

CLASS NUMBER FORMULA FOR DIHEDRAL EXTENSIONS

LUCA CAPUTO and FILIPPO A. E. NUCCIO MORTARINO MAJNO DI
CAPRIGLIO 

Univ Lyon, Université Jean Monnet Saint-Étienne, CNRS UMR 5208, Institut Camille Jordan,
F-42023 Saint-Étienne, France
e-mails: luca.caputo@gmx.com; filippo.nuccio@univ-st-etienne.fr

(Received 16 June 2018; revised 4 March 2019; accepted 13 March 2019;
first published online 21 May 2019)

Abstract. We give an algebraic proof of a class number formula for dihedral extensions of number fields of degree $2q$, where q is any odd integer. Our formula expresses the ratio of class numbers as a ratio of orders of cohomology groups of units and allows one to recover similar formulas which have appeared in the literature. As a corollary of our main result, we obtain explicit bounds on the (finitely many) possible values which can occur as ratio of class numbers in dihedral extensions. Such bounds are obtained by arithmetic means, without resorting to deep integral representation theory.

2010 *Mathematics Subject Classification.* Primary: 11R29, 11R20; Secondary: 11R34, 11R37

1. Introduction. Let k be a number field and let M/k be a finite Galois extension. For a subgroup $H \subseteq \text{Gal}(M/k)$, let χ_H denote the rational character of the permutation representation defined by the $\text{Gal}(M/k)$ -set $\text{Gal}(M/k)/H$. If M/k is non-cyclic, then there exists a relation

$$\sum_H n_H \cdot \chi_H = 0,$$

where $n_H \in \mathbb{Z}$ are not all 0 and H runs through the subgroups of $\text{Gal}(M/k)$. Using the formalism of Artin L -functions and the formula for the residue at 1 of the Dedekind zeta-function, Brauer showed in [5] that the above relation translates into the following formula:

$$\prod_H (h_{M^H})^{n_H} = \prod_H \left(\frac{w_{M^H}}{R_{M^H}} \right)^{n_H}, \quad (1.1)$$

where, for a number field E , h_E , R_E , and w_E denote the class number, the regulator, and the order of the group of roots of unity of E , respectively.

Although the regulator of a number field is in general an irrational number, the right-hand side of the above equality is clearly rational, being equal to the left-hand side. As a matter of fact, Brauer himself proved that when $k = \mathbb{Q}$, the regulator can be translated into an algebraic invariant of the Galois structure of the unit group. It is therefore natural to look for an algebraic proof of Brauer's formula, independent of any analytical result. Brauer also showed that the left-hand side of equation (1.1) can take only finitely many values as M ranges over all Galois extension of \mathbb{Q} with Galois group isomorphic to a fixed finite group. It thus becomes interesting to look for an explicit description of a finite set of integers (as small as possible) containing all the values which are attainable by the class number ratio, as well as for generalizations beyond the case $k = \mathbb{Q}$.

Historically, these questions were investigated for the first time in the case where $M = \mathbb{Q}(\sqrt{d}, \sqrt{-d})$ (with $d > 1$ a square-free integer). In this case, Dirichlet showed, by analytical means, that

$$\frac{h_M}{h_{\mathbb{Q}(\sqrt{d})}h_{\mathbb{Q}(\sqrt{-d})}} = \frac{1}{2}Q,$$

where Q is 1 or 2 depending on whether a certain unit of M has norm 1 or not in $\mathbb{Q}(\sqrt{-1})$ (see [8]). Hilbert later gave an algebraic proof of the above equality (see [11, 16] for a more general result).

Another interesting particular case is that of dihedral extensions, which is the one we focus on in this paper. This setting has already been considered by other authors: notably, Walter computed explicitly in [22] the regulator term, building upon Brauer’s previous work and obtained a refined class number formula in the dihedral case over an arbitrary base field k , still relying on analytical results about Artin L -functions (Walter’s result actually holds for more general Frobenius groups). Bartel provided a different representation-theoretic interpretation of Walter’s result in [2], a result which was later generalized to a much larger family of groups in [3].

Our main result is the following theorem whose proof is purely algebraic and does not rely on any argument involving L -functions.

THEOREM 3.14. *Let L/k be a Galois extension of number fields whose Galois group $D = \text{Gal}(L/k)$ is dihedral of order $2q$ with q odd. Let $\Sigma \subseteq D$ be a subgroup of order 2 and $G \subseteq D$ be the subgroup of order q . Set $K = L^\Sigma$ and $F = L^G$. Then*

$$\frac{h_L h_k^2}{h_F h_K^2} = \frac{\widehat{h}^0(D, \mathcal{O}_L^\times \otimes \mathbb{Z}[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times \otimes \mathbb{Z}[\frac{1}{2}])} = \frac{\widehat{h}^0(D, \mathcal{O}_L^\times)}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times)} \frac{\widehat{h}^{-1}(\Sigma, \mathcal{O}_L^\times)}{\widehat{h}^0(\Sigma, \mathcal{O}_L^\times)}.$$

Here, \mathcal{O}_L^\times is the group of units of L and, for a subgroup $H \subseteq D$ and an integer i , $\widehat{h}^i(H, B)$ denotes the order of the i th Tate cohomology group of H with values in the H -module B .

Similar algebraic proofs have appeared in the literature although, as far as we know, only for special cases. Halter-Koch in [9] and Moser in [18] analyzed the case of a dihedral extension of \mathbb{Q} of degree $2p$, where p is an odd prime. They express the ratio of class numbers in terms of a unit index, proving that in this setting one has

$$\frac{h_L}{h_F h_K^2} = (\mathcal{O}_L^\times : \mathcal{O}_K^\times \mathcal{O}_{K'}^\times \mathcal{O}_F^\times) p^{-r},$$

where K' is a Galois conjugate of K in L , and $r = 1$ if F is imaginary and 2 otherwise. Their result was generalized by Jaulent in [12], who gave an algebraic proof of a similar formula for dihedral extensions of degree $2p^s$ when the ground field k is \mathbb{Q} or an imaginary quadratic field and $s \geq 1$ is any integer. Jaulent actually obtained his result as a particular case of a formula for Galois extensions over an arbitrary ground field with Galois group of the form $\mathbb{Z}/p^s \rtimes T$ where T is an abelian group of exponent dividing $p - 1$. In such general formula, the ratio of class numbers is expressed in terms of orders of cohomology groups of units, as in our Theorem 3.14. This approach was not developed further and in fact Jaulent’s paper is not cited in subsequent works in the literature.

The study of class number formulas for dihedral extensions from an algebraic viewpoint was taken up more than 20 years later by Lemmermeyer. In [17], he generalized Halter-Koch’s formula to arbitrary ground fields, always under the assumption that the degree is $2p$ and under some ramification condition.

The quoted works also provide an explicit description of the finitely many possible values which may occur as class number ratio, clearly only under their working assumptions. These values are obtained using the explicit classification of the indecomposable integral representations of D , in order to find an exhaustive list of the possible indexes of units which can appear as regulator ratios. This classification is not available for dihedral groups of arbitrary order $2q$, as discussed in the introduction of [10], for instance. Combining our formula with the knowledge of the Herbrand quotient of the units for the cyclic subextension L/F , we find a finite set of integers containing all the attainable values of the ratio of class numbers, without resorting to any integral representation-theoretic results. This indicates that the traditional way of expressing the class number ratio as a unit index, although suggestive, is less effective than our cohomological approach for the purpose of determining the possible values of the ratio of class numbers.

Our main results in this direction are the following two corollaries. For a number field M , denote by $\mu_M(q^\infty)$ the roots of unity in M of q -power order and by $\mu_M(q)$ the subgroup of $\mu_M(q^\infty)$ of elements killed by q . Set

$$\beta_M(q) = \begin{cases} 0 & \text{if } \mu_M(q) \text{ is trivial,} \\ 1 & \text{otherwise.} \end{cases}$$

Give a prime number ℓ , v_ℓ denotes the ℓ -adic valuation.

COROLLARY 3.15. *Let $a = \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + \beta_F(q) + 1$ and $b = \text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) + \beta_k(q)$. Then, for every prime ℓ , the following bounds hold:*

$$-av_\ell(q) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq bv_\ell(q).$$

In particular, if F is totally real of degree $[F : \mathbb{Q}] = 2d$, then

$$-2dv_\ell(q) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq (d - 1)v_\ell(q).$$

In case F is assumed to be a CM field and $k = F^+$ is its totally real subfield, we can strengthen our bounds as follows.

COROLLARY 3.18. *Assume that F is a CM field of degree $[F : \mathbb{Q}] = 2d$ and that k is its totally real subfield. Let s be the order of the quotient $((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q$ and let t be the order of $\mu_F(q^\infty) / \mu_F(q)$. Then, for every prime ℓ ,*

$$-v_\ell(q) - v_\ell(s) - v_\ell(t) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq (d - 1)v_\ell(q).$$

When $q = p$ is prime and $k = \mathbb{Q}$, we can further improve Corollary 3.15 and prove in Corollary 3.20 that the ratio of class numbers satisfies

$$\frac{h_L}{h_F h_K^2} \in \left\{ 1, \frac{1}{p}, \frac{1}{p^2} \right\}.$$

This answers the MathOverflow question [1] of Bartel, who asks for a proof of this fact that does not rely on the analytical class number formula, nor on any integral representation theory. Our Corollary 3.15 actually shows that a similar result holds without the assumption that $k = \mathbb{Q}$ or that $q = p$ be prime.

We now briefly describe the structure of the paper. Section 2 contains all the technical algebraic lemmas used in the rest of the paper. The proof of Theorem 3.14, which is divided

in two parts, is contained in Section 3. The proof of the 2-part follows a strategy of Walter (see [22]), combining an elementary result about D -modules and a simple arithmetic piece of information. On the other hand, the proof for the odd components heavily relies on cohomological class field theory and is partly inspired by the proof of Chevalley’s ambiguous class number formula. Since the extension L/k is non-abelian, we cannot apply class field theory directly; however, since we are restricted to odd parts, the action of $\Delta = \text{Gal}(F/k)$ on the cohomology of $G = \text{Gal}(L/F)$ can be described very explicitly as discussed in Section 2. We conclude the article with Section 4 where we translate our cohomological formula in an explicit unit index (see Corollary 4.2).

2. Cohomological preliminaries. This section contains all the technical algebraic tools we need in the rest of the paper. We fix an odd positive integer $q \geq 3$ and we let D denote the dihedral group of order $2q$. We choose generators $\sigma, \rho \in D$ such that

$$\sigma^2 = \rho^q = 1, \quad \sigma\rho = \rho^{-1}\sigma.$$

We set $\Sigma := \langle \sigma \rangle$, $\Sigma' := \langle \sigma\rho \rangle$ and $G := \langle \rho \rangle$, $\Delta := D/G$. We say that an abelian group B is uniquely 2-divisible when multiplication by 2 is an automorphism of B . As we shall see below, the D -Tate cohomology group $\widehat{H}^i(D, B)$ of a uniquely 2-divisible D -module B is canonically isomorphic to the subgroup of $\widehat{H}^i(G, B)$ on which Δ acts trivially. We find a similar cohomological description for the subgroup $\widehat{H}^i(G, B)$ on which Δ acts as -1 : the precise statement is given in Proposition 2.1.

NOTATION. Given a group Γ and a Γ -module B , we denote by B^Γ (resp. B_Γ) the maximal submodule (resp. the maximal quotient) of B on which Γ acts trivially. We will sometimes refer to B^Γ (resp. B_Γ) as the invariants (resp. coinvariants) of B . Moreover, let $N_\Gamma = \sum_{\gamma \in \Gamma} \gamma \in \mathbb{Z}[\Gamma]$ be the norm, $B[N_\Gamma]$ the kernel of multiplication by N_Γ and I_Γ the augmentation ideal of $\mathbb{Z}[\Gamma]$ defined as

$$I_\Gamma := \text{Ker}(\mathbb{Z}[\Gamma] \longrightarrow \mathbb{Z}), \quad \text{where the morphism is induced by } \gamma \mapsto 1 \text{ for all } \gamma \in \Gamma.$$

For every $i \in \mathbb{Z}$, let $\widehat{H}^i(\Gamma, B)$ denote the i th Tate cohomology group of Γ with values in B . Similarly, for $i \geq 0$, $H^i(\Gamma, B)$ (resp. $H_i(\Gamma, B)$) is the i th cohomology (resp. homology) group of Γ with values in B . For standard properties of these groups (which will be implicitly used without specific mention), the reader is referred to [7, Chapter XII]. If B' is another Γ -module and $f: B \rightarrow B'$ is a homomorphism of abelian groups, we say that f is Γ -equivariant (resp. Γ -antievvariant) if $f(\gamma b) = \gamma f(b)$ (resp. $f(\gamma b) = -\gamma f(b)$) for every $\gamma \in \Gamma$ and $b \in B$. Suppose now that $\Gamma = \{1, \gamma\}$ has order 2. An object B of the category of uniquely 2-divisible Γ -modules admits a functorial decomposition $B = B^+ \oplus B^-$ where we denote by B^+ (resp. B^-) the maximal submodule on which Γ acts trivially (resp. as -1). Such decomposition is obtained by writing $b = \frac{1+\gamma}{2}b + \frac{1-\gamma}{2}b$ for $b \in B$. Then

$$B^\Gamma = B^+ \cong B/B^- = B_\Gamma. \tag{2.1}$$

We now go back to our setting and concentrate on the case where Γ is equal to a subquotient of D . Observe that, if B is a uniquely 2-divisible D -module, then B^H is again uniquely 2-divisible for every subgroup $H \subseteq D$. In particular, for every $i \in \mathbb{Z}$, the map

$$\widehat{H}^i(\Delta, B^G) \xrightarrow{-2} \widehat{H}^i(\Delta, B^G)$$

is an automorphism and therefore

$$\widehat{H}^i(\Delta, B^G) = 0, \tag{2.2}$$

because these groups are killed by $2 = |\Delta|$. Using this we prove the next proposition which is the key of all our cohomological computations.

PROPOSITION 2.1. *Let B be a uniquely 2-divisible D -module. Then, for every $i \in \mathbb{Z}$, restriction induces isomorphisms*

$$\widehat{H}^i(D, B) \cong \widehat{H}^i(G, B)^+.$$

Moreover, the Tate isomorphism $\widehat{H}^i(G, B) \cong \widehat{H}^{i+2}(G, B)$ is Δ -antiequivariant. In particular, for every $i \in \mathbb{Z}$, there are isomorphisms

$$\begin{aligned} \widehat{H}^i(G, B)^- &\cong \widehat{H}^{i+2}(G, B)^+ \cong \widehat{H}^{i+2}(D, B) \\ \widehat{H}^i(G, B)^+ &\cong \widehat{H}^{i+2}(G, B)^- \cong \widehat{H}^i(D, B) \end{aligned}$$

of abelian groups.

Proof. We start by proving the first isomorphisms for $i \in \mathbb{Z}$ with $i \neq 0, -1$, that is, for standard cohomology and homology. Since $H^i(\Delta, B^G) = H_i(\Delta, B^G) = 0$ by (2.2), using the Hochschild–Serre spectral sequence (see, for instance, [7, Chapter XVI, Section 6]), we deduce that restriction induces isomorphisms $H^i(D, B) \cong H^i(G, B)^\Delta = H^i(G, B)^+$ and $H_i(D, B) \cong H_i(G, B)_\Delta = H_i(G, B)^+$ for $i \geq 0$.

We now consider the case $i = 0$. Restriction induces a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & N_D B & \longrightarrow & H^0(D, B) & \longrightarrow & \widehat{H}^0(D, B) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (N_G B)^+ & \longrightarrow & H^0(G, B)^+ & \longrightarrow & \widehat{H}^0(G, B)^+ \longrightarrow 0. \end{array} \tag{2.3}$$

The bottom row is exact since $N_G B$ is uniquely 2-divisible, hence Δ -cohomologically trivial as shown in (2.2). We showed above that the central vertical arrow is an isomorphism. In particular, the right vertical arrow is surjective. It is also injective since restriction followed by corestriction is multiplication by 2 which is an automorphism of $\widehat{H}^0(D, B)$. Therefore,

$$\widehat{H}^0(G, B)^+ \cong \widehat{H}^0(D, B)$$

as claimed. The proof is similar in degree -1 , by writing $\widehat{H}^{-1}(D, B) = \text{Ker}(N_D : H_0(D, B) \rightarrow N_D B)$ and similarly for G .

Finally, we discuss the Δ -antiequivariance of Tate isomorphisms. Recall that, for any $i \in \mathbb{Z}$, the Tate isomorphism is given by the cup product with a fixed generator χ of $H^2(G, \mathbb{Z})$:

$$\begin{aligned} \widehat{H}^i(G, B) &\longrightarrow \widehat{H}^{i+2}(G, B) \\ x &\longmapsto x \cup \chi. \end{aligned}$$

As in [7, Chapter X, Section 7], we let $\delta \in \Delta$ be the non-trivial element and we denote by c_δ the automorphism induced by δ on G -Tate cohomology of B . Then c_δ is multiplied by -1 on $H^2(G, \mathbb{Z})$: indeed, since δ acts as -1 on G , it also acts as -1 on $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Our claim follows by considering the isomorphism of Δ -modules $\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$ given by the connecting homomorphism of the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

of G -modules with trivial action. Then, by [7, Chapter XII, Section 8, (14)],

$$c_\delta(x \cup \chi) = -(c_\delta x) \cup \chi,$$

which establishes the result. □

REMARK 2.2. The above proposition implies, in particular, that the Tate cohomology of a uniquely 2-divisible D -module is periodic of period 4. Indeed, if B is such a module and $i \in \mathbb{Z}$, we have isomorphisms

$$\widehat{H}^i(D, B) \cong \widehat{H}^i(G, B)^+ \cong \widehat{H}^{i+2}(G, B)^- \cong \widehat{H}^{i+4}(G, B)^+ \cong \widehat{H}^{i+4}(D, B).$$

In fact, one can prove that the cohomology of every D -module is periodic of period 4 (cf. [7, Theorem XII.11.6]).

REMARK 2.3. If B is a uniquely 2-divisible D -module such that $\widehat{H}^j(G, B) = 0$ for some $j \in \mathbb{Z}$, then

$$\widehat{H}^{j+2i}(D, B) = 0 \quad \text{for all } i \in \mathbb{Z}.$$

Indeed, we have seen in the above proposition that $\widehat{H}^{j+2i}(D, B) \subseteq \widehat{H}^{j+2i}(G, B)$. On the other hand, the periodicity of Tate cohomology for the cyclic group G implies that $\widehat{H}^{j+2i}(G, B) \cong \widehat{H}^j(G, B) = 0$.

We now give a description of some cohomology groups of D with values in a D -module B in terms of explicit subquotients of B . We start with the following lemma.

LEMMA 2.4. *Let B be a D -module. Then*

$$I_G B \subseteq B^\Sigma + B^{\Sigma'}.$$

Proof. This is shown in [17, Lemma 3.4], and we recall here the details of the proof. For every $b \in B$, we have

$$(1 - \rho)b = -((1 + \sigma)\rho)b + (1 + \sigma\rho)b.$$

It follows that

$$\begin{aligned} I_G B &= (1 - \rho)B \subseteq ((1 + \sigma)\rho)B + (1 + \sigma\rho)B = (1 + \sigma)B + (1 + \sigma\rho)B \\ &= N_\Sigma B + N_{\Sigma'} B \subseteq B^\Sigma + B^{\Sigma'}. \end{aligned}$$

□

Let B be a D -module. Observe that $B^{\Sigma'} = \rho^t(B^\Sigma)$ for any $t \in \mathbb{Z}$ such that $2t \equiv -1 \pmod{q}$. Indeed, one easily checks that $\rho^t(B^\Sigma) = B^{\rho^t \Sigma \rho^{-t}}$. Now, observing that $\rho^t \sigma \rho^{-t} = \sigma \rho^{-2t} = \sigma \rho$, we deduce that $\rho^t \Sigma \rho^{-t} = \langle \sigma \rho \rangle = \Sigma'$ and therefore $B^{\Sigma'} = \rho^t(B^\Sigma)$. In particular, a generic element $b_1 + b_2 \in B^\Sigma + B^{\Sigma'}$ can be written as

$$b_1 + b_2 = b_1 + \rho^t(b') = b_1 + b' - (1 - \rho^t)b' \in B^\Sigma + I_G B$$

for some $b' \in B^\Sigma$. Using Lemma 2.4, we deduce that

$$B^\Sigma + B^{\Sigma'} = B^\Sigma + I_G B = B^{\Sigma'} + I_G B \tag{2.4}$$

and, in particular, if B is uniquely 2-divisible,

$$(B^\Sigma + B^{\Sigma'})^- = (I_G B)^-, \tag{2.5}$$

since Σ acts trivially on $(B^\Sigma + I_G B)/I_G B$.

LEMMA 2.5. *Let B be a uniquely 2-divisible D -module. There are isomorphisms of abelian groups*

$$\left(B[N_G] \cap (B^\Sigma + B^{\Sigma'}) \right) / I_G B \cong \widehat{H}^{-1}(D, B)$$

and

$$B[N_G] / \left((B^\Sigma + B^{\Sigma'}) \cap B[N_G] \right) \cong H^1(D, B).$$

Proof. Consider the short exact sequence defining $\widehat{H}^{-1}(G, B)$:

$$0 \longrightarrow I_G B \longrightarrow B[N_G] \longrightarrow \widehat{H}^{-1}(G, B) \longrightarrow 0.$$

Since B is uniquely 2-divisible, taking Σ -invariants and using Proposition 2.1, we get an exact sequence

$$0 \longrightarrow I_G B \cap B^\Sigma \longrightarrow B[N_G] \cap B^\Sigma \longrightarrow \widehat{H}^{-1}(D, B) \longrightarrow 0. \tag{2.6}$$

Since $I_G B \subseteq B^\Sigma + B^{\Sigma'}$ by Lemma 2.4, we can consider the quotient $(B[N_G] \cap (B^\Sigma + B^{\Sigma'})) / I_G B$, as well as the map

$$(B[N_G] \cap B^\Sigma) / (I_G B \cap B^\Sigma) \longrightarrow \left(B[N_G] \cap (B^\Sigma + B^{\Sigma'}) \right) / I_G B$$

induced by the inclusion $B[N_G] \cap B^\Sigma \subseteq B[N_G] \cap (B^\Sigma + B^{\Sigma'})$. The above map is clearly injective and is also surjective since

$$B^\Sigma + I_G B = B^\Sigma + B^{\Sigma'}$$

by (2.4). This, together with the exact sequence in (2.6), proves the first isomorphism of the lemma.

For the second isomorphism, note that, by Proposition 2.1, we have an isomorphism of abelian groups:

$$H^1(D, B) \cong \widehat{H}^{-1}(G, B) / \widehat{H}^{-1}(D, B). \quad \square$$

Observe that the proof of Lemma 2.5 actually shows that

$$\begin{aligned} \widehat{H}^{-1}(G, B)^+ &= \left(B[N_G] \cap (B^\Sigma + B^{\Sigma'}) \right) / I_G B \quad \text{and} \\ \widehat{H}^{-1}(G, B)^- &= B[N_G] / \left((B^\Sigma + B^{\Sigma'}) \cap B[N_G] \right). \end{aligned} \tag{2.7}$$

Another consequence of Lemma 2.4 is the following.

LEMMA 2.6. *Let B be a uniquely q -divisible finite D -module. There is a direct-sum decomposition*

$$B/B^D \cong B^G/B^D \oplus (B^\Sigma + B^{\Sigma'})/B^D$$

which implies, upon taking the quotient by B^G/B^D ,

$$B/B^G \cong B^\Sigma/B^D \oplus B^{\Sigma'}/B^D.$$

Proof. We are thankful to the referee for suggesting us the following proof, which simplifies the one in our original version.

One can easily check that there is a relation

$$N_D - N_G - \sum_{\substack{\tilde{\Sigma} < D \\ |\tilde{\Sigma}|=2}} N_{\tilde{\Sigma}} = -q$$

in $\mathbb{Z}[D]$. In particular, since multiplication by q is an automorphism of B , we have

$$B = \left(N_D - N_G - \sum_{\substack{\tilde{\Sigma} < D \\ |\tilde{\Sigma}|=2}} N_{\tilde{\Sigma}} \right) B \subseteq B^G + \sum_{\substack{\tilde{\Sigma} < D \\ |\tilde{\Sigma}|=2}} B^{\tilde{\Sigma}} \subseteq B,$$

so that in fact

$$B = B^G + \sum_{\substack{\tilde{\Sigma} < D \\ |\tilde{\Sigma}|=2}} B^{\tilde{\Sigma}}. \tag{2.8}$$

Now we claim that

$$\sum_{\substack{\tilde{\Sigma} < D \\ |\tilde{\Sigma}|=2}} B^{\tilde{\Sigma}} = B^{\Sigma} + B^{\Sigma'}. \tag{2.9}$$

To see this, it is enough to show that for every subgroup $\tilde{\Sigma} \subset D$ of order 2, we have $B^{\tilde{\Sigma}} \subseteq B^{\Sigma} + B^{\Sigma'}$. Let $\tilde{\Sigma} = \langle \sigma \rho^i \rangle$ where either $i = 2j$ or $i = 2j + 1$ for some $j \in \mathbb{Z}$ and let $b \in B^{\tilde{\Sigma}}$. Then $\rho^j b \in B^{\rho^j \tilde{\Sigma} \rho^{-j}}$ and $\rho^j \tilde{\Sigma} \rho^{-j} = \langle \sigma \rho^{i-2j} \rangle$ are either Σ or Σ' , according as i is even or odd. Thus,

$$b = (1 - \rho^j)b + \rho^j b \in I_G B + (B^{\Sigma} + B^{\Sigma'}) = B^{\Sigma} + B^{\Sigma'}$$

by Lemma 2.4. Therefore, (2.9) holds and (2.8) becomes

$$B = B^G + (B^{\Sigma} + B^{\Sigma'}).$$

To show that this sum is direct modulo B^D , let $b \in B^G \cap (B^{\Sigma} + B^{\Sigma'})$, so that $b = b_1 + b_2$ with $b_1 \in B^{\Sigma}$ and $b_2 \in B^{\Sigma'}$. Then

$$b = \frac{1}{q} N_G b = \frac{1}{q} N_G b_1 + \frac{1}{q} N_G b_2,$$

which implies $b \in B^D$ since $N_G b_i \in B^D$ for $i = 1, 2$. □

To use the above results in the next sections, we systematically tensor the module of interest with $\mathbb{Z}[\frac{1}{2}]$. When no ambiguity is possible, if $f: B \rightarrow B'$ is a homomorphism of abelian groups, we will still denote by f the map $f[\frac{1}{2}]: B[\frac{1}{2}] \rightarrow B'[\frac{1}{2}]$.

We constantly use that, for every D -module B and every subgroup $H \subseteq D$, there are isomorphisms

$$\widehat{H}^i(H, B[\frac{1}{2}]) \cong \widehat{H}^i(H, B)[\frac{1}{2}]$$

for all $i \in \mathbb{Z}$. This is quite straightforward, but we sketch an argument, writing

$$\Lambda = \mathbb{Z}[H] \quad \text{and} \quad \Lambda' = \mathbb{Z}[H][\frac{1}{2}].$$

The fact that $\mathbb{Z}[\frac{1}{2}]$ is \mathbb{Z} -flat implies that $H^0(H, B)[\frac{1}{2}] = \text{Hom}_\Lambda(\mathbb{Z}, B)[\frac{1}{2}]$ coincides with $\text{Hom}_{\Lambda'}(\mathbb{Z}[\frac{1}{2}], B[\frac{1}{2}])$. On the other hand, a Λ' -linear homomorphism from $\mathbb{Z}[\frac{1}{2}]$ to $B[\frac{1}{2}]$ is uniquely determined by its value on 1, as is every Λ -homomorphism from \mathbb{Z} to $B[\frac{1}{2}]$, showing that $\text{Hom}_{\Lambda'}(\mathbb{Z}[\frac{1}{2}], B[\frac{1}{2}]) = \text{Hom}_\Lambda(\mathbb{Z}, B[\frac{1}{2}]) = H^0(H, B[\frac{1}{2}])$. Therefore, the right-derived functors of the functor $\mathcal{F}_1: B \mapsto H^0(H, B[\frac{1}{2}])$ and of $\mathcal{F}_2: B \mapsto H^0(H, B)[\frac{1}{2}]$ coincide. Those of the first are $R^i\mathcal{F}_1(B) = H^i(H, B[\frac{1}{2}])$ and those of the second are $R^i\mathcal{F}_2(B) = H^i(H, B)[\frac{1}{2}]$, for $i \geq 0$: this follows from a computation with the Grothendieck spectral sequence of a composition of functors, using that $-\otimes\mathbb{Z}[\frac{1}{2}]$ is acyclic by assumption. It follows that $H^i(H, B[\frac{1}{2}])$ and $H^i(H, B)[\frac{1}{2}]$ are isomorphic. A similar argument is valid for H -homology. The remaining cases of Tate cohomology in degrees $-1, 0$ can be treated directly by writing the Tate cohomology groups as a kernel and a cokernel, respectively (cf. [7, Chapter XII, Section 2]).

For an abelian group B and a natural number n , we set $B(n) = \{b \in B : nb = 0\}$.

LEMMA 2.7. *Let B be D -module such that $B(q) = B(q)^G$. Then the inclusion $B(q) \subseteq B$ induces equalities*

$$\text{Ker}(\widehat{H}^{-1}(G, B(q)) \longrightarrow \widehat{H}^{-1}(G, B)) = I_G B \cap B(q)^G = I_G B \cap B^G.$$

If, moreover, B is uniquely 2-divisible, then

$$\text{Ker}(\widehat{H}^{-1}(D, B(q)) \longrightarrow \widehat{H}^{-1}(D, B)) = I_G B \cap B(q)^D = I_G B \cap B^D.$$

Proof. Since $B(q)$ has trivial action of G by assumption, $I_G(B(q)) = 0$ and N_G is multiplication by q on $B(q)$ and so is the trivial map. Hence, $\widehat{H}^{-1}(G, B(q)) = B(q)$ and we obtain the first equality of the statement since

$$\begin{aligned} \text{Ker}(\widehat{H}^{-1}(G, B(q)) \longrightarrow \widehat{H}^{-1}(G, B)) &= \text{Ker}(B(q) \longrightarrow B[N_G]/I_G B) = I_G B \cap B(q) \\ &= I_G B \cap B(q)^G. \end{aligned}$$

As for the second, there is an obvious inclusion $I_G B \cap B(q)^G \subseteq I_G B \cap B^G$. To prove the reverse inclusion, it is enough to observe that every $x \in I_G B \cap B^G$ satisfies $qx = N_G x$ (because $x \in B^G$) and also $N_G x = 0$ (since $x \in I_G B \subseteq B[N_G]$). Thus we have $x \in I_G B \cap B^G \cap B(q) = I_G B \cap B(q)^G$.

When B is uniquely 2-divisible, by taking plus parts in the above equalities and applying Proposition 2.1, we obtain the second claim. □

We conclude this section with two lemmas which give some relations between the cohomology of D and that of its subgroups, without the assumption that the underlying module is uniquely 2-divisible.

LEMMA 2.8. *Let $H \subseteq D$ be a subgroup, let B be an H -module, and let $j \in \mathbb{Z}$ be an integer. Suppose that, for every prime p , $\widehat{H}^j(H_p, B) = 0$, where H_p is a p -Sylow subgroup of H . Then $\widehat{H}^i(H, B) = 0$ for every $i \equiv j \pmod{2}$.*

Proof. Under our assumptions, for every prime p , $\widehat{H}^i(H_p, B)$ is trivial for every $i \equiv j \pmod{2}$ since p -Sylow subgroups of H are cyclic and the Tate cohomology of cyclic groups is periodic of period 2. Since the restriction map

$$\widehat{H}^i(H, B) \longrightarrow \widehat{H}^i(H_p, B)$$

is injective on the p -primary component of $\widehat{H}^i(H, B)$, we deduce that $\widehat{H}^i(H, B) = 0$ for every $i \equiv j \pmod{2}$. □

LEMMA 2.9. *Let B a D -module. Then, for every $i \in \mathbb{Z}$, the restriction*

$$\text{res}_\Sigma^D : \widehat{H}^i(D, B) \longrightarrow \widehat{H}^i(\Sigma, B)$$

maps the 2-primary component of $\widehat{H}^i(D, B)$ isomorphically onto $\widehat{H}^i(\Sigma, B)$.

Proof. As observed in the proof of Lemma 2.8, we only need to show surjectivity. The image of the 2-component is the subset of stable elements of $\widehat{H}^i(\Sigma, B)$ (see [7, Chapter XII, Theorem 10.1]). Recall that an element $a \in \widehat{H}^i(\Sigma, B)$ is called stable if, for every $\tau \in D$,

$$\text{res}_{\tau\Sigma\tau^{-1}\cap\Sigma}^\Sigma(a) = \text{res}_{\tau\Sigma\tau^{-1}\cap\Sigma}^{\tau\Sigma\tau^{-1}} c_\tau(a),$$

where c_τ denotes the map $\widehat{H}^i(\Sigma, B) \rightarrow \widehat{H}^i(\tau\Sigma\tau^{-1}, B)$ induced by conjugation by τ . When $\tau \notin \Sigma$, then $\tau\Sigma\tau^{-1} \cap \Sigma$ is trivial and the above equality holds for every $a \in \widehat{H}^i(\Sigma, B)$. When $\tau \in \Sigma$, then $\tau\Sigma\tau^{-1} = \Sigma$ and the two restriction maps appearing in the above equality are in fact the identity map. The same holds for c_τ (see [7, Chapter XII, Section 8, (5)]), proving that every element in $\widehat{H}^i(\Sigma, B)$ is stable. □

3. Class number formula. We now come to the proof of the odd part of the class number formula. Still under the notation introduced in the previous section, we consider the following arithmetic setting. Let k be a number field and let L/k be a Galois extension whose Galois group is isomorphic to D . We fix such an isomorphism and we simply write $D = \text{Gal}(L/k)$. Let F/k be the subextension of L/k fixed by G and let K/k (resp. K'/k) be the subextension of L/k fixed by Σ (resp. Σ'). In particular, F/k is quadratic with Galois group $\Delta := \text{Gal}(F/k)$.

We begin by introducing a four-term exact sequence involving the class groups of L and K . By looking at the orders of groups in this sequence, we already get a formula involving the odd components of class numbers of L and K . The rest of the section is devoted to expressing the remaining factors in terms of the odd components of the class numbers of F and k and the orders of the cohomology group of units of L . As a corollary of the formula, using the value of the Herbrand quotient of units for the extension L/F , we easily obtain bounds on the ratio of class numbers of subfields of L .

NOTATION. For a number field M , we write Cl_M for the class group of M . For an extension of number fields M_2/M_1 , $\iota_{M_2/M_1} : Cl_{M_1} \rightarrow Cl_{M_2}$ and $N_{M_2/M_1} : Cl_{M_2} \rightarrow Cl_{M_1}$ denote the map induced by extending ideals from M_1 to M_2 and by taking the norm of ideals from M_2 to M_1 , respectively.

Consider the exact sequence

$$1 \rightarrow \text{Ker } \eta \longrightarrow Cl_K \oplus Cl_{K'} \xrightarrow{\eta} Cl_L \longrightarrow Cl_L / \text{Im } \eta \rightarrow 1, \tag{3.1}$$

where the map η is defined via the formula

$$\eta(c, c') = \iota_{L/K}(c)\iota_{L/K'}(c') \quad \text{for } c \in Cl_K, c' \in Cl_{K'}. \tag{3.2}$$

Tensoring with $\mathbb{Z}[\frac{1}{2}]$, we immediately obtain the formula

$$|Cl_L[\frac{1}{2}]| = |Cl_K[\frac{1}{2}]|^2 \frac{(Cl_L[\frac{1}{2}] : \text{Im } \eta[\frac{1}{2}])}{|\text{Ker } \eta[\frac{1}{2}]|}. \tag{3.3}$$

Observe also that the map $\iota_{L/K}[\frac{1}{2}] : Cl_K[\frac{1}{2}] \rightarrow Cl_L[\frac{1}{2}]$ is injective, since $N_{L/K} \circ \iota_{L/K}$ is multiplied by $2 = [L : K]$ on Cl_K .

REMARK 3.1. Let B be an abelian group and $B' \subseteq B$ a subgroup of B . Let $f : B \rightarrow C$ be a homomorphism of abelian groups. Then there is an exact sequence

$$0 \longrightarrow \text{Ker } f / (\text{Ker } f \cap B') \longrightarrow B/B' \longrightarrow f(B)/f(B') \longrightarrow 0.$$

It follows in particular that

$$(B : B') = (f(B) : f(B')) \cdot (\text{Ker } f : \text{Ker } f \cap B'), \tag{3.4}$$

meaning that if two of the above indices are finite, so is the third and the above equality holds.

For a group H and a H -module B , we denote by $\widehat{h}^i(H, B)$ (resp. $h^i(H, B)$) the order of $\widehat{H}^i(H, B)$ (resp. the order of $H^i(H, B)$), whenever this is defined.

PROPOSITION 3.2. *We have an equality*

$$(Cl_L[\frac{1}{2}] : \text{Im } \eta[\frac{1}{2}]) = \frac{|Cl_L[\frac{1}{2}]^G|}{\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|}$$

and an isomorphism

$$\text{Ker } \eta[\frac{1}{2}] \cong H^0(D, Cl_L[\frac{1}{2}]).$$

In particular,

$$|Cl_L[\frac{1}{2}]| = |Cl_K[\frac{1}{2}]|^2 \frac{|Cl_L[\frac{1}{2}]^G|}{h^0(D, Cl_L[\frac{1}{2}]) \widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|}.$$

Proof. Observe that, using equation (3.4) applied to $f = N_G$, $B = Cl_L$, $B' = \text{Im } \eta$, we get

$$(Cl_L : \text{Im } \eta) = (N_G Cl_L : N_G(\text{Im } \eta)) \cdot (Cl_L[N_G] : \text{Im } \eta \cap Cl_L[N_G]).$$

Now observe that

$$\text{Im } \eta = \iota_{L/K}(Cl_K)\iota_{L/K'}(Cl_{K'})$$

and

$$(Cl_L[\frac{1}{2}])^\Sigma = \iota_{L/K}(Cl_K[\frac{1}{2}]), \quad (Cl_L[\frac{1}{2}])^{\Sigma'} = \iota_{L/K'}(Cl_{K'}[\frac{1}{2}]), \tag{3.5}$$

so that

$$\text{Im } \eta[\frac{1}{2}] = Cl_L[\frac{1}{2}]^\Sigma Cl_L[\frac{1}{2}]^{\Sigma'}.$$

Therefore, using Lemma 2.5, we deduce that

$$(Cl_L[\frac{1}{2}] : \text{Im } \eta[\frac{1}{2}]) = (N_G Cl_L[\frac{1}{2}] : N_D Cl_L[\frac{1}{2}]) \cdot h^1(D, Cl_L[\frac{1}{2}]),$$

because

$$N_D Cl_L[\frac{1}{2}] = N_G(N_\Sigma Cl_L[\frac{1}{2}]) = N_G(Cl_L[\frac{1}{2}]^\Sigma) = N_G(\iota_{L/K}(Cl_K[\frac{1}{2}])) = N_G(\iota_{L/K'}(Cl_{K'}[\frac{1}{2}])),$$

since $\widehat{H}^0(\Sigma, Cl_L[\frac{1}{2}]) = 0$. Now observe that

$$|N_G Cl_L[\frac{1}{2}]| = \frac{|Cl_L[\frac{1}{2}]^G|}{\widehat{h}^0(G, Cl_L[\frac{1}{2}])}.$$

The first equality of the proposition follows, since

$$\frac{h^1(D, Cl_L[\frac{1}{2}])}{h^1(G, Cl_L[\frac{1}{2}])} = \frac{1}{\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}])}$$

by Proposition 2.1 and because the finiteness of $Cl_L[\frac{1}{2}]$ implies $\widehat{h}^0(G, Cl_L[\frac{1}{2}]) = h^1(G, Cl_L[\frac{1}{2}])$.

As for the second statement of the proposition, let θ be the map

$$\theta: \text{Ker } \eta[\frac{1}{2}] \longrightarrow H^0(D, Cl_L[\frac{1}{2}])$$

defined by $\theta(c, c') = \iota_{L/K}(c)$. Since $\iota_{L/K}(c) = \iota_{L/K'}(c')^{-1}$ in Cl_L by definition of η , both Σ and Σ' fix $\iota_{L/K}(c)$, so the map θ takes values in $H^0(D, Cl_L)$. We claim that it is an isomorphism. First, θ is injective because $\iota_{L/K}: Cl_K[\frac{1}{2}] \rightarrow Cl_L[\frac{1}{2}]$ is injective, as observed after equation (3.3). To check surjectivity, note that, since every $b \in H^0(D, Cl_L[\frac{1}{2}])$ is fixed by both Σ and Σ' , we can write such b as $b = \iota_{L/K}(c) = \iota_{L/K'}(c')$ for some $c \in Cl_K[\frac{1}{2}]$, $c' \in Cl_{K'}[\frac{1}{2}]$, using equation (3.5). In particular, $(c, (c')^{-1}) \in \text{Ker } \eta[\frac{1}{2}]$ and $b = \theta(c, (c')^{-1})$, which shows the claimed isomorphism and hence the second statement of the proposition.

The last formula of the proposition comes from equation (3.3) using the first two assertions. □

We now want to translate cohomology groups of $Cl_L[\frac{1}{2}]$ into cohomology groups of $\mathcal{O}_L^\times[\frac{1}{2}]$. To achieve this we make intensive use of the following commutative diagram of Galois modules with exact rows and columns:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathcal{O}_M^\times & \longrightarrow & M^\times & \longrightarrow & P_M \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathcal{U}_M & \longrightarrow & \mathbb{A}_M^\times & \longrightarrow & I_M \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathcal{Q}_M & \longrightarrow & \mathcal{C}_M & \longrightarrow & Cl_M \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
 \end{array} \tag{3.6}$$

Here, we use the following notation for a number field M : \mathcal{O}_M is the ring of integers, I_M is the group of fractional ideals, P_M is the group of principal ideals, \mathbb{A}_M^\times is the idèles group, \mathcal{C}_M is the idèles class group, \mathcal{U}_M is the group of idèles of valuation 0 at every finite place and \mathcal{Q}_M is defined by the exactness of the diagram. We refer the reader to [21] for the class field theory results that we use.

PROPOSITION 3.3. *Let $H \subseteq D$ be any subgroup and j be an odd integer. Then*

$$\widehat{H}^j(H, I_L) = \widehat{H}^j(H, C_L) = \widehat{H}^j(H, L^\times) = \widehat{H}^j(H, \mathbb{A}_L^\times) = 0.$$

Proof. By Lemma 2.8, we only need to prove that $H^1(H, B) = 0$ where B is any of the modules $I_L, C_L, L^\times, \mathbb{A}_L^\times$ and H is cyclic. This is Hilbert’s Theorem 90 when $B = L^\times, \mathbb{A}_L^\times$ and follows from [21, Theorem 9.1] when $B = C_L$. For $B = I_L$, let $M \subseteq L$ be the subfield of L fixed by H . There is an H -equivariant isomorphism

$$I_L \cong \bigoplus_{\mathfrak{l} \subseteq \mathcal{O}_M} \mathbb{Z}[H/H(\mathfrak{L})], \tag{3.7}$$

where \mathfrak{l} runs over the primes of M and $H(\mathfrak{L})$ denotes the decomposition group in L/M of a fixed prime \mathfrak{L} of L above \mathfrak{l} . Hence, by Shapiro’s lemma,

$$H^1(H, I_L) \cong \bigoplus_{\mathfrak{l} \subseteq \mathcal{O}_M} H^1(H(\mathfrak{L}), \mathbb{Z}).$$

The statement follows, since $H^1(H(\mathfrak{L}), \mathbb{Z}) = \text{Hom}(H(\mathfrak{L}), \mathbb{Z}) = 0$. □

We can now move towards the proof of our main result, contained in Theorem 3.14.

PROPOSITION 3.4. *We have isomorphisms*

$$\widehat{H}^0(D, Cl_L[\frac{1}{2}]) \cong H^1(D, Q_L[\frac{1}{2}]) \quad \text{and} \quad \widehat{H}^{-1}(D, Cl_L[\frac{1}{2}]) \cong \widehat{H}^0(D, Q_L[\frac{1}{2}]).$$

Proof. From the long exact D -Tate cohomology sequence of the bottom row of Diagram (3.6), we get an exact sequence

$$\widehat{H}^{-1}(D, Cl_L) \longrightarrow \widehat{H}^0(D, Q_L) \longrightarrow \widehat{H}^0(D, C_L) \longrightarrow \widehat{H}^0(D, Cl_L) \longrightarrow H^1(D, Q_L). \tag{3.8}$$

The rightmost map is surjective and the leftmost map is injective thanks to Proposition 3.3. Tensoring the sequence with $\mathbb{Z}[\frac{1}{2}]$, the middle term of equation (3.8) becomes trivial, since class field theory gives an isomorphism

$$\widehat{H}^0(D, C_L) \xrightarrow{\cong} D^{ab} \cong \mathbb{Z}/2\mathbb{Z}. \tag{3.9} \quad \square$$

The following proposition is the dihedral analogue of Chevalley’s Ambiguous Class Number Formula (which holds for cyclic groups). Our proof is inspired by the cohomological proof of Chevalley’s formula (see [13, Lemma 4.1]).

PROPOSITION 3.5. *Let $H \subseteq D$ be a subgroup and let M be the subfield of L fixed by H . There is a long exact sequence*

$$\begin{aligned} 0 \longrightarrow \text{Ker } \iota_{L/M} \longrightarrow H^1(H, \mathcal{O}_L^\times) \longrightarrow H^1(H, \mathcal{U}_L) \longrightarrow H^0(H, Cl_L)/\iota_{L/M}(Cl_M) \\ \longrightarrow H^1(H, P_L) \longrightarrow 0. \end{aligned}$$

In particular,

$$\frac{h^1(H, \mathcal{U}_L[\frac{1}{2}])h^1(H, P_L[\frac{1}{2}])}{h^0(H, Cl_L[\frac{1}{2}])} = \frac{h^1(H, \mathcal{O}_L^\times[\frac{1}{2}])}{|Cl_M[\frac{1}{2}]|}.$$

Proof. From the rightmost column of Diagram (3.6), we get a commutative diagram with exact rows

$$\begin{array}{ccccccc}
 0 & \longrightarrow & P_M & \longrightarrow & I_M & \longrightarrow & Cl_M \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \iota_{L/M} \\
 0 & \longrightarrow & H^0(H, P_L) & \longrightarrow & H^0(H, I_L) & \longrightarrow & H^0(H, Cl_L) \longrightarrow H^1(H, P_L) \longrightarrow 0.
 \end{array}$$

The exactness of the bottom row follows from Proposition 3.3. Applying the snake lemma, we get the exact sequence

$$\begin{aligned}
 0 \longrightarrow \text{Ker } \iota_{L/M} \longrightarrow H^0(H, P_L)/P_M \longrightarrow H^0(H, I_L)/I_M \longrightarrow \\
 \longrightarrow H^0(H, Cl_L)/\iota_{L/M}(Cl_M) \longrightarrow H^1(H, P_L) \longrightarrow 0.
 \end{aligned} \tag{3.10}$$

Now, from the upper row of Diagram (3.6), we get the exact sequence

$$0 \longrightarrow M^\times / \mathcal{O}_M^\times = P_M \longrightarrow H^0(H, P_L) \longrightarrow H^1(H, \mathcal{O}_L^\times) \longrightarrow 0.$$

We thus obtain an isomorphism

$$H^0(H, P_L)/P_M \cong H^1(H, \mathcal{O}_L^\times). \tag{3.11}$$

As for the middle term of equation (3.10), consider the central row of Diagram (3.6). Using that $H^1(H, \mathbb{A}_L^\times) = 0$ by Proposition 3.3, we get an exact sequence

$$0 \longrightarrow M^\times / \mathcal{U}_M = I_M \longrightarrow H^0(H, I_L) \longrightarrow H^1(H, \mathcal{U}_L) \longrightarrow 0.$$

This gives an isomorphism

$$H^0(H, I_L)/I_M \cong H^1(H, \mathcal{U}_L). \tag{3.12}$$

Plugging (3.11) and (3.12) in the exact sequence (3.10), we obtain the exact sequence of the statement. The formula for the orders follows since

$$|\text{Ker } \iota_{L/M}| \cdot |\iota_{L/M}(Cl_M)| = |Cl_M|. \quad \square$$

REMARK 3.6. Observe that the norm $N_{L/k} : C_L[\frac{1}{2}] \rightarrow C_k[\frac{1}{2}]$ is surjective (for this remark only, we extend the notation $N_{L/k}$ also to denote the corresponding morphism on idèle class groups and similarly for $\iota_{L/k}$). Indeed, Hilbert’s Theorem 90 implies that $C_L^D = \iota_{L/k}(C_k)$ and, in particular, $\iota_{L/k} : C_k \rightarrow C_L$ is injective. Since $N_D C_L = \iota_{L/k}(N_{L/k}(C_L))$, we deduce that

$$\widehat{H}^0(D, C_L) = C_L^D / N_D C_L = \iota_{L/k}(C_k) / \iota_{L/k}(N_{L/k}(C_L)) \cong C_k / N_{L/k}(C_L).$$

In particular, since $\widehat{H}^0(D, C_L[\frac{1}{2}]) = 0$ by class field theory (see (3.9)), we find that $C_k[\frac{1}{2}] = N_{L/k}(C_L[\frac{1}{2}])$. Looking at the commutative diagram with exact rows

$$\begin{array}{ccccc}
 C_L & \longrightarrow & Cl_L & \longrightarrow & 0 \\
 \downarrow N_{L/k} & & \downarrow N_{L/k} & & \\
 C_k & \longrightarrow & Cl_k & \longrightarrow & 0,
 \end{array}$$

we deduce that $N_{L/k}: Cl_L[\frac{1}{2}] \rightarrow Cl_k[\frac{1}{2}]$ must be surjective too. Moreover, since $N_D Cl_L = \iota_{L/k}(N_{L/k}(Cl_L))$, we find that

$$N_D Cl_L[\frac{1}{2}] = \iota_{L/k}(Cl_k[\frac{1}{2}]) \tag{3.13}$$

and in particular,

$$\widehat{H}^0(D, Cl_L[\frac{1}{2}]) = H^0(D, Cl_L[\frac{1}{2}]) / \iota_{L/k}(Cl_k[\frac{1}{2}]).$$

PROPOSITION 3.7. *Let $H \subseteq D$ be any subgroup and let M be the subfield of L fixed by H . There is an exact sequence*

$$0 \longrightarrow \widehat{H}^{-1}(H, P_L) \longrightarrow \widehat{H}^0(H, \mathcal{O}_L^\times) \longrightarrow \widehat{H}^0(H, \mathcal{U}_L) \longrightarrow \widehat{H}^0(H, \mathcal{Q}_L) \longrightarrow \text{Ker } \iota_{L/M} \longrightarrow 0.$$

In particular,

$$\frac{\widehat{h}^0(D, \mathcal{U}_L[\frac{1}{2}]) \widehat{h}^{-1}(D, P_L[\frac{1}{2}])}{\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|} = \frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{|Cl_k[\frac{1}{2}]|}.$$

Proof. From the long exact sequence of Tate cohomology of the left-hand column of Diagram (3.6), we get an exact sequence

$$\widehat{H}^0(H, \mathcal{O}_L^\times) \longrightarrow \widehat{H}^0(H, \mathcal{U}_L) \longrightarrow \widehat{H}^0(H, \mathcal{Q}_L) \longrightarrow H^1(H, \mathcal{O}_L^\times) \longrightarrow H^1(H, \mathcal{U}_L).$$

By Proposition 3.5, we know that

$$\text{Ker}(H^1(H, \mathcal{O}_L^\times) \rightarrow H^1(H, \mathcal{U}_L)) = \text{Ker}(\iota_{L/M}).$$

Now observe that

$$\text{Ker}(\widehat{H}^0(H, \mathcal{O}_L^\times) \rightarrow \widehat{H}^0(H, \mathcal{U}_L)) = \text{Ker}(\widehat{H}^0(H, \mathcal{O}_L^\times) \rightarrow \widehat{H}^0(H, L^\times)). \tag{3.14}$$

This follows from the commutative diagram

$$\begin{array}{ccc} \widehat{H}^0(H, \mathcal{O}_L^\times) & \longrightarrow & \widehat{H}^0(H, L^\times) \\ \downarrow & & \downarrow \\ \widehat{H}^0(H, \mathcal{U}_L) & \hookrightarrow & \widehat{H}^0(H, \mathbb{A}_L^\times), \end{array}$$

where the injectivity of bottom horizontal and right vertical arrows follow from Proposition 3.3. The exact sequence of the statement follows since

$$\text{Ker}(\widehat{H}^0(H, \mathcal{O}_L^\times) \rightarrow \widehat{H}^0(H, L^\times)) = \widehat{H}^{-1}(H, P_L)$$

by Proposition 3.3. The last assertion follows by Proposition 3.4 and equation (3.13). \square

REMARK 3.8. Concerning the cokernel of $\iota_{L/M}$, similar techniques as in the above proof allow to give a cohomological interpretation. Taking H -cohomology of the bottom row of Diagram (3.6) and recalling that $H^1(H, \mathcal{C}_L) = 0$, we get a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{Q}_M & \longrightarrow & \mathcal{C}_M & \longrightarrow & Cl_M \longrightarrow 0 \\ & & \downarrow & & \parallel & & \downarrow \iota_{L/M} \\ 0 & \longrightarrow & \mathcal{Q}_L^H & \longrightarrow & \mathcal{C}_L^H & \longrightarrow & Cl_L^H \longrightarrow H^1(H, \mathcal{Q}_L) \longrightarrow 0. \end{array}$$

Applying the snake lemma to the above diagram, we obtain an isomorphism

$$\text{Coker } \iota_{L/M} \cong H^1(H, Q_L), \tag{3.15}$$

which will be useful when considering the 2-part of our main result.

We now give an explicit description of the D -cohomology of \mathcal{U}_L , using local class field theory. We need the following notation.

NOTATION. If M is a subfield of L , we denote by $T(L/M)$ the set of primes in M which ramify in L/M . We also write $T(L/k) = T_s(L/k) \amalg T_r(L/k) \amalg T_i(L/k)$ where the sets $T_s(L/k)$, $T_r(L/k)$, and $T_i(L/k)$ contain the primes in $T(L/k)$ which, respectively, split, ramify, and remain inert in the subextension F/k . For each prime \mathfrak{l} of k , we denote by $e_{\mathfrak{l}}$ and $f_{\mathfrak{l}}$ its ramification index and inertia degree, respectively, in L/k . For a prime \mathfrak{L} of L , we denote by $D(\mathfrak{L})$ the decomposition group of \mathfrak{L} in L/k . Given a prime \mathfrak{r} of $M \subseteq L$, we use the notation $\mathcal{O}_{M,\mathfrak{r}}^\times$ instead of $\mathcal{O}_{M_\tau}^\times$ to denote the units of the local field M_τ , in order to lighten typography.

We start with a lemma describing the cohomology of local units.

LEMMA 3.9. *Let $\mathfrak{l} \in T(L/k)$ be a prime and let $\mathfrak{L} \subseteq \mathcal{O}_L$ be a prime in L above \mathfrak{l} .*

- (a) *If $\mathfrak{l} \in T_i(L/k)$, then $f_{\mathfrak{l}} = 2$ and $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) = 0$.*
- (b) *If $\mathfrak{l} \in T_r(L/k)$, then $f_{\mathfrak{l}} = 1$ and $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/2$.*
- (c) *If $\mathfrak{l} \in T_s(L/k)$, then $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/e_{\mathfrak{l}}$.*

Moreover, for any $\mathfrak{l} \in T(L/k)$, we have $H^1(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/e_{\mathfrak{l}}$.

Proof. Consider the following diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{O}_{L,\mathfrak{L}}^\times & \longrightarrow & L_{\mathfrak{L}}^\times & \xrightarrow{v_{\mathfrak{L}}} & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \uparrow f_{\mathfrak{l}} \\ 0 & \longrightarrow & \mathcal{O}_{k,\mathfrak{l}}^\times & \longrightarrow & k_{\mathfrak{l}}^\times & \xrightarrow{v_{\mathfrak{l}}} & \mathbb{Z} \longrightarrow 0, \end{array}$$

where the left and central vertical maps are the norms and $v_{\mathfrak{l}}$ and $v_{\mathfrak{L}}$ are the \mathfrak{l} -adic and the \mathfrak{L} -adic valuation, respectively. The snake lemma, together with local class field theory, gives an exact sequence

$$0 \longrightarrow \widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \longrightarrow D(\mathfrak{L})^{\text{ab}} \longrightarrow \mathbb{Z}/f_{\mathfrak{l}} \longrightarrow 0.$$

If $\mathfrak{l} \in T_i(L/k) \cup T_r(L/k)$, then $D(\mathfrak{L})$ has order divisible by 2 so it must be dihedral or cyclic of order 2. In both cases, $D(\mathfrak{L})^{\text{ab}} \cong \mathbb{Z}/2$ and therefore $f_{\mathfrak{l}}$ divides 2, by the above exact sequence. When $\mathfrak{l} \in T_i(L/k)$, we must have $f_{\mathfrak{l}} = 2$ and $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) = 0$. When $\mathfrak{l} \in T_r(L/k)$, we deduce $f_{\mathfrak{l}} = 1$, because otherwise $f_{\mathfrak{l}}e_{\mathfrak{l}} = |D(\mathfrak{L})|$ would be divisible by 4 and this is absurd: so $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/2$. Finally, if $\mathfrak{l} \in T_s(L/k)$, then $D(\mathfrak{L})^{\text{ab}} = D(\mathfrak{L})$ is cyclic and, since $f_{\mathfrak{l}}e_{\mathfrak{l}} = |D(\mathfrak{L})|$, we deduce that $\widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/e_{\mathfrak{l}}$.

To prove the assertion on H^1 , apply the snake lemma to the commutative diagram with exact rows

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathcal{O}_{k,\mathfrak{l}}^\times & \longrightarrow & k_{\mathfrak{l}}^\times & \xrightarrow{v_{\mathfrak{l}}} & \mathbb{Z} \longrightarrow 0 \\
 & & \parallel & & \parallel & & \downarrow \scriptstyle -e_{\mathfrak{l}} \\
 0 & \longrightarrow & (\mathcal{O}_{L,\mathfrak{L}}^\times)^{D(\mathfrak{L})} & \longrightarrow & (L_{\mathfrak{L}}^\times)^{D(\mathfrak{L})} & \xrightarrow{v_{\mathfrak{L}}} & \mathbb{Z} \longrightarrow H^1(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \longrightarrow H^1(D(\mathfrak{L}), L_{\mathfrak{L}}^\times) = 0
 \end{array}$$

to deduce an isomorphism

$$H^1(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/e_{\mathfrak{l}}. \quad \square$$

PROPOSITION 3.10. *With the notation introduced before Lemma 3.9, there are isomorphisms*

$$\widehat{H}^0(D, \mathcal{U}_L) \cong \bigoplus_{\mathfrak{l} \in T_s(L/k)} (\mathbb{Z}/e_{\mathfrak{l}}) \oplus \bigoplus_{\mathfrak{l} \in T_r(L/k)} (\mathbb{Z}/2)$$

and

$$H^1(D, \mathcal{U}_L) \cong \bigoplus_{\mathfrak{l} \in T_s(L/k)} (\mathbb{Z}/e_{\mathfrak{l}}) \oplus \bigoplus_{\mathfrak{l} \in T_l(L/k)} (\mathbb{Z}/e_{\mathfrak{l}}) \oplus \bigoplus_{\mathfrak{l} \in T_r(L/k)} (\mathbb{Z}/e_{\mathfrak{l}}).$$

Proof. For every prime \mathfrak{l} of k , we fix a prime $\mathfrak{L}|\mathfrak{l}$ in L . By combining [21, Proposition 7.2] with the fact that local units are cohomologically trivial in unramified extension (see [20, Chapter 1, Proposition 1]), we find

$$\widehat{H}^i(D, \mathcal{U}_L) \cong \bigoplus_{\mathfrak{l} \subseteq \mathcal{O}_k} \widehat{H}^i(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \bigoplus_{\mathfrak{l} \in T(L/k)} \widehat{H}^i(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \quad \text{for all } i \in \mathbb{Z}. \quad (3.16)$$

The proposition follows from Lemma 3.9. □

Recall that, by Proposition 2.1, we have an isomorphism of Δ -modules

$$H^1(G, \mathcal{U}_L[\frac{1}{2}]) \cong H^1(D, \mathcal{U}_L[\frac{1}{2}]) \oplus \widehat{H}^{-1}(D, \mathcal{U}_L[\frac{1}{2}]).$$

The following corollary gives another decomposition of $H^1(G, \mathcal{U}_L[\frac{1}{2}])$, only as abelian groups, which turns out to be more useful than the above in the proof of Theorem 3.14.

COROLLARY 3.11. *There is an isomorphism of abelian groups:*

$$H^1(G, \mathcal{U}_L[\frac{1}{2}]) \cong H^1(D, \mathcal{U}_L[\frac{1}{2}]) \oplus \widehat{H}^0(D, \mathcal{U}_L[\frac{1}{2}]).$$

Proof. The same arguments leading to (3.16) give an isomorphism

$$H^1(G, \mathcal{U}_L) \cong \bigoplus_{\mathfrak{l} \subseteq \mathcal{O}_F} H^1(G(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times)$$

where, for each prime \mathfrak{l} in F , we have fixed a prime \mathfrak{L} in L above \mathfrak{l} . Therefore, it is enough to show that, for each prime \mathfrak{l} of k ,

$$\bigoplus_{\mathfrak{l}|\mathfrak{l}} H^1(G(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times[\frac{1}{2}]) \cong H^1(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times[\frac{1}{2}]) \oplus \widehat{H}^0(D(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times[\frac{1}{2}]). \quad (3.17)$$

Arguing in a similar way as we did in the final part of the proof of Lemma 3.9, we get an isomorphism

$$H^1(G(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times) \cong \mathbb{Z}/e_{\mathfrak{l}},$$

where $e_{\tilde{l}}$ is the ramification index of \tilde{l} in L/F . Now if $\mathfrak{l} \in T_s(L/k) \cup T_i(L/k)$, then $e_{\tilde{l}} = e_{\mathfrak{l}}$, while, if $\mathfrak{l} \in T_r(L/k)$, then $e_{\tilde{l}} = e_{\mathfrak{l}}/2$. Thus

$$\bigoplus_{\tilde{l}|\mathfrak{l}} H^1(G(\mathfrak{L}), \mathcal{O}_{L,\mathfrak{L}}^\times[\frac{1}{2}]) \cong \begin{cases} \mathbb{Z}/e_{\mathfrak{l}} \oplus \mathbb{Z}/e_{\mathfrak{l}} & \text{if } \mathfrak{l} \in T_s(L/k) \\ \mathbb{Z}/e_{\mathfrak{l}} & \text{if } \mathfrak{l} \in T_i(L/k) \\ \mathbb{Z}/\frac{e_{\mathfrak{l}}}{2} & \text{if } \mathfrak{l} \in T_r(L/k). \end{cases} \tag{3.18}$$

Therefore, (3.17) follows by Lemma 3.9. □

We now come to the main result of this section. We begin with a result taken from [22], which we reprove here for completeness; to state it, we introduce the notation B_2 for the 2-primary component of an abelian group B .

PROPOSITION 3.12 (Walter, cf. [22, Theorem 5.3]). *There is an isomorphism*

$$(Cl_L/\iota_{L/F}Cl_F)_2 \cong (Cl_K/\iota_{K/k}Cl_k)_2 \oplus (Cl_{K'}/\iota_{K'/k}Cl_k)_2.$$

Proof. A discussion analogous to the one following equation (3.3) implies that the arrows $\iota_{L/F}$, $\iota_{K/k}$ and $\iota_{K'/k}$ are injections when restricted to the 2-primary components of class groups, because their composition with $N_{L/F}$, $N_{K/k}$ and $N_{K'/k}$, respectively, is multiplied by q . To lighten typesetting, we suppress these arrows from the notation along the proof, identifying their domain with their image.

We first claim that extending ideals to L induce isomorphisms

$$(Cl_L^\Sigma/Cl_L^D)_2 \cong (Cl_K/Cl_k)_2 \quad \text{and} \quad (Cl_L^{\Sigma'}/Cl_L^D)_2 \cong (Cl_{K'}/Cl_k)_2. \tag{3.19}$$

We prove the first isomorphism, the proof for the second being analogous. Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & (Cl_k)_2 & \longrightarrow & (Cl_K)_2 & \longrightarrow & (Cl_K/Cl_k)_2 \longrightarrow 0 \\ & & \downarrow \iota_{L/k} & & \downarrow \iota_{L/k} & & \downarrow \\ 0 & \longrightarrow & (Cl_L^D)_2 & \longrightarrow & (Cl_L^\Sigma)_2 & \longrightarrow & (Cl_L^\Sigma/Cl_L^D)_2 \longrightarrow 0. \end{array} \tag{3.20}$$

Thanks to Proposition 3.5, we have isomorphisms

$$(\text{Ker } \iota_{L/k})_2 \cong \text{Ker} \left(H^1(D, \mathcal{O}_L^\times)_2 \longrightarrow H^1(D, \mathcal{U}_L)_2 \right)$$

and

$$(\text{Ker } \iota_{L/K})_2 \cong \text{Ker} \left(H^1(\Sigma, \mathcal{O}_L^\times)_2 \longrightarrow H^1(\Sigma, \mathcal{U}_L)_2 \right),$$

and Lemma 2.9 shows that these two kernels are isomorphic. Similarly, the isomorphisms

$$(\text{Coker } \iota_{L/k})_2 \cong H^1(D, \mathcal{Q}_L)_2 \quad \text{and} \quad (\text{Coker } \iota_{L/K})_2 \cong H^1(\Sigma, \mathcal{Q}_L)_2$$

discussed in equation (3.15), again combined with Lemma 2.9, show that the cokernels are isomorphic. Applying the snake lemma to the commutative diagram (3.20), we establish (3.19).

We now apply Lemma 2.6 to the module $B = (Cl_L)_2$: we find an isomorphism

$$(Cl_L/Cl_L^G)_2 \cong (Cl_L^\Sigma/Cl_L^D)_2 \oplus (Cl_L^{\Sigma'}/Cl_L^D)_2,$$

which, in light of equation (3.19), we rewrite as

$$(Cl_L/Cl_L^G)_2 \cong (Cl_K/Cl_k)_2 \oplus (Cl_{K'}/Cl_k)_2.$$

We conclude the proof by observing that the map $\iota_{L/F}$ induces an isomorphism $(Cl_L^G)_2 \cong (Cl_F)_2$ since 2 is coprime to $q = [L : F]$. □

REMARK 3.13. It is easy to see that Proposition 3.12 holds more generally for ℓ -parts, where ℓ is a prime not dividing q . We observe, moreover, that it is essentially an algebraic result and very little arithmetic is needed to prove it. In fact, the class field theory we used in the proof can be avoided by extending the use of Lemma 2.9.

Furthermore, using some integral representation theory, one can show an even more precise result: for every prime $\ell \nmid q$ there is an isomorphism

$$(Cl_L)_\ell \oplus (Cl_k)_\ell^2 \cong (Cl_F)_\ell \oplus (Cl_K)_\ell^2. \tag{3.21}$$

This can be proved as follows. By looking at the corresponding characters, one first observes that there is an isomorphism of $\mathbb{Q}[D]$ -modules

$$\mathbb{Q}[D] \oplus \mathbb{Q}^2 \cong \mathbb{Q}[D/G] \oplus \mathbb{Q}[D/\Sigma]^2.$$

Thanks to Conlon’s induction theorem, this implies an isomorphism of $\mathbb{Z}_{(\ell)}[D]$ -modules

$$\mathbb{Z}_{(\ell)}[D] \oplus \mathbb{Z}_{(\ell)}^2 \cong \mathbb{Z}_{(\ell)}[D/G] \oplus \mathbb{Z}_{(\ell)}[D/\Sigma]^2$$

(see for instance the proof of [2, Proposition 3.9]). The above isomorphism in turn induces (3.21), since class groups form a cohomological Mackey functor (in the sense of [4], see specifically [4, Corollary 1.4]).

For a number field M , we let $h_M = |Cl_M|$ denote the class number of M .

THEOREM 3.14. *Let L/k be a Galois extension of number fields whose Galois group $D = \text{Gal}(L/k)$ is dihedral of order $2q$ with q odd. Let $\Sigma \subseteq D$ be a subgroup of order 2 and $G \subseteq D$ be the subgroup of order q . Set $K = L^\Sigma$ and $F = L^G$. Then*

$$\frac{h_L h_k^2}{h_F h_K^2} = \frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} = \frac{\widehat{h}^0(D, \mathcal{O}_L^\times) \widehat{h}^{-1}(\Sigma, \mathcal{O}_L^\times)}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times) \widehat{h}^0(\Sigma, \mathcal{O}_L^\times)}.$$

Proof. We start by proving the first equality. Concerning the 2-part, this an immediate consequence of Proposition 3.12, observing that the cohomology groups with values in the uniquely 2-divisible module $\mathcal{O}_L^\times[\frac{1}{2}]$ have trivial 2-components.

We now focus on the odd part. From Proposition 3.2, we have

$$|Cl_L[\frac{1}{2}]| = |Cl_K[\frac{1}{2}]|^2 \frac{|Cl_L[\frac{1}{2}]^G|}{h^0(D, Cl_L[\frac{1}{2}]) \widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) |N_D Cl_L[\frac{1}{2}]|}. \tag{3.22}$$

Note that Proposition 3.5 with $H = G$ gives

$$|Cl_L[\frac{1}{2}]^G| = |Cl_F[\frac{1}{2}]| \cdot \frac{h^1(G, \mathcal{U}_L[\frac{1}{2}]) h^1(G, P_L[\frac{1}{2}])}{h^1(G, \mathcal{O}_L^\times[\frac{1}{2}])}, \tag{3.23}$$

and we can also replace the term $h^1(G, P_L[\frac{1}{2}])$ by $h^1(D, P_L[\frac{1}{2}]) \widehat{h}^{-1}(D, P_L[\frac{1}{2}])$ in view of Proposition 2.1. By Corollary 3.11, we have

$$h^1(G, \mathcal{U}_L[\frac{1}{2}]) = h^1(D, \mathcal{U}_L[\frac{1}{2}]) \widehat{h}^0(D, \mathcal{U}_L[\frac{1}{2}]). \tag{3.24}$$

Thus (3.22) becomes

$$\begin{aligned} \frac{|Cl_L[\frac{1}{2}]|}{|Cl_K[\frac{1}{2}]|^2} &= \frac{|Cl_L[\frac{1}{2}]^G|}{h^0(D, Cl_L[\frac{1}{2}])\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|} \\ \text{(by (3.23))} &= |Cl_F[\frac{1}{2}]| \cdot \frac{h^1(G, \mathcal{U}_L[\frac{1}{2}])h^1(D, P_L[\frac{1}{2}])\widehat{h}^{-1}(D, P_L[\frac{1}{2}])}{h^1(G, \mathcal{O}_L^\times)h^0(D, Cl_L[\frac{1}{2}])\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|} \\ \text{(by (3.24))} &= |Cl_F[\frac{1}{2}]| \cdot \frac{h^1(D, \mathcal{U}_L[\frac{1}{2}])h^1(D, P_L[\frac{1}{2}])}{h^1(G, \mathcal{O}_L^\times[\frac{1}{2}])h^0(D, Cl_L[\frac{1}{2}])} \cdot \frac{\widehat{h}^0(D, \mathcal{U}_L[\frac{1}{2}])\widehat{h}^{-1}(D, P_L[\frac{1}{2}])}{\widehat{h}^{-1}(D, Cl_L[\frac{1}{2}]) \cdot |N_D Cl_L[\frac{1}{2}]|} \\ \text{(by Proposition 3.7)} &= |Cl_F[\frac{1}{2}]| \cdot \frac{h^1(D, \mathcal{U}_L[\frac{1}{2}])h^1(D, P_L[\frac{1}{2}])}{h^1(G, \mathcal{O}_L^\times[\frac{1}{2}])h^0(D, Cl_L[\frac{1}{2}])} \cdot \frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{|Cl_k[\frac{1}{2}]|} \\ \text{(by Proposition 3.5 with } H = D) &= \frac{|Cl_F[\frac{1}{2}]|}{h^1(G, \mathcal{O}_L^\times[\frac{1}{2}])} \cdot \frac{h^1(D, \mathcal{O}_L^\times[\frac{1}{2}])}{|Cl_k[\frac{1}{2}]|} \cdot \frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{|Cl_k[\frac{1}{2}]|} \\ \text{(by Proposition 2.1)} &= \frac{|Cl_F[\frac{1}{2}]|}{|Cl_k[\frac{1}{2}]|^2} \cdot \frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])}. \end{aligned}$$

This completes the proof of the first equality of the theorem.

To obtain the second equality in the statement, observe that

$$\widehat{H}^i(D, \mathcal{O}_L^\times[\frac{1}{2}]) \cong \widehat{H}^i(D, \mathcal{O}_L^\times) / \widehat{H}^i(D, \mathcal{O}_L^\times)_2,$$

where $\widehat{H}^i(D, \mathcal{O}_L^\times)_2$ is the 2-primary component of $\widehat{H}^i(D, \mathcal{O}_L^\times)$. We conclude by Lemma 2.9. □

Now we recall the definition of the Herbrand quotient of a G -module B as

$$\vartheta(G, B) = \frac{\widehat{h}^0(G, B)}{h^1(G, B)},$$

whenever the quotient is well-defined. The following result will be crucial for our computations.

HERBRAND QUOTIENT OF UNITS (see [14, Corollary 2 of Theorem 1, Chapter IX]).
The Herbrand quotient of the G -module \mathcal{O}_L^\times is

$$\vartheta(G, \mathcal{O}_L^\times) = \frac{1}{q}.$$

Using the value of the Herbrand quotient of units, we can easily obtain bounds on the value of the ratio of class numbers of subfields of L . For a number field M , we set

$$\beta_M(q) = \begin{cases} 0 & \text{if } \mu_M(q) \text{ is trivial,} \\ 1 & \text{otherwise} \end{cases}$$

where μ_M denotes the group of roots of unity of M and $\mu_M(n)$ is the subgroup of roots of unity of M killed by $n \geq 1$. In what follows, for a prime number ℓ , v_ℓ denotes the ℓ -adic valuation.

COROLLARY 3.15. *Let notation be as in Theorem 3.14. For every prime ℓ , the following bounds hold:*

$$-av_\ell(q) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq bv_\ell(q),$$

where $a = \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + \beta_F(q) + 1$ and $b = \text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) + \beta_k(q)$. In particular, if F is totally real of degree $[F : \mathbb{Q}] = 2d$, then

$$-2dv_\ell(q) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq (d - 1)v_\ell(q).$$

Proof. Thanks to Theorem 3.14, we only have to prove that the prescribed bounds hold for the ratio

$$\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) / \widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}]).$$

Observe that $\widehat{H}^0(G, \mathcal{O}_L^\times[\frac{1}{2}]) = \mathcal{O}_F^\times[\frac{1}{2}] / N_G \mathcal{O}_L^\times[\frac{1}{2}]$ is a quotient of $\mathcal{O}_F^\times[\frac{1}{2}]$ annihilated by q . In particular, its order divides $q^{\text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + \beta_F(q)}$. Using the value of the Herbrand quotient of units, we therefore have

$$\begin{aligned} v_\ell \left(\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) &\leq v_\ell \left(\widehat{h}^{-1}(G, \mathcal{O}_L^\times[\frac{1}{2}]) \right) = v_\ell(q) + v_\ell \left(\widehat{h}^0(G, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \\ &\leq v_\ell(q) + (\beta_F(q) + \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times))v_\ell(q) \\ &= av_\ell(q). \end{aligned}$$

We deduce that

$$\begin{aligned} v_\ell \left(\frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} \right) &= v_\ell \left(\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) - v_\ell \left(\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \\ &\geq -v_\ell \left(\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \geq -av_\ell(q). \end{aligned}$$

Similarly, $\widehat{H}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) = \mathcal{O}_k^\times[\frac{1}{2}] / N_D \mathcal{O}_L^\times[\frac{1}{2}]$ is a quotient of $\mathcal{O}_k^\times[\frac{1}{2}]$ annihilated by q . In particular, its order divides $q^{\text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) + \beta_k(q)}$ and therefore

$$v_\ell \left(\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \leq v_\ell(q^{\text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) + \beta_k(q)}) = bv_\ell(q).$$

We deduce that

$$\begin{aligned} v_\ell \left(\frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} \right) &= v_\ell \left(\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) - v_\ell \left(\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \\ &\leq v_\ell \left(\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) \right) \leq bv_\ell(q). \end{aligned}$$

When F is totally real, it contains no roots of unity different from ± 1 , so that $a = 2d$ and $b = (d - 1)$. □

REMARK 3.16. It would be interesting to understand to what extent the bounds of Corollary 3.15 are optimal. To be more precise, for given $a, b \in \mathbb{Z}$, consider the set

$$S(a, b) = \{c \in \mathbb{Q} \text{ such that } -av_\ell(q) \leq v_\ell(c) \leq bv_\ell(q), \text{ for every prime } \ell\}.$$

One could ask whether, for every $a \geq 1$ and $b \geq 0$ and every $c \in S(a, b)$, there exist a number field k_c , a quadratic extension F_c/k_c satisfying

$$a = \text{rk}_{\mathbb{Z}}(\mathcal{O}_{F_c}^{\times}) + \beta_{F_c}(q) + 1 \quad \text{and} \quad b = \text{rk}_{\mathbb{Z}}(\mathcal{O}_{k_c}^{\times}) + \beta_{k_c}(q)$$

and a dihedral extensions L_c/k_c of degree $2q$ such that $F_c \subseteq L_c$ and

$$\frac{h_{L_c} h_{k_c}^2}{h_{F_c} h_{K_c}^2} = c,$$

where K_c/k_c is a subextension of L_c/k_c of degree q .

The bounds of Corollary 3.15 hold in full generality, that is, for an arbitrary base field k . When k is totally real and F is a CM field, these bounds can be improved, as we show in Corollary 3.18, which generalizes [2, Example 6.3]. We start with the following lemma, whose first statement is well-known.

LEMMA 3.17. *We have*

$$\mu_F = \mu_L \quad \text{and} \quad \mu_k = \mu_K.$$

Moreover, the intersection $I_G \mathcal{O}_L^{\times} \cap \mathcal{O}_F^{\times}$ is a finite cyclic group and there is a Δ -antiequivariant isomorphism

$$\left((\mathcal{O}_L^{\times})^q \cap \mathcal{O}_F^{\times} \right) / (\mathcal{O}_F^{\times})^q \cong I_G \mathcal{O}_L^{\times} \cap \mathcal{O}_F^{\times}.$$

In particular, we have isomorphisms of abelian groups

$$\left((\mathcal{O}_L^{\times})^q \cap \mathcal{O}_F^{\times} / (\mathcal{O}_F^{\times})^q \right)^{\mp} \cong \left(I_G \mathcal{O}_L^{\times} \cap \mathcal{O}_F^{\times} \right)^{\pm}.$$

Proof. Let ζ be a root of unity of L , and set $M = k(\zeta)$. Then M/k is an abelian extension of k contained in L and therefore $M \subseteq F$. In particular, $\mu_F = \mu_L$ and, taking Σ -invariants, $\mu_k = \mu_K$, so that the first statement is proved.

To prove the rest of the lemma, consider the Kummer sequence

$$1 \longrightarrow \mu_L(q) \longrightarrow \mathcal{O}_L^{\times} \xrightarrow{(\cdot)^q} (\mathcal{O}_L^{\times})^q \longrightarrow 1. \tag{3.25}$$

Taking G -cohomology, we obtain a Δ -equivariant isomorphism

$$\left((\mathcal{O}_L^{\times})^q \cap \mathcal{O}_F^{\times} \right) / (\mathcal{O}_F^{\times})^q = \text{Ker} \left(H^1(G, \mu_L(q)) \rightarrow H^1(G, \mathcal{O}_L^{\times}) \right). \tag{3.26}$$

Using Proposition 2.1, we deduce a Δ -antiequivariant isomorphism

$$\left((\mathcal{O}_L^{\times})^q \cap \mathcal{O}_F^{\times} \right) / (\mathcal{O}_F^{\times})^q \cong \text{Ker} \left(\widehat{H}^{-1}(G, \mu_L(q)) \rightarrow \widehat{H}^{-1}(G, \mathcal{O}_L^{\times}) \right).$$

By the first statement of the lemma, the D -module $B = \mathcal{O}_L^{\times} \left[\frac{1}{2} \right]$ satisfies $B(q)^G = B(q)$ and we can apply Lemma 2.7. In particular, we obtain a Δ -antiequivariant isomorphism

$$\left((\mathcal{O}_L^{\times})^q \cap \mathcal{O}_F^{\times} \right) / (\mathcal{O}_F^{\times})^q \cong I_G \mathcal{O}_L^{\times} \cap \mathcal{O}_F^{\times}.$$

Observe that, again by Lemma 2.7, $I_G \mathcal{O}_L^{\times} \cap \mathcal{O}_F^{\times}$ is equal to $I_G \mathcal{O}_L^{\times} \cap \mu_F(q) \subseteq \mu_F$, whence the claim that it is cyclic. □

We can now state the following result which sharpens Corollary 3.15 under the assumption that F is a CM field and $F^+ = k$. We write $\mu_F(q^{\infty})$ to denote the roots of unity $\zeta \in \mu_F$ such that $\zeta^{q^m} = 1$ for some $m \geq 0$: it is clearly a finite group.

COROLLARY 3.18. *With notation as in Theorem 3.14, assume moreover that F is a CM field of degree $[F : \mathbb{Q}] = 2d$ and that k is its totally real subfield. Let s be the order of the quotient $((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q$ and let t be the order of $\mu_F(q^\infty) / \mu_F(q)$. Then, for every prime ℓ ,*

$$-v_\ell(q) - v_\ell(s) - v_\ell(t) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right) \leq (d - 1)v_\ell(q).$$

Proof. Again, it suffices to study the ratio $\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}]) / \widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])$, thanks to Theorem 3.14. For $i = -1, 0$ we write $\widehat{h}^i(D, \mathcal{O}_L^\times[\frac{1}{2}]) = \widehat{h}^i(G, \mathcal{O}_L^\times) / \widehat{h}^i(G, \mathcal{O}_L^\times)^-$, where we denote by $\widehat{h}^i(G, \mathcal{O}_L^\times)^-$ the order of the minus part of $\widehat{H}^i(G, \mathcal{O}_L^\times)$ (observe that $\widehat{H}^i(G, \mathcal{O}_L^\times) = \widehat{H}^i(G, \mathcal{O}_L^\times[\frac{1}{2}])$ since G is of odd order). We find

$$\frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} = \frac{\widehat{h}^0(G, \mathcal{O}_L^\times)}{\widehat{h}^{-1}(G, \mathcal{O}_L^\times)} \cdot \frac{\widehat{h}^{-1}(G, \mathcal{O}_L^\times)^-}{\widehat{h}^0(G, \mathcal{O}_L^\times)^-} = \frac{1}{q} \cdot \frac{\widehat{h}^{-1}(G, \mathcal{O}_L^\times)^-}{\widehat{h}^0(G, \mathcal{O}_L^\times)^-}. \tag{3.27}$$

We now use that F is a CM field and $F = k^+$. Starting from the tautological exact sequence defining $\widehat{H}^0(G, \mathcal{O}_L^\times)$, we can consider its minus part to obtain

$$0 \longrightarrow (\mathbb{N}_{L/F} \mathcal{O}_L^\times[\frac{1}{2}])^- \longrightarrow (\mathcal{O}_F^\times[\frac{1}{2}])^- \longrightarrow \widehat{H}^0(G, \mathcal{O}_L^\times)^- \longrightarrow 0.$$

The quotient $\mathcal{O}_F^\times / \mathcal{O}_k^\times \mu_F$ is of order 1 or 2 by [13, Chapter XIII, Section 2, Lemma 1] and, in particular, $(\mathcal{O}_F^\times[\frac{1}{2}])^- = \mu_F[\frac{1}{2}]$. Since the rightmost term of the above sequence is killed by q , the sequence can be rewritten as

$$0 \longrightarrow (\mathbb{N}_{L/F} \mathcal{O}_L^\times[\frac{1}{2}])^- \longrightarrow \mu_F(q^\infty) \longrightarrow \widehat{H}^0(G, \mathcal{O}_L^\times)^- \longrightarrow 0. \tag{3.28}$$

On the other hand, thanks to Lemma 3.17, the G -action on μ_L is trivial and (as in the proof of Lemma 2.7) we find $\mu_F(q) = \widehat{H}^{-1}(G, \mu_L(q)) = \widehat{H}^0(G, \mu_L(q))$. By considering the Kummer sequence (3.25) and taking the minus part of its G -cohomology, we obtain

$$\begin{array}{ccccccc}
 0 & \longrightarrow & I_G \mathcal{O}_L^\times \cap \mu_F(q) & \longrightarrow & \widehat{H}^{-1}(G, \mu_L(q))^- = \mu_F(q) & \longrightarrow & \widehat{H}^{-1}(G, \mathcal{O}_L^\times)^- \\
 & & & & & & \uparrow \\
 & & & & & & \widehat{H}^{-1}(G, (\mathcal{O}_L^\times)^q)^- \longrightarrow \mu_F(q) = \widehat{H}^0(G, \mu_L(q))^- \longrightarrow Y \longrightarrow 0, \\
 & & & & & & \tag{3.29}
 \end{array}$$

where $Y \subseteq \widehat{H}^0(G, \mathcal{O}_L^\times)^-$ is defined by the exactness of the diagram. Taking orders in the above long exact sequence, we deduce

$$\widehat{h}^{-1}(G, \mathcal{O}_L^\times)^- = \frac{\widehat{h}^{-1}(G, (\mathcal{O}_L^\times)^q)^- \cdot |Y|}{|I_G \mathcal{O}_L^\times \cap \mu_F(q)|}$$

while (3.28) implies that $\widehat{h}^0(G, \mathcal{O}_L^\times)^- \leq |\mu_F(q^\infty)|$. Therefore, (3.27) becomes

$$\frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} \geq \frac{1}{q} \cdot \frac{\widehat{h}^{-1}(G, (\mathcal{O}_L^\times)^q)^- \cdot |Y|}{|I_G \mathcal{O}_L^\times \cap \mu_F(q)|} \cdot \frac{1}{|\mu_F(q^\infty)|}.$$

The second line of the long exact sequence (3.29) shows that $\widehat{h}^{-1}(G, (\mathcal{O}_L^\times)^q)^- \cdot |Y| \geq |\mu_F(q)|$, so that we obtain

$$\frac{\widehat{h}^0(D, \mathcal{O}_L^\times[\frac{1}{2}])}{\widehat{h}^{-1}(D, \mathcal{O}_L^\times[\frac{1}{2}])} \geq \frac{1}{q} \cdot \frac{1}{|I_G \mathcal{O}_L^\times \cap \mu_F(q)|} \cdot \frac{1}{t}. \tag{3.30}$$

Since $\mu_F[\frac{1}{2}] = \mathcal{O}_F^\times[\frac{1}{2}]^-$, we have $I_G \mathcal{O}_L^\times \cap \mu_F(q) = (I_G \mathcal{O}_L^\times \cap \mu_F)^- = (I_G \mathcal{O}_L^\times \cap \mathcal{O}_F^\times)^-$, by Lemma 2.7, and applying Lemma 3.17 we deduce that $I_G \mathcal{O}_L^\times \cap \mu_F(q)$ is of order s because

$$((\mathcal{O}_L^\times)^q \cap \mathcal{O}_F^\times / (\mathcal{O}_F^\times)^q)^+ = ((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q.$$

Taking ℓ -adic valuations in (3.30), we obtain the bound

$$-v_\ell(q) - v_\ell(s) - v_\ell(t) \leq v_\ell \left(\frac{h_L h_k^2}{h_F h_K^2} \right).$$

As for the other inequality of the corollary, we argue as in Corollary 3.15 observing that since k is totally real, $\beta_k(q) = 1$ and $\text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) = d - 1$. □

REMARK 3.19. The quotient $((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q$ has exponent dividing q and is cyclic (by Lemma 3.17), hence its order s divides q . We claim that $s = q$ if and only if $K = k(\sqrt[q]{u})$ for some unit $u \in \mathcal{O}_k^\times$. This is equivalent to the fact that, given $u \in (\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times$, the class $[u] \in ((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q$ has order strictly less than q if and only if $k(x) \subsetneq K$, where $x \in \mathcal{O}_K^\times$ is such that $x^q = u$. Note that $k(x) \subsetneq K$ precisely when $X^q - u$ is reducible, a condition equivalent to the existence of a prime $p | q$ such that $u \in (\mathcal{O}_k^\times)^p$ (see [15, Chapter VI, Theorem 9.1]). We are thus reduced to show that the class $[u] \in ((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^q$ has order strictly less than q if and only if there is $p | q$ such that $u \in (\mathcal{O}_k^\times)^p$.

If $u \in (\mathcal{O}_k^\times)^p$, then clearly $u^{q/p} \in (\mathcal{O}_k^\times)^q$ and the order of $[u]$ strictly divides q . Suppose, conversely, that $[u]$ has order q/p for some prime p , so $u^{q/p} \in (\mathcal{O}_k^\times)^q$, and let $v \in \mathcal{O}_k^\times$ be such that $u^{q/p} = v^q$. We deduce that $v^q = (x^{q/p})^q$ or, equivalently, $x^{q/p} = v\zeta$ for some $\zeta \in \mu_K$. Hence $x^{q/p} \in \mathcal{O}_k^\times$, by Lemma 3.17, and therefore $u = x^q = (x^{q/p})^p \in (\mathcal{O}_k^\times)^p$. This shows our claim.

When $q = p$ is a prime and $\mu_F(p^\infty) = \mu_F(p)$, we can restate Corollary 3.18 by saying that the ratio of class numbers equals p^m for some $-2 \leq m \leq (d - 1)$ or $-1 \leq m \leq (d - 1)$ according to whether $K = k(\sqrt[p]{u})$ for some $u \in \mathcal{O}_k^\times$, or not.

The next corollary (which generalizes [9, Section 4] and [18, Théorème IV.1]) shows that if $k = \mathbb{Q}$ even sharper bounds hold.

COROLLARY 3.20. *Let L/\mathbb{Q} be a dihedral extension of degree $2q$ where q is odd, and let F/\mathbb{Q} be the quadratic extension contained in L . Denote by K the field fixed by a subgroup of order 2 in $\text{Gal}(L/\mathbb{Q})$. Then, for every prime ℓ ,*

$$0 \geq v_\ell \left(\frac{h_L}{h_F h_K^2} \right) \geq \begin{cases} -2v_\ell(q) & \text{if } F \text{ is real quadratic} \\ -v_\ell(q) & \text{if } F \text{ is imaginary quadratic.} \end{cases}$$

Proof. The case when F is real quadratic is already contained in Corollary 3.15. If F is totally imaginary, it is a CM field, so that we can apply Corollary 3.18: we need to prove that $s = t = 1$. Recall that s was defined as the order of the quotient

$$((\mathcal{O}_K^\times)^q \cap \{\pm 1\}) / \{\pm 1\},$$

which is trivial. As for t , the only case in which $\mu_F(q^\infty) \neq 1$ occurs when $F = \mathbb{Q}(\sqrt{-3})$ and $3 \mid q$, but in this case $\mu_F(q^\infty) = \mu_F(q)$, so $t = 1$. □

4. Class number formula in terms of a unit index. In this section, we rewrite the formula of Theorem 3.14 in a form more similar to the one often found in the literature, namely replacing the orders of cohomology groups by the index of a subgroup of the group of units of L .

NOTATION. Recall that for an abelian group B and a natural number n , we write $B(n) = \{b \in B : nb = 0\}$. We set

$$\text{tor}_{\mathbb{Z}}(B) = \bigcup_{n \in \mathbb{N}} B(n)$$

for the torsion subgroup of B and $\bar{B} = B / \text{tor}_{\mathbb{Z}}(B)$ for the maximal torsion-free quotient of B .

PROPOSITION 4.1. *When B is a D -module which is \mathbb{Z} -finitely generated, the following formula holds:*

$$\frac{\widehat{h}^0(D, B[\frac{1}{2}])}{\widehat{h}^{-1}(D, B[\frac{1}{2}])} = (B : B^\Sigma + B^{\Sigma'} + B^G) \vartheta(G, B) \frac{|I_G B \cap B^D|}{|I_G B \cap B^G|} q^{\text{rk}_{\mathbb{Z}}(B^D) - \text{rk}_{\mathbb{Z}}(B^G)}.$$

Proposition 4.1, as well as its proof, is purely algebraic and requires no arithmetic. We postpone its proof after Theorem 4.3 and focus here on its arithmetic application.

COROLLARY 4.2. *With notation as in Theorem 3.14, one has*

$$\frac{h_L h_k^2}{h_F h_K^2} = (\mathcal{O}_L^\times : \mathcal{O}_K^\times \mathcal{O}_{K'}^\times \mathcal{O}_F^\times) \frac{q^{(\text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) - \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) - 1)}}{((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times : (\mathcal{O}_k^\times)^q)}.$$

and the term $((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times : (\mathcal{O}_k^\times)^q)$ divides q .

Proof. The formula follows by combining Theorem 3.14, Proposition 4.1, the value of the Herbrand quotient of units, and Lemma 3.17. □

The formula of Corollary 4.2 is similar to those appeared in the literature (see the Introduction for references). Sometimes the right-hand side is expressed differently but this is just a matter of rearranging terms. For instance, we prove below that Bartel’s formula in [2] coincides with ours when q is a prime.

THEOREM 4.3 (Bartel, see [2, Theorem 1.1]). *Let L/k be a Galois extensions of number fields with Galois group D_{2p} for p an odd prime, let F be the intermediate quadratic extension and K, K' be distinct intermediate extensions of degree p . Set δ to be 3 if K/k is obtained by adjoining the p th root of a non-torsion unit (thus so is L/F) and 1 otherwise. Then we have*

$$\frac{h_L h_k^2}{h_F h_K^2} = p^{\alpha/2} \cdot (\mathcal{O}_L^\times : \mathcal{O}_K^\times \mathcal{O}_{K'}^\times \mathcal{O}_F^\times),$$

where $\alpha = 2 \text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) - \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) - \frac{\text{rk}_{\mathbb{Z}}(\mathcal{O}_L^\times) - \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times)}{p-1} - \delta$.

REMARK 4.4. Observe that Bartel’s theorem assumes that $q = p$ is an odd prime. However, Bartel’s formulation is more general than the one given above, since he obtains

a formula for general S -class numbers where S is any finite set of primes in k containing the archimedean ones. Since the proof of Theorem 3.14 ultimately relies on the study of G -cohomology of Diagram (3.6) and a S -version of the diagram exists, our main result should easily generalize to S -class numbers and S -units.

Proof. Observe that since L/F is Galois of odd order, we have $\text{rk}_{\mathbb{Z}}(\mathcal{O}_L^\times) = p \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + (p - 1)$ and so

$$\frac{\text{rk}_{\mathbb{Z}}(\mathcal{O}_L^\times) - \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times)}{p - 1} = \frac{(p - 1)(\text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + 1)}{p - 1} = \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + 1.$$

Therefore,

$$\alpha = 2 \text{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) - 2 \text{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) - 1 - \delta.$$

Using this expression for α and comparing Corollary 4.2 with the statement of the theorem, we simply need to show that

$$p^{\frac{\delta-1}{2}} = ((\mathcal{O}_K^\times)^p \cap \mathcal{O}_k^\times : (\mathcal{O}_k^\times)^p).$$

By definition of δ , the above reduces, using that $((\mathcal{O}_K^\times)^p \cap \mathcal{O}_k^\times) / (\mathcal{O}_k^\times)^p$ is cyclic by Lemma 3.17, to prove that

$$((\mathcal{O}_K^\times)^p \cap \mathcal{O}_k^\times : (\mathcal{O}_k^\times)^p) \neq 0 \iff K = k(\sqrt[p]{u}) \quad \text{for some } u \in \mathcal{O}_k^\times,$$

and this is clear (see also Remark 3.19). □

We now prove Proposition 4.1. The strategy follows very closely the one of [6, Section 2], which, in turn, is partly inspired by [17, Section 5].

LEMMA 4.5. *Let B be a D -module which is \mathbb{Z} -finitely generated. Then the index of $B^\Sigma + B^{\Sigma'} + B^G$ in B is finite and*

$$(B : B^\Sigma + B^{\Sigma'} + B^G) = (N_G B : N_G(B^\Sigma + B^{\Sigma'} + B^G)) \cdot (B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)).$$

Moreover, the three terms appearing in the above equality are coprime to any prime not dividing q .

Proof. By equation (3.4) with $f = N_G$ and $B' = B^\Sigma + B^{\Sigma'} + B^G$, we only need to verify that the above indices are finite. Since B is \mathbb{Z} -finitely generated, all G -Tate cohomology groups of B are finite of exponent dividing q . In particular, $B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)$ is of finite index in $B[N_G]$ since it contains $I_G B$ by Lemma 2.4. This argument also shows that $(B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G))$ is coprime to any prime not dividing q . On the other hand, $N_G(B^\Sigma + B^{\Sigma'} + B^G)$ contains $q(B^G)$, so its index in B^G is finite and coprime to any prime not dividing q . The same holds, therefore, for the index of $N_G(B^\Sigma + B^{\Sigma'} + B^G)$ in $N_G B$, since $N_G B \subseteq B^G$. This finishes the proof. □

We now analyze separately the two factors of the right-hand side of the equality of Lemma 4.5.

LEMMA 4.6. *Let B be a D -module which is \mathbb{Z} -finitely generated. Then the following equality holds:*

$$(N_G B : N_G(B^\Sigma + B^{\Sigma'} + B^G)) = \frac{\widehat{h}^0(D, B[\frac{1}{2}]) (B^G : q(B^G))}{\widehat{h}^0(G, B[\frac{1}{2}]) (B^D : q(B^D))}.$$

Proof. Every factor appearing in the formula of the statement is coprime to any prime not dividing q by Lemma 4.5. This means that, replacing B by $B[\frac{1}{2}]$, we can assume that B is uniquely 2-divisible (note that Tate cohomology groups remain finite) so that Σ -Tate cohomology of B is trivial, and similarly for Σ' . In particular,

$$N_G(B^\Sigma) = N_G(N_\Sigma B) = N_D B$$

and similarly $N_G(B^{\Sigma'}) = N_G(N_{\Sigma'} B) = N_D B$. Therefore,

$$\begin{aligned} (N_G B : N_G(B^\Sigma + B^{\Sigma'} + B^G)) &= (N_G B : q(B^G) + N_D B) \\ &= \frac{(B^G : q(B^G) + N_D B)}{\widehat{h}^0(G, B)} \\ &= \frac{(B^G : q(B^G))}{(q(B^G) + N_D B : q(B^G)) \cdot \widehat{h}^0(G, B)} \\ &= \frac{(B^G : q(B^G))}{(N_D B : q(B^G \cap N_D B)) \cdot \widehat{h}^0(G, B)} \\ \text{(see (4.1) below)} &= \frac{(B^G : q(B^G))}{(N_D B : q(B^D)) \cdot \widehat{h}^0(G, B)} \\ &= \frac{(B^G : q(B^G)) \cdot \widehat{h}^0(D, B)}{(B^D : q(B^D)) \cdot \widehat{h}^0(G, B)}. \end{aligned}$$

We have used that

$$q(B^G) \cap N_D B = q(B^D). \tag{4.1}$$

To see this, first observe that $q(B^G) \cap B^D = q(B^D)$ because the surjective map $B^G \xrightarrow{q} q(B^G)$ stays surjective after taking Σ -invariants, since B^G is uniquely 2-divisible. In particular, we have $q(B^G) \cap N_D B \subseteq q(B^D)$ which implies

$$q(B^G) \cap N_D B = q(B^D) \cap N_D B.$$

Now (4.1) follows since

$$q(B^D) \cap N_D B = q(B^D),$$

because

$$q(B^D) = N_G(B^D) = N_G(N_\Sigma(B^G)) = N_D(B^G) \subseteq N_D B. \quad \square$$

LEMMA 4.7. *Let B be a D -module which is \mathbb{Z} -finitely generated. Then*

$$(B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)) = \frac{h^1(G, B[\frac{1}{2}]) \cdot (I_G B \cap B^G(q) : I_G B \cap B^D(q))}{\widehat{h}^{-1}(D, B[\frac{1}{2}]) \cdot (B^G(q) : B^D(q))}.$$

Proof. Observe that $(B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G))$ is coprime to any prime not dividing q (by Lemma 4.5). The same holds for all the factors of the right-hand side of the equality of the lemma. This means that, replacing B by $B[\frac{1}{2}]$, we can assume that B is uniquely 2-divisible.

Observe first that

$$\begin{aligned} (B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)) &= \frac{(B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'}))}{(B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G) : B[N_G] \cap (B^\Sigma + B^{\Sigma'}))} \\ &\text{(by Lemma 2.5)} = \frac{h^1(D, B)}{(B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G) : B[N_G] \cap (B^\Sigma + B^{\Sigma'}))}. \end{aligned}$$

Since $h^1(D, B) = \widehat{h}^{-1}(G, B) / \widehat{h}^{-1}(D, B)$ by Proposition 2.1, we only need to prove that

$$(B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G) : B[N_G] \cap (B^\Sigma + B^{\Sigma'})) = \frac{(B^G(q) : B^D(q))}{(I_G B \cap B^G(q) : I_G B \cap B^D(q))}.$$

To prove the above equality, observe that Σ acts as -1 on the quotient

$$\frac{B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)}{B[N_G] \cap (B^\Sigma + B^{\Sigma'})}$$

by (2.7). In particular, we have

$$\begin{aligned} \frac{B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)}{B[N_G] \cap (B^\Sigma + B^{\Sigma'})} &= \left(\frac{B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)}{B[N_G] \cap (B^\Sigma + B^{\Sigma'})} \right)^- \\ &= \frac{(B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G))^-}{(B[N_G] \cap (B^\Sigma + B^{\Sigma'}))^-} \\ &\text{(by (2.5))} = \frac{(B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G))^-}{(I_G B)^-}. \end{aligned}$$

Now note that $B^\Sigma + B^{\Sigma'} = I_G B + B^\Sigma$ by (2.4), so that

$$\begin{aligned} B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G) &= B[N_G] \cap (I_G B + B^\Sigma + B^G) \\ &= I_G B + (B[N_G] \cap (B^\Sigma + B^G)) \end{aligned}$$

and taking minus parts we obtain

$$\begin{aligned} (I_G B + (B[N_G] \cap (B^\Sigma + B^G)))^- &= (I_G B)^- + (B[N_G] \cap (B^\Sigma + B^G))^- \\ &= (I_G B)^- + B[N_G] \cap (B^G)^- \\ &= (I_G B)^- + (B^G(q))^- \\ &= (I_G B + B^G(q))^- . \end{aligned}$$

Here, we have used that for uniquely 2-divisible Σ -modules B_1 and B_2 , we have $(B_1 + B_2)^- = \frac{1-\sigma}{2}(B_1 + B_2) = \frac{1-\sigma}{2}B_1 + \frac{1-\sigma}{2}B_2 = B_1^- + B_2^-$. Therefore,

$$\begin{aligned} \frac{B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)}{B[N_G] \cap (B^\Sigma + B^{\Sigma'})} &= \frac{(I_G B + B^G(q))^-}{(I_G B)^-} \\ &\cong \frac{(B^G(q))^-}{(I_G B \cap B^G(q))^-} \\ &= \frac{B^G(q)/B^D(q)}{(I_G B \cap B^G(q))/(I_G B \cap B^D(q))} \end{aligned}$$

and this concludes the proof of the lemma. □

Let B be a finitely generated \mathbb{Z} -module and let m be a positive natural number. Then we have

$$|B(m)| \cdot m^{\text{rk}_{\mathbb{Z}}(B)} = (B : mB).$$

Indeed, let $\pi : B \rightarrow \bar{B} = B/\text{tor}_{\mathbb{Z}}(B)$ be the projection map. It induces a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(m) & \longrightarrow & B & \xrightarrow{m} & B & \longrightarrow & B/mB & \longrightarrow & 0 \\ & & & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi_m & & \\ 0 & \longrightarrow & \bar{B} & \xrightarrow{m} & \bar{B} & \longrightarrow & \bar{B}/m\bar{B} & \longrightarrow & 0, & & \end{array}$$

where π_m is the map induced by π on B/mB . The snake lemma gives an exact sequence of finite abelian groups

$$0 \longrightarrow B(m) \longrightarrow \text{tor}_{\mathbb{Z}}(B) \xrightarrow{m} \text{tor}_{\mathbb{Z}}(B) \longrightarrow \text{Ker } \pi_m \longrightarrow 0.$$

On the other hand, we have the tautological exact sequence

$$0 \longrightarrow \text{Ker } \pi_m \longrightarrow B/mB \longrightarrow \bar{B}/m\bar{B} \longrightarrow 0.$$

Taking cardinalities we obtain

$$|B(m)| = |\text{Ker } \pi_m| = \frac{(B : mB)}{(\bar{B} : m\bar{B})} = (B : mB)m^{-\text{rk}_{\mathbb{Z}}(B)}, \tag{4.2}$$

as claimed.

Proof of Proposition 4.1. Combining Lemmas 4.5, 4.6 and 4.7, we get

$$\begin{aligned} (B : B^\Sigma + B^{\Sigma'} + B^G) &= (N_G B : N_G (B^\Sigma + B^{\Sigma'} + B^G)) \cdot (B[N_G] : B[N_G] \cap (B^\Sigma + B^{\Sigma'} + B^G)) \\ &= \frac{\widehat{h}^0(D, B[\frac{1}{2}]) \cdot (B^G : q(B^G))}{\widehat{h}^0(G, B[\frac{1}{2}]) \cdot (B^D : q(B^D))} \frac{h^1(G, B[\frac{1}{2}]) \cdot (I_G B \cap B^G(q) : I_G B \cap B^D(q))}{\widehat{h}^{-1}(D, B[\frac{1}{2}]) \cdot (B^G(q) : B^D(q))} \\ &= \frac{(B^G : q(B^G))}{(B^D : q(B^D)) \cdot (B^G(q) : B^D(q))} \frac{\widehat{h}^0(D, B[\frac{1}{2}])}{\widehat{h}^{-1}(D, B[\frac{1}{2}])} \frac{(I_G B \cap B^G(q) : I_G B \cap B^D(q))}{\vartheta(G, B)}. \end{aligned}$$

Now observe that, in light of equation (4.2), we have

$$\frac{(B^G : q(B^G))}{(B^D : q(B^D))} = q^{\text{rk}_{\mathbb{Z}}(B^G) - \text{rk}_{\mathbb{Z}}(B^D)} (B^G(q) : B^D(q)). \quad \square$$

ACKNOWLEDGMENT. This paper has a long history. We started working on it in 2007, during a summer school in Iwasawa theory held at McMaster University, following a suggestion of Ralph Greenberg. At the time, our main focus was on what we called “fake \mathbb{Z}_p -extensions” and the formula for dihedral extensions was simply a tool which we obtained by translating the right-hand side of equation (1.1) into a unit index essentially using linear algebra. We posted a version of our work (quite different from the present one) on arXiv in 2009, and it became part of the second author’s PhD thesis [19]. At that time, we were confident that our techniques would easily generalize to cover other classes of extensions, so we decided to wait. Then basically nothing happened until the autumn of 2016 when the second author came across a question [1] posted by Alex Bartel on MathOverflow. This motivated us to revise and improve our work, and to split the original version in two articles. This is the first of the two papers, concentrating on the class number formula for finite dihedral extensions, while in the second, which is still in progress, we focus on fake \mathbb{Z}_p -extensions. We are grateful to Henri Johnston for encouraging us to take up this revision task and to Alex Bartel for some comments on a preliminary version. We also thank the anonymous referee for useful comments and suggestions which improved the presentation of our paper.

REFERENCES

1. A. Bartel, Class groups in dihedral extensions – some sort of Spiegelungssatz? <https://mathoverflow.net/q/73033>.
2. A. Bartel, On Brauer–Kuroda type relations of S -class numbers in dihedral extensions, *J. Reine Angew. Math.* **668** (2012), 211–244.
3. A. Bartel and B. de Smit, Index formulae for integral Galois modules, *J. Lond. Math. Soc.* (2) **88**(3) (2013), 845–859. MR 3145134.
4. R. Boltje, Class group relations from Burnside ring idempotents, *J. Number Theory* **66**(2) (1997), 291–305.
5. R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, *Math. Nachr.* **4** (1951), 158–174.
6. L. Caputo, The Brauer–Kuroda formula for higher S -class numbers in dihedral extensions of number fields, *Acta Arith.* **151**(3) (2013), 217–239.
7. H. Cartan and S. Eilenberg, *Homological algebra* (Princeton University Press, Princeton, NJ, 1956).
8. G. L. Dirichlet, Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. Première partie, *J. Reine Angew. Math.* **24** (1842), 291–371.
9. F. Halter-Koch, Einheiten und Divisorenklassen in Galois’schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl l , *Acta Arith.* **33**(4) (1977), 355–364.
10. A. Heller and I. Reiner, Representations of cyclic groups in ring of integers, II, *Ann. Math.* **77**(2) (1963), 318–328.
11. D. Hilbert, Ueber den Dirichlet’schen biquadratischen Zahlkörper, *Math. Ann.* **45**(3) (1894), 309–340.
12. J.-F. Jaulent, Unités et classes dans les extensions métabéliennes de degré nl^f sur un corps de nombres algébriques, *Ann. Inst. Fourier (Grenoble)* **31**(1) (1981), ix–x, 39–62.
13. S. Lang, *Cyclotomic fields I and II*, combined second edition, Graduate Texts in Mathematics, vol. 121 (Springer-Verlag, New York, 1990), with an Appendix by Karl Rubin.
14. S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, 2nd edition (Springer-Verlag, New York, 1994).

15. S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, 3rd edition (Springer-Verlag, New York, 2002).
16. F. Lemmermeyer, Kuroda's class number formula, *Acta Arith.* **66**(3) (1994), 245–260.
17. F. Lemmermeyer, Class groups of dihedral extensions, *Math. Nachr.* **278**(6) (2005), 679–691.
18. N. Moser, Unités et nombre de classes d'une extension galoisienne diédrale de \mathbf{Q} , *Abh. Math. Sem. Univ. Hamburg* **48** (1979), 54–75.
19. F. A. E. Nuccio Mortarino Majno di Capriglio, On \mathbf{Z}_p -extensions of real abelian number fields, PhD Thesis (University of Rome La Sapienza, 2009).
20. J.-P. Serre, Local class field theory, in *Algebraic Number Theory, Proc. Instructional Conf., Brighton, 1965* (Thompson, Washington, D.C., 1967), 128–161.
21. J. T. Tate, Global class field theory, in *Algebraic Number Theory, Proc. Instructional Conf., Brighton, 1965* (Thompson, Washington, D.C., 1967), 162–203.
22. C. D. Walter, A class number relation in Frobenius extensions of number fields, *Mathematika* **24**(2) (1977), 216–225. MR 0472768.

