On fake $\mathbb{Z}_p$-extensions of number fields

Luca Caputo and Filippo Alberto Edoardo Nuccio

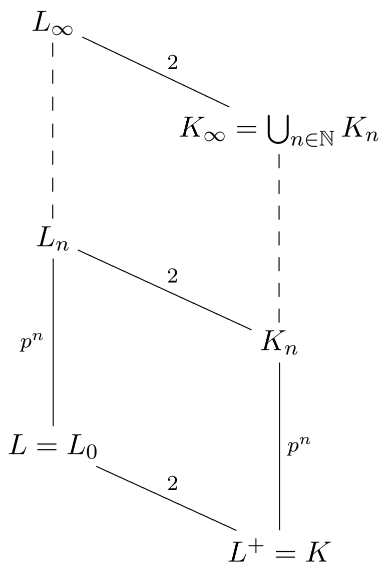
May 10, 2009

Abstract -For an odd prime number p, let L_∞ be the $\mathbb{Z}_p$-anticyclotomic extension of an imaginary quadratic field L. We focus on the non-normal subextension K_∞ of L_∞ fixed by a subgroup of order 2 in $\mathrm{Gal}(L_\infty/\mathbb{Q})$. After providing a general result for dihedral extensions, we study the growth of the p-part of the class group of the subfields of $K_\infty/\mathbb{Q}$, providing a formula of Iwasawa type. Furthermore, we describe the structure of the projective limit of these class groups.

2000 Mathematical Subject Classification: Primary 11R23 Secondary 11R20

1 Introduction

The aim of the present paper is to study the growth of class numbers along a tower of extensions which is not Galois over the ground field. More precisely, let p be an odd prime, let L be a CM field and let L_∞/L be a $\mathbb{Z}_p$-extension such that L_∞/L^+ is pro-p-dihedral (meaning that $\mathrm{Gal}(L_\infty/F^+)$ is a projective limit of dihedral groups of order $2p^n, n \geqslant 1$). We set $K = L^+$. Hence the situation is as follows:



Such an extension always exists and, under Leopoldt conjecture for L with respect to the prime p, there are precisely $n/2$ of them if $n = [L : \mathbb{Q}]$. Note that $\mathrm{Gal}(L_\infty/K)$ is the semidirect product of $\mathrm{Gal}(L_\infty/L) \rtimes \Delta$ where $\Delta = \mathrm{Gal}(L/K)$. For every $m \geqslant 1$, denote by K_m the subfield of L_∞ which is fixed by $\mathrm{Gal}(L_\infty/L_m) \rtimes \Delta$. Note that $\mathrm{Gal}(L_m/K)$ is a dihedral group (isomorphic to D_{p^m}).

Setting $K_\infty = \cup K_m$, the extension K_∞/K shares some similarities with $\mathbb{Z}_p$-extensions, still behaving in a different way. In particular it can be seen as a particular case of what may be called a *fake* $\mathbb{Z}_p$-extension. Here is the definition that we propose

Definition. *Let p be a prime number, let K be a number field and let K_∞/K be a* non *Galois extension. Suppose that there exists a Galois extension L/K disjoint from K_∞/K such that LK_∞ is a Galois closure of K_∞/K. If LK_∞/L is a $\mathbb{Z}_p$-extension, then K_∞/K is called a fake $\mathbb{Z}_p$-extension.*

Our strategy to study the growth is to use a class number formula at finite levels and then to pass to the limit. This formula is not new (see for example [HK], [Ja1], [Le]...): anyway, we shall give a proof of it which seems to be different from others that can be found in the literature. For a number field M, let h_M denote its class number, R_M its regulator and E_M the group of units of M modulo torsion. In Section 2 we prove by analytic means (essentially Brauer formula for Artin L-functions) the following result:

Theorem. *Let q be an odd natural number and let F/K be a Galois extension whose Galois group is isomorphic to the dihedral group with $2q$ elements D_q. Let L (resp. k) be the field fixed by the cyclic subgroup of order q (resp. by one of the subgroups of order 2) of $\mathrm{Gal}(F/K)$. Then*

$$h_F = h_L \frac{h_k^2}{h_K^2} \cdot \frac{R_k^2 R_L}{R_K^2 R_F} \; .$$

In order to pass to the limit we need to give an algebraic interpretation to the ratio of regulators which appears in the theorem. This is done in Section 3, essentially by an elementary but rather technical linear algebra computation. The result is as follows:

Proposition. *With notations as above, let $k' = \rho(k)$ where ρ is a generator of the cyclic subgroup of order q in $\mathrm{Gal}(F/K)$. Then the following equality holds:*

$$[E_F : E_k E_{k'} E_L] = \frac{q R_k^2 2^{n-1}}{Q R_F R_K} \; .$$

where $n = [K : \mathbb{Q}]$.

Putting togheter the preceding theorem and the last proposition, we get a formula in Theorem 3.4 relating the class numbers of L, F, K and k involving only algebraic objects.

In Section 4, we take $K = \mathbb{Q}$. L is therefore an imaginary quadratic field and there is only one $\mathbb{Z}_p$-extension of L which is pro-p-dihedral over K, the so-called *anticyclotomic* $\mathbb{Z}_p$-extension of L, which we denote by L_∞. The main result of the section is then (notation as in the diagram at the beginning)

Theorem. *Let p^{ε_m} be the order of the p-Sylow class group of K_m. Then there exist integers μ_K, λ_K, ν_K such that*

$$2\varepsilon_m = \mu_K p^m + \lambda_K m + \nu_K \qquad \text{for} \quad m \gg 0 \ .$$

The main ingredients of the proof are the p-part of the formula proved in Section 2 and Section 3, Iwasawa's formula for L_∞/L and the interpretation of a quotient of units as a cohomology group (see Proposition 4.4). The more "Iwasawa Theory" approach of passing to the limit on this quotient and then descending fails here as the characteristic power series involved is T, as discusses after Proposition 4.4. We also give an intepretation of the invariants μ_K and λ_K in terms of the invariants μ_L and λ_L relative to L_∞/L (in fact we also get a proof of the parity of λ_K). In particular we find

$$\mu_L = \mu_K \quad \text{and} \quad \lambda_K = \lambda_L + \lambda_{\mathfrak{P}}$$

where $\lambda_{\mathfrak{P}}$ is the Iwasawa λ-invariant relative to the Λ-module ($\Lambda = \mathbb{Z}_p[\![T]\!]$) which is the projective limit of the cyclic subgroups of Cl_{L_m} generated by the classes of the products of all prime ideals of L_m which lie over p. It is worth mentioning that R. Gillard proved in [Gi] that

$$\lambda_L \equiv \mu_L \pmod 2 \quad \text{and} \quad \mu_L \leqslant 1 \ ,$$

the latter inequality becoming an equality if and only if p splits in L.

Section 5 is devoted to the study of the exact sequence

$$0 \to \mathrm{Ker}(\iota_m) \longrightarrow A_{K_m} \oplus A_{K'_m} \xrightarrow{\iota_m} A_{L_m} \longrightarrow A_{L_m}/A_{K_m}A_{K'_m} \to 0 \ . \qquad (1)$$

Here we denote by A_M the p-Sylow of the class group of any number field M. If M_∞/M is a $\mathbb{Z}_p$-extension or a fake $\mathbb{Z}_p$-extension, let $X_{M_\infty/M}$ (or X_M if the (fake) $\mathbb{Z}_p$-extension is clear) be the projective limit of A_{M_n} with respect to the norm map. Moreover

$$\iota_m\left(([I],\,[I'])\right) = [II'\mathcal{O}_{L_m}]$$

if I (resp. I') is an ideal of K_m (resp. K'_m). Here we are identifying A_{K_m} and $A_{K'_m}$ with their isomorphic images in A_{L_m} (the extension maps

$A_{K_m} \to A_{L_m}$ and $A_{K'_m} \to A_{L_m}$ are injections since L_m/K_m and L_m/K'_m are of degree $2 \neq p$). Passing to projective limit with respect to norms we get

$$0 \to \mathrm{Ker}(\iota_\infty) \longrightarrow X_K \oplus X_{K'} \xrightarrow{\iota_\infty} X_L \longrightarrow X_L/X_K X_{K'} \to 0\ . \tag{2}$$

Then the main result of Section 5 is

Theorem. *The following holds*

1. $\mathrm{Ker}(\iota_\infty)$ *is a $\mathbb{Z}_p$-module of rank 1 if p splits in L and it is finite otherwise;*

2. $X_L/X_K X_{K'}$ *is finite and its order divides $h_L^{(p)}/p^{n_0}$.*

where n_0 is the smallest natural number such that L_∞/L_{n_0} is totally ramified at every prime above p and $h_L^{(p)}$ denotes the order of the p-Sylow subgroup of the class group of L. In particular, X_L is finitely generated as $\mathbb{Z}_p$-module if and only if X_K is finitely generated as $\mathbb{Z}_p$-module and its rank is twice the rank of X_K if p does not split and $2\mathrm{rk}_{\mathbb{Z}_p} X_K + 1$ if p splits.

The tecniques involved in the proof give also an algebraic proof (only for odd parts) of the formula proved in Section 2 and Section 3.

Aknowledgements We would like to thank Ralph Greenberg for suggesting us to work on this topic and for many useful comments. Moreover, we thank Jean-François Jaulent for informing us that most of the results of this paper were proved with different techniques in [Ja2].

2 Class numbers formula for dihedral extensions.

Let q be an odd natural number. Let K be a number field and let F/K be a Galois extension whose Galois group is isomorphic to the dihedral group D_q (we shall identify from now on $\mathrm{Gal}(F/K)$ with D_q). Recall that D_q is the group generated by ρ and σ with relations

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

In particular D_q contains the cyclic group C_q of order q generated by ρ. Let L be the subextension of F/K fixed by C_q. Similarly, let k be the subextension of F/K fixed by the subgroup generated by σ.
Let M be a subextension of F/K: for a complex representation of $\mathrm{Gal}(F/M)$ with character χ, we consider the attached Artin L-function that we denote by $L(s, \chi, F/M)$ where $s \in \mathbb{C}$ has real part bigger than 1. We denote by χ_0^M the trivial character of $\mathrm{Gal}(F/M)$: note that

$$L(s, \chi_0^M, F/M) = \zeta_M(s)$$

where ζ_M is the Dedekind zeta function of M. We use here the notation $\zeta_M^*(s)$ for the special value of ζ_M at $s \in \mathbb{C} \setminus \{1\}$: by definition, $\zeta_M^*(s)$ is the first nontrivial coefficient in the Taylor expansion of ζ_M around s. By Dirichlet's theorem, we have

$$\zeta_M^*(0) = -\frac{h_M}{w_M} R_M \ , \tag{3}$$

where w_M is the number of roots of unity contained in M (this formula comes from the formula for the residue at 1 of ζ_M and the functional equation, see [Na], chapter 7). This notation will be used throughout of the paper.

We briefly recall how the irreducible characters of D_q are defined (for everything concerning representation theory in the following see [Se1], I, §5.3). There are two representations of degree 1, namely

$$\chi_0(\rho^a\sigma^b) = 1 \quad \text{for each } 0 \leqslant a \leqslant q-1,\ 0 \leqslant b \leqslant 1 \ ,$$

$$\chi_1(\rho^a\sigma^b) = (-1)^b \quad \text{for each } 0 \leqslant a \leqslant q-1,\ 0 \leqslant b \leqslant 1 \ .$$

Observe that $\chi_0^k = \chi_0$. Furthermore there are $q-1$ representations of degree 2, namely $\psi_1, \ldots, \psi_{(q-1)}$ which are defined by

$$\psi_h(\rho^a) = \begin{pmatrix} \zeta_q^{ha} & 0 \\ 0 & \zeta_q^{-ha} \end{pmatrix}, \qquad \psi_h(\rho^a\sigma) = \begin{pmatrix} 0 & \zeta_q^{-ha} \\ \zeta_q^{ha} & 0 \end{pmatrix} \ \forall\, 0 \leqslant a \leqslant q-1 \ .$$

for every $1 \leqslant h \leqslant q-1$, where ζ_q is a primitive q-th root of unity.

Proposition 2.1. *Let $r = (q-1)/2$. Then the representations*

$$\chi_0,\ \chi_1,\ \psi_1,\ \psi_2,\ \ldots,\ \psi_r$$

are the irreducible representations of D_q.

Proof. See [Se1], I, §5.3. □

In the following we shall denote by $\chi^{(h)}$ the character of ψ_h. Furthermore, if H is a subgroup of D_q and χ is a character of H whose corresponding representations is ψ, we denote by $\mathrm{Ind}_H^{D_q}\chi$ the character of the representation of D_q induced by ψ. Then we have

$$\left(\mathrm{Ind}_H^{D_q}\chi\right)(u) = \sum_{\substack{r \in R \\ r^{-1}ur \in H}} \chi(r^{-1}ur) \ , \tag{4}$$

where R is any system of representatives for D_q/H. The next lemma describes the characters of some induced representations in terms of the irreducible characters.

Lemma 2.2. *The following holds*

$$\mathrm{Ind}_{\{1\}}^{D_q}\chi_0^L = \chi_0 + \chi_1 + 2\sum_{h=1}^{r}\chi^{(h)} , \tag{5}$$

$$\mathrm{Ind}_{\langle\sigma\rangle}^{D_q}\chi_0^K = \chi_0 + \sum_{h=1}^{r}\chi^{(h)} , \tag{6}$$

$$\mathrm{Ind}_{C_q}^{D_q}\chi_0^F = \chi_0 + \chi_1 . \tag{7}$$

Proof. Equality in (5) follows from the fact that both terms equal the character of the regular representation of D_q.
In order to prove (6) we use (4) with $H = \langle\sigma\rangle$: choose $R = C_q$. Then clearly

$$\left(\mathrm{Ind}_{\langle\sigma\rangle}^{D_q}\chi_0^K\right)(\rho^a) = \begin{cases} q & \text{if } a = 0 \\ 0 & \text{if } 0 < a \leqslant q-1 \end{cases}$$

and

$$\left(\mathrm{Ind}_{\langle\sigma\rangle}^{D_q}\chi_0^K\right)(\rho^a\sigma) = 1$$

for every $0 \leqslant a \leqslant q-1$ (since $\rho^{-c}\rho^a\sigma\rho^c \in \langle\sigma\rangle$ if and only if $a \equiv 2c \pmod q$ and the latter has only one solution). On the other hand, the right-hand side of (6) verifies

$$\left(\chi_0 + \sum_{h=1}^{r}\chi^{(h)}\right)(1) = q$$

and, if $0 < a \leqslant q-1$,

$$\Big(\chi_0 + \sum_{h=1}^{r}\chi^{(h)}\Big)(\rho^a) = 1 + \sum_{h=1}^{r}\left(\zeta_q^{ha} + \zeta_q^{-ha}\right) = 1 + \sum_{h=1}^{q-1}\zeta_q^{ha} = 1 - 1 = 0 .$$

Furthermore, if $0 \leqslant a \leqslant q-1$,

$$\Big(\chi_0 + \sum_{h=1}^{r}\chi^{(h)}\Big)(\rho^a\sigma) = 1 + 0 = 1$$

which completes the proof of (6); (7) can be proven similarly. □

From now on, we let $\mu(M)$ denote the group of roots on unity of a number field M.

Lemma 2.3. *The following holds*

$$\mu(k) = \mu(K), \qquad \mu(F) = \mu(L) .$$

Proof. Let $\zeta \in \mu(F) \setminus \mu(K)$ be a root of unity of F which does not lie in K, and set $M = K(\zeta)$. Then M/K is a nontrivial abelian extension of K contained in F. In particular $\mathrm{Gal}(F/M)$ contains the commutator subgroup of D_q which is equal to C_q. Therefore, M/K being nontrivial, $\mathrm{Gal}(F/M) = C_q$ and $M = L$. This shows at once that $\mu(L) = \mu(F)$ and $\mu(k) = \mu(K)$ (since $F \cap k = K$). □

Theorem 2.4. *The following equality holds*

$$\zeta_F(s) = \zeta_L(s)\frac{\zeta_k(s)^2}{\zeta_K(s)^2}$$

for each $s \in \mathbb{C} \setminus \{1\}$. *In particular*

$$h_F = h_L \frac{h_k^2}{h_K^2} \cdot \frac{R_k^2 R_L}{R_K^2 R_F} ,$$

and $R_k^2 R_L / R_K^2 R_F$ *is a rational number.*

Proof. In the following we use various known properties of Artin L-functions: for their proofs see [He], §3. First of all note that, for every $s \in \mathbb{C}$ such that $\mathrm{Re}\, s > 1$,

$$\zeta_F(s) = L(s,\, \chi_0^F,\, F/F) =$$

$$= L(s,\, \mathrm{Ind}_{\{1\}}^{D_q} \chi_0^F,\, F/K) = L(s,\, \chi_0 + \chi_1 + 2\sum_{h=1}^{r} \chi^{(h)},\, F/K) =$$

$$= L(s,\, \chi_0,\, F/K) L(s,\, \chi_1,\, F/K) \prod_{h=1}^{r} L(s, \chi^{(h)},\, F/K)^2$$

by Lemma 2.2.
Now we consider ζ_k: we have

$$\zeta_k(s) = L(s,\, \chi_0^k,\, F/k) =$$

$$= L(s,\, \mathrm{Ind}_{\langle\sigma\rangle}^{D_q} \chi_0^k,\, F/K) = L(s,\, \chi_0 + \sum_{h=1}^{r} \chi^{(h)},\, F/K) =$$

$$= L(s,\, \chi_0,\, F/K) \prod_{h=1}^{r} L(s, \chi^{(h)},\, F/K)$$

by Lemma 2.2. Lastly, we consider ζ_L: we have

$$\zeta_L(s) = L(s,\, \chi_0^L,\, F/L) =$$

$$= L(s,\, \mathrm{Ind}_{C_q}^{D_q} \chi_0^k,\, F/K) = L(s,\, \chi_0 + \chi_1,\, F/K) =$$

$$= L(s,\, \chi_0,\, F/K) L(s, \chi_1,\, F/K)$$

again by Lemma 2.2. Hence

$$\zeta_F(s) = \zeta_L(s)\frac{\zeta_k(s)^2}{\zeta_K(s)^2} \tag{8}$$

for $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$ because

$$\zeta_K(s) = L(s,\, \chi_0,\, F/K)\ .$$

We deduce that (8) holds for every $s \in \mathbb{C} \smallsetminus \{1\}$. In particular the left and the right terms have the same special value at 0. We then deduce from (3) that

$$h_F = h_L \frac{h_k^2}{h_K^2} \cdot \frac{R_k^2 R_L}{R_K^2 R_F} \cdot \frac{w_K^2 w_F}{w_k^2 w_L} \tag{9}$$

and the formula in our statement then comes from Lemma 2.3. □

3 Algebraic interpretation of regulators

We shall now prove an algebraic interpretation of the term $(R_k^2 R_L)/(R_K^2 R_F)$ appearing in Theorem 2.4. An algebraic proof of the formula resulting from (9) can also be found in [HK], [Ja1], [Le] (see also the last section). The notation is the same as in Section 2, but we fix the following convention for the rest of this section:

> K is totally real of degree n over $\mathbb{Q}$ while F is totally imaginary (thus of degree $2qn$). Therefore L is a CM-field and $L^+ = K$.

As usual, $r_1(M)$ and $r_2(M)$ denote the number of real and imaginary places, respectively, of a number field M, and we recall the notation $r = (q-1)/2$ introduced in Proposition 2.1: we have

Lemma 3.1. *With the above convention, $r_1(k) = n$ and $r_2(k) = n(q-1)/2 = nr$.*

Proof. Since F is totally imaginary every infinite prime $\vartheta_i' : F \hookrightarrow \mathbb{C}$ of F has a decomposition subgroup of order 2 inside D_q. On the other hand, the number of real embeddings of k coincides with the number of infinite primes of k that ramify in F/k, therefore such that $\mathcal{I}(\vartheta_i') \subseteq \operatorname{Gal}(F/k)$ where $\mathcal{I}(\vartheta_i')$ is the decomposition group of ϑ_i': this is equivalent to $\mathcal{I}(\vartheta_i') = \operatorname{Gal}(F/k)$. Inside F there are exactly q fields of index 2, and they are all isomorphic to k: therefore the number of infinite primes of F such that $\mathcal{I}(\vartheta_i') = \operatorname{Gal}(F/k)$ must coincide with the number of infinite primes such that $\mathcal{I}(\vartheta_j') = \operatorname{Gal}(F/k')$ for every k' conjugate to k. Since there are exactly nq infinite primes in F, Dirichlet's Box Principle tells us that exactly n decomposition subgroups coincide with $\operatorname{Gal}(F/k)$, as stated. □

Let now $1 \neq \rho \in D_q$ be an automorphism of F fixing K of order q and set $k' = \rho(k)$. Since σ and ρ generate D_q and k is fixed by σ, if $\rho(k) = k$ then k would be a normal extension of K: therefore $k' \neq k$. We set $E_F = \mathcal{O}_F^\times / \mathrm{tor}_\mathbb{Z} \mathcal{O}_F^\times$ and similarly for k, k', L and K. Note that there are canonical embeddings $E_k \hookrightarrow E_F$, $E_{k'} \hookrightarrow E_F$ and $E_L \hookrightarrow E_F$. Moreover, it is not hard to see that

$$E_k E_{k'} = \mathcal{O}_k^\times \mathcal{O}_{k'}^\times / \mathrm{tor}_\mathbb{Z}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times)$$

(both groups are subgroups of E_F).

Lemma 3.2. *$\mathcal{O}_k^\times \mathcal{O}_{k'}^\times$ is of finite index in $\mathcal{O}_F^\times$ and $E_k E_{k'}$ is of finite index in E_F.*

Proof. Clearly it is enough to prove the first assertion, since we have an exact sequence

$$0 \to \mathrm{tor}_\mathbb{Z} \mathcal{O}_F^\times / \mathrm{tor}_\mathbb{Z}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) \to \mathcal{O}_F^\times / \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \to E_F / E_k E_{k'} \to 0.$$

Thanks to Lemma 3.1, $\mathrm{rk}_\mathbb{Z} \mathcal{O}_F^\times = nq - 1$ while $\mathrm{rk}_\mathbb{Z} \mathcal{O}_k^\times = \mathrm{rk}_\mathbb{Z} \mathcal{O}_{k'}^\times = n(r+1) - 1$. Therefore all we need to prove is that $\mathcal{O}_k^\times \cap \mathcal{O}_{k'}^\times \subseteq \mathcal{O}_K^\times$: indeed, this would imply that $\mathcal{O}_k^\times \cap \mathcal{O}_{k'}^\times = \mathcal{O}_K^\times$, and so $\mathrm{rk}_\mathbb{Z}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) = \mathrm{rk}_\mathbb{Z} \mathcal{O}_k^\times + \mathrm{rk}_\mathbb{Z} \mathcal{O}_{k'}^\times - \mathrm{rk}_\mathbb{Z} \mathcal{O}_K^\times = nq - 1$ which is precisely $\mathrm{rk}_\mathbb{Z} \mathcal{O}_F^\times$.
But the inclusion $\mathcal{O}_k^\times \cap \mathcal{O}_{k'}^\times \subseteq \mathcal{O}_K^\times$ is immediate once we know that $k \cap k' = K$; and this is clear, for $\mathrm{Gal}(F/k \cap k')$ contains both σ and $\rho\sigma$, and thus both σ and ρ. Hence $\mathrm{Gal}(F/k \cap k') = D_q = \mathrm{Gal}(F/K)$, from which $k \cap k' = K$. □

Remark. The above proof shows, in particular, that $\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times$ (resp. $E_k E_{k'} E_L$) is of finite index in $\mathcal{O}_F^\times$ (resp. E_F).

As in the proof of Lemma 3.2, the units of k have $\mathbb{Z}$-rank equal to $n(r+1) - 1$, while those of K and of L have $\mathbb{Z}$-rank equal to $n - 1$; finally, then, $\mathrm{rk}_\mathbb{Z}(\mathcal{O}_F^\times) = nq - 1$. By the elementary divisors theorem and Lemma 2.3, we can choose subsets $\{\eta_j\}_{j=1}^{n(r+1)} \subseteq \mathcal{O}_k^\times$ and $\{a_j\}_{j=1}^n \subseteq \mathbb{N}$ such that

$$\mathcal{O}_k^\times = \mathrm{tor}_\mathbb{Z} \mathcal{O}_K^\times \oplus \bigoplus_{j=1}^{n(r+1)} \eta_j^\mathbb{Z} \quad \text{and} \quad \mathcal{O}_K^\times = \mathrm{tor}_\mathbb{Z} \mathcal{O}_K^\times \oplus \bigoplus_{j=1}^{n} \eta_j^{a_j \mathbb{Z}} \tag{10}$$

(recall that $\mathrm{tor}_\mathbb{Z} \mathcal{O}_K^\times = \mathrm{tor}_\mathbb{Z} \mathcal{O}_k^\times$, by Lemma 2.3). Then

$$\mathcal{O}_{k'}^\times = \mathrm{tor}_\mathbb{Z} \mathcal{O}_K^\times \oplus \bigoplus_{j=1}^{n(r+1)} \rho(\eta_j)^\mathbb{Z}.$$

Moreover we also have

$$\mathcal{O}_k^\times \mathcal{O}_{k'}^\times = \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) \oplus \bigoplus_{j=1}^{n(r+1)} \eta_j^{\mathbb{Z}} \oplus \bigoplus_{j=n+1}^{n(r+1)} \rho(\eta_j)^{\mathbb{Z}}. \tag{11}$$

This can be seen as follows: first of all we show that

$$\bigoplus_{j=1}^{n(r+1)} \eta_j^{\mathbb{Z}} \cap \bigoplus_{j=n+1}^{n(r+1)} \rho(\eta_j)^{\mathbb{Z}} = \{1\}.$$

Suppose that we have

$$\prod_{j=1}^{n(r+1)} \eta_j^{b_j} \prod_{j=n+1}^{n(r+1)} \rho(\eta_j)^{c_j} = 1.$$

Then

$$\prod_{j=n+1}^{n(r+1)} \rho(\eta_j)^{c_j} \in \mathcal{O}_k^\times \cap \mathcal{O}_{k'}^\times = \mathcal{O}_K^\times = \mathrm{tor}_{\mathbb{Z}} \mathcal{O}_K^\times \oplus \bigoplus_{j=1}^{n} \eta_j^{a_j \mathbb{Z}}.$$

Now note that $\rho(\eta_j) = \eta_j \zeta_j$ where $\zeta_j \in \mathrm{tor}_{\mathbb{Z}} \mathcal{O}_F^\times$ is an a_j-th root of unity (this follows from $\rho(\eta_j^{a_j}) = \eta_j^{a_j}$ which holds because $\eta_j^{a_j} \in K$). This means that

$$\prod_{j=n+1}^{n(r+1)} \rho(\eta_j)^{c_j} = \zeta \prod_{j=n+1}^{n(r+1)} \eta_j^{c_j} = \xi \prod_{j=1}^{n} \eta_j^{a_j d_j}$$

for some $\xi \in \mathrm{tor}_{\mathbb{Z}} \mathcal{O}_K^\times$ and $\zeta = \prod \zeta_j^{c_j}$. This equation can actually be seen in $\mathcal{O}_F^\times$ and gives $\zeta = \xi$ and $c_j = 0$ for any $n+1 \leqslant j \leqslant n(r+1)$ and $d_j = 0$ for any $1 \leqslant j \leqslant n$ since

$$(\mathrm{tor}_{\mathbb{Z}} \mathcal{O}_F^\times \cap \mathrm{tor}_{\mathbb{Z}} \mathcal{O}_K^\times) \oplus \bigoplus_{j=1}^{n(r+1)} \eta_j^{\mathbb{Z}} = \{1\}.$$

But then we also have $b_j = 0$ for any $1 \leqslant j \leqslant n(r+1)$. Therefore (11) is proved and we have

$$R_F[E_k E_{k'}^\times] = R_F \left[\bigoplus_{j=1}^{n(r+1)} \eta_j^{\mathbb{Z}} \oplus \bigoplus_{j=n+1}^{n(r+1)} \rho(\eta_j)^{\mathbb{Z}} \right]$$

where, for a subgroup $A \subseteq E_F$, $R_F[A]$ denotes its regulator.

Remark. Before we prove the main result of this section we observe that

$$\prod_{j=1}^{n} a_j = |\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times / \mathcal{O}_K^\times)| \tag{12}$$

(which is clear from (10)) and there is an isomorphism

$$\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times)/\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times \cong \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times/\mathcal{O}_K^\times). \tag{13}$$

To see this, consider the map

$$\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) \xrightarrow{\phi} \mathcal{O}_k^\times/\mathcal{O}_K^\times$$

defined by $\phi(xx') = [x]$, where $x \in \mathcal{O}_k^\times$, $x' \in \mathcal{O}_{k'}^\times$ and $xx' \in \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times)$. First of all, this definition makes sense, since if $xx' = yy'$ with $y \in \mathcal{O}_k^\times$ and $y' \in \mathcal{O}_{k'}^\times$, then $xy^{-1} = (x')^{-1}y' \in \mathcal{O}_k \cap \mathcal{O}_{k'} = \mathcal{O}_K$ (and therefore $\phi(yy') = [y] = [x]$). Now clearly $\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_K^\times) = \ker\phi$ (once more because $\mathcal{O}_k \cap \mathcal{O}_{k'} = \mathcal{O}_K$) and of course $\mathrm{Im}\phi \subseteq \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times/\mathcal{O}_K^\times)$. On the other hand, suppose that $x \in \mathcal{O}_k^\times$ and there exists $n \in \mathbb{N}$ such that $x^n \in \mathcal{O}_K^\times$. Then $(x\rho(x^{-1}))^n = 1$ (recall that $\rho(k) = k'$) which means that $x\rho^{-1}(x^{-1}) \in \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times)$ and $\phi(x\rho(x^{-1})) = [x]$. This proves $\mathrm{Im}\phi = \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times/\mathcal{O}_K^\times)$ and therefore ϕ gives an isomorphism as in (13). In particular using (12) and (13), we get

$$\prod_{j=1}^{n} a_j = (\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times). \tag{14}$$

Proposition 3.3. *The following equality holds:*

$$(\mathcal{O}_F^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times) = \frac{qR_k^2 R_L}{R_K^2 R_F} (\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \cap \mathcal{O}_L^\times : \mathcal{O}_K^\times)\,.$$

Proof. Note that

$$(\mathcal{O}_F^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times) = \frac{(\mathcal{O}_F^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times)}{(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times)} =$$

$$= \frac{(E_F : E_k E_{k'})(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times))}{(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times)}.$$

This follows from the fact that the natural map

$$\mathcal{O}_k^\times \mathcal{O}_{k'}^\times/\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) \longrightarrow E_k E_k' = \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_F^\times)/\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_F^\times)$$

is an isomorphism. Now

$$\frac{(E_F : E_k E_{k'})(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times))}{(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times)} =$$

$$= \frac{(E_F : E_k E_{k'})(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times))}{(\mathcal{O}_L^\times : \mathcal{O}_K^\times)} (\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \cap \mathcal{O}_L^\times : \mathcal{O}_K^\times).$$

Hence we need to prove that

$$\frac{(E_F : E_k E_{k'})(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times))}{(\mathcal{O}_L^\times : \mathcal{O}_K^\times)} = \frac{qR_k^2 R_L}{R_K^2 R_F}. \tag{15}$$

We first prove that

$$R_L[E_k E_{k'}] = \frac{q2^{n-1}(R_k)^2}{R_K}(\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times). \tag{16}$$

Thanks to Lemma 3.1 we define $\gamma'_l : k \hookrightarrow \mathbb{R}$ for $0 \leqslant l \leqslant n-1$ to be the real embeddings of k and $\tau'_i : k \hookrightarrow \mathbb{C}$ for $1 \leqslant i \leqslant nr$ to be the non-equivalent imaginary embeddings[1] of k. Analogously, let $\vartheta'_i : F \hookrightarrow \mathbb{C}$ for $0 \leqslant i \leqslant nq-1$ be the non-equivalent (imaginary) embeddings of F. We order them so that ϑ'_{lq} extends γ'_l for $0 \leqslant l \leqslant n-1$; while ϑ'_{lq+i} and ϑ'_{lq+i+r} extend τ'_{lr+i} for $0 \leqslant l \leqslant n-1$ and for $1 \leqslant i \leqslant r$. Without loss of generality (changing ρ if necessary in another element of order q) we can also assume that $\rho(\vartheta'_{lq+i}) = \vartheta'_{lq+i+1}$ for $0 \leqslant i \leqslant r-1$ and $0 \leqslant l \leqslant n-1$. The relation $\rho\sigma = \sigma\rho^{-1}$ together with $\sigma(\vartheta'_{lq+i}) = \vartheta'_{lq+i+r}$ then gives

$$\begin{cases} \rho(\vartheta'_{lq+i}) & = \vartheta'_{lq+i+1} & 0 \leqslant i \leqslant r-1, 0 \leqslant l \leqslant n-1 \\ \rho(\vartheta'_{lq+r}) & = \vartheta'_{(l+1)q-1} & 0 \leqslant l \leqslant n-1 \\ \rho(\vartheta'_{lq+r+1}) & = \vartheta'_{lq} & 0 \leqslant l \leqslant n-1 \\ \rho(\vartheta'_{lq+r+j}) & = \vartheta'_{lq+r+j-1} & 2 \leqslant j \leqslant r, 0 \leqslant l \leqslant n-1 \; . \end{cases} \tag{17}$$

By definition, setting $\vartheta_i = 2\log|\vartheta'_i|, \tau_i = 2\log|\tau'_i|$ and $\gamma_l = \log|\gamma'_l|$, the regulators take the form

$$R_F[\langle \eta_1, \ldots, \rho(\eta_{n(r+1)-1})\rangle] = \left| \det \begin{pmatrix} \vartheta_i(\eta_j)_{\substack{0\leqslant i\leqslant nq-2 \\ 1\leqslant j\leqslant n-1}} \\ \hline \vartheta_i(\eta_j)_{\substack{0\leqslant i\leqslant nq-2 \\ n\leqslant j\leqslant n(r+1)-1}} \\ \hline \vartheta_i(\rho(\eta_j))_{\substack{0\leqslant i\leqslant nq-2 \\ n\leqslant j\leqslant n(r+1)-1}} \end{pmatrix} \right|$$

and[2]

$$R_k = \left| \det \left(\gamma_l(\eta_j)_{\substack{0\leqslant l\leqslant n-1 \\ 1\leqslant j\leqslant n(r+1)-1}} \;\middle|\; \tau_i(\eta_j)_{\substack{1\leqslant i\leqslant nr-1 \\ 1\leqslant j\leqslant n(r+1)-1}} \right) \right| .$$

Before rewriting $\vartheta_i(\eta_j)$ in terms of the τ_i's, two remarks are in order. First of all, the lowest part of the matrix defining the first regulator can be rewritten in terms of the $\vartheta_i(\eta_j)$ only, thanks to (17). Secondly, in the definition of a

[1]The reason for the primes will appear shortly.

[2]In the next and in the last formula we use a somehow non- standard notation to write matrices. It should though be clear from the contest what we mean: in the last formula the matrix naturally splits vertically in three submatrices, each of one we describe explicitely. In the following, the splitting is horizontal.

regulator in F (resp. in k), only $nq-1$ (resp. $n(r+1)-1$) embeddings play a role, since the units lie in the subspace defined by

$$\vartheta_{nq-1} = -\sum_{i=0}^{nq-2} \vartheta_i \quad \big(resp.\ \tau_{nr} = -\sum_{l=0}^{n-1} \gamma_l - \sum_{i=1}^{nr-1} \tau_i\big)\ . \tag{18}$$

In the sequel this relations will be used: moreover, unlike (18) that holds for all units in F, there is also the relation

$$\vartheta_{(n-1)q}(\eta_j^{a_j}) = -\sum_{l=0}^{n-2} \vartheta_{lq}(\eta_j^{a_j}) \qquad \forall\ 1 \leqslant j \leqslant n-1$$

since $\eta_j^{a_j} \in E_K$ for $1 \leqslant j \leqslant n-1$. But then of course

$$\vartheta_{(n-1)q}(\eta_j) = -\sum_{l=0}^{n-2} \vartheta_{lq}(\eta_j) \qquad \forall\ 1 \leqslant j \leqslant n-1. \tag{19}$$

Observe now that our ordering ensures us that for all $1 \leqslant j \leqslant n(r+1)-1$ we have $\vartheta_{lq+i}(\eta_j) = \tau_{lr+i}(\eta_j)$ if $0 \leqslant l \leqslant n-1$ and $1 \leqslant i \leqslant r$; that we have $\vartheta_{lq+i+r}(\eta_j) = \tau_{lr+i}(\eta_j)$ if $0 \leqslant l \leqslant n-1$ and $1 \leqslant i \leqslant r$; and $\vartheta_{lq}(\eta_j) = 2\gamma_l(\eta_j)$ for $0 \leqslant l \leqslant n-1$. Putting all together, (16) has been reduced (use (17), (18), (10) and (14)) to the equation

$$|\det(\Xi)| = \frac{q|\det(\Psi)|^2 2^{n-1}}{|\det(\Phi)|^{-1}} \prod_{j=1}^{n} a_j = \frac{q|\det(\Psi)|^2 2^{n-1}}{|\det(\Phi)|^{-1}} (\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}} \mathcal{O}_K^\times) \tag{20}$$

for the three matrices appearing below in (21), and whose determinants give the regulators we are computing: we should thus introduce some notation in order to define them.

- **A** $A[l] \in \mathcal{M}_{(n-1)\times(r+1)}(\mathbb{R})$ is the matrix $A[l]_{i,j} = \tau_{lr+i}(\eta_j)$ for $0 \leqslant l \leqslant n-1$, $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant n-1$; and $A[l]_{0,j} = 2\gamma_l(\eta_j)$ for $0 \leqslant l \leqslant n-1$ and $1 \leqslant j \leqslant n-1$. First of all, using (18), we have $A[n-1]_{r,j} = -\sum_{i=0}^{n-1} \gamma_i(\eta_j) - \sum_{i=1}^{nr-1} \tau_i(\eta_j) = -\sum_{l=0}^{n-1} \frac{A[l]_{0,j}}{2} - \sum_{l=0}^{n-1}\sum_{i=1}^{r-1} A[l]_{i,j} - \sum_{l=1}^{n-1} A[l-1]_{r,j}$ for all $1 \leqslant j \leqslant n-1$. Thanks to (19) we also have $A[n-1]_{0,j} = -\sum_{l=0}^{n-2} 2\gamma_l(\eta_j) = -\sum_{l=0}^{n-2} A[l]_{0,j}$ for every $1 \leqslant j \leqslant n-1$, finally finding $A[n-1]_{r,j} = -\sum_{l=0}^{n-1}\sum_{i=1}^{r-1} A[l]_{i,j} - \sum_{l=1}^{n-1} A[l-1]_{r,j}$ for all $1 \leqslant j \leqslant n-1$.

B For $0 \leqslant l \leqslant n-2$, $B[l] \in \mathcal{M}_{(n-1)\times r}(\mathbb{R})$ is the matrix $B[l]_{i,j} = \tau_{lr+i}(\eta_j) = A[l]_{i,j}$ for $1 \leqslant j \leqslant n-1$ and $1 \leqslant i \leqslant r$, while $B[n-1] \in \mathcal{M}_{(n-1)\times(r-1)}(\mathbb{R})$ is the matrix $B[n-1]_{i,j} = \tau_{(n-1)r+i}(\eta_j) = A[n-1]_{i,j}$ for $1 \leqslant j \leqslant n-1$ and $1 \leqslant i \leqslant r-1$ (this modification of the last $B[l]$ comes from the fact that the $(nq-1)$-st embedding ϑ_{nq-1} does not show up in the regulator, thanks to (18): the same phenomenon will appear below in $\mathbf{D}$ and in $\widetilde{\mathbf{D}}$).

C We now define $C[l] \in \mathcal{M}_{(nr)\times(r+1)}(\mathbb{R})$ to be the matrix $C[l]_{i,j} = \tau_{lr+i}(\eta_j)$ for $0 \leqslant l \leqslant n-1$, $n \leqslant j \leqslant n(r+1)-1$, $1 \leqslant i \leqslant r$ and $C[l]_{0,j} = 2\gamma_l(\eta_j)$ for $0 \leqslant l \leqslant n-1$, $n \leqslant j \leqslant n(r+1)-1$. Here again, by (18), we find $C[n-1]_{r,j} = -\sum_{l=0}^{n-1} \frac{C[l]_{0,j}}{2} - \sum_{l=0}^{n-1}\sum_{i=1}^{r-1} C[l]_{i,j} - \sum_{l=1}^{n-1} C[l-1]_{r,j}$ for all $n \leqslant j \leqslant n(r+1)-1$.

D For $0 \leqslant l \leqslant n-2$ we define $D[l] \in \mathcal{M}_{(nr)\times r}(\mathbb{R})$ to be the matrix $D[l]_{i,j} = \tau_{lr+i}(\eta_j) = C[k]_{i,j}$ for $n \leqslant j \leqslant n(r+1)-1$ and $1 \leqslant i \leqslant r$ while, as before, $D[n-1] \in \mathcal{M}_{(nr)\times(r-1)}(\mathbb{R})$ is the matrix $D[n-1]_{i,j} = \tau_{(n-1)r+i}(\eta_j) = C[n-1]_{i,j}$ for $n \leqslant j \leqslant n(r+1)-1$ and $1 \leqslant i \leqslant r-1$.

Finally, we let ρ act on these last two sets of matrices: but we use (17) to write their elements as other embeddings of the same units.

$\widetilde{\mathbf{C}}$ We set $\tilde{C}[l] \in \mathcal{M}_{(nr)\times(r+1)}(\mathbb{C})$ to be the matrix $\tilde{C}[l]_{i,j} = \tau_{lr+i+1}(\eta_j) = C[l]_{i+1,j}$ for $0 \leqslant l \leqslant n-1$, $n \leqslant j \leqslant n(r+1)-1$, $0 \leqslant i \leqslant r-1$ and $\tilde{C}[l]_{r,j} = \tau_{(l+1)r}(\eta_j) = \tilde{C}[l]_{r-1,j}$ for $0 \leqslant l \leqslant n-1$, $n \leqslant j \leqslant n(r+1)-1$. Applying (18) we find $\tilde{C}[n-1]_{r,j} = \tilde{C}[n-1]_{r-1,j} = -\sum_{i=0}^{n-1} \frac{\tilde{C}[i]_{0,j}}{2} - \sum_{l=0}^{n-1}\sum_{i=1}^{r-1} \tilde{C}[l]_{i,j} - \sum_{l=1}^{n-1} \tilde{C}[l-1]_{r,j}$ for all $n \leqslant j \leqslant n(r+1)-1$.

$\widetilde{\mathbf{D}}$ For $0 \leqslant l \leqslant n-2$, we define $\tilde{D}[l] \in \mathcal{M}_{(nr)\times(r)}(\mathbb{C})$ to be the matrix $\tilde{D}[l]_{i,j} = \tau_{lr+i-1}(\eta_j) = C[l]_{i-1,j}$ for $n \leqslant j \leqslant n(r+1)-1$ and $2 \leqslant i \leqslant r$ and $\tilde{D}[l]_{1,j} = 2\gamma_l(\eta_j) = C[l]_{0,j}$ for $n \leqslant j \leqslant n(r+1)-1$; for $l = n-1$, $\tilde{D}[n-1] \in \mathcal{M}_{(nr)\times(r-1)}(\mathbb{C})$ is the matrix $\tilde{D}[n-1]_{i,j} = \tau_{(n-1)r+i-1}(\eta_j) = C[n-1]_{i-1,j}$ for $n \leqslant j \leqslant n(r+1)-1$ and $2 \leqslant i \leqslant r-1$ while $\tilde{D}[n-1]_{1,j} = 2\gamma_{(n-1)}(\eta_j) = C[n-1]_{0,j}$ for $n \leqslant j \leqslant n(r+1)-1$.

Observe that our indexing of elements in the various submatrices might be confusing: indeed, the *row* index always starts from 1, as well as the column index for $\mathbf{B}$ and for $\mathbf{D}$, $\widetilde{\mathbf{D}}$ while the *column* index for $\mathbf{A}$ and for $\mathbf{C}$, $\widetilde{\mathbf{C}}$ starts with 0: this is consistent with our indexing for the embeddings. We agree to denote with M^i the i-th column of a matrix M and with M_i its i-th row and, finally, we introduce the notation ${}_2M$ to denote the matrix such that ${}_2M^0 = (1/2)M^0$ and ${}_2M^i = M^i$ for $i \geqslant 1$. Having set all this up, we put

$$\Xi = \left(\begin{array}{c|c|c|c|c|c|c} A[0] & B[0] & A[1] & B[1] & \cdots & A[n-1] & B[n-1] \\ \hline C[0] & D[0] & C[1] & D[1] & \cdots & C[n-1] & D[n-1] \\ \hline \tilde{C}[0] & \tilde{D}[0] & \tilde{C}[1] & \tilde{D}[1] & \cdots & \tilde{C}[n-1] & \tilde{D}[n-1] \end{array}\right), \qquad (21)$$

$$\Psi = \left(\begin{array}{c|c|c|c} {}_2A[0] & {}_2A[1] & \dots & \left(\frac{A[n-1]^0}{2}, A[n-1]^1, \dots, A[n-1]^{r-2}\right) \\ \hline {}_2B[0] & {}_2B[1] & \dots & \left(\frac{B[n-1]^0}{2}, B[n-1]^1, \dots, B[n-1]^{r-2}\right) \end{array}\right) \qquad (21)$$

and

$$\Phi = \frac{1}{2}\Big(A[0]^0, A[1]^0, \dots, A[n-2]^0\Big)\,. \qquad (21)$$

To check (20) is a straightforward but pretty cumbersome row-and-columns operation. We give all the details in the case $n = 1$ in the Appendix (the general case being a similar but much lengthier and heavier computation). Hence (16) holds and in particular (see [Wa], Lemma 4.15)

$$(E_F : E_kE_{k'}) = \frac{R_F[E_kE_{k'}]}{R_F} = \frac{2^{n-1}qR_k^2}{R_KR_F}(\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times). \qquad (22)$$

Now note that, using Lemma 2.3, we get

$$\frac{(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times))}{(\mathcal{O}_L^\times : \mathcal{O}_K^\times)} = \frac{(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times)}{(\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times)(E_L : E_K)(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_L^\times : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times)}$$

$$= \frac{1}{(\mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times) : \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_K^\times)Q}$$

where $Q = (\mathcal{O}_L^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_L^\times)\mathcal{O}_K^\times) = (E_L : E_K)$ is equal to 1 or 2 (see Theorem 4.12 of [Wa]). Now by (22) we have

$$(E_F : E_kE_{k'}) = \frac{2^{n-1}qR_k^2(\mathcal{O}_L^\times : \mathcal{O}_K^\times)}{QR_KR_F(\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times))}$$

which is exactly (15), thanks to Proposition 4.16 of [Wa]. □

Theorem 3.4. *[See [HK] Satz 5, [Ja1] Proposition 12, [Le] Theorem 2.2] Let q be an odd number and let K be a totally real number field. For every totally imaginary dihedral extension F/K of degree $2q$ the equality*

$$h_F = \frac{(\mathcal{O}_F^\times : \mathcal{O}_k^\times\mathcal{O}_{k'}^\times\mathcal{O}_L^\times)}{(\mathcal{O}_k^\times\mathcal{O}_{k'}^\times \cap \mathcal{O}_L^\times : \mathcal{O}_K^\times)} \cdot \frac{h_Lh_k^2}{qh_K^2}$$

holds, where $k \subset F$ is a subfield of index 2, $k' = \rho(k)$ for some element of order q in $\mathrm{Gal}(F/K)$ *and $L \subset F$ is the subfield of index q.*

Proof. Just apply Theorem 2.4 together with Proposition 3.3. □

Remark. Note that, when $K = \mathbb{Q}$, then

$$(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times \cap \mathcal{O}_L^\times : \mathcal{O}_K^\times) = 1.$$

This can be seen as follows: suppose $x \in \mathcal{O}_k^\times$, $x' \in \mathcal{O}_{k'}^\times$ and $xx' \in \mathcal{O}_L^\times$. Then $(xx')^{12} = 1$, since

$$\mathcal{O}_L^\times = \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_L^\times)$$

because L is imaginary quadratic. This implies that

$$x^{12} \in \mathcal{O}_k^\times \cap \mathcal{O}_{k'}^\times = \mathcal{O}_{\mathbb{Q}}^\times = \{\pm 1\}.$$

In particular $x \in \mathrm{tor}_{\mathbb{Z}}\mathcal{O}_k^\times$ and, since $\mu(k) = \mu(\mathbb{Q})$, we must have $x = 1$ or $x = -1$ (see also [HK], Satz 5).

4 Iwasawa type class number formula.

In this section we consider the behaviour of the class number in a tower of dihedral fields. First of all, recall the following classical definition:

Definition 4.1. *Let K be a number field and let p be a prime number. A Galois extension K_∞/K such that* $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ *is called a $\mathbb{Z}_p$-extension. In this case,*

$$\bigcup_{n\in\mathbb{N}} K_n = K_\infty \supset \ldots \supset K_n \supset K_{n-1} \supset \ldots K_1 \supset K_0 = K\ ,$$

where K_n/K is a Galois extension such that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

The behaviour of the class number in this tower is controlled by a celebrated theorem of Kenkichi Iwasawa, namely

Theorem (K. Iwasawa, [Iw], Theorem 4.2)**.** *Let K_∞/K be a $\mathbb{Z}_p$-extension and let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist three integers μ, λ and ν such that*

$$e_n = \mu p^n + \lambda n + \nu \qquad \text{for } n \gg 0\,.$$

We want now to investigate if the same holds in a more general setting, namely dropping the Galois condition. We start with the following

Definition 4.2. *Let p be a prime number, let K be a number field and let K_∞/K be a* non *Galois extension. Suppose that there exists a Galois extension L/K disjoint from K_∞/K such that LK_∞ is a Galois closure of K_∞/K. If LK_∞/L is a $\mathbb{Z}_p$-extension, then K_∞/K is called a fake $\mathbb{Z}_p$-extension.*

Remark. If K_∞/K is a fake $\mathbb{Z}_p$-extension as in Definiton 4.2, then

$$\mathrm{Gal}(LK_\infty/K) \cong \mathrm{Gal}(LK_\infty/L) \rtimes \mathrm{Gal}(LK_\infty/K_\infty).$$

Indeed, one can also formulate the definition of fake $\mathbb{Z}_p$-extensions in terms of structures of Galois groups. Moreover K_∞ is then the union

$$K_\infty = \bigcup_{n\in\mathbb{N}} K_n$$

where K_n is the extension of K fixed by $\mathrm{Gal}(LK_\infty/L)^{p^n} \rtimes \mathrm{Gal}(LK_\infty/K_\infty)$, of degree p^n. Note, moreover, that K_n/K is the only subextension of K_∞/K of degree p^n and every subextension of K_∞/K is one of the K_n, a property which is also enjoyed by $\mathbb{Z}_p$-extension. It would be interesting to know whether or not this property characterize (fake)-$\mathbb{Z}_p$-extensions. We thank Gabriele Dalla Torre for many fruitful discussions on this subject.

As an example of a fake $\mathbb{Z}_p$-extension, let L be an imaginary quadratic field and let p be an odd prime: it is known (see, for instance, [Wa], chapter 13) that the compositum of its $\mathbb{Z}_p$-extensions has Galois group isomorphic to $\mathbb{Z}_p^2$. Since $\mathrm{Gal}(L/\mathbb{Q})$ acts semisimply on this Galois group, it decomposes $\mathbb{Z}_p^2$ accordingly to its characters, giving two independent $\mathbb{Z}_p$-extensions, both Galois over $\mathbb{Q}$: the cyclotomic $\mathbb{Z}_p$-extension L_{cyc} and the anticyclotomic one L_∞. The first one is cyclic over $\mathbb{Q}$, the second one is pro-dihedral, namely,

$$\mathrm{Gal}(L_{cyc}/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{while} \quad \mathrm{Gal}(L_\infty/\mathbb{Q}) \cong \varprojlim D_{p^n} \ .$$

Let D_{p^∞} be the pro-dihedral group isomorphic to $\mathrm{Gal}(L_\infty/\mathbb{Q})$: it admits two topological generators, which we consider fixed from now on, σ and ρ_∞ such that

$$\sigma^2 = 1 \qquad \sigma\rho_\infty = \rho_\infty^{-1}\sigma \ . \tag{23}$$

If L_n is the n-th layer of the anticyclotomic extension of L, then $L_n = L_\infty^{\langle \rho_\infty^{p^n} \rangle}$ (where $\langle \rho_\infty^{p^n} \rangle$ denotes the closed subgroup of D_{p^∞} generated by $\rho_\infty^{p^n}$): we define, accordingly, $K_n = L_\infty^{\langle \rho_\infty^{p^n}, \sigma \rangle} \subset L_n$ (where $\langle \rho_\infty^{p^n}, \sigma \rangle$ denotes the closed subgroup of D_{p^∞} generated by $\rho_\infty^{p^n}$ and σ). Then K_n is a (non normal) extension of $K = \mathbb{Q}$ of degree p^n and we set $K_\infty = L_\infty^{\langle \sigma \rangle}$ to find a diagram of fields as in the introduction. Therefore $K_\infty/\mathbb{Q}$ is a fake $\mathbb{Z}_p$-extension.

Another example may be the following: let $K = \mathbb{Q}(\zeta_p)$ where p is a primitive p-th root of unity and let $a \in K^\times$, $a \notin \mu_p$. Then $K(\sqrt[p^\infty]{a})/K$ is a fake $\mathbb{Z}_p$-extension, as it can easily be seen by taking $L = F(\zeta_{p^\infty})$: this case would fit in a much more general setting, as the one introduced in [VV], and we hope to investigate it in a future work.

In the sequel we study the pro-dihedral case over $\mathbb{Q}$, with notations introduced in the above example. The main result of this section is then Theorem 4.7 below. The strategy for the study of the growth of the class number in this setting is given by Theorem 3.4. In the following, we shall always make the following

[H] Hypothesis: If $p = 3$, then $L \neq \mathbb{Q}(\sqrt{-3})$

This is not a real restriction, since in that case the class groups of K_n, L_n and L have trivial 3-Sylow subgroups and any of the stated result trivially holds. For $n \geqslant 1$, we define

$$P_n = \mathcal{O}_{K_n}^\times \mathcal{O}_{K_n'}^\times \otimes \mathbb{Z}_p, \quad U_n = \mathcal{O}_{L_n} \otimes \mathbb{Z}_p, \quad R_n = U_n/P_n$$

where the inclusion $P_n \hookrightarrow U_n$ is induced by the injection $\mathcal{O}_{K_n}^\times \mathcal{O}_{K_n'}^\times \hookrightarrow E_{L_n}$: therefore $|R_n|$ is the p-part of the quotient of units appearing in Theorem 3.4 (note that E_L is trivial thanks to assumption **[H]**). Morever, we can also write

$$P_n = E_{K_n} E_{K_n'} \otimes \mathbb{Z}_p \quad \text{and} \quad U_n = E_{L_n} \otimes \mathbb{Z}_p$$

because $\mathrm{tor}_{\mathbb{Z}} \mathcal{O}_{K_n}^\times$ and $\mathrm{tor}_{\mathbb{Z}} \mathcal{O}_{L_n}^\times$ are always of order coprime to p, again by **[H]**. Note that P_n, U_n and R_n are D_{p^n}-modules (see for example [HK], Lemma 1). We let $\Gamma = \mathrm{Gal}(L_\infty/L)$ and we write $G_n = \Gamma/\Gamma^{p^n} = \mathrm{Gal}(L_n/L)$ (or, more generally, $G_{m,n} = \mathrm{Gal}(L_m/L_n)$ for $m \geqslant n \geqslant 0$), while we henceforth call Δ the group $\mathrm{Gal}(L/\mathbb{Q})$ and we fix a subgroup of $\mathrm{Gal}(L_\infty/\mathbb{Q})$, also called Δ, mapping isomorphically onto $\mathrm{Gal}(L/\mathbb{Q})$ via restriction. Finally, $\Lambda = \mathbb{Z}_p[[\Gamma]]$ will be the completed group algebra of Γ, isomorphic to $\mathbb{Z}_p[[T]]$ by the choice of a topological generator γ_0 of Γ.

What we want to do is to compare the action of G_n with that of D_{p^n}, by comparing their cohomology. We start with the following cohomological result which is certainly well-know but difficult to find in print. As a matter of notation, recall that if H is a group and B an H-module, then B^H denotes invariants, B_H coinvariants, $N_H = \sum_{h \in H} h \in \mathbb{Z}[H]$ the norm, $B[N_H]$ the kernel of multiplication by the norm and I_H the augmentation ideal.

Proposition 4.3. *Let A be a 2-divisible abelian D_{p^n}-module: then, for every $i \geqslant 0$, there are canonical isomorphisms induced by restriction (or corestriction)*

$$H^i(D_{p^n}, A) \cong H^i(G_n, A)^\Delta ,$$
$$H_i(D_{p^n}, A) \cong H_i(G_n, A)_\Delta .$$

Moreover,

$$\widehat{H}^0(D_{p^n}, A) \cong \widehat{H}^0(G_n, A)^\Delta$$

and

$$\widehat{H}^{-1}(D_{p^n}, A) \cong \widehat{H}^{-1}(G_n, A)_\Delta \cong \widehat{H}^{-1}(G_n, A)^\Delta \ .$$

Finally, the Tate isomophism $\widehat{H}^i(G_n, A) \cong \widehat{H}^{i+2}(G_n, A)$ is Δ-antiequivariant, so that (as D_{p^n}-modules with trivial action)

$$\widehat{H}^{-1}(D_{p^n}, A) = \widehat{H}^{-1}(G_n, A)^\Delta = \widehat{H}^1(G_n, A)/\widehat{H}^1(D_{p^n}, A)$$

and

$$\widehat{H}^1(D_{p^n}, A) = \widehat{H}^1(G_n, A)^\Delta = \widehat{H}^{-1}(G_n, A)/\widehat{H}^{-1}(D_{p^n}, A)$$

Proof. The first isomorphism is an immediate application of the Hochschild-Serre Spectral Sequence (see, for instance, [We], 6.8). We now consider Tate cohomology: taking Δ-invariants in the tautological sequence

$$0 \to N_{G_n}A \to H^0(G_n, A) \to \widehat{H}^0(G_n, A) \to 0$$

we find (use, as before, that $N_{G_n}A$ is 2-divisible, thus its Δ-cohomology is trivial) $\widehat{H}^0(G_n, A)^\Delta = H^0(G_n, A)^\Delta/(N_{G_n}A)^\Delta$. Since, as observed, $N_{G_n}A$ has trivial Δ-cohomology and Δ is a cyclic group,

$$\widehat{H}^0(\Delta, N_{G_n}A) \cong H^2(\Delta, N_{G_n}A) = 0$$

so that $(N_{G_n}A)^\Delta = N_\Delta N_{G_n}A = N_{D_{p^n}}A$ and finally (using the first isomorphism in our statement)

$$\widehat{H}^0(G_n, A)^\Delta = H^0(G_n, A)^\Delta/(N_{G_n}A)^\Delta = H^0(D_{p^n}, A)/N_{D_{p^n}}A = \widehat{H}^0(D_{p^n}, A)$$

as claimed. In degree -1, take Δ-coinvariants of the tautological exact sequence defining the Tate group to get the sequence

$$0 \to \widehat{H}^{-1}(G_n, A)_\Delta \to H_0(G_n, A)_\Delta \to (A/A[N_{G_n}])_\Delta \to 0 \ . \qquad (24)$$

where, as before, we have $(A/A[N_{G_n}])_\Delta = A_\Delta/A[N_{G_n}]_\Delta$. Take now Δ-coninvariants in the exact sequence

$$0 \to A[N_{G_n}] \to A \to N_{G_n}A \to 0 \qquad (25)$$

to identify the quotient $A_\Delta/A[N_{G_n}]_\Delta$ with $(N_{G_n}A)_\Delta$. We claim that

$$A/A[N_{D_{p^n}}] \xrightarrow{N_{G_n}} (N_{G_n}A)_\Delta = N_{G_n}A/I_\Delta(N_{G_n}A) \qquad (26)$$

is an isomorphism: first of all, the map is well defined, since for every $x \in A[N_{D_{p^n}}]$, we have $N_{G_n}(x) \in N_{G_n}(A)[N_\Delta] = (I_\Delta)N_{G_n}(A)$ because

$\widehat{H}^{-1}(\Delta, N_{G_n}) = H^1(\Delta, N_{G_n}) = 0$. The same argument shows injectivity, since for every $a \in A$ such that $N_\Delta(N_{G_n}(a)) = 0$, we have $N_{D_{p^n}}(a) = 0$, while surjectivity is obvious. Plugging now the isomorphism of (26) in (24) through the identification induced by (25) we find

$$0 \to \widehat{H}^{-1}(G_n, A)_\Delta \to H_0(D_{p^n}, A) \to A/A[N_{D_{p^n}}] \to 0 \ .$$

showing our claim. The fact now that $\widehat{H}^{-1}(G_n, A)^\Delta = \widehat{H}^{-1}(G_n, A)_\Delta$ comes from splitting any 2-divisible Δ-module M as $M = M^+ \oplus M^-$ *canonically*, writing $m = (m+\delta m)/2 + (m-\delta m)/2$: here we denote by M^+ the eigenspace on which Δ acts trivially and by M^- the eigenspace on which it acts as -1. Then $M^\Delta = M^+ = M/M^- = M_\Delta$.

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

$$\begin{array}{ccc} \widehat{H}^i(G_n, A) & \longrightarrow & \widehat{H}^{i+2}(G_n, A) \\ x & \longmapsto & x \cup \chi \end{array}$$

The action of $\delta \in \Delta$ on $\widehat{H}^i(G_n, A)$ is δ_* in the notation of [NSW], I.5 and this action is -1 on $H^2(G_n, \mathbb{Z})$ as can immediately be seen through the isomorphism $H^2(G_n, \mathbb{Z}) \cong \mathrm{Hom}(G_n, \mathbb{Q}/\mathbb{Z})$ (see [We], example 6.7.10). Then, by Proposition 1.5.3 of [NSW], $\delta_*(x \cup \chi) = -(\delta_* x) \cup \chi$ which gives the result. □

The key tool for studying the growth of the p-part of h_{K_n} along the fake $\mathbb{Z}_p$-extension is to interpret the quotient R_n as a cohomology group. We have the following

Proposition 4.4. *With notations as above, for every $n \geqslant 0$ there is an isomorphisms of abelian groups*

$$R_n \cong H^1(G_n, U_n)^\Delta \cong H^1(D_{p^n}, U_n) \ .$$

Proof. Along the proof, set $V_n = E_{K_n} \otimes \mathbb{Z}_p$, $V'_n = E_{K'_n} \otimes \mathbb{Z}_p$. $U_n/I_{G_n}U_n$ is a 2-divisible Δ-module. Hence

$$U_n/I_{G_n}U_n = (U_n/I_{G_n}U_n)^+ \oplus (U_n/I_{G_n}U_n)^- \ ,$$

as in the proof of Proposition 4.3. Moreover, we claim that

$$(U_n/I_{G_n}U_n)^+ = (U_n/I_{G_n}U_n)^\Delta = V_n V'_n/I_{G_n}U_n \ : \tag{27}$$

this is quite clear by definition of the action of Δ since

$$V_n I_{G_n} U_n/I_{G_n}U_n = (U_n/I_{G_n}U_n)^{\langle\sigma\rangle} = (U_n/I_{G_n}U_n)^\Delta$$

but also

$$V_n' I_{G_n} U_n / I_{G_n} U_n = (U_n / I_{G_n} U_n)^{\langle \rho^2 \sigma \rangle} = (U_n / I_{G_n} U_n)^{\Delta} \ .$$

We deduce that

$$V_n V_n' I_{G_n} U_n / I_{G_n} U_n = (U_n / I_{G_n} U_n)^{\Delta} \ ,$$

and since

$$I_{G_n} U_n \subseteq V_n V_n'$$

(see for example [Le], Lemma 3.3) we get (27). Then

$$R_n = U_n / I_{G_n} U_n \Big/ V_n V_n' / I_{G_n} U_n \cong (U_n / I_{G_n} U_n)^{-}$$

as Δ-modules. Since $U_n / I_{G_n} U_n = \widehat{H}^{-1}(G_n, U_n)$ we find, by Proposition 4.3, that

$$R_n = \widehat{H}^{-1}(G_n, U_n) / \widehat{H}^{-1}(G_n, U_n)^{\Delta} = \widehat{H}^1(D_{p^n}, U_n) \ . \tag{28}$$

□

Corollary 4.5. *R_n is a G_n-module with trivial action and the injection $i_n : U_n \hookrightarrow U_{n+1}$ induces an injective map*

$$i_n : R_n \hookrightarrow R_{n+1} \ .$$

Proof. By the first equality in (28), the action of G_n on R_n is trivial since R_n is a quotient of a trivial G_n-module. Now the induced map $i_n : R_n \to R_{n+1}$ corresponds to the restriction on minus parts of

$$i_n : U_n / I_{G_n} U_n \to U_{n+1} / I_{G_{n+1}} U_{n+1} \ .$$

The commutativity of the diagram

$$\begin{array}{ccc} \widehat{H}^{-1}(G_n, U_n) & \xrightarrow{\ i_n\ } & \widehat{H}^{-1}(G_{n+1}, U_{n+1}) \\ \cong \big\downarrow \cup\chi & & \cong \big\downarrow \cup\chi \\ \widehat{H}^1(G_n, U_n) & \xhookrightarrow{\ \mathrm{inf}\ } & \widehat{H}^1(G_{n+1}, U_{n+1}) \end{array}$$

is immediate to check and proves our statement. □

Remark. For $m \geqslant n \geqslant 0$, let $N_{m,n} : L_m \to L_n$ be the usual "arithmetic" norm. With the same notation we will also indicate the induced maps on E_{L_n}, or on E_{K_n}, as well as on P_n and U_n. One can check that this induces a well-defined map $N_{m,n} : R_m \to R_n$, so that we can form the projective limits of the tautological exact sequence

$$0 \longrightarrow P_n \longrightarrow U_n \longrightarrow R_n \longrightarrow 0$$

to get an exact sequence

$$0 \longrightarrow \varprojlim P_n := P_\infty \longrightarrow \varprojlim U_n := U_\infty \longrightarrow \varprojlim R_n := R_\infty \longrightarrow 0 \qquad (29)$$

that is exact on the right since $\varprojlim^1 P_n = 0$ as all the P_n's are compact modules (see, for instance, [We], Proposition 3.5.7): in particular, $R_\infty \cong U_\infty / P_\infty$ as Λ-modules. In Iwasawa theory, one classically tries to get information at finite levels from the study of some Λ-module, via the so-called *co-descent* maps: indeed, if $Z = \varprojlim Z_n$ is a Λ-module one has a co-descent map $k_n : (Z)_{\Gamma_n} \to Z_n$. Since the size of $(Z)_{\Gamma_n}$ is well-behaved with respect to n, if one can bound the orders of $\ker(k_n)$ and of $\operatorname{coker}(k_n)$ indipendently of n, then one can also control the growth of Z_n. Unfortunately, we cannot apply this strategy to study the order of R_n, since Corollary 4.5 shows, by passing to the limit, that the Λ-module R_∞ has a trivial action of Γ and this is precisely the obstruction for the boundness of $\ker(k_n)$ and of $\operatorname{coker}(k_n)$.

Before stating our main result, we need a general lemma. In the following, for a number field M, denote by A_M the p-Sylow subgroup of the class group of M (isomorphic to the maximal p-quotient of the class group).

Lemma 4.6. *Let M_∞/M be a $\mathbb{Z}_p$-extension in which all primes above p are ramified. For every sufficiently large n (*i. e.* large enough that all primes above p are totally ramified in M_∞/M_n) let $\mathfrak{p}_{1,n}, \ldots, \mathfrak{p}_{s,n}$ be the primes in M_n above p and let $\mathfrak{P}_n = \prod_{i=1}^{s} \mathfrak{p}_{i,n}$ be their product. Then there exist two integers $\lambda_{\mathfrak{P}}, \nu_{\mathfrak{P}}$ independent of n such that the order of the the projection of the class of $\mathfrak{P}_n$ in A_{M_n} is $n\lambda_{\mathfrak{P}} + \nu_{\mathfrak{P}}$.*

Proof. For every $n \in \mathbb{N}$, let H_n be the cyclic subgroup of A_{M_n} generated by the projection of $\mathfrak{P}_n$. Clearly, the H_n's form a projective system and we set $Y = \varprojlim H_n$. Setting $X = \varprojlim A_{M_n}$, then $Y \subseteq X$ is a Λ-module and X/Y is a noetherian Λ-module (it corresponds to the maximal unramified extension of M_∞ in which the product of all Frobenius automorphisms of primes above p is trivial): let μ, λ, ν be the Iwasawa invariants of X. Then X/Y also admits three Iwasawa invariants $\tilde{\lambda}, \tilde{\mu}, \tilde{\nu}$: moreover, Y is clearly finitely generated over $\mathbb{Z}_p$, so $\tilde{\mu} = \mu$. Setting $\lambda_{\mathfrak{P}} = \lambda - \tilde{\lambda}$ and $\nu_{\mathfrak{P}} = \nu - \tilde{\nu}$ we establish the Lemma. □

Remark. Observe that the proof itself shows that Y is procyclic, so it is either finite or free of rank 1 over $\mathbb{Z}_p$ and, accordingly, $\lambda_{\mathfrak{P}} \leqslant 1$. We will come later on this. Now we go back to our anticyclotomic setting.

Theorem 4.7. *Let p^{ε_n} be the order of the p-Sylow class group of K_n. Then there exist integers μ_K, λ_K, ν_K such that*

$$2\varepsilon_n = \mu_K p^n + \lambda_K n + \nu_K \qquad \text{for} \quad n \gg 0\ .$$

Proof. As it is well-known (see, for instance, [Wa], Lemma 13.3) only primes above p may ramify in L_∞/L and at least one of those must eventually ramify, while the fact that $L_n/\mathbb{Q}$ is Galois for every n shows that, if one is ramified in L_n so is the other (if it exists) and with the same ramification index. Let thus n_0 be the smallest integer such that they are totally ramified in L_∞/L_{n_0} and assume $n \geqslant \max\{n_0, \tilde{n}\}$ where $\tilde{n}$ is the smallest integer such that the formula in Iwasawa's theorem (see the beginning of this section) for L_∞/L applies. Then by Theorem 3.4 applied with $k = K_n$ and $F = L_n$ we have

$$2\varepsilon_n = e_n - r_n + n - f = \mu_L p^n + (\lambda_L + 1)n + \nu' - r_n\ , \tag{30}$$

where $|R_n| = p^{r_n}$, $|A_L| = p^f$, $\nu' = \nu_L - f$ and μ_L, λ_L, ν_L are the Iwasawa invariants of L_∞/L. We thus want to control the growth of r_n along the tower. To do this, we apply Proposition 4.4 studying explicitly $H^1(D_{p^n}, U_n)$, since

$$r_n = v_p(|H^1(D_{p^n}, U_n)|)\ . \tag{31}$$

To analyze $H^1(D_{p^n}, U_n)$, set $B^\diamond := B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for any abelian group B: this is an exact functor so we have the exact sequence

$$0 \to U_n \to (L_n^\times)^\diamond \to Pr_n^\diamond \to 0$$

where Pr_n is the group of principal ideals of L_n. Taking D_{p^n}-cohomology we get, by Hilbert 90, an isomorphism[3]

$$(Pr_n^\diamond)^{D_{p^n}}/(\mathbb{Q}^\times)^\diamond \cong H^1(D_{p^n}, U_n)\ . \tag{32}$$

On the other hand, the exact sequence

$$0 \to Pr_n^\diamond \to Id_n^\diamond \to A_{L_n} \to 0 \tag{33}$$

[3] We use, here and in what follows, that for every G-module A, there is an isomorphism $H^q(G, A) \otimes \mathbb{Z}_p \cong H^q(G, A \otimes \mathbb{Z}_p)$ holding for every $q \geqslant 0$. This is an easy exercise about the Grothendieck spectral sequence for the functors $(-) \otimes \mathbb{Z}_p$ and $(-)^G$. To verify that tensoring with $\mathbb{Z}_p$ sends injective G-modules to G-acyclic, use the explicit description in [Se2], chapitre VII. For the equivalent result in Tate cohomology apply Proposition 4.3 together with the above remark. René Schoof pointed out to us that one can also prove directly the isomorphism $\widehat{H}^q(G, A) \otimes \mathbb{Z}_p \cong \widehat{H}^q(G, A \otimes \mathbb{Z}_p)$ by tensoring the complex giving raise to Tate cohomology with $\mathbb{Z}_p$.

defining the class group (so Id_n is the group of fractional ideals of L_n) induces an inclusion

$$(Pr_n^\diamond)^{D_{p^n}}/(\mathbb{Q}^\times)^\diamond \hookrightarrow (Id_n^\diamond)^{D_{p^n}}/(\mathbb{Q}^\times)^\diamond \, .$$

This last quotient is fairly explicit: indeed, an ideal $I = \prod \mathfrak{q}_i^{a_i}$ is fixed by D_{p^n} if and only if every prime appears with the same exponent with all its D_{p^n}-conjugates: for a prime $\mathfrak{l}$ call the product of all this conjugates $Orb(\mathfrak{l})$. Then clearly (recall that all modules here are $\mathbb{Z}_p$-modules, so primes ramified only in $L/\mathbb{Q}$ generate the same module as the rational prime below them)

$$Orb(\mathfrak{l})^{\mathbb{Z}_p} = \begin{cases} \ell^{\mathbb{Z}_p} & \text{where } \mathfrak{l} \mid \ell \in \mathbb{Q} \quad \text{if } \mathfrak{l} \nmid p \\ \\ \mathfrak{P}_n^{\mathbb{Z}_p} = (\prod_{\mathfrak{p}_n \mid p \text{ in } L_n} \mathfrak{p}_n)^{\mathbb{Z}_p} & \text{where } \mathfrak{P}_n^{p^{n-n_0}} = p \in \mathbb{Q} \quad \text{if } \mathfrak{l} \mid p \end{cases} .$$

The fact that these are the only possibilities for ramification follows from the definition of n_0: moding now out by $(\mathbb{Q}^\times)^\diamond$ we find

$$(Id_n^\diamond)^{D_{p^n}}/(\mathbb{Q}^\times)^\diamond = \mathfrak{P}_n^{\mathbb{Z}_p}/p^{\mathbb{Z}_p} \cong \mathbb{Z}/p^{n-n_0}\mathbb{Z} \, ,$$

and accordingly

$$(Pr_n^\diamond)^{D_{p^n}}/(\mathbb{Q}^\times)^\diamond = \mathfrak{P}_n^{p^{h_n}\mathbb{Z}_p}/p^{\mathbb{Z}_p} \cong \mathbb{Z}/(p^{n-n_0-h_n})\mathbb{Z}$$

where p^{h_n} is the order of the class of $\mathfrak{P}_n$ in A_{L_n}. Applying Lemma 4.6 we find $h_n = \lambda_{\mathfrak{P}} n + \nu_{\mathfrak{P}}$ and this, together with (32), shows that

$$H^1(D_{p^n}, U_n) \cong \mathbb{Z}/p^{(1-\lambda_{\mathfrak{P}})n - n_0 - \nu_{\mathfrak{P}}}\mathbb{Z} \, .$$

We now achieve the proof of the theorem plugging this information in (31) in order to find the existence of suitable invariants λ_r and ν_r such that $r_n = \lambda_r n + \nu_r$, so that equation (30) becomes our statement. □

Remark. Following explicitly the proof, one finds that $\lambda_r = 1 - \lambda_{\mathfrak{P}}$, which is at most 1 by the above remark, and $\nu_r = -n_0 - \nu_{\mathfrak{P}}$. Accordingly,

$$\mu_K = \mu_L \, , \qquad \lambda_K = \lambda_L + 1 - \lambda_r = \lambda_L + \lambda_{\mathfrak{P}} \, , \qquad \nu_K = \nu_L - f + n_0 + \nu_{\mathfrak{P}} \, :$$

in particular, λ_K is either λ_L or $\lambda_L + 1$ and it is *even*: to see this, just use our formula to write explicitly $2(\varepsilon_{n+1} - \varepsilon_n)$. Analogously one can prove that $\mu_K \equiv \nu_K \pmod 2$.

Definition 4.8. *Denote by p^{h_n} the order of the class of $\mathfrak{P}_n$ in A_{L_n}, where $\mathfrak{P}_n$ is the product of all primes above p in L_n. Moreover, let n_0 be the smallest integer such that L_∞/L_{n_0} is totally ramified.*

For later use, we extract the following result from the proof of the theorem.

Proposition 4.9. *There is a short exact sequence*

$$0 \to H^1(D_{p^n}, U_n) \to \mathbb{Z}/p^{n-n_0}\mathbb{Z} \to H^0(D_{p^n}, A_{L_n}) \to 0$$

and isomorphisms

$$H^1(D_{p^n}, U_n) \cong \mathbb{Z}/p^{n-n_0-h_n}\mathbb{Z}, \quad H^0(D_{p^n}, A_{L_n}) \cong \mathbb{Z}/p^{h_n}\mathbb{Z} .$$

Proof. In the long exact D_{p^n}-cohomology sequence of

$$0 \to U_n \to (L_n^\times)^\diamond \to Pr_n^\diamond \to 0$$

one has $H^1(D_{p^n}, (L_n^\times)^\diamond) = 0$ by Hilbert 90 together with $H^2(D_{p^n}, U_n) = H^2(G_n, U_n)^\Delta = \widehat{H}^0(G_n, U_n)^- = 0$ as $U_0 = 0$; thus $H^1(D_{p^n}, Pr_n^\diamond) = 0$. Taking D_{p^n}-cohomology in (33) one finds

$$0 \to H^0(D_{p^n}, Pr_n^\diamond) \to H^0(D_{p^n}, Id_n^\diamond) \to H^0(D_{p^n}, A_{L_n}) \to 0$$

and, moding out by $(\mathbb{Q}^\times)^\diamond$,

$$H^0(D_{p^n}, Pr_n^\diamond)/(\mathbb{Q}^\times)^\diamond \hookrightarrow H^0(D_{p^n}, Id_n^\diamond)/(\mathbb{Q}^\times)^\diamond \twoheadrightarrow H^0(D_{p^n}, A_{L_n}) \; ; \qquad (34)$$

Since in the proof of Theorem 4.7 we found isomorphisms

$$H^0(D_{p^n}, Pr_n^\diamond)/(\mathbb{Q}^\times)^\diamond \cong H^1(D_{p^n}, U_n) \cong \mathbb{Z}/p^{n-n_0-h_n}\mathbb{Z},$$

$$H^0(D_{p^n}, Id_n^\diamond)/(\mathbb{Q}^\times)^\diamond \cong \mathbb{Z}/p^{n-n_0}\mathbb{Z} ,$$

the exact sequence (34) becomes that of our statement. □

Corollary 4.10. *R_n is a cyclic group of order $p^{n-n_0-h_n}$ and R_∞ is procyclic.*

Proof. Combine Proposition 4.4 with Proposition 4.9. □

We stress on the fact that the preceding result gives also a way to compute R_n directly (*i. e.* without Theorem 3.4).

Applying the Snake Lemma to multiplication-by-$(\gamma_n - 1)$ (where γ_n is a topological generator of Γ_n) to the sequence in (29) gives the fundamental exact sequence

$$U_\infty^{\Gamma_n} \longrightarrow R_\infty \longrightarrow (P_\infty)_{\Gamma_n} \longrightarrow (U_\infty)_{\Gamma_n} \longrightarrow R_\infty \longrightarrow 0 \, . \qquad (35)$$

where $(R_\infty)^{\Gamma_n} = R_\infty = (R_\infty)_{\Gamma_n}$ since R_∞ has trivial Γ action by Corollary 4.5. The next proposition shows that actually $(U_\infty)^{\Gamma_n} = 0$; it crucially depends on a result of Jean-Robert Belliard (see [Be]).

Proposition 4.11. *P_∞ and U_∞ are free Λ-modules of rank* 1.

Proof. By [Gre], Proposition 1, we know that the projective limit U'_∞ of the p-units along the anticyclotomic extension is Λ-free of rank 1. Now, Proposition 1.3 of [Be] gives a sufficient condition for a projective limit to be free. Namely, suppose that a projective system of $\mathbb{Z}_p[G_n]$-modules $(Z_n)_{n\in\mathbb{N}}$, equipped with norm maps $N_{m,n} : Z_m \to Z_n$ and extension maps $i_{n,m} : Z_n \to Z_m$ (both for $m \geqslant n \geqslant 0$) verifying the obvious relations, satisfies the following conditions:

1. There exists another projective system $W_n \supseteq Z_n$ with norm and injection maps inducing the above maps on Z_n by restriction such that $W_\infty = \varprojlim W_n$ is Λ-free;

2. Extension maps $i_{n,m} : W_n \hookrightarrow W_m^{G_{m,n}}$ are injective for $m \geqslant n \geqslant 0$;

3. $Z_m^{G_{m,n}} = i_{n,m}(Z_n)$ (at least for $m \geqslant n \gg 0$) ,

then $Z_\infty = \varprojlim Z_n$ is also Λ-free.

First of all we apply this result to $U_\infty \subseteq U'_\infty$, finding that it is Λ-free, and of Λ-rank equal to 1 thanks to the exact sequence

$$0 \longrightarrow U_\infty \longrightarrow U'_\infty \xrightarrow{\prod v_{\mathfrak{p}}} \mathbb{Z}_p[S_\infty] \longrightarrow 0$$

where S_∞ is the (finite) set of p-places in L_∞ (the right arrow is the product of all $\mathfrak{p}$-valuations for $\mathfrak{p} \mid p$): in particular, $U_\infty^{\Gamma_n} = 0$. Then we apply the proposition again with $Z_n = P_n$ and $W_n = U_n$: in fact, only the third condition needs to be checked and that comes from the Snake Lemma applied to the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_n & \longrightarrow & U_n & \longrightarrow & R_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i_{n,m}} & & \downarrow{\scriptstyle i_{n,m}} & & \downarrow{\scriptstyle i_{n,m}} & & \\
0 & \longrightarrow & P_n^{G_{n,m}} & \longrightarrow & U_n^{G_{n,m}} & \longrightarrow & R_m^{G_{n,m}} & &
\end{array}$$

noting that the vertical arrow in the middle is an isomorphism and the right-hand vertical arrow is injective by Corollary 4.5. Thus we get that P_∞ is Λ-free: its Λ-rank is equal to the Λ-rank of U_∞ by Lemme 1.1 of [Be] together with (35), since we have already proved that $U_\infty^{\Gamma_n} = 0$. □

This Proposition already shows that either $R_\infty = 0$ or R_∞ is free of rank 1 over $\mathbb{Z}_p$: indeed, (29) shows that R_∞ injects in $(P_\infty)_{\Gamma_n}$ for all n, as $(R_\infty)_{\Gamma_n} = R_\infty$. On the other hand, P_∞ being free, the $\mathbb{Z}_p$-rank of $(P_\infty)_\Gamma$ coincides with the Λ-rank of P_∞ which is 1 by the above Proposition. As $\mathbb{Z}_p$ does not admit any finite non-trivial submodules, the only possibilities for R_∞ are 0 or $\mathbb{Z}_p$.

Otherwise we can argue as follows: by Corollary 4.5 we know that $R_n \cong \mathbb{Z}/p^{(1-\lambda_{\mathfrak{P}})n-c}\mathbb{Z}$ for some constant c. If $\lambda_{\mathfrak{P}} = 0$ then $R_\infty \cong \mathbb{Z}_p$. If $\lambda_{\mathfrak{P}} = 1$ then the R_n's have bounded orders: since transition maps are induced by norms (as $R_n \hookrightarrow R_{n+1}$ by Corollary 4.5, we need not to distinguish between *algebraic* and *arithmetic* norm) and Proposition 4.4 shows that G_n acts trivially on R_n, R_∞ is the projective limit of cyclic groups of bounded order with respect to multiplication by p, so it is 0. We have thus proved

Corollary 4.12. *With notations as in Theorem 4.7, if $\lambda_{\mathfrak{P}} = 1$ then $R_\infty = 0$ and if $\lambda_{\mathfrak{P}} = 0$ then R_∞ is free of rank 1 over $\mathbb{Z}_p$.*

Remark. In the proof of Theorem 5.9 below we will show that $\lambda_{\mathfrak{P}} = 1$ if p splits in F and $\lambda_{\mathfrak{P}} = 0$ if p does not.

5 Structure of X_K

We now want to connect the study of X_L and X_K: we recall that

$$X_L := \varprojlim A_{L_n} \quad \text{and} \quad X_K := \varprojlim A_{K_n},$$

projective limits being taken with respect to norms. If L_∞/L were the cyclotomic $\mathbb{Z}_p$-extension of L, then X_L would be known to be $\mathbb{Z}_p$-finitely generated by a celebrated result of B. Ferrero and L. Washington (see [FW]), but for the anticyclotomic extension this is no more the case (see [Gi] and [Ja2]). We are interested in giving conditions for X_K to be finitely generated as $\mathbb{Z}_p$-module. Our strategy is to study the quotient $X_L/X_K X_{K'}$. The following exact sequence is then useful

$$0 \to \mathrm{Ker}(\iota_n) \longrightarrow A_{K_n} \oplus A_{K'_n} \xrightarrow{\iota_n} A_{L_n} \longrightarrow A_{L_n}/A_{K_n}A_{K'_n} \to 0 \qquad (36)$$

where

$$\iota_n\big(([I],\, [I'])\big) = [II'\mathcal{O}_{L_n}]$$

if $I \subset \mathcal{O}_{K_n}$ and $I' \subseteq \mathcal{O}_{K'_n}$ are ideals. Passing to projective limit we get

$$0 \to \mathrm{Ker}(\iota_\infty) \longrightarrow X_K \oplus X_{K'} \xrightarrow{\iota_\infty} X_L \longrightarrow X_F/X_K X_{K'} \to 0 \qquad (37)$$

and

$$\mathrm{Ker}(\iota_\infty) = \varprojlim \mathrm{Ker}(\iota_n)\ .$$

We will describe $\mathrm{Ker}(\iota_n)$ and $A_{L_n}/A_{K_n}A_{K'_n}$ in terms of cohomology groups. The following diagram will be useful:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_n & \longrightarrow & (L_n^\times)^\diamond & \longrightarrow & Pr_n^\diamond & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{U}_n^\diamond & \longrightarrow & \mathcal{J}_n^\diamond & \longrightarrow & Id_n^\diamond & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Q_n & \longrightarrow & \mathcal{C}_n^\diamond & \longrightarrow & A_{L_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
\tag{38}
$$

Here $\mathcal{J}_n$ is the idèles group, $\mathcal{C}_n$ is the idèles class group, $\mathcal{U}_n$ is the group of idèles units, Id_n is the group of ideals and Pr_n is the group of principal ideals of L_n. Remember that for an abelian group B we set $B^\diamond := B \otimes \mathbb{Z}_p$.

Proposition 5.1. *We have*

$$\mathrm{Ker}(\iota_n) \cong H^0(D_{p^n}, A_{L_n}) \cong H^1(D_{p^n}, Q_n)$$

and

$$\widehat{H}^{-1}(D_{p^n}, A_{L_n}) \cong \widehat{H}^0(D_{p^n}, Q_n) \ .$$

Proof. Let φ be the map

$$\varphi : \mathrm{Ker}(\iota_n) \longrightarrow H^0(D_{p^n}, A_{L_n})$$

defined by $\varphi([I],[I'])) = \iota_{K_n}([I])$. Since $\iota_{K_n}([I']) = \iota_{K_n'}([I])^{-1}$, both σ and $\rho\sigma$ fix $\iota_{K_n}([I])$, so the map takes indeed value in $H^0(D_{p^n}, A_{L_n})$. We claim that φ is an isomorphism. It is clearly injective: to check surjectivity, just observe that $A_{L_n}^{\langle\sigma\rangle} = \iota_{K_n}(A_{K_n})$ (and analogously for $\sigma\rho$), so that, for every $[J] \in H^0(D_{p^n}, A_{L_n})$, we can write $[J] = \iota_{K_n}([I]) = \iota_{K_n'}([I'])$ and $[J] = \varphi([I],[I'])$ and the claim is established.
Now consider the exact sequence

$$0 \to Q_n \to \mathcal{C}_n^\diamond \to A_{L_n} \to 0$$

as in diagram (38). We take D_{p^n}-Tate cohomology, making constant use of Proposition 4.3, and we get

$$
\begin{aligned}
0 \to \widehat{H}^{-1}(D_{p^n}, A_{L_n}) \to \widehat{H}^0(D_{p^n}, Q_n) \to \widehat{H}^0(D_{p^n}, \mathcal{C}_n^\diamond) \\
\to \widehat{H}^0(D_{p^n}, A_{L_n}) \to \widehat{H}^1(D_{p^n}, Q_n) \to 0 \ ,
\end{aligned}
\tag{39}
$$

since by class field theory $\widehat{H}^i(G_n, \mathcal{C}_n^\diamond) = 0$ if $i \equiv 1 \pmod 2$ and

$$|\widehat{H}^i(D_{p^n}, \mathcal{C}_n^\diamond)| = |\widehat{H}^i(G_n, \mathcal{C}_n^\diamond)^\Delta| .$$

However, also the middle term in the exact sequence (39) is trivial, since class field theory gives a Δ-modules isomorphism

$$\widehat{H}^0(G_n, \mathcal{C}_n^\diamond) \xrightarrow{\cong} \mathrm{Gal}(L_n/L)$$

and the latter has no Δ-invariants (since $\mathrm{Gal}(L_n/\mathbb{Q})$ is dihedral). Note that

$$\widehat{H}^0(D_{p^n}, A_{L_n}) = H^0(D_{p^n}, A_{L_n})$$

since $A_{L_n}[N_{D_{p^n}}] = A_{L_n}$ because $A_{\mathbb{Q}} = 0$. □

Lemma 5.2. *Let g denote the number of primes above p in L (hence $g \in \{1, 2\}$) and let n_0 be as in Definition 4.8. Then $\widehat{H}^0(D_{p^n}, \mathcal{U}_n^\diamond)$ is a cyclic group of order $p^{(g-1)(n-n_0)}$ and $\widehat{H}^1(D_{p^n}, \mathcal{U}_n^\diamond)$ is a cyclic group of order p^{n-n_0}.*

Proof. We start by studying G_n-cohomology. Local class field theory gives Δ-equivariant identifications

$$\widehat{H}^0(G_n, \mathcal{U}_n^\diamond) \cong I(\mathfrak{p}_1) \times I(\mathfrak{p}_2) \quad \text{resp. } \widehat{H}^0(G_n, \mathcal{U}_n^\diamond) \cong I(\mathfrak{p}_1)$$

where $I(\mathfrak{p}_i)$ is the inertia subgroup inside G_n of the prime $\mathfrak{p}_i$ of L above p, accordingly as p splits or not in L (here and in the rest of the proof, we let $i = 1, 2$ if p splits, while $i = 1$ if p does not split). Analogously,

$$\begin{aligned} H^1(G_n, \mathcal{U}_n^\diamond) &\cong \widehat{H}^1(G_n, \mathcal{O}_{n,\mathfrak{P}_1}^\times) \times \widehat{H}^1(G_n, \mathcal{O}_{n,\mathfrak{P}_2}^\times) \\ \text{resp.} \quad H^1(G_n, \mathcal{U}_n^\diamond) &\cong \widehat{H}^1(G_n, \mathcal{O}_{n,\mathfrak{P}_1}^\times) \end{aligned}$$

where $\mathcal{O}_{n,\mathfrak{P}_i}^\times$ are the local units at the prime $\mathfrak{P}_i$ of L_n above p, accordingly again as p splits or not in L.
Concerning $\widehat{H}^0$, it is clear how Δ acts on the cohomology group, since if there is only one inertia group it acts on it as -1; and if there are two of them it acts on -1 on each subgroup, and permutes them. Since the inertia subgroups are cyclic of order p^{n-n_0}, we get our claim, using that $\widehat{H}^0(D_{p^n}, \mathcal{U}_n^\diamond) = \widehat{H}^0(G_n, \mathcal{U}_n^\diamond)^\Delta$. Passing now to $\widehat{H}^1$, we observe that $\widehat{H}^{-1}(G_n, \mathcal{O}_{n,\mathfrak{P}_i}^\times)$ is generated by $\rho\pi/\pi$ for some chosen uniformizer π of a fixed completion $L_{n,\mathfrak{P}_i}$ of L_n at $\mathfrak{P}_i$. The action of Δ is $\delta(\rho\pi/\pi) = (\rho^{-1}\delta\pi)/\delta\pi \equiv \rho^{-1}\pi/\pi \pmod{I_{G_n}\mathcal{O}_{n,\mathfrak{P}_i}^\times}$: starting from

$$\rho^2\pi/\rho\pi \equiv \rho\pi/\pi \pmod{I_{G_n}\mathcal{O}_{n,\mathfrak{P}_i}^\times}$$

one finds $\rho^2\pi/\pi \equiv (\rho\pi/\pi)^2 \pmod{I_{G_n}\mathcal{O}_{n,\mathfrak{P}_i}^\times}$ and, inductively, $\rho^{-1}\pi/\pi \equiv (\rho\pi/\pi)^{-1} \pmod{I_{G_n}\mathcal{O}_{n,\mathfrak{P}_i}^\times}$ so that Δ acts as -1 on $\widehat{H}^{-1}(G_n, \mathcal{O}_{n,\mathfrak{P}_i}^\times)$. Again, the fact that this group is cyclic of order p^{n-n_0} by local class field theory, together with $\widehat{H}^1(D_{p^n}, \mathcal{U}_n^\diamond) = \widehat{H}^1(G_n, \mathcal{U}_n^\diamond)^-$ shows our result. □

Proposition 5.3. *There is an exact sequence*

$$0 \to \widehat{H}^0(D_{p^n}, \mathcal{U}_n^\diamond) \to \widehat{H}^0(D_{p^n}, Q_n) \xrightarrow{0} R_n \xrightarrow{\alpha} \widehat{H}^1(D_{p^n}, \mathcal{U}_n^\diamond) \to \mathrm{Ker}(\iota_n) \to 0 \, .$$

Hence we get

$$\widehat{H}^0(D_{p^n}, \mathcal{U}_n^\diamond) \cong \widehat{H}^0(D_{p^n}, Q_n)$$

and the short exact sequence

$$0 \to R_n \to \widehat{H}^1(D_{p^n}, \mathcal{U}_n^\diamond) \to \mathrm{Ker}(\iota_n) \to 0 \, .$$

In particular,

$$\mathrm{Ker}(\iota_n) \cong \mathbb{Z}/p^{h_n}\mathbb{Z}$$

where h_n is as in Definition 4.8.

Proof. The exact sequence is (a short piece of) the long exact sequence of D_{p^n}-Tate cohomology of the righthand column of diagram (38): here R_n and $\mathrm{Ker}(\iota_n)$ appear thanks to Proposition 4.4 and Proposition 5.1. Now note that

$$\widehat{H}^1(D_{p^n}, \mathcal{U}_n^\diamond) \cong \mathbb{Z}/p^{n-n_0}\mathbb{Z}$$

by Lemma 5.2. Moreover,

$$\mathrm{Ker}(\iota_n) = H^0(D_{p^n}, A_{L_n})$$

by Proposition 5.1 and

$$R_n = H^1(D_{p^n}, U_n)$$

by Proposition 4.4. Hence, using Proposition 4.9, we deduce that α is necessarily injective, so the third map is necessarily 0. □

Lemma 5.4. *The following inclusions hold*

$$I_{G_n} A_{L_n} \subseteq \iota_{K_n}(A_{K_n})\iota_{K_n'}(A_{K_n'}) \subseteq A_{L_n}[N_{G_n}].$$

Proof. For the inclusion $I_{G_n} A_{L_n} \subseteq \iota_{K_n}(A_{K_n})\iota_{K_n'}(A_{K_n'})$ see for example Lemma 3.3 of [Le], using that $(1+\sigma)A_{L_n} = \iota_{K_n}(A_{K_n})$ and $(1+\rho^2\sigma)A_{L_n} = \iota_{K_n'}(A_{K_n'})$. Then note that the norm element $N_{D_{p^n}} \in \mathbb{Z}_p[D_{p^n}]$ is the zero map on A_{L_n} since $\mathbb{Z}$ is principal, hence

$$N_{G_n}(\iota_{K_n}(A_{K_n})) = N_{G_n}((1+\sigma)A_{L_n}) = N_{D_{p_n}}(A_{L_n}) = 0$$

and the analogous result holds for $A_{K_n'}$, thereby proving the claimed inclusion. □

Lemma 5.5. *For every $n \geqslant 0$ there is an isomorphism*

$$A_{L_n}[N_{G_n}]/A_{K_n}A_{K'_n} \cong H^1(D_{p^n}, A_{L_n}) \ .$$

Proof. The proof goes exactly in the same way as in Proposition 4.4, except for the fact that here we cannot replace $A_{L_n}[N_{G_n}]$ with A_{L_n} (but we can use Lemma 5.4 above). □

Collecting together these results we can give an algebraic proof of a version of the formula in Theorem 3.4. We need to recall a well known result. If M_1/M_0 is any finite Galois extension, we shall denote by $Ram(M_1/M_0)$ the product of the ramification indexes in M_1/M_0 of the (finite) primes of M_0. Then we have the following formula, coming from a computation with Herbrand quotients:

Fact 5.6 (Ambiguous Class Number Formula)**.** *Let M_1/M_0 be a finite Galois extension of odd degree and set $G = \mathrm{Gal}(M_1/M_0)$. Then*

$$|Cl_{M_1}^G| = \frac{|Cl_{M_0}|Ram(M_1/M_0)}{[M_1 : M_0](E_{M_0} : E_{M_0} \cap N_{M_1/M_0}(M_1^\times))} \ .$$

Proof. See [Gra], II 6.2.3. □

Proposition 5.7. *The following formula holds (compare with Theorem 3.4)*

$$h_{L_n}^{(p)} = \frac{(h_{K_n}^{(p)})^2 h_L^{(p)} |R_n|}{p^n} \ .$$

Proof. From the exact sequence (36) we deduce that

$$h_{L_n} = \frac{h_{K_n}^2 |A_{L_n}/A_{K_n}A_{K'_n}|}{|\mathrm{Ker}(\iota_n)|} \ .$$

Note that

$$|A_{L_n}/A_{K_n}A_{K'_n}| = |A_{L_n}[N_{G_n}]/A_{K_n}A_{K'_n}||A_{L_n}/A_{L_n}[N_{G_n}]| =$$

$$= |H^1(D_{p^n}, A_{L_n})||N_{G_n}(A_{L_n})| \ ,$$

using Lemma 5.5. Moreover, by the Ambiguous Class Number Formula,

$$|N_{G_n}(A_{L_n})| = \frac{|A_{L_n}^{G_n}|}{|\widehat{H}^0(G_n, A_{L_n})|} = \frac{h_L^{(p)} Ram(L_n/L)}{p^n |H^1(G_n, A_{L_n})|}$$

(we use the fact that $|\widehat{H}^0(G_n, A_{L_n})| = |H^1(G_n, A_{L_n})|$). Now observe that

$$\frac{|H^1(D_{p^n}, A_{L_n})|}{|H^1(G_n, A_{L_n})|} = \frac{1}{|\widehat{H}^{-1}(D_{p^n}, A_{L_n})|} = \frac{1}{|\widehat{H}^0(D_{p^n}, Q_n)|}$$

by Proposition 5.1 and Proposition 4.3. Furthermore

$$\frac{1}{|\widehat{H}^0(D_{p^n}, Q_n)|} = \frac{1}{|\widehat{H}^0(D_{p^n}, \mathcal{U}_n^{\diamond})|} ,$$

by Proposition 5.3. Hence we get

$$|A_{L_n}/A_{K_n}A_{K'_n}| = \frac{h_L^{(p)} Ram(L_n/L)}{p^n|\widehat{H}^0(D_{p^n}, \mathcal{U}_n^{\diamond})|} .$$

Now $b_n = n - n_0$. Then

$$Ram(L_n/L) = p^{gb_n}$$

(where g is the same as in Lemma 5.2) and

$$|\widehat{H}^0(D_{p^n}, \mathcal{U}_n^{\diamond})| = p^{(g-1)b_n} .$$

by Lemma 5.2. Therefore,

$$|A_{L_n}/A_{K_n}A_{K'_n}| = \frac{h_L^{(p)} p^{gb_n}}{p^{(g-1)b_n+n}} = \frac{h_L^{(p)}}{p^{n_0}} \tag{40}$$

and

$$h_{L_n}^{(p)} = \frac{(h_{K_n}^{(p)})^2 h_L^{(p)} p^{b_n}}{p^n|\mathrm{Ker}(\iota_n)|} .$$

Using once more Proposition 5.3 we deduce that

$$|R_n||\mathrm{Ker}(\iota_n)| = p^{b_n}$$

which gives the formula of the proposition. □

Remark. We want to stress here that our proof works as well in a more general setting. Indeed, we assumed that L_n/L is part of the anticyclotomic extension because this is the context for our further application. But since both Proposition 5.3, 5.1 and Lemma 5.2 continue to hold true, *mutatis mutandis*, for any dihedral extension, the above proposition can be proven in the same way for any such a dihedral extension. Moreover, as pointed out for example by Lemmermeyer in [Le], Theorem 2.2, the formula above is trivially true for any odd prime number $\ell \neq p$: summarizing, our proof can be generalized to show (algebraically) that for any dihedral extension $F/\mathbb{Q}$ of degree p^n, the relation

$$h_F = \frac{h_k^2 h_L [\mathcal{O}_L^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_L^\times]}{p^n}$$

holds, up to powers of 2.

Now we make some remarks about the structure of X_K. First we need a lemma:

Lemma 5.8. *Suppose that p splits in L: then for any prime $\mathfrak{p}$ over p in L, the union $(L_{cyc}L_\infty)_\mathfrak{p}$ of all completions at p of the finite layers of $L_{cyc}L_\infty/L$ is a $\mathbb{Z}_p$-extension over $(L_{cyc})_\mathfrak{p}$.*

Proof. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the two primes of F above p. Let H be the maximal subextension of $F_{cyc}F_\infty/F$ such that $\mathfrak{p}_1$ is totally split in H/F. By global class field theory, explicitely writing down the normic subgroups corresponding to H and to $F_{cyc}F_\infty$, one sees that H/F must be finite. The lemma now follows since the decomposition group of $\mathfrak{p}_1$ (and therefore also that of $\mathfrak{p}_2$) in $\mathrm{Gal}(F_{cyc}F_\infty/F)$ is of $\mathbb{Z}_p$-rank 2. □

Theorem 5.9. $\mathrm{Ker}(\iota_\infty)$ *is a $\mathbb{Z}_p$-module of rank 1 if p splits in L and it is finite otherwise. Moreover, $X_L/X_K X_{K'}$ is finite and its order divides $h_L^{(p)}/p^{n_0}$. In particular X_L is finitely generated as $\mathbb{Z}_p$-module if and only if X_K is.*

Proof. Before starting the proof, observe that $\mathrm{Ker}(\iota_\infty)$ is a $\mathbb{Z}_p$-module of rank at most 1 (use the fact that each $\mathrm{Ker}(\iota_n)$ is cyclic, see Proposition 5.3).

Suppose now that p splits in L, say $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. Let $\mathfrak{P}_{i,1}, \dots, \mathfrak{P}_{i,s}$ be the prime ideals of L_∞ which lie above $\mathfrak{p}_i$ (clearly $s = p^a$ for some $a \in \mathbb{N}$) for $i = 1, 2$. Let, as before, n_0 be the smallest natural number such that L_∞/L_{n_0} is totally ramified. Set $L' = L_{cyc}L_\infty$ and note that L'/L_∞ is unramified everywhere: indeed, L'/L_∞ is clearly unramified at every prime which does not lie above p. On the other hand, $L'_{\mathfrak{P}_{i,j}}/L_{\infty\,\mathfrak{P}_{i,j}}$ must be unramified because $\mathbb{Q}_p = L_{\mathfrak{p}_i}$ admits only two independent $\mathbb{Z}_p$-extension, one being the unramified one. Let now M_∞ be the maximal unramified abelian pro-p-extension of L_∞ (hence $L' \subseteq M_\infty$). For each $i = 1, 2$ and $j = 1, \dots, s$, consider the Frobenius $\mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty)$ of $\mathfrak{P}_{i,j}$ in M_∞/L_∞ which is an element of infinite order since its restriction $\mathrm{Frob}(\mathfrak{P}_{i,j}, L'/L_\infty)$ to L' is of infinite order by Lemma 5.8. Furthermore $\mathrm{Gal}(L_\infty/\mathbb{Q})$ acts by conjugation on the set $\{\mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty)\}_{i=1,2;\, j=1,\dots,s}$: in other words if $\tau \in \mathrm{Gal}(L_\infty/\mathbb{Q})$ we have

$$\tau \cdot \mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty) = \widetilde{\tau}\mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty)\widetilde{\tau}^{-1} = \mathrm{Frob}(\widetilde{\tau}(\mathfrak{P}_{i,j}))\ .$$

where $\widetilde{\tau}$ is an extension of τ to M_∞. On the other hand we must have

$$\widetilde{\tau}\mathrm{Frob}(\mathfrak{P}_{i,j}, L'/L_\infty)\widetilde{\tau}^{-1} = \mathrm{Frob}(\mathfrak{P}_{i,j}, L'/L_\infty)$$

because $L'/\mathbb{Q}$ is a Galois extension whose Galois group is isomorphic to

$$\mathrm{Gal}(L'/L_\infty) \times \mathrm{Gal}(L_\infty/\mathbb{Q}) .$$

In particular we deduce that

$$\prod_{i=1}^{2}\prod_{j=1}^{s} \mathrm{Frob}(\mathfrak{P}_{i,j}, L'/L_\infty) = \mathrm{Frob}(\mathfrak{P}_{1,1}, L'/L_\infty)^{2s}.$$

Hence this product is an element of infinite order in $\mathrm{Gal}(L'/L_\infty)$ and the same holds for the products of $\mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty)$. It corresponds by class field theory to

$$\varprojlim [\mathfrak{P}_n] \in X_L$$

where $\mathfrak{P}_n$ is the product of all primes above p in L_n. Now note that

$$\mathrm{Ker}(\iota_n) = H^0(D_{p^n},\, A_{L_n}) = \langle[\mathfrak{P}_n]\rangle \cong \mathbb{Z}/p^{h_n}\mathbb{Z}.$$

In fact, clearly

$$H^0(D_{p^n},\, A_{L_n}) \supseteq \langle[\mathfrak{P}_n]\rangle$$

and both groups have order p^{h_n} (use Proposition 4.9). Hence $\mathrm{Ker}(\iota_\infty)$ is infinite since it contains an element of infinite order and it has $\mathbb{Z}_p$-rank 1).

Now suppose that p does not split in L and let again M_∞/L_∞ be the maximal pro-p abelian extension of L_∞ everywhere unramified, so that we have an isomorphism $\mathrm{Gal}(M_\infty/L_\infty) \cong X_L$. Let M_0/L_∞ be the fixed field by $TX_L \subset X_L$, viewing X_L as a Λ-module: then M_0 is the maximal unramified extension of L_∞ which is pro-p abelian over L (see [Wa], chapter 13) and we let $\mathscr{G} = \mathrm{Gal}(M_0/L)$. Since $\mathscr{G}$ is abelian, we can speak of the inertia subgroup $\mathscr{I} \lhd \mathscr{G}$ of $\mathfrak{p}$ (the unique prime in L above p): then $M^{\mathscr{I}}/L$ is an abelian extension everywhere unramified, thus finite. This shows that p is finitely split and has finite inertia degree in M_0/L. Therefore M_0/L_∞ is finite, being unramified everywhere, and then its Galois group (which is isomorphic to X_L/TX_L) is finite. The exact sequence

$$0 \to \mathrm{Ker}(\cdot T) \to X_L \xrightarrow{\cdot T} X_L \to X_L/TX_L \to 0$$

shows that $\mathrm{Ker}(\cdot T) = \mathrm{Ker}(\gamma_0 - 1) = X_L^\Gamma$ is finite (recall that the isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$ is induced by $\gamma_0 - 1 \mapsto T$, where γ_0 is a fixed topological generator of Γ). Since $\mathfrak{P}_n$ is clearly fixed by Γ, we see that their projective limit Y is in X_L^Γ and is therefore finite. In particular, their order p^{h_n} is bounded, and since $\mathrm{Ker}(\iota_n)$ has order p^{h_n} by Proposition 5.3, we immediately see that $\mathrm{Ker}(\iota_\infty)$ is finite (actually $Y = \mathrm{Ker}(\iota_\infty)$).
The second assertion of the theorem is exactly (40) and then the last one easily follows from (37). $\square$

Remark. Suppose that $\mu_L = 0$: therefore X_K is a finitely generated $\mathbb{Z}_p$-module and λ_{X_K} is its rank. From (37) we deduce that

$$\lambda_K = 2\lambda_{X_K}$$

thanks to the remark after Theorem 4.7.

Examples. Suppose that the p-Hilbert class field of L is cyclic and that it is contained in the compositum of the $\mathbb{Z}_p$-extensions of L. Then it must be in L_∞ (A_L^Δ is trivial since $A_\mathbb{Q} = 0$). With this in mind we give the following examples:

- Take $L = \mathbb{Q}(\sqrt{-191})$. Then the 13-Hilbert class field is cyclic of order 13 and is contained in the compositum of the $\mathbb{Z}_{13}$-extensions of L (see [Gra], Examples 2.6.3). Then $n_0 = 1$ and we have $h_L^{(13)} = 13^{n_0} = 13$ and this gives $X_L = X_K X_{K'}$ by Theorem 5.9.
- Take $L = \mathbb{Q}(\sqrt{-383})$. Then the 17-Hilbert class field is cyclic of order 17 but linearly disjoint from the compositum of the $\mathbb{Z}_{17}$-extensions of L (see [Gra], Examples 2.6.3). In particular $n_0 = 0$ and $X_L/X_K X_{K'}$ is cyclic of order dividing 17 by Theorem 5.9. Actually $X_L/X_K X_{K'}$ is of order 17: for, L_∞/L is totally ramified and this implies that the arithmetic norms $A_{L_m} \to A_{L_n}$ are surjective for every $m \geqslant n \geqslant 0$. Then it is easy to see that the arithmetic norms $A_{L_m}/A_{K_m}A_{K'_m} \to A_{L_n}/A_{K_n}A_{K'_n}$ are surjective too, for every $m \geqslant n \geqslant 0$. Since each $A_{L_n}/A_{K_n}A_{K'_n}$ is of order 17 by (40) we are done.

Appendix

In this appendix we perform the computations needed in Proposition 3.3.

Lemma. *With notations introduced in section 3, $|\det(M)| = q|\det(A)|^2$, where*

$$M = \left(\begin{array}{c|c} {A^i}_{0\leqslant i\leqslant r-1} & {B^i}_{0\leqslant i\leqslant r-1} \\ \hline {C^i}_{0\leqslant i\leqslant r-1} & {D^i}_{0\leqslant i\leqslant r-1} \end{array} \right), \ A = \big((1/2)A^0, A^1, \ldots, A^{r-1}\big)$$

are the matrices appearing in Proposition 3.3. Therefore they are defined as follows:

$$A^i = \begin{cases} \begin{pmatrix} 2\gamma(\eta_1) \\ \vdots \\ 2\gamma(\eta_r) \end{pmatrix} & \text{for } i = 0 \\ \begin{pmatrix} \tau_i(\eta_1) \\ \vdots \\ \tau_i(\eta_r) \end{pmatrix} & \text{for } 1 \leqslant i \leqslant r-1 \end{cases},$$

$$B^i = \begin{cases} \begin{pmatrix} -\sum_{j=1}^{r-1} \tau_j(\eta_1) - \gamma(\eta_1) \\ \vdots \\ -\sum_{j=1}^{r-1} \tau_j(\eta_r) - \gamma(\eta_r) \end{pmatrix} & \text{for } i = 0 \\ \begin{pmatrix} \tau_i(\eta_1) \\ \vdots \\ \tau_i(\eta_r) \end{pmatrix} = A^i & \text{for } 1 \leqslant i \leqslant r-1 \end{cases},$$

$$C^i = \begin{cases} \begin{pmatrix} \tau_{i+1}(\eta_1) \\ \vdots \\ \tau_{i+1}(\eta_r) \end{pmatrix} = A^{i+1} & \text{for } 0 \leqslant i \leqslant r-2 \\ B^0 & \text{for } i = r-1 \end{cases}$$

and

$$D^i = \begin{cases} B^0 & \text{for } i = 0 \\ A^{i-1} & \text{for } 1 \leqslant i \leqslant r-1 \end{cases}.$$

Proof. In what follows we will transform M in another matrix N (appearing below) with trivial upper-right and lower-left blocks, and we do this by elementary operations that don't change the (absolute value of the) determinant.

Writing M^i for the i-th column ($1 \leqslant i \leqslant 2r$) of M, let's perform the substitution $M^i \mapsto M^i - M^{i-r}$ for $r+2 \leqslant i \leqslant q-1$ and $M^{r+1} \mapsto M^{r+1} + \sum_{i=1}^{r} M^i$. M then becomes

$$M' = \left(\begin{array}{c|c} A^i{}_{0\leqslant i\leqslant r-1} & E^i{}_{0\leqslant i\leqslant r-1} \\ \hline C^i{}_{0\leqslant i\leqslant r-1} & F^i{}_{0\leqslant i\leqslant r-1} \end{array} \right)$$

where A^i and C^i are as above, while $E^0 = A^0/2$, $E^i = \underline{0}$ for $1 \leqslant i \leqslant r-1$, $F^0 = D^0 + \sum C^i$ and $F^i = D^i - C^i$ for $i > 0$, *i. e.*

$$F^i = \begin{cases} B^0 + \sum_{j=0}^{r-1} C^j = 2B^0 + \sum_{j=1}^{r-1} A^j & \text{for } i = 0 \\ A^{i-1} - A^{i+1} & \text{for } 1 \leqslant i \leqslant r-2 \\ A^{r-2} - B^0 & \text{for } i = r-1 \end{cases}.$$

Before going further, let's kill the first column in the upper right block: it is enough to subtract from this column (it is the $r+1$-th) a half of the first one, namely $M'^{r+1} \mapsto M'^{r+1} - (1/2)M'^1$, thus finding

$$M'' = \left(\begin{array}{c|c} A^i{}_{0\leqslant i\leqslant r-1} & 0 \\ \hline C^i{}_{0\leqslant i\leqslant r-1} & G^i{}_{0\leqslant i\leqslant r-1} \end{array} \right)$$

where

$$G^i = \begin{cases} B^0 - (1/2)A^0 - (1/2)A^1 & \text{for } i = 0 \\ A^{i-1} - A^{i+1} & \text{for } 1 \leqslant i \leqslant r-2 \\ A^{r-2} - B^0 & \text{for } i = r-1 \end{cases} .$$

We can now use all the G^i's freely without changing the other blocks. In particular, we will in the sequel operate in the submatrix formed by the G^i's. Observe, first of all, that

$$\sum_{i=1}^{r-2} G^i = A^0 + A^1 - A^{r-2} - A^{r-1}.$$

Using this, let's substitute $G^0 \mapsto G^0 + (1/2)\sum G^i$, finding $B^0 - (1/2)A^{r-2} - (1/2)A^{r-1} := X$ in the first column. Another step is now to change this in $X \mapsto X + (1/2)G^{r-1} = (1/2)B^0 - (1/2)A^{r-1}$: M has now been reduced to

$$M''' = \left(\begin{array}{c|c} A^i{}_{0\leqslant i\leqslant r-1} & 0 \\ \hline C^i{}_{0\leqslant i\leqslant r-1} & H^i{}_{0\leqslant i\leqslant r-1} \end{array} \right)$$

where

$$H^i = \begin{cases} (1/2)B^0 - (1/2)A^{r-1} & \text{for } i = 0 \\ A^{i-1} - A^{i+1} & \text{for } 1 \leqslant i \leqslant r-2 \\ A^{r-2} - B^0 & \text{for } i = r-1 \end{cases} .$$

Now we should transform $H^{r-1} \mapsto H^{r-1} + 2H^0 = A^{r-2} - A^{r-1} := H'^{r-1}$. Keeping on setting $H^i \mapsto H^i - H'^{i+1}$ for $1 \leqslant i \leqslant r-2$ we inductively build a matrix N whose determinant satisfies $\det(N) = (1/2)\det(M)$, namely

$$N = \left(\begin{array}{c|c} A^i{}_{0\leqslant i\leqslant r-1} & 0 \\ \hline C^i{}_{0\leqslant i\leqslant r-1} & H'^i{}_{0\leqslant i\leqslant r-1} \end{array} \right)$$

where

$$H'^i = \begin{cases} B^0 - A^{r-1} & \text{for } i = 0 \\ A^{i-1} - A^i & \text{for } 1 \leqslant i \leqslant r-1 \end{cases} .$$

Now we can finally perform our last transformations: the idea is to reduce the right bottom block of N to a matrix having qA^1 as second column. First of all, we substitute $H'^1 \mapsto H'^1 + 2H'^0 := T_1$: clearly every other column is unchanged, while this second column becomes

$$A^0 - A^1 + 2B^0 - 2A^{r-1} = \begin{pmatrix} -3\tau_1(\eta_1) - \sum_{i=2}^{r-2} 2\tau_i(\eta_1) - 4\tau_{r-1}(\eta_1) \\ \vdots \\ -3\tau_1(\eta_r) - \sum_{i=2}^{r-2} 2\tau_i(\eta_r) - 4\tau_{r-1}(\eta_r) \end{pmatrix}.$$

Now we can repeatedly subtract to this column suitable multiples of the H'^i's in order to be left only with $-qA^1$: in fact, we define inductively the matrix (as before, we perform these substitution only in the submatrix formed by the H'^i's)

$$\Pi_j := \left(H'^0, \underbrace{T_{j-1} - 2j \cdot H'^{r+1-j}}_{T_j}, H'^2, \dots, H'^{r-1} \right) \ , \ 2 \leqslant j \leqslant r-1 \ .$$

The definition of the H'^i's implies that $T_j = T_{j-1} - 2jA^{r-j} + 2jA^{r+1-j}$ so that T_j verifies

$$T_j = \begin{pmatrix} -3\tau_1(\eta_1) - \displaystyle\sum_{i=2}^{r-1-j} 2\tau_i(\eta_1) - 2(j+1)\tau_{r-j}(\eta_1) \\ \vdots \\ -3\tau_1(\eta_r) - \displaystyle\sum_{i=2}^{r-1-j} 2\tau_i(\eta_r) - 2(j+1)\tau_{r-j}(\eta_r) \end{pmatrix} , 2 \leqslant j \leqslant r-3$$

and, for the remaining cases (as degenerate versions of the same formula),

$$T_{r-2} = \begin{pmatrix} -3\tau_1(\eta_1) - (q-3)\tau_2(\eta_1) \\ \vdots \\ -3\tau_1(\eta_r) - (q-3)\tau_2(\eta_r) \end{pmatrix} , \ T_{r-1} = \begin{pmatrix} -q\tau_1(\eta_1) \\ \vdots \\ -q\tau_1(\eta_r) \end{pmatrix} = -qA^1 \ .$$

Recalling now the definition of N and that the performed transformations do not change the left hand blocks of it, we find

$$\begin{aligned} |\det(M)| =& \frac{1}{2} |\det(N)| = \\ =& \frac{q}{2} \left| \det \left(\begin{array}{c|c} A^i{}_{0 \leqslant i \leqslant r-1} & 0 \\ \hline C^i{}_{0 \leqslant i \leqslant r-1} & \Pi'_{r-1} \end{array} \right) \right| , \end{aligned} \tag{41}$$

where Π'_{r-1} is as Π_{r-1} but with the second column divided by $-q$. Looking now at the definition of H'^i's shows that we can still transform

$$\Pi'_{r-1} \mapsto \left(B^0, A^1, A^2, \dots, A^r \right) \ ,$$

since $A^2 = A^1 - H'^2$, $A^3 = A^2 - H'^3$ and so on. For exactly the same reason, the first column B^0 may safely be substituted by $(1/2)A^0$ so that finally

$$\Pi'_{r-1} \mapsto \left((1/2)A^0, A^1, \dots, A^{r-1} \right)$$

and (41) shows that

$$|\det(M)| = \frac{q}{4} \left| \det \left(\begin{array}{c|c} A^i{}_{0 \leqslant i \leqslant r-1} & 0 \\ \hline C^i{}_{0 \leqslant i \leqslant r-1} & A^i{}_{0 \leqslant i \leqslant r-1} \end{array} \right) \right| .$$

At last, one can use the bottom right block to kill the bottom left one without changing the upper left block, simply by the definition of the C^i's: thus

$$|\det(M)| = \frac{q}{4}\left|\det\left(\begin{array}{c|c} {A^i}_{0\leqslant i\leqslant r-1} & 0 \\ \hline 0 & {A^i}_{0\leqslant i\leqslant r-1}\end{array}\right)\right| = q|\det(A)|^2 \ ,$$

as we wanted. □

References

[Be] J.-R. Belliard, *Sous-modules d'unités en théorie d'Iwasawa*, Publ. Math. UFR Sci. Tech. Besançon, Univ. Franche-Comté, (2002).

[FW] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. CIX (1979), 377-395.

[Gi] R. Gillard, *Remarques sur certaines extensions prodiédrales de corps de nombres*, C. R. Acad. Sci. Paris Sér. A-B 282 n. 1 (1976), A13-A15.

[Gra] G. Gras, *Class field theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

[Gre] C. Greither, *Sur les normes universelles dans les $\mathbb{Z}_p$-extensions*, J. Théor. Nombres Bordeaux. **6** (1994), 205-220.

[HK] F. Halter-Koch, *Einheiten und Divisorenklassen in Galois'schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung 2ℓ für eine ungerade Primzahl ℓ*, Acta Arith. XXXIII (1977), 355-364.

[He] H. A. Heilbronn, *Zeta-functions and L-functions* in *Algebraic Number Theory, Proceedings of an istructional conference organized by the London Mathematical Society*, edited by J.W.S. Cassels and A. Frölich, Academic Press, 1967.

[Iw] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of Number Fields*, Ann. of Math. LXLVIII, (1973), 246-326.

[Ja1] J.-F. Jaulent, *Unités et classes dans les extensions métabeliénnes de degré $n\ell^s$ sur un corps de nombres algébriques*, Ann. Inst. Fourier (Grenoble) 31 n. 1 (1981), 39-62.

[Ja2] J.-F. Jaulent, *Sur la théorie des genres dans les tours métabeliénnes*, Séminaire de Theorie de Nombres 1981/82, Univ. Bordeaux 1, exposé n. 24 (1982), 18 pp.

[Le] F. Lemmermeyer, *Class groups of dihedral extensions*, Math. Nachr. CCLXXVIII (2005), 679-691.

[Na] W. Narkiewicz, *Elementary and analytic Theory of Algebraic Numbers*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der matematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

[Se1] J.-P. Serre, *Représentations linéaires des groupes finis*, Collection Méthodes, Hermann, Paris, 1967.

[Se2] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1967.

[Ta] J. T. Tate, *Global Class Field Theory* in *Algebraic Number Theory, Proceedings of an istructional conference organized by the London Mathematical Society*, edited by J.W.S. Cassels and A. Frölich, Academic Press, 1967.

[VV] O. Venjakob and D. Vogel, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. Reine Angew. Math. **559** (2003), 153-191.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, GTM 83, Springer-Verlag, Berlin, 1997.

[We] C. A. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics 38, Cambridge University Press, Cambridge, 1997.

Luca Caputo
Dipartimento di Matematica
Università di Pisa
Largo Bruno Pontecorvo, 5
56127 - Pisa - ITALY
caputo@mail.dm.unipi.it

Filippo A. E. Nuccio
Dipartimento di Matematica
Università "La Sapienza"
Piazzale Aldo Moro, 5
00185 - Rome - ITALY
nuccio@mat.uniroma1.it
Corresponding author