L, 1) = 4$ and we let K denote any one of the four real sextic dihedral fields containing L for which $f_{K/L} = 1$, and set $N = KM$, a dihedral CM-field of degree 12. In Table 2 we give the values of $h^-_{N/M}$ for these four N's.

Now, $f = 211$ is the least positive integer for which $N(3, L, f) > 0$ and since $f = 211$ is prime we have $N(3, L, 211) = 1$, and $Nd(3, L, 211) = 9$, and we let K denote any one of the nine real sextic dihedral fields containing L for which $f_{K/L} = 211$, and set $N = KM$, a dihedral CM-field of degree 12. In Table 3 we give the values of $h^-_{N/M}$ for these nine N's.

3. Choose $M = \mathbb{Q}(\sqrt{-3}, \sqrt{-35})$ and $L = \mathbb{Q}(\sqrt{105})$. Let K_9 be the only real dihedral field of degree 18, cyclic of degree 9 over L for which $f_{K_9/L} = 27$. Let K_3/L be the cyclic cubic subextension of K_9/L and notice that K_3 is a real dihedral field of degree 6 such that $f_{K_3/L} = 9$. Set $N_{12} = K_3 M$ and $N_{36} = K_9 M$. Then N_{12} and N_{36} are dihedral CM-fields of degree 12 and 36 and relative class numbers 1 and 327^2, respectively.

Table 1

D_1	D_2	d_L	h_L	p	f	$h^-_{N/M} =$
-7	-67	469	3	3	62	24, 30, 45
-11	-43	473	3	3	85	27, 45, 108
-4	-235	940	6	3	91	36, 60, 72
-8	-163	1304	3	3	53	27, 30, 51
-4	-427	1708	6	3	227	66, 168, 270
-19	-267	5073	6	3	55	36, 81, 99
-19	-43	817	5	5	79	820, 1345, 4225, 6505, 12980
-67	-115	7705	10	5	55	6301, 6921, 24671, 33916, 34751

Table 1 (cont.)

D_1	D_2	d_L	h_L	p	f	$h^-_{N/M} =$
-67	-91	6097	14	7	1189	765 104 081
						4 066 653 227
						10 008 078 059
						13 699 296 569
						13 721 986 264
						16 694 290 249
						16 782 950 947
-67	-427	28609	14	7	167	49 494 697
						69 531 448
						153 177 143
						308 444 857
						562 737 259
						636 146 917
						662 575 151

Table 2

Case	1	2	3	4
$h^-_{N/M}$	16	16	16	37

Table 3

Case	1	2	3	4	5	6	7	8	9
$h^-_{N/M}$	2932	2968	3073	3463	3712	3754	7684	8338	8491

References

[Cox] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.

[FQ] A. Fröhlich and J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. 20 (1973), 125–138.

[Has] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. 31 (1930), 565–582.

[Jan] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.

[Lef] Y. Lefeuvre, *Corps diédraux à multiplication complexe principaux*, preprint, Univ. Caen, 1999, submitted.

[LL] Y. Lefeuvre and S. Louboutin, *The class number one problem for the dihedral CM-fields*, in: Proc. ICM 1998 satellite conference, Algebraic Number Theory and Diophantine Analysis, Graz.

[Lou] S. Louboutin, *Computation of relative class numbers of CM-fields by using Hecke L-functions*, Math. Comp., to appear.

[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.

[LP] S. Louboutin and Y.-H. Park, *Class number problems for dicyclic CM-fields*, preprint, Univ. Caen, 1998.

[Mar] J. Martinet, *Sur l'arithmétique des extensions à groupe de Galois diédral d'ordre* 2p, Ann. Inst. Fourier (Grenoble) 19 (1969), 1–80.

[Por] J. Porusch, *Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage*, Math. Z. 37 (1933), 134–160.

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

Department of Mathematics
Korea University
136-701 Seoul, Korea
E-mail: youngho@semi.korea.ac.kr

Received on 5.5.1998
and in revised form on 29.9.1998 (3373)