On Z_p-extensions of real abelian number fields

Fillipo A.E. Nuccio Mortarino Majno di Capriglio

Università degli Studi di Roma
"La Sapienza"

Facoltà di Scienze Matematiche Fisiche e Naturali
Dottorato di Ricerca in Matematica
XX Ciclo

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

Candidato
Filippo A. E. Nuccio
Mortarino Majno di Capriglio

Relatore

prof. René Schoof

Commissione
prof. Massimo Bertolini
prof. Roberto Dvornicich
prof. Riccardo Salvati Manni

Que otros se enorgullezcan por lo que han escrito,
yo me enorgullezco por lo que he leído.

Jorge Luis Borges, "Elogio de la sombra" 1969

Acknowledgments

There are many people I shall need to thank for the help I received in these four years - both inside and outside mathematical departments. Nevertheless, I want to thank three persons in particular because I owe them most of what I have learnt during my PhD and because they have helped me in so many different ways.

The first one is my advisor, René Schoof. His guidance and help have been extremely reassuring and I am unable to list all the Mathematics I have learnt from him. Let me just mention the two class field theory courses he gave during my first two years of PhD and the peculiar point of view he shared with me about Iwasawa theory. Seeing him at work has surely been the best stimulus for studying algebraic geometry.

Secondly, I would like to thank Daniel Barsky for proposing me to work on p-adic zeta functions and for the "groupe de travail" we organised while I was in Paris in Spring 2006. Although I was unable to pursue the project we undertook together, I found his help tremendously influencing to understand the p-adic analysis involved in Iwasawa theory.

Thirdly, I cannot forget that almost all the Iwasawa theory I know and most of the cohomological techniques I can use derive from the afternoons I spent in the office of David Vauclair, both during my stay in Caen in 2007 and afterwards.

I finally wish to thank Gabriel Chênevert for a careful reading of this thesis and for the discussions we had both in Paris and in Leiden. Despite their informal character, I hardly realize how instructive they were.

Con scadenza grosso modo settimanale, il sito internet di Repubblica *propone un sondaggio sull'attualità politica e sociale. Una percentuale oscillante fra l'*1% *e il* 3% *di coloro che esprimono un'opinione si reca volontariamente e spontaneamente sulla pagina del sondaggio per votare* Non so.
Non essendo in grado di apprezzare pienamente il significato del gesto, intendo dedicare loro questa tesi.

Contents

Introduction

Let K be a number field and let p be a prime number. It is by now a very classical result that the growth of the p-part of the class number along any $\mathbb{Z}_p$-extension K_∞/K is controlled by an asymptotical formula. More precisely, we have the following

Theorem 1 (Iwasawa, [Iwa73])**.** *Let K_∞/K be a $\mathbb{Z}_p$-extension and p^{e_n} be the order of the p-Sylow subgroup of the class group of K_n, the subfield of degree p^n. Then there exist three integers μ, λ, ν such that*

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

In their celebrated work [FW79] Bruce Ferrero and Lawrence Washington proved that $\mu = 0$ if K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension of an abelian base field. In 1976 Ralph Greenberg studied in his thesis [Gre76] some criterion for λ to be 0 when the ground field is totally real and the extension is the cyclotomic one. Since then, the condition $\lambda = 0$ has become a conjecture, known as "Greenberg's Conjecture" although Greenberg himself never stated it as such. The conjecture has been verified computationally in many cases using different techniques: see, for instance, [FT95], [IS97], [KS95], [Nis06], [OT97], [Tay00] and the references there.
Greenberg's conjecture may be seen as a generalization of a long-standing conjecture by Vandiver, predicting that for every prime number p, the class number of $\mathbb{Q}(\zeta_p)^+$, the totally real subfield of the p-th cyclotomic field, is never divisible by p. Indeed, we have the following well-known result:

Theorem 2 ([Was97], Proposition 13.36)**.** *Let K be a number field in which there is a unique prime above the prime number p and let K_∞/K be a totally ramified $\mathbb{Z}_p$-extension of K. Then*

$$p \nmid |Cl_K| \iff p \nmid |Cl_{K_n}| \quad \text{for all } n \geq 0 \, .$$

Since $\mathbb{Q}(\zeta_{p^\infty})^+/\mathbb{Q}(\zeta_p)^+$ satisfies the hypothesis of the theorem, Vandiver's conjecture would clearly imply $\lambda = 0$ for this extension. On the other hand, it is still unknown whether $\lambda = 0$ for the extension would imply that $p \nmid |Cl_{\mathbb{Q}(\zeta_p)^+}|$. Observe that Vandiver's conjecture has been checked numerically for all $p < 12 \times 10^6$ in [BCE$^+$01] but for the moment the best theoretical result on the conjecture is the following

Theorem 3 (Soulé, [Sou99])**.** *Let i be odd and assume $p > i^{224i^4}$. Then the eigenspace of $Cl_{\mathbb{Q}(\zeta_p)} \otimes \mathbb{Z}_p$ on which $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts as ω^{p-i} is trivial, where ω is the Teichmüller character.*

We remark that in Washington's book [Was97] a heuristic argument is presented (see Chapter 8, §3), according to which Vandiver's Conjecture should be *false*. The argument is based on the idea that the probability that an eigenspace is non-trivial is equally distributed in the interval $1 \leq i \leq p$ (for odd i's): it might thus need some refinement in view of Soulé's result above.

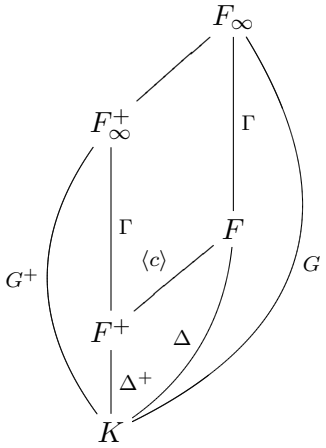
On the other side, there are some theoretical argument that might suggest the validity of Greenberg's Conjecture. In 1995, James Kraft and René Schoof proposed in [KS95] a procedure to check Greenberg's Conjecture - the paper only deals with the case of a real quadratic number field in which p does not split, but this plays a minor role in their argument - and their work gives strong theoretical evidence for the conjecture. The idea is to work with cyclotomic units rather then with ideal classes: indeed, a celebrated theorem by Warren Sinnott (see [Sin81]) shows that for all $n \geq 0$ the class number of K_n (assuming that the degree $[K : \mathbb{Q}]$ is prime to p) coincides up to factors prime to p with the index of the submodule of "cyclotomic units" inside the full group of units $\mathcal{O}_{K_n}^\times$. One can therefore check if the class numbers stabilize by checking the stabilization of the index of these cyclotomic units. Call B_n the quotient of $\mathcal{O}_{K_n}^\times$ by the cyclotomic units at level n: by a very elegant, but elementary, commutative algebra argument over the ring $R_n := \mathbb{Z}/p^{n+1}\mathbb{Z}[G_n]$ (where $G_n = \mathrm{Gal}(K_n/K)$), Kraft and Schoof can describe concretely the structure of $\mathrm{Hom}(B_n, \mathbb{Q}_p/\mathbb{Z}_p)$ - itself again of the same order as B_n and Cl_{K_n} (up to p-units). They show it is cyclic over R_n and the ideal of relations is generated by Frobenius elements of primes $\ell_1, \cdots, \ell_k$ that split completely in $K_n(\zeta_{p^{n+1}})$. If one can prove that at least two of these Frobenius elements are prime to each other, then the ideal of relations is the whole ring, the module is trivial and the conjecture is verified. This is not always the case, but the same strategy shows that if for every n there exists two Frobenius elements that generate an ideal in R_n whose index is independent of n, then the conjecture holds

true. Looking at the computations gathered in the paper, as n grows and ℓ runs through many totally split primes, the elements of R_n corresponding to Frob_ℓ look "random", and one can therefore expect the conjecture to hold.

Another reason to believe Greenberg's Conjecture may come from the so-called "Main Conjecture" (now a theorem, proven by Barry Mazur and Andrew Wiles, [MW84]). Let K be a totally real number field, that we also assume to be abelian, and let $F = K(\zeta_p)$: F is then a CM field and we denote by F^+ its maximal real subfield. Consider the cyclotomic $\mathbb{Z}_p$-extension F_∞/F (and analogously F_∞^+/F^+) and set $\Gamma = \mathrm{Gal}(F_\infty/F) \cong \mathrm{Gal}(F_\infty^+/F^+)$, $\Delta = \mathrm{Gal}(F/K)$ and $\Delta^+ = \mathrm{Gal}(F^+/K)$. We also put $G = \mathrm{Gal}(F_\infty/K) \cong \Gamma\times\Delta$ and $G^+ = \mathrm{Gal}(F_\infty^+/K) \cong \Gamma\times\Delta^+$ and accordingly define their Iwasawa algebras $\Lambda(G)$ and $\Lambda(G^+)$ where, for any profinite group Π, we set

$$\Lambda(\Pi) = \varprojlim \mathbb{Z}_p[\Pi/H]$$

for H running through all open, normal subgroups of Π. We therefore get a diagram of fields



Denoting by L_n the p-Hilbert class field of F_n, the extension L_∞/F_∞ is the maximal everywhere unramified abelian p-extension of F_∞ where we have set $L_\infty = \cup L_n$. The Galois group $X := \mathrm{Gal}(L_\infty/F_\infty)$ is a finitely generated $\mathbb{Z}_p$-module (see [FW79]) and it carries a natural action of G coming from the Artin isomorphism

$$X \cong \varprojlim (Cl_{F_n} \otimes \mathbb{Z}_p) \ ,$$

the projective limit being taken with respect to norm maps: it is therefore a $\Lambda(G)$-module.

The unique element c of order 2 in Δ acts semisimply on every $\Lambda(G)$-module M and decomposes it canonically as

$$M \cong M^+ \oplus M^- \tag{1}$$

where c acts trivially on M^+ and as -1 on M^-. We can apply this both to $\Lambda(G)$ itself, finding that $\Lambda(G)^+ \cong \Lambda(G^+)$ (see [CS06], Lemma 4.2.1) and to X: it is then a standard fact that $X^+ \cong \mathrm{Gal}(L_\infty^+/F_\infty^+)$ as $\Lambda(G^+)$-modules, where $L_\infty^+ \subseteq L_\infty$ is the maximal everywhere unramified abelian p-extension of F_∞^+. By the classical theory of Iwasawa algebras (see the Appendix of [CS06]) there exists *characteristic ideals*, say $I \subseteq \Lambda(G)$ and $I^+ \subseteq \Lambda(G^+)$ such that $\Lambda(G)/I \sim X$ and $\Lambda(G^+)/I^+ \sim X^+$ where $\sim$ denotes *pseudo-isomorphism*; moreover, the Iwasawa algebras $\Lambda(G)$ and $\Lambda(G^+)$ are each isomorphic, as $\Lambda(\Gamma)$-modules, to respectively $|\Delta|$ and $|\Delta|/2 = |\Delta^+|$ copies of $\mathbb{Z}_p[[T]]$, itself isomorphic to $\mathbb{Z}_p[[\Gamma]]$ by sending a topological generator γ of Γ to $1+T$. Through these isomorphisms the ideals I and I^+ become generated by suitable collections of polynomials, say $I = \langle f_1, \dots, f_{|\Delta|} \rangle$ and $I^+ = \langle f_1^+, \dots, f_{|\Delta|/2}^+ \rangle$. One checks easily that these polynomials are related to the Iwasawa invariants by $\lambda(X) = \sum \deg(f_i)$ and $\lambda(X^+) = \sum \deg(f_i^+)$. Therefore Greenberg's conjecture says that all polynomials $f_i^+(T)$ are constant or, equivalently (the equivalence follows from [FW79]), that $I^+ = \Lambda(G^+)$. Before passing to the analytic side of the Main Conjecture, we remark that our notation I^+ is consistent with (1), because the characteristic ideal of X^+ and the $+$-part of the characteristic ideal of X, seen as a $\Lambda(G)$-module, coincide.

On the analytic side, Iwasawa together with Kubota and Leopoldt proved the existence of a p-adic pseudo-measure (see [Ser78]) $\zeta_{K,p}$ such that[1]

$$\int_G \chi_{K,p}^n \mathrm{d}\zeta_{K,p} = E(p)\zeta_K(1-n) \quad \text{for all integers } n \geq 1 \tag{2}$$

where $\zeta_K(s)$ is the usual complex Dedekind zeta-function of K, $\chi_{K,p}$ is the p-adic cyclotomic character of $\mathrm{Gal}(\bar{K}/K)$ and $E(p)$ is an Euler factor that is never 0 (mod p). By a classical theorem in p-adic analysis due to Kurt Mahler (see [Mah58]), there exists a correspondence $\mathcal{M}$ - called the "Mahler transform" - between the p-adic measures on G (*resp.* on G^+) and the Iwasawa algebra $\Lambda(G)$ (*resp.* $\Lambda(G^+)$). Let $\Theta(G)$ and $\Theta(G^+)$ be the

[1] We recall that a p-adic measure μ on G is a continuous functional $\mu : \mathcal{C}(G, \mathbb{C}_p) \to \mathbb{C}_p$ subject to the condition $\mu(f) \in \mathbb{Z}_p$ when $f(G) \subseteq \mathbb{Z}_p$. A pseudo-measure ζ is an element of the total quotient ring of the $\mathbb{Z}_p$-algebra of p-adic measures such that $\zeta(1-g)$ is a measure for all $g \in G$.

augmentation ideals in $\Lambda(G)$ and $\Lambda(G^+)$, respectively: since $\zeta_{K,p}$ is a pseudo-measure we have $\mathcal{M}(\zeta_{K,p})\Theta(G) \subseteq \Lambda(G)$. Moreover, since the Dedekind zeta function ζ_K vanishes for all even negative integers, (2) shows that all odd powers of the cyclotomic character have trivial integral against $\zeta_{K,p}$; carefully pinning down the Δ-action one sees that this forces $\zeta_{K,p}$ to be in the +-part and we have $\mathcal{M}(\zeta_{K,p})\Theta(G^+) \subseteq \Lambda(G^+)$. We need a final remark: an old theorem of Iwasawa (see [Iwa73]) shows that there exists a finitely generated, torsion $\Lambda(G)$-module $\mathscr{X}$ such that $\mathscr{X}^+ \sim X^-$. We do not discuss this module, and simply use this result to find an action of $\Lambda(G^+)$ on I^-. Then the Main Conjecture states that

$$I^- = \mathcal{M}(\zeta_{K,p})\Theta(G^+) \tag{3}$$

as ideals of $\Lambda(G^+)$.

We want now to show that on one hand Greenberg's Conjecture implies Mazur and Wiles' result, and on the other hand that the conjecture would follow from a "more general" Main Conjecture, namely

$$I = \mathcal{M}(\zeta_{K,p})\Theta(G);. \tag{4}$$

as $\Lambda(G)$-ideals. To do this, we recall the following fundamental theorem of Iwasawa:

Theorem 4 (Iwasawa, [Iwa64])**.** *Assume that for every n there is only one prime $\mathfrak{p}_n$ above p in F_n. Let $\mathcal{U}_n^1$ be the local units of $F_{n,\mathfrak{p}_n}^+$ that are $1 \pmod{\mathfrak{p}_n}$ and let C_n^1 be the p-adic completion of the image of cyclotomic units in $\mathcal{U}_n^1$. Let $\mathcal{U}_\infty^1$ and C_∞^1 be the projective limits with respect to norms: then the characteristic ideal of $\mathcal{U}_\infty^1/C_\infty^1$ as $\Lambda(G^+)$-module is $\mathcal{M}(\zeta_{K,p})\Theta(G^+)$.*

The assumption that there is a unique prime in F_n above p is clearly not necessary, but it simplifies drastically our exposition. Class field theory gives an exact sequence

$$0 \to E_\infty^1/C_\infty^1 \to \mathcal{U}_\infty^1/C_\infty^1 \to \mathscr{X}^+ \to X^+ \to 0\,,$$

where E_∞^1 is the projective limit of global units of F_n^+ that are $1 \pmod{\mathfrak{p}_n}$. Since the characteristic ideal of the second module is described by Theorem 4 and that of the third module is I^- by Iwasawa's result quoted above, $X^+ = 0$ implies a divisibility $I^- \mid \mathcal{M}(\zeta_{K,p})\Theta(G^+)$: then the classical Class Number Formula turns this divisibility into an equality, giving (3). On the other hand, assume (4): writing $X = X^+ \oplus X^-$ we get $I = I^+I^-$ and

$$I^+I^- = \big(\mathcal{M}(\zeta_{K,p})\Theta(G)\big)^+ \oplus \big(\mathcal{M}(\zeta_{K,p})\Theta(G)\big)^-$$

as $\Lambda(G)$-modules. But since $\zeta_{K,p} \in \Lambda(G)^+$, we find that $\big(\mathcal{M}(\zeta_{K,p})\Theta(G)\big)^- = 0$ and hence

$$I^+I^- = \big(\mathcal{M}(\zeta_{K,p})\Theta(G)\big)^+ = \mathcal{M}(\zeta_{K,p})\Theta(G^+)$$

as $\Lambda(G^+)$-modules: combining this with (3) we get $I^+ = \Lambda(G^+)$, which is precisely Greenberg's Conjecture.

The first two chapters of my thesis deal with Greenberg's conjecture. The first reproduces the work [CN08a] - written with Luca Caputo - and presents a condition for $\lambda = 0$ for some abelian field. This condition is far from being necessary. The second chapter is the paper [Nuc09] and it investigates a consequence of the conjecture for abelian number fields in which the rational prime p splits completely: namely, it shows that the equality of orders $|B_n| = |Cl_{K_n} \otimes \mathbb{Z}_p|$ coming from Sinnott's work hinted at above, does not imply that a certain *natural* map between these groups is an isomorphism, and explicitely computes the kernel and the cokernel of the map. The interest of this analysis comes again from [KS95], where it was shown that if p does not split in K, then Greenberg's conjecture implies that the above natural map is indeed an isomorphism.

The third chapter is the work [CN08b], again written with Luca Caputo, and deals with a non-Galois extension in Iwasawa Theory. This is the definition that we propose:

Definition 1. *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.*

We then prove that the same Iwasawa formula as in Theorem 1 above holds also for the fake $\mathbb{Z}_p$-extension where $K = \mathbb{Q}$, L is imaginary quadratic and $L_\infty = LK_\infty$ is the anti-cyclotomic $\mathbb{Z}_p$-extension of L, so that K_∞ is the subextension of L_∞ fixed by any subgroup of order 2 inside the pro-dihedral group $\mathrm{Gal}(L_\infty/\mathbb{Q})$. In the last section of the paper we also investigate the algebraic structure of the projective limit of the class groups along this fake $\mathbb{Z}_p$-extension.

References

[BCE+01] Joe Buhler, Richard Crandall, Reijo Ernvall, Tauno Metsänkylä, and M. Amin Shokrollahi, *Irregular primes and cyclotomic invariants to 12 million*, J. Symbolic Comput. **31** (2001), no. 1-2,

89–96, Computational algebra and number theory (Milwaukee, WI, 1996).

[CN08a] Luca Caputo and Filippo Alberto Edoardo Nuccio, *A criterion for Greenberg's conjecture*, Proc. Amer. Math. Soc. **136** (2008), no. 8, 2741–2744.

[CN08b] ———, *On fake $\mathbf{Z}_p$-extensions of number fields*, submitted, arXiv: 0807:1135.

[CS06] J. Coates and R. Sujatha, *Cyclotomic fields and zeta values*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006.

[FT95] Takashi Fukuda and Hisao Taya, *The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), no. 3, 277–292.

[FW79] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[Gre76] Ralph Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284.

[IS97] Humio Ichimura and Hiroki Sumida, *On the Iwasawa invariants of certain real abelian fields*, Tohoku Math. J. (2) **49** (1997), no. 2, 203–215.

[Iwa64] Kenkichi Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **16** (1964), 42–82.

[Iwa73] ———, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[KS95] James S. Kraft and René Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), no. 1-2, 135–155, Special issue in honour of Frans Oort.

[Mah58] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math. **199** (1958), 23–34.

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.

[Nis06] Yoshinori Nishino, *On the Iwasawa invariants of the cyclotomic $\mathbf{Z}_2$-extensions of certain real quadratic fields*, Tokyo J. Math. **29** (2006), no. 1, 239–245.

[Nuc09] Filippo Alberto Edoardo Nuccio, *Cyclotomic units and class groups in $\mathbf{Z}_p$-extensions of real abelian fields*, Math. Proc. Cambridge Philos. Soc. (2009), to appear, arXiv: 0821:0784.

[OT97] Manabu Ozaki and Hisao Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437–444.

[Ser78] Jean-Pierre Serre, *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C. R. Acad. Sci. Paris Sér. A-B **287** (1978), no. 4, A183–A188.

[Sin81] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980/81), no. 2, 181–234.

[Sou99] C. Soulé, *Perfect forms and the Vandiver conjecture*, J. Reine Angew. Math. **517** (1999), 209–221.

[Tay00] Hisao Taya, *Iwasawa invariants and class numbers of quadratic fields for the prime* 3, Proc. Amer. Math. Soc. **128** (2000), no. 5, 1285–1292.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

A Criterion for Greenberg's Conjecture

Luca Caputo and Filippo Alberto Edoardo Nuccio

June 8th, 2007

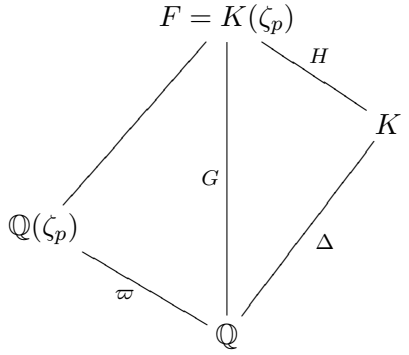
Abstract

We give a criterion for the vanishing of the Iwasawa λ invariants of totally real number fields K based on the class number of $K(\zeta_p)$ by evaluating the p-adic L functions at $s = -1$.

2000 Mathematical Subject Classification: Primary $11R23$; Secondary $11R70$

1 Introduction

Let K be a real abelian number field and let p be an odd prime. Set $F = K(\zeta_p)$ where ζ_p is a primitive p-th rooth of unity and $H = \mathrm{Gal}(F/K)$. Set, moreover, $G = \mathrm{Gal}(F/\mathbb{Q})$ and $\varpi = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. So the diagram of our extensions is as follows:



Let $\tilde{\omega} : H \to \mathbb{Z}_p^\times$ and $\omega : \varpi \to \mathbb{Z}_p^\times$ be the Teichmüller characters of K and $\mathbb{Q}$, respectively. We give (Theorem 2.3) a criterion under which a set of odd Iwasawa invariants associated to F vanish: by means of a Spiegelungssatz, these odd invariants make their even mirrors vanish too. In the case $p = 3$

(Corollary 2.5) or $p = 5$ and $[K : \mathbb{Q}] = 2$ (Theorem 2.7) this allows us to verify a conjecture of Greenberg for the fields satisfying our criterion.

2 Main result

Proposition 2.1. *The following equality holds*

$$rk_p\big(\mathrm{K}_2(\mathcal{O}_K)\big) = rk_p\big((Cl'_F)_{\omega^{-1}}\big) + |S|$$

where $\mathrm{K}_2(\mathcal{O}_K)$ *is the tame kernel of* K*-theory,* Cl'_F *is the class group of the ring* $\mathcal{O}_F[1/p]$ *(and we take its* $\tilde{\omega}^{-1}$*-component for the action of* H*) and* S *is the set of* p*-adic primes of* K *which split completely in* F*.*

Proof. This result dates back to Tate: for an explicit reference see [Gra] Theorem 7.7.3.1. □

Proposition 2.2. *Suppose that* $\mathbb{Q}(\zeta_p)$ *is linearly disjoint from* K *over* $\mathbb{Q}$*. Then the following equalities holds*

$$v_p\big(|\mathrm{K}_2(\mathcal{O}_K)|\big) = v_p\big(\zeta_K(-1)\big) \quad \text{if } p \geq 5$$

$$v_3\big(|\mathrm{K}_2(\mathcal{O}_K)|\big) = v_3\big(\zeta_K(-1)\big) + 1$$

where v_p *denotes the standard* p*-adic valuation and* ζ_K *is the Dedekind zeta function for* K*.*

Proof. The Birch-Tate conjecture which has been proved by Mazur, Wiles and by Greither (since it is a consequence of the Main Conjecture in Iwasawa theory) tells that

$$\frac{|K_2(\mathcal{O}_K)|}{w_2} = \zeta_K(-1)$$

where

$$w_2 = \max\{n \in \mathbb{N} \,|\, \text{the exponent of } \mathrm{Gal}(K(\zeta_n)/K) \text{ is } 2\}$$

By our hypothesis, $\mathbb{Q}(\zeta_p)$ is linearly disjoint from K over $\mathbb{Q}$. Hence F/K is Galois with cyclic Galois group of order $p-1$. If $p = 3$, then for the same argument $3|w_2$ but $9 \nmid w_2$ since $K(\zeta_9)/K$ has degree 6. Taking p-adic valuation we get the claim. □

Theorem 2.3. *Let* $p \geq 5$*. Suppose that the following holds*

- K *and* $\mathbb{Q}(\zeta_p)$ *are linearly disjoint over* $\mathbb{Q}$*;*

- *the set S of Proposition (2.2) is empty;*
- *the Main Conjecture of Iwasawa theory holds for F.*

Then, if p does not divide the order of $Cl_F(\tilde{\omega}^{-1})$, $\lambda_{\chi\omega^2}(F) = 0$ for all characters χ of Δ.

Proof. First of all, we should just prove the theorem for non-trivial characters of Δ, since $\lambda_{\omega^2} = 0$ as it corresponds to the ω^2-part of the cyclotomic extension of $\mathbb{Q}(\zeta_p)$, which is always trivial: indeed, $B_{1/2} = -1/2$, and then Herbrand's theorem and Leopoldt's Spiegelungssatz ([Was], theorems 6.7 and 10.9) give $\lambda_{\omega^2} = 0$.
By hypothesis, the set S of Proposition (2.1) is empty. Therefore $rk_p(\mathrm{K}_2(\mathcal{O}_K)) = 0$ and Proposition (2.2) (that we can apply because K verifies its hypothesis) together with $p \geq 5$ tells us that $v_p(\zeta_K(-1)) = 0$. Since we can factor

$$\zeta_K(s) = \prod_{(\chi \in \hat{\Delta})} L(s,\chi) = \zeta_{\mathbb{Q}}(s) \prod_{\chi \neq 1} L(s,\chi)$$

we find that

$$v_p\big(\zeta_K(-1)\big) = \sum_{\chi \neq 1} v_p\big(L(-1,\chi)\big) = 0 \tag{2.1}$$

The interpolation formula for the p-adic L-function (see [Was], chapter 5) tells us that

$$L_p(-1,\chi) = \big(1 - \chi\omega^{-2}(p)p\big)L(-1,\chi\omega^{-2}); \tag{2.2}$$

now we invoke the Main Conjecture as stated in ([Gre], page 452) to relate these L functions with the characteristic polynomials of some sub-modules of the Iwasawa module $X_\infty(F)$. Observe that the hypothesis of linear disjointness tells us that $\hat{G} \cong \hat{\Delta} \times \hat{\varpi}$ so we can split

$$X_\infty(F) \cong \bigoplus_{\chi \in \Delta} \bigoplus_{i=1}^{p-1} X_\infty(F)(\chi\omega^i)$$

where G acts on $X_\infty(F)(\chi\omega^i)$ as $g \cdot x = (\chi\omega^i)(g)x$ for all $g \in G$ and $x \in X$. Then the Main Conjecture for F allows us to write $L_p(-1,\chi\omega^i) = f(-p/(1+p), \chi^{-1}\omega^{1-i})$ for all even $2 \leq i \leq p-1$, where $f(T, \chi^{-1}\omega^{1-i}) \in \mathbb{Z}_p[T]$ is the characteristic polynomial of $X_\infty(F)(\chi^{-1}\omega^{1-i})$: thus $L_p(-1,\chi\omega^i)$ is $\mathbb{Z}_p$-integral. Applying this for $i = 2$ and plugging it in (2.2) we find $v_p\big(L(-1,\chi)\big) \geq 0$ for all χ, and thanks to (2.1) we indeed find $v_p\big(L(-1,\chi)\big) = 0$ for all $\chi \in \hat{\Delta}$, so

$$v_p\big(L_p(-1,\chi\omega^2)\big) = 0 \qquad \forall\, \chi \in \hat{\Delta}\,.$$

If we now apply again the Main Conjecture we find that this corresponds to

$$v_p\Big(f\big(\frac{1}{1+p}-1,\chi^{-1}\omega^{-1}\big)\Big)=v_p\Big(f\big(\frac{-p}{1+p},\chi^{-1}\omega^{-1}\big)\Big)=0 \qquad \forall\,\chi\in\hat{\Delta}\,.$$

Since $f(T,\chi^{-1}\omega^{-1})\in\mathbb{Z}_p[T]$, is distinguished (see [Was], chapter 7) this is possible if and only if $\deg_T\big(f(T,\chi^{-1}\omega^{-1})\big)=0$; but this is precisely the Iwasawa invariant $\lambda_{\chi^{-1}\omega^{-1}}$, so we have

$$\lambda_{\chi^{-1}\omega^{-1}}=0 \qquad \forall\,\chi\in\hat{\Delta}\,.$$

Since the inequality $\lambda_{\chi^{-1}\omega^{-1}}\geq\lambda_{\chi\omega^2}$ is classical and well-known (see, for instance, [BN] section 4), we achieve the proof. □

Remark 2.4. *We should ask that the Main Conjecture holds for K to apply it in the form of [Gre]. For this, it is enough that there exists a field E that is unramified at p and such that $F=E(\zeta_p)$, as it is often the case in the applications. Moreover, we remark that the hypotheses of the theorem are trivially fulfilled if p is unramified in $K/\mathbb{Q}$.*

Corollary 2.5. *Assume $p=3$. If 3 does not divide the order of $Cl_F(\tilde{\omega}^{-1})$ and it is unramified in K, then $\lambda(K)=\lambda(F)=0$.*

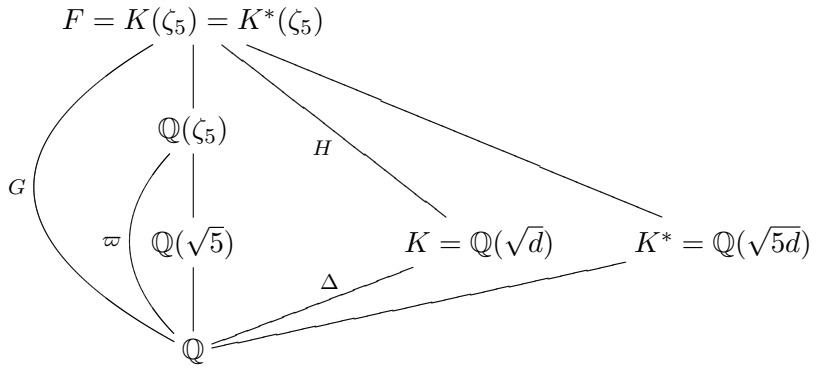
Proof. First of all, the Theorem applies for $p=3$ also, since we still have (2.1) thanks to $\zeta(-1)=-1/12$: moreover, K is clearly disjoint from $\mathbb{Q}(\sqrt{-3})=\mathbb{Q}(\zeta_3)$, as it is unramified, and F/K is ramified, so $S=\emptyset$. But in this case we have $\omega^2=1$, so the statement of the Theorem is that all Iwasawa invariants λ_χ vanish for $\chi\in\hat{\Delta}$ and their sum is precisely $\lambda(K)$. Concerning $\lambda(F)$, in the proof of the Theorem we first prove that all $\lambda_{\chi\omega}$ vanish, and deduce from it the vanishing of their "mirror" parts. □

Remark 2.6. *In the case $K=\mathbb{Q}(\sqrt{d})$ is real quadratic, this is a classical result of Scholtz (although it is expressed in term of Iwasawa invariants), see [Was] Theorem 10.10.*

Theorem 2.7. *Let K be a real quadratic field and suppose that $5\nmid|Cl_F|$. Then $\lambda(K)=0$.*

Proof. Write $K=\mathbb{Q}(\sqrt{d})$ and let χ be its non-trivial character: the result being well-known if $d=5$ we assume throughout that $d\neq 5$. Then we should consider two cases, namely $5\mid d$ and $5\nmid d$. We have the following

diagram of fields (we don't draw the whole of it):



Suppose first of all that $5 \mid d$ or that 5 is inert in $K/\mathbb{Q}$. Since $5 \nmid [F : K]$, our hypothesis implies that $5 \nmid |Cl_K|$ (see [Was] Lemma 16.15). But then we would trivially have $\lambda(K) = 0$ as an easy application of Nakayama's Lemma (see [Was] Proposition 13.22). We can thus suppose that 5 splits in $K/\mathbb{Q}$. We then apply Theorem 2.3 to K^* instead of K: since $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$, our field is linearly disjoint over $\mathbb{Q}$ from $\mathbb{Q}(\zeta_5)$ and $S = \emptyset$ thanks to degree computations. Moreover the Main conjecture holds for F since $F = K(\zeta_5)$ and K is totally real and unramified at 5. We find that $\lambda_{\omega^2\chi^*} = 0$ where χ^* is the non-trivial character of K^*. But clearly $\chi^* = \chi\omega^2$ so $\lambda_\chi = 0$. Since the Iwasawa invariant associated to the trivial character is $\lambda(\mathbb{Q}) = 0$ we have $\lambda(K) = \lambda(\mathbb{Q}) + \lambda_\chi = 0$. □

References

[BN] R. Badino and T. Nguyen Quang Do, *Sur les égalités du miroir et certaines formes faibles de la Conjecture de Greenberg*, Manuscripta Mathematica, **CXVI**, 323-340 (2005)

[Gra] G. Gras, *Class field theory: from theory to practice*, SMM, Springer-Verlag 2005

[Gre] C. Greither, *Class groups of abelian fields, and the main conjecture*, Annales de l'institut Fourier, **XLII**, 449-499 (1992)

[Was] L. Washington, *Introduction to Cyclotomic Fields*, GTM, Springer-Verlag 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

Cyclotomic Units and Class Groups in $\mathbb{Z}_p$-extensions of Real Abelian Felds

Filippo Alberto Edoardo Nuccio

December 3rd, 2008

Abstract

For a real abelian number field F and for a prime p we study the relation between the p-parts of the class groups and of the quotients of global units modulo cyclotomic units along the cyclotomic $\mathbb{Z}_p$-extension of F. Assuming Greenberg's conjecture about the vanishing of the λ-invariant of the extension, a map between these groups has been constructed by several authors, and shown to be an isomorphism if p does not split in F. We focus in the split case, showing that there are, in general, non-trivial kernels and cokernels.

2000 Mathematical Subject Classification: $11R23$, $11R29$

1 Introduction

Let $F/\mathbb{Q}$ be a real abelian field of conductor f and let Cl_F be its ideal class group. A beautiful formula for the order of this class group comes from the group of cyclotomic units: this is a subgroup of the global units $\mathcal{O}_F^\times$ whose index is linked to the order of Cl_F. To be precise, we give the following definition ([Sin81], section 4):

Definition 1.1. *For integers $n > 1$ and a not divisible by n, let ζ_n be a primitive n-th root of unity. Then $Norm_{F\cap\mathbb{Q}(\zeta_n)}^{\mathbb{Q}(\zeta_n)}(1-\zeta_n^a) \in F$ and we define the cyclotomic numbers D_F to be the subgroup of $F^\times$ generated by -1 and $Norm_{F\cap\mathbb{Q}(\zeta_n)}^{\mathbb{Q}(\zeta_n)}(1-\zeta_n^a)$ for all $n > 1$ and all a not divisible by n. Then we define the cyclotomic units of F to be*

$$Cyc_F := D_F \cap \mathcal{O}_F^\times$$

Sinnott proved in [Sin81], Theorem 4.1 together with Proposition 5.1, the following theorem:

Theorem (Sinnott)**.** *There exists an explicit constant κ_F divisible only by* 2 *and by primes dividing* $[F:\mathbb{Q}]$ *such that*

$$[\mathcal{O}_F^\times : Cyc_F] = \kappa_F |Cl_F| \ .$$

Let now p be an odd prime that does not divide $[F:\mathbb{Q}]$: by tensoring $\mathcal{O}_F^\times$, Cyc_F and Cl_F with $\mathbb{Z}_p$ we get an equality

$$[\mathcal{O}_F^\times \otimes \mathbb{Z}_p : Cyc_F \otimes \mathbb{Z}_p] = |Cl_F \otimes \mathbb{Z}_p|$$

and it is natural to ask for an algebraic interpretation of this. Moreover, observe that our assumption $p \nmid [F:\mathbb{Q}]$ makes the Galois group $\Delta := \mathrm{Gal}(F/\mathbb{Q})$ act on the modules appearing above through one-dimensional characters, and we can decompose them accordingly: in the sequel we write $M(\chi)$ for every $\mathbb{Z}[\Delta]$-module M to mean the submodule of $M \otimes \mathbb{Z}_p$ of M on which Δ acts as χ, where $\chi \in \hat{\Delta}$ (see the beginning of Section 3 for a precise discussion). Then an even more optimistic question is to hope for a character-by-character version of Sinnott's theorem, namely

$$[\mathcal{O}_F^\times \otimes \mathbb{Z}_p(\chi) : Cyc_F \otimes \mathbb{Z}_p(\chi)] \stackrel{?}{=} |Cl_F \otimes \mathbb{Z}_p(\chi)| \tag{1.1}$$

and then ask for an algebraic interpretation of this. Although it is easy to see that these Δ-modules are in general not isomorphic (see the example on page 143 of [KS95]), it can be shown that they sit in an exact sequence for a wide class of fields arising in classical Iwasawa theory. More precisely, let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension of F and let $\Gamma = \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$: then

$$F_\infty = \bigcup_{n \geq 0} F_n \supset \ldots \supset F_n \supset F_{n-1} \supset \ldots \supset F_0 = F$$

where F_n/F is a cyclic extension of degree p^n whose Galois group is isomorphic to Γ/Γ^{p^n}. In a celebrated work (see [Iwa73]) Iwasawa gives a formula for the growth of the order of $Cl_{F_n} \otimes \mathbb{Z}_p$: he proves that there are three integers μ, λ and ν, and an index $n_0 \geq 0$, such that

$$|Cl_{F_n} \otimes \mathbb{Z}_p| = p^{\mu p^n + \lambda n + \nu} \ \text{ for every } n \geq n_0 \ .$$

Moreover, Ferrero and Washington proved in [FW79] that the invariant μ vanishes. A long-standing conjecture by Greenberg (see [Gre76], where

conditions for this vanishing are studied) predicts that $\lambda = 0$: according to the conjecture the p-part of the class groups should stay bounded in the tower.

Although a proof of this conjecture has never been provided, many computational checks have been performed verifying the conjecture in many cases (see, for instance, [KS95]). Under the assumptions $\lambda = 0$ and $\chi(p) \neq 1$, *i. e.* p does not split in F, some authors (see [BNQD01], [KS95], [Kuz96] and [Oza97]) were able to construct an explicit isomorphism

$$\alpha : \big(Cl_{F_n} \otimes \mathbb{Z}_p\big)(\chi) \cong \big(\mathcal{O}_{F_n}^{\times}/Cyc_{F_n} \otimes \mathbb{Z}_p\big)(\chi) \tag{1.2}$$

if n is big enough. Although the construction of the above morphism works also in the case $\chi(p) = 1$, as detailed in the beginning of Section 5, the split case seems to have never been addressed. We focus then on this case, and study the map in this contest, still calling it α. Our main result is the following (see Corollary 5.2)

Theorem. *With notations as above, assume that χ is a character of Δ such that $\chi(p) = 1$ and that $\lambda = 0$. Then, for sufficiently big n, there is an exact sequence*

$$0 \longrightarrow \mathrm{K} \to \big(Cl_{F_n} \otimes \mathbb{Z}_p\big)(\chi) \xrightarrow{\alpha} \big(\mathcal{O}_{F_n}^{\times}/Cyc_{F_n} \otimes \mathbb{Z}_p\big)(\chi) \to \mathrm{C} \to 0 \ :$$

both the kernel K *and the cokernel* C *of α are cyclic groups with trivial Γ-action of order $|L_p(1,\chi)|_p^{-1}$ where $L_p(s,\chi)$ is the Kubota-Leopoldt p-adic L-function.*

Acknowledgments This work is part of my PhD thesis, written under the supervision of René Schoof. I would like to take this opportunity to thank him not only for proposing me to work on this subject and for the help he gave me in writing this paper, but especially for all the time and patience he put in following me through my PhD and for the viewpoint on Mathematics he suggested me.

2 Some Tate Cohomology

In this section we briefly recall some well-known facts that are useful in the sequel. Throughout, L/K is a cyclic extension of number fields, whose Galois group we denote by G. In our application, K and L will usually be layers F_m and F_n of the cyclotomic $\mathbb{Z}_p$-extension for some $n \geq m$, but we prefer here not to restrict to this special case.

We need to introduce some notation. Let

$$\mathbb{U}_K = \prod_{v\nmid\infty} \mathcal{O}_{K,v}^{\times} \times \prod_{v|\infty} K_v^{\times}$$

be the idèle units, *i. e.* idèles having valuation 0 at all finite place v (we refer the reader to sections $14-19$ of Cassels' paper in [CF86] for basic properties of idèles and idèles class group) and let Σ be the set of places of K that ramify in L/K. It is known (see section 1.4 of Serre's paper in [CF86]) that the Tate cohomology of local units in an unramified extension of local fields is trivial: therefore Shapiro's Lemma (see Proposition 7.2 of Tate's paper in [CF86],) gives

$$\hat{H}^q(G, \mathbb{U}_L) = \hat{H}^q(G, \prod_{v\in\Sigma}\prod_{w|v} \mathcal{O}_{L,w}^{\times}) \cong \prod_{v\in\Sigma} \hat{H}^q(G_v, \mathcal{O}_{L,w}^{\times}),$$

where we fix a choice of a place w of L above v for every $v \in \Sigma$ and we denote by G_v its decomposition group in G; we will make this identification throughout. We denote the product of local units at places $v \in \Sigma$ appearing above by U_Σ. Consider the following commutative diagram of G-modules:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_L^{\times} & \longrightarrow & L^{\times} & \longrightarrow & \mathrm{Pr}_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{U}_L & \longrightarrow & \mathbb{A}_L^{\times} & \longrightarrow & \mathrm{Id}_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Q_L & \longrightarrow & C_L & \longrightarrow & Cl_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{2.1}$$

Here Id_L and Pr_L denote the group of all fractional ideals of L and of principal ideals, respectively; while C_L is the group of idèle classes and $Q_L = \mathbb{U}_L/\mathcal{O}_L^{\times}$.

Lemma 2.1. *Consider the following diagram induced by (2.1):*

$$\begin{array}{ccc} & & \hat{H}^{-1}(G,\mathbb{U}_L) \\ & & \Big\downarrow{\scriptstyle \beta} \\ \hat{H}^0(G,Cl_L) & \xrightarrow{\pi} & \hat{H}^{-1}(G,Q_L)\ . \end{array}$$

Then $\mathrm{Im}(\beta) = \pi(\overline{\Sigma^G})$ *where* Σ^G *are the primes in* L *above* Σ *fixed by* G *and* $\overline{\Sigma^G}$ *is their image in* $\hat{H}^0(G,Cl_L)$.

Proof. First of all, the above decomposition

$$\hat{H}^{-1}(G,U_\Sigma) \cong \prod_{v\in\Sigma} \hat{H}^{-1}(G,\prod_{w|v} \mathcal{O}_w^\times)$$

allows to write $\beta = \prod \beta_v$ where β_v is the restriction of β to the v-th factor $\hat{H}^{-1}(G,\prod \mathcal{O}_w^\times)$; we therefore fix a place $v \in \Sigma$ and we show that $\mathrm{Im}(\beta_v) = \pi(\overline{\mathfrak{p}_{w_1}\cdots\mathfrak{p}_{w_g}})$ where the $\mathfrak{p}_{w_i}$'s are the primes of L above v. This follows from the fact that $\hat{H}^{-1}(G,\prod \mathcal{O}_w^\times)$ is a product of g (the number of places $w \mid v$) cyclic groups, each of order e_v, the ramification index of v in L/K. Now fix a uniformizer $\pi_{w_i} \in \mathcal{O}_{w_i}$ for all $w_i \mid v$ and chose a generator σ_v of G_v: we have

$$\beta_v(\pi_{w_1}^{1-\sigma_v},\ldots,\pi_{w_g}^{1-\sigma_v}) = \pi(\overline{\mathfrak{p}_{w_1}\cdots\mathfrak{p}_{w_g}})\ ,$$

as can immediately be seen from the commutativity of

$$\begin{array}{ccc} \hat{H}^0(G,\mathrm{Id}_L) & \longrightarrow & \hat{H}^{-1}(G,\prod_{w|v}\mathcal{O}_w^\times) \\ \Big\downarrow{\scriptstyle 1-\sigma} & & \Big\downarrow{\scriptstyle \beta_v} \\ \hat{H}^0(G,Cl_L) & \xrightarrow{\pi} & \hat{H}^{-1}(G,Q_L) \end{array}$$

where σ is a generator of G (inducing σ_v through $G_v \hookrightarrow G$). □

Proposition 2.2 (See [Iwa73])**.** *Let* $\jmath : Cl_K \to Cl_L$ *be the map induced by extending fractional ideals of* $\mathcal{O}_K$ *to* $\mathcal{O}_L$. *Then*

$$\mathrm{Ker}(\jmath) \cong \mathrm{Ker}\Big(\hat{H}^1(G,\mathcal{O}_L^\times) \to \hat{H}^1(G,U_\Sigma)\Big)\ .$$

Proof. We simply apply Snake Lemma twice. First of all, apply it to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q_K & \longrightarrow & C_K & \longrightarrow & Cl_K & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow \jmath & & \\ 0 & \longrightarrow & Q_L^G & \longrightarrow & C_L^G & \longrightarrow & Cl_L^G & \longrightarrow & \hat{H}^1(G, Q_L) \ : \end{array}$$

it shows $\mathrm{Ker}(\jmath) \cong Q_L^G/Q_K$. Then apply it to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \mathbb{U}_K & \longrightarrow & Q_K & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow & & \\ 0 & \longrightarrow & (\mathcal{O}_L^\times)^G & \longrightarrow & (\mathbb{U}_L)^G & \longrightarrow & Q_L^G & \longrightarrow & \hat{H}^1(G, \mathcal{O}_L^\times) \ , \end{array}$$

finding $Q_L^G/Q_K \cong \mathrm{Ker}\Big(\hat{H}^1(G, \mathcal{O}_L^\times) \to \hat{H}^1(G, U_\Sigma)\Big)$. □

Remark. The above proof does not use the hypothesis that G be cyclic. In fact, we will in the sequel we apply the proposition assuming this cyclicity, finding $\mathrm{Ker}(\jmath) \cong \mathrm{Ker}\Big(\hat{H}^{-1}(G, \mathcal{O}_L^\times) \to \hat{H}^{-1}(G, U_\Sigma)\Big)$. We remark that in his thesis [Gre76] Greenberg gives the following criterion: $\lambda = 0$ if and only if the map $\jmath$ relative to the cyclic extension F_n/F, restricted to p-Sylow subgroups, becomes 0 for sufficiently large n. This will be the starting point for our proof of Theorem 5.1.

Finally, we state a Lemma about the cohomology of the direct product of two groups. The main source for this is [Sch90]. Suppose that F is a Galois subfield of K such that L/F is Galois with $\mathrm{Gal}(L/F) \cong \Delta \times G$ where $\Delta = \mathrm{Gal}(K/F)$ is abelian and the isomorphism above is induced by restriction. Then every "arithmetic" module attached to L comes equipped with a natural action of $\Delta \times G$ and we want to compare this action with the natural one on the Tate cohomology of G. We have the following

Lemma 2.3. *[[Sch90], Section 4] Suppose that G is a p-group and that $p \nmid |\Delta|$. Let M be a $\mathbb{Z}[\Delta \times G] - module$: then, for every $q \in \mathbb{Z}$, the natural map*

$$\hat{H}^q(G, M \otimes \mathbb{Z}_p)^\Delta \longrightarrow \hat{H}^q\Big(G, (M \otimes \mathbb{Z}_p)^\Delta\Big) \ .$$

is an isomorphism (of abelian groups with trivial $\Delta \times G$-action).

3 Cyclotomic Units

Fix from now on a non-trivial character $\chi \neq 1$ of Δ and an odd prime $p \nmid [F : \mathbb{Q}]$ such that $\chi(p) = 1$. We set $R = \mathbb{Z}_p[\mathrm{Im}(\chi)]$ and we let $\delta \in \Delta$ act on R by $x \mapsto \chi(\delta)x$. In this way, R becomes a $\mathbb{Z}_p[\Delta]$-algebra. For every $\mathbb{Z}[\Delta]$-module M we denote by $M(\chi)$ the χ-eigenspace of $M \otimes \mathbb{Z}_p$ for the action of Δ: there is an isomorphism of R-modules $M(\chi^{-1}) \cong \big((M \otimes \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} R\big)^{\Delta}$ (our notation is consistent with that of [Rub00], Section 1.6, where all this is properly spelled out: we denote by R what Rubin calls $\mathcal{O}$). In particular, with notations and assumption as in Lemma 2.3,

$$\hat{H}^q(G, M(\chi)) \cong \hat{H}^q(G, M)(\chi) \qquad \forall\, q \in \mathbb{Z}\,. \tag{3.1}$$

It is easy to see that $Cl_F(\chi)$ is isomorphic via the norm to the p-part of the class group of $F^{\mathrm{Ker}\chi}$, a field in which p splits completely (see [Sch90] for more details). Analogously, $\mathcal{O}_F^\times/Cyc_F(\chi)$ is isomorphic to $\big(\mathcal{O}^\times_{F^{\mathrm{Ker}\chi}}/Cyc_{F^{\mathrm{Ker}\chi}}\big) \otimes \mathbb{Z}_p$: replacing if necessary F by $F^{\mathrm{Ker}\chi}$ we can therefore assume that p splits completely in F, and we assume this throughout.

We now go back to the situation described in the introduction: let then F_∞/F be the $\mathbb{Z}_p$-extension of F and denote by Γ its Galois group. For every n and for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{F_n}$ dividing p, we let $\mathcal{O}^\times_{F_n,\mathfrak{p}}$ denote the local units at $\mathfrak{p}$. Then we set

$$U_n := \big(\prod_{\mathfrak{p}|p} \mathcal{O}^\times_{F_n,\mathfrak{p}}\big)(\chi)$$

and analogously

$$\mathcal{O}_n^\times := \mathcal{O}^\times_{F_n}(\chi) \quad \text{and} \quad Cyc_n := Cyc_{F_n}(\chi)\,.$$

Observe that since in a $\mathbb{Z}_p$-extension only primes above p ramify, the set Σ of Section 2 relative to F_n/F is $\Sigma = \{\mathfrak{p} \subset \mathcal{O}_F,\ \mathfrak{p}|p\}$ for all n and our notation is consistent with the one introduced there. We finally set

$$B_n := \mathcal{O}_n^\times/Cyc_n\,, \quad \mathcal{B}_n := U_n/Cyc_n \quad \text{and} \quad A_n := Cl_{F_n}(\chi)\,.$$

By Sinnot's theorem above, together with Theorem 5.3 in [Sin81] that guarantees $p \nmid \kappa_{F_n}$ for all n, the groups $Cl_{F_n} \otimes \mathbb{Z}_p$ and $\big(\mathcal{O}^\times_{F_n}/Cyc_{F_n}\big) \otimes \mathbb{Z}_p$ have the same order. The character-by-character version of this result is much deeper: it is known as Gras' Conjecture, and is a consequence of the (now proven) Main Conjecture of Iwasawa Theory, as detailed in [Gre77] or in

[BNQD01]. It follows that $|A_n| = |B_n|$ for all $n \geq 0$.

Remark. The semi-local units considered by Gillard in his paper [Gil79b] are products over all $\mathfrak{p}$ above p of local units that are 1 (mod $\mathfrak{p}$). In our situation, all completions $F_\mathfrak{p}$ at primes $\mathfrak{p} \mid p$ are isomorphic to $\mathbb{Q}_p$, so the two definitions coincide and U_n is a free $\mathbb{Z}_p$-module of rank 1.
Moreover, since p splits completely in $F/\mathbb{Q}$, all primes above p totally ramify in F_n/F and the subgroup of fractional ideals in F_n having support above p is isomorphic to $\mathbb{Z}[\Delta]$. After tensoring with R, we can consider the χ-eigenspace, that is still cyclic (as an R-module, now) and so is its projection to A_n. Thus, it makes sense to speak of *the subgroup of A_n of primes above p*, a cyclic group that we denote by Π_n. Since it is contained in $A_n^{G_n}$, we can use (3.1) to restate Lemma 2.1 saying that (with the same notation introduced there) $\beta(\hat{H}^{-1}(G_{n,m}, U_n)) = \pi(\Pi_n)$ for all $n \geq m$.

We now investigate in some detail the structure of Cyc_n. First of all, letting f be the conductor of F, we define the unit

$$\eta_n := \left(\mathrm{Norm}_{F_n}^{\mathbb{Q}(\zeta_{fp^{n+1}})} \left(1 - \zeta_{fp^{n+1}}\right) \right)^{\sum_{\delta \in \Delta} \chi(\delta^{-1})\delta} \in Cyc_n \ .$$

It is a unit since $p \nmid f$ because p splits completely in F, it is cyclotomic by definition and we projected it in the χ-component: morever, Sinnott's description of cyclotomic units shows that $Cyc_n = \eta_0 \mathbb{Z}_p \times \eta_n \mathbb{Z}_p[G_n]$ (see, for instance, section 3 of [Gil79a] for details). In particular, we have an isomorphism of G_n-modules $Cyc_n \cong \mathbb{Z}_p \times I_{G_n}$ where I_{G_n} is the augmentation ideal in $\mathbb{Z}_p[G_n]$, and we find a split exact sequence

$$0 \longrightarrow \langle \eta_n \rangle \longrightarrow Cyc_n \longrightarrow \langle \eta_0 \rangle \longrightarrow 0 \tag{3.2}$$

where we denote, here and in what follows, by $\langle \eta_0 \rangle$ and $\langle \eta_n \rangle$ the $\mathbb{Z}_p[G_n]$-modules generated by η_0 and η_n respectively: by the above isomorphisms, (3.2) corresponds to the sequence

$$0 \longrightarrow I_{G_n} \longrightarrow I_{G_n} \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow 0 \ . \tag{3.3}$$

Lemma 3.1. *We have $\hat{H}^0(G_{n,m}, \langle \eta_n \rangle) = 0$ and $\hat{H}^{-1}(G_{n,m}, \langle \eta_0 \rangle) = 0$. Thus, the natural map $\hat{H}^q(G_{n,m}, Cyc_n) \cong \hat{H}^q(G_{n,m}, \langle \eta_0 \rangle) \times \hat{H}^q(G_{n,m}, \langle \eta_n \rangle)$ induced by 3.2 gives isomorphisms of Δ-modules*

$$\hat{H}^0(G_{n,m}, Cyc_n) \cong \hat{H}^0(G_{n,m}, \langle \eta_0 \rangle)$$

and

$$\hat{H}^{-1}(G_{n,m}, Cyc_n) \cong \hat{H}^{-1}(G_{n,m}, \langle \eta_n \rangle) \ .$$

Both are cyclic groups of order p^n .

Proof. The exact sequence

$$0 \longrightarrow I_{G_n} \longrightarrow \mathbb{Z}_p[G_n] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

immediately shows, since $\hat{H}^q(G_{n,m}, \mathbb{Z}_p[G_n]) = 0$ for all q, that $\hat{H}^0(G_{n,m}, I_{G_n})$ $\cong \hat{H}^{-1}(G_{n,m}, \mathbb{Z}_p) = 0$. The $\mathbb{Z}_p[G_n]$-isomorphisms $\langle \eta_n \rangle \cong I_{G_n}$ and $\langle \eta_0 \rangle \cong \mathbb{Z}_p$ give the result. □

Suppose now that $\lambda = 0$. The estension F_∞/F is totally ramified since p splits in F and the norm maps $N_m^n : A_n \to A_m$ are surjective by class field theory for all $n \geq m$; assuming $\lambda = 0$ and chosing m big enough, the orders of A_n and A_m coincide, and these norm maps are actually isomorphisms. Therefore the projective limit $X = \varprojlim A_n$ with respect to norms stabilizes to a finite group and $A_n \cong X$ for all $n \gg 0$ (we introduce here the notation $a \gg b$, equivalent to $b \ll a$, to mean that there exists a $b_0 \geq b$ such that what we are stating holds for all $a \geq b_0$). In particular, the action of Γ on X must factor through a certain quotient $G_m = \Gamma/\Gamma^{p^m}$. Therefore $G_{n,m}$ acts trivially on A_n for all $n \geq m$ and the $G_{n,m}$-norm $N_{G_{n,m}} = \sum_{\tau \in G_{n,m}} \tau$ acts on A_n as multiplication by p^{n-m}. Choosing n big enough so that $p^{n-m} A_n = 0$, we find $N_{G_{n,m}} A_n = 0$ and

$$\begin{aligned} \hat{H}^0(G_{n,m}, A_n) =& A_n^{G_{n,m}}/N_{G_{n,m}} A_n = A_n \\ &= A_n[N_{G_{n,m}}]/I_{G_{n,m}} A_n = \hat{H}^{-1}(G_{n,m}, A_n) \end{aligned} \tag{3.4}$$

where $I_{G_{n,m}}$ is the augmentation ideal of $\mathbb{Z}_p[G_{n,m}]$. Hence we find $A_n \cong$ $\hat{H}^{-1}(G_{n,m}, A_n) \cong \hat{H}^0(G_{n,m}, A_n)$, whenever $\lambda = 0$ and $n \gg m \gg 0$. A similar argument leads to the equivalent of (3.4) for B_n, namely $\hat{H}^q(G_{n,m}, B_n) \cong$ B_n for all $q \in \mathbb{Z}$.

Lemma 3.2. *If* $\lambda = 0$ *and* $m \gg 0$*, the natural map*

$$H^1(G_{n,m}, Cyc_n) \longrightarrow H^1(G_{n,m}, \mathcal{O}_n^\times)$$

is injective for all $n \geq m$.

Proof. Taking $G_{n,m}$-cohomology in the exact sequence defining B_n gives

$$0 \longrightarrow H^0(G_{n,m}, Cyc_n) \longrightarrow H^0(G_{n,m}, \mathcal{O}_n^\times) \longrightarrow H^0(G_{n,m}, B_n) \longrightarrow \\ \longrightarrow H^1(G_{n,m}, Cyc_n) \longrightarrow H^1(G_{n,m}, \mathcal{O}_n^\times)\ . \quad (3.5)$$

Since $G_{n,m}$-invariants of Cyc_n and $\mathcal{O}_n^\times$ are Cyc_m and $\mathcal{O}_m^\times$ respectively, we find $\mathrm{Ker}\Big(H^1(G_{n,m}, Cyc_n) \longrightarrow H^1(G_{n,m}, \mathcal{O}_n^\times)\Big) = B_n^{G_{n,m}}/B_m$. Assuming that m is big enough and $\lambda = 0$ implies that the orders of B_n and B_m coincide, and the same holds, *a fortiori*, for $B_n^{G_{n,m}}$ and B_m. Thus, the above kernel is trivial. □

4 Semi-local Units modulo Cyclotomic Units

We now state a very useful result about semi-local units in our setting; it can already be found in a paper by Iwasawa [Iwa60]. We keep the same notation introduced in the previous section and we make from now on constant use of Lemma 2.3 above, especially in the form of the isomorphism in (3.1).

Definition 4.1. *We define U_n^1 to be the kernel $U_n^1 = \mathrm{Ker}(N_0^n : U_n \to U_0)$ and we set $\mathcal{B}_n^1 = U_n^1/\langle \eta_n \rangle$.*

Proposition 4.2. *The natural map $U_n^1 \times U_0 \hookrightarrow U_n$ induced by injections is an isomorphism of G_n-modules. It induces a decomposition $\mathcal{B}_n \cong \mathcal{B}_n^1 \times \mathcal{B}_0$.*

Proof. Consider the exact sequence induced by the norm map N_0^n

$$0 \longrightarrow U_n^1 \longrightarrow U_n \longrightarrow N_0^n(U_n) \subseteq U_0 \longrightarrow 0\ .$$

Since the extension $F_{n,\mathfrak{p}_n}/F_{0,\mathfrak{p}_0}$ is cyclic and totally ramified, local class field theory shows that $\hat{H}^0(G_n, U_n) = U_0/N_0^n(U_n)$ is a cyclic group of order p^n. As $U_0 \cong \mathbb{Z}_p$ this shows $N_0^n(U_n) = U_0^{p^n}$ and since U_0 contains no roots of unity of p-power order we can identify this group with U_0 simply by extracting p^n-th roots. We find

$$0 \longrightarrow U_n^1 \longrightarrow U_n \overset{\sqrt[p^n]{N_0^n}}{\longrightarrow} U_0 \longrightarrow 0\ . \quad (4.1)$$

Since the natural embedding $U_0 \hookrightarrow U_n$ is a G_n-linear section of (4.1), it splits the sequence and therefore gives an isomorphism $U_n^1 \times U_0 \cong U_n$.

The fact that this splitting induces an isomorphism $\mathcal{B}_n \cong \mathcal{B}_n^1 \times \mathcal{B}_0$ simply follows from the commutativity of the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle \eta_n \rangle & \longrightarrow & Cyc_n & \xrightarrow{\sqrt[p^n]{N_0^n}} & \langle \eta_0 \rangle & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U_n^1 & \longrightarrow & U_n & \xrightarrow{\sqrt[p^n]{N_0^n}} & U_0 & \longrightarrow & 0\ . \end{array}$$

□

More useful than the splitting itself is the following easy consequence:

Corollary 4.3. *For every $n \geq m \geq 0$ and for every $q \in \mathbb{Z}$ the natural maps*

$$\hat{H}^q(G_{n,m}, U_n) \to \hat{H}^q(G_{n,m}, U_n^1) \times \hat{H}^q(G_{n,m}, U_0)$$

and

$$\hat{H}^q(G_{n,m}, \mathcal{B}_n) \to \hat{H}^q(G_{n,m}, \mathcal{B}_n^1) \times \hat{H}^q(G_{n,m}, \mathcal{B}_0)\ .$$

induced by Proposition 4.2 are isomorphisms of abelian groups. Thus there are identifications $\hat{H}^{-1}(G_{n,m}, U_n) = \hat{H}^{-1}(G_{n,m}, U_n^1)$ and $\hat{H}^0(G_{n,m}, U_n) = \hat{H}^0(G_{n,m}, U_0)$.

Proof. The splitting of the cohomology groups follows immediately from the Proposition. Concerning the cohomology of U_n, we observe that, since $G_{n,m}$ acts trivially on the torsion-free module U_0, the group $\hat{H}^0(G_{n,m}, U_0)$ is cyclic of order p^{n-m} while $\hat{H}^{-1}(G_{n,m}, U_0) = 0$. This already implies that $\hat{H}^{-1}(G_{n,m}, U_n) = \hat{H}^{-1}(G_{n,m}, U_n^1)$. It also shows that $\hat{H}^0(G_{n,m}, U_n^1)$ must be trivial because $\hat{H}^0(G_{n,m}, U_n)$ is itself cyclic of order p^{n-m} by local class field theory. □

Lemma 4.4. *For every $m \geq 0$ and for every $n \gg m$ there are isomorphisms $\hat{H}^q(G_{n,m}, \mathcal{B}_n^1) \cong \mathbb{Z}_p/L_p(1, \chi)$ and $\hat{H}^q(G_{n,m}, \mathcal{B}_0) \cong \mathbb{Z}_p/L_p(1, \chi)$ holding for every $q \in \mathbb{Z}$.*

Proof. Let $\Lambda := \mathbb{Z}_p[[T]]$ and fix an isomorphism $\varpi : \Lambda \cong \mathbb{Z}_p[[\Gamma]]$. This isomorphism fixes a choice of a topological generator $\varpi(1+T) =: \gamma_0$ of Γ and we denote by $\kappa \in \mathbb{Z}_p^\times$ the element $\varepsilon_{cyc}(\gamma_0)$ where

$$\varepsilon_{cyc} : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathbb{Z}_p^\times$$

is the cyclotomic character of F. The main tool of the proof will be Theorem 2 of [Gil79b], that gives isomorphisms of $\mathbb{Z}_p[[\Gamma]]$-modules

$$\mathcal{B}_0 \cong \mathbb{Z}_p/L_p(1,\chi) \qquad \text{and} \qquad \mathcal{B}_n \cong \Lambda/(f(T),\omega_n(T)/T) \tag{4.2}$$

where $\omega_n(T) = (1+T)^{p^n} - 1$ and $f(T) \in \Lambda$ is the power series verifying $f(\kappa^s - 1) = L_p(1-s,\chi)$ for all $s \in \mathbb{Z}_p$. We make Γ act on the modules appearing in (4.2) by $\gamma_0 \cdot x = \varpi(\gamma_0)x = (1+T)x$ for all $x \in \mathcal{B}_0$ (*resp.* all $x \in \mathcal{B}_n$): this induces the action of $G_{n,m}$ we need to compute the cohomology with respect to.

Starting with $\mathcal{B}_0$, observe that the action of Γ, and thus of its subquotient $G_{n,m}$, is trivial on the *finite group* $\mathcal{B}_0$: as in (3.4) we get

$$\hat{H}^q(G_{n,m},\mathcal{B}_0) \cong \mathcal{B}_0 \qquad \text{for all } n \gg m \gg 0\ .$$

and we apply (4.2) to get our claim.

Now we compute $\hat{H}^{-1}(G_{n,m},\mathcal{B}_n^1)$: by its very definition, $\hat{H}^{-1}(G_{n,m},\mathcal{B}_n^1) = \mathcal{B}_n^1[N_{G_{n,m}}]/I_{G_{n,m}}\mathcal{B}_n^1$. Applying ϖ we find $I_{G_{n,m}} \cong \omega_m(T)(\Lambda/\omega_n(T))$ and $\varpi(N_{G_{n,m}}) = \nu_{n,m}(T)$ where $\nu_{n,m}(T) := \omega_n(T)/\omega_m(T)$. Hence

$$\hat{H}^{-1}(G_{n,m},\mathcal{B}_n^1) \cong \frac{\{g(T) \in \Lambda \;\Big|\; g(T)\nu_{n,m}(T) \in (f(T),\omega_n(T)/T)\}}{(f(T),\omega_n(T)/T,\omega_m(T))}\ .$$

As observed in [Gil79b], Lemma 5, $f(T)$ and $\omega_n(T)/T$ have no common zeroes. Therefore a relation

$$g(T)\frac{\omega_n(T)}{\omega_m(T)} = a(T)f(T) + b(T)\frac{\omega_n(T)}{T}$$

implies $\nu_{n,m}(T) \mid a(T)$ and we find $g(T) = c(T)f(T) + b(T)\omega_m(T)/T$ for some $c(T) \in \Lambda$: thus,

$$\begin{aligned}\hat{H}^{-1}(G_{n,m},\mathcal{B}_n^1) &\cong \frac{(f(T),\omega_m(T)/T)}{(f(T),\omega_n(T)/T,\omega_m(T))} \\ &\cong \frac{(\omega_m(T)/T)}{(f(T),\omega_n(T)/T,\omega_m(T))}\ .\end{aligned}$$

The evaluation map $g(T)\omega_m(T)/T \mapsto g(0)$ gives an isomorphism

$$\frac{(\omega_m(T)/T)}{(\omega_m(T))} \cong \mathbb{Z}_p$$

and we find

$$\frac{(\omega_m(T)/T)}{(f(T),\omega_n(T)/T,\omega_m(T))} \cong \mathbb{Z}_p/\big(f(0),\omega_n(0)\big)\ .$$

Since this last module is $\mathbb{Z}_p/f(0)$ as soon as n is big enough and, by definition, $f(0) = L_p(1,\chi)$, we get our claim for $q=-1$. Using now that $\mathcal{B}_n^1$ is finite and therefore has a trivial Herbrand quotient, we know that the order of $\hat{H}^0(G_{n,m},\mathcal{B}_n^1)$ is again $|L_p(1,\chi)|_p^{-1}$: the fact that it is a cyclic group comes from the exact sequence

$$0 \to \hat{H}^0(G_{n,m},\mathcal{B}_n^1) \to \hat{H}^0(G_{n,m},U_n^1) \to \hat{H}^0(G_{n,m},\langle\eta_n\rangle) \to \\ \to \hat{H}^1(G_{n,m},\mathcal{B}_n^1) \to 0$$

since $\hat{H}^0(G_{n,m},U_n^1)$ is itself cyclic, as discussed in Corollary 4.3.
Finally, the fact that $G_{n,m}$ is cyclic gives isomorphisms in Tate cohomology $\hat{H}^{2q}(G_{n,m},M) \cong \hat{H}^0(G_{n,m},M)$ for all modules M (and analogously $\hat{H}^{2q+1}(G_{n,m},M) \cong \hat{H}^{-1}(G_{n,m},M)$), so the claim for all q's follows from our computation in the cases $q=0,-1$. □

Proposition 4.5. *Recall that $X = \varprojlim A_n$: then, $|X^\Gamma| \stackrel{p}{=} L_p(1,\chi)$, where by $a \stackrel{p}{=} b$ we mean $ab^{-1} \in \mathbb{Z}_p^\times$.*

Proof. Let L_0 be the maximal pro-p abelian extension of F_∞ everywhere unramified and let M_0 be the maximal pro-p abelian extension of F_∞ unramified outside p. We claim that $L_0 = M_0$. This follows from the fact that for every $\mathfrak{p} \subseteq \mathcal{O}_F$ dividing p, the local field $F_\mathfrak{p}$ is $\mathbb{Q}_p$, since p splits completely, and it therefore admits only two independent $\mathbb{Z}_p$-extensions by local class field theory. In particular, every pro-p extension of $F_{\infty,\mathfrak{p}}$ that is abelian over $F_\mathfrak{p}$ must be unramified, so $M_0 = L_0$. Now let $Y := \mathrm{Gal}(L_\infty/F_\infty)$ where L_∞ is the maximal pro-p abelian extension of F_∞ everywhere unramified: then the Artin reciprocity map gives an isomorphism $X \cong Y(\chi)$; also, let M_∞ be the maximal pro-p abelian extension of F_∞ unramified outside p and $\mathscr{Y} := \mathrm{Gal}(M_\infty/F_\infty)$. A classical argument (see [Was97], chapter 13) shows that $Y_\Gamma = \mathrm{Gal}(L_0/F_\infty)$ and $\mathscr{Y}_\Gamma = \mathrm{Gal}(M_0/F_\infty)$: our claim above implies that $Y_\Gamma = \mathscr{Y}_\Gamma$. Since the actions of Δ and Γ commute with each other, this also shows $X_\Gamma = \mathscr{Y}(\chi)_\Gamma$. Combine this with the following exact sequence induced by multiplication by $\gamma_0 - 1$ where γ_0 is a topological generator of Γ

$$0 \longrightarrow X(\chi)^\Gamma \longrightarrow X(\chi) \stackrel{\gamma_0-1}{\longrightarrow} X(\chi) \longrightarrow X(\chi)_\Gamma \longrightarrow 0\ :$$

it gives $|X^\Gamma| = |X_\Gamma| = |\mathscr{Y}(\chi)_\Gamma|$. The Main Conjecture of Iwasawa Theory, as proved by Rubin in the appendix of [Lan90], shows that the characteristic polynomial of $\mathscr{Y}(\chi)$ is $F(T)$ where $F(T)$ is the distinguished polynomial determined by $L_p(1-s,\chi) \stackrel{p}{=} F\big((1+p)^s - 1\big)$ for all $s \in \mathbb{Z}_p$. Since $\mathscr{Y}$ contains no non-zero finite Γ-submodules (see [NSW00]), we find $\mathscr{Y}^\Gamma = 0$ and the order of $\mathscr{Y}(\chi)_\Gamma$ is $F(0) \stackrel{p}{=} L_p(1,\chi)$. □

Corollary 4.6. *If $\lambda = 0$, then Π_n is a cyclic group of order $|L_p(1,\chi)|_p^{-1}$ for every $n \gg 0$.*

Proof. Indeed, Theorem 2 in [Gre76] shows that $\lambda = 0$ if and only if $X^\Gamma = \Pi_n$. The result now follows from the proposition and from the remark of section 3. □

5 Main result

We are now in position of proving our main result. We stick to the notation introduced in Section 3. Let $n \geq 0$ and let $Q_n := (\mathbb{U}_{F_n})(\chi)/\mathcal{O}_n^\times = Q_{F_n}(\chi)$ as in Section 2: consider the exact sequence

$$0 \longrightarrow \mathcal{O}_n^\times \longrightarrow \mathbb{U}_{F_n}(\chi) \longrightarrow Q_n \longrightarrow 0\ .$$

Since $Cyc_n \subseteq \mathcal{O}_n^\times$, it induces an exact sequence

$$0 \longrightarrow B_n \longrightarrow \mathbb{U}_{F_n}(\chi)/Cyc_n \longrightarrow Q_n \longrightarrow 0\ ,$$

and the Tate cohomology of $\mathbb{U}_{F_n}(\chi)/Cyc_n$ coincides with that of $\mathcal{B}_n$, as discussed in Section 2. For every $m \leq n$ the cyclicity of Tate cohomology for cyclic groups induces an exact square

$$\begin{array}{ccc} \hat{H}^0(G_{n,m}, Q_n) & \xrightarrow{\alpha_{[0,1]}} & \hat{H}^{-1}(G_{n,m}, B_n) \\ \uparrow & & \downarrow \\ \hat{H}^0(G_{n,m}, \mathcal{B}_n) & & \hat{H}^{-1}(G_{n,m}, \mathcal{B}_n) \\ \uparrow & & \downarrow \\ \hat{H}^0(G_{n,m}, B_n) & \xleftarrow[\alpha_{[1,0]}]{} & \hat{H}^{-1}(G_{n,m}, Q_n)\ . \end{array} \tag{5.1}$$

Pick now $q \in \mathbb{Z}$ and consider the exact sequence

$$0 \longrightarrow Q_n \longrightarrow C_{F_n}(\chi) \longrightarrow A_n \longrightarrow 0 \ : \tag{5.2}$$

as the actions of $G_{n,m}$ and of Δ commute, we have $\hat{H}^q(G_{n,m}, C_n(\chi)) \cong \hat{H}^q(G_{n,m}, C_n)(\chi)$; global class field theory (see section 11.3 of Tate's paper in [CF86]) shows that $\hat{H}^q(G_{n,m}, C_n)(\chi) \cong \hat{H}^{q+2}(G_{n,m}, \mathbb{Z}(\chi)) = 0$ because we assumed $\chi \neq 1$. Therefore the long exact cohomology sequence of (5.2) induces isomorphisms

$$\hat{H}^q(G_{n,m}, A_n) \cong \hat{H}^{q+1}(G_{n,m}, Q_n) \quad \text{for every } q \in \mathbb{Z} \ . \tag{5.3}$$

Remark. Observe that our discussion never uses the assumption $\chi(p) = 1$. Indeed, the maps $\alpha_{[0,1]}$ and $\alpha_{[1,0]}$ are defined whenever $\chi \neq 1$ and are indeed the same maps appearing in Proposition 2.6 of [KS95], where the case $\chi(p) \neq 1$ is treated. As discussed in the introduction, in that case they turned out to be isomorphism if $\lambda = 0$ (see also [BNQD01], [Kuz96] and [Oza97]). We are going to see this is not the case if $\chi(p) = 1$.

Theorem 5.1. *Assume $\lambda = 0$ and $n \gg m \gg 0$. Then the kernels $\mathrm{Ker}(\alpha_{[0,1]})$, $\mathrm{Ker}(\alpha_{[1,0]})$ and the cokernels $\mathrm{Coker}(\alpha_{[0,1]})$, $\mathrm{Coker}(\alpha_{[1,0]})$ are cyclic groups of order $|L_p(1,\chi)|_p^{-1}$.*

Proof. We start by determining $\mathrm{Ker}(\alpha_{[0,1]})$. Choose m big enough so that $|A_{m+k}| = |A_m|$ for all $k \geq 0$ and $n \geq m$ big enough so that $\hat{H}^q(G_{n,m}, A_n) = A_n$. As in the remark of Section 2, Proposition 2 of [Gre76] shows that $\lambda = 0$ implies $A_m = \mathrm{Ker}(\jmath_{m,n})$ if n is sufficiently large. Combining Proposition 2.2 with (5.3), this gives an injection

$$\hat{H}^0(G_{n,m}, Q_n) \hookrightarrow \hat{H}^{-1}(G_{n,m}, \mathcal{O}_n^\times) \ . \tag{5.4}$$

Consider now the following commutative diagram, whose row and column are exact and where the injectivity of the vertical arrow in the middle follows from Lemma 3.2:

$$\begin{array}{ccccc} & & \hat{H}^{-1}(G_{n,m}, B_n) & & \\ & \overset{\alpha_{[0,1]}}{\nearrow} & \uparrow & & \\ \hat{H}^0(G_{n,m}, Q_n) & \hookrightarrow & \hat{H}^{-1}(G_{n,m}, \mathcal{O}_n^\times) & \longrightarrow & \hat{H}^{-1}(G_{n,m}, U_n) \\ & & \uparrow & \overset{\psi}{\nearrow} & \\ & & \hat{H}^{-1}(G_{n,m}, Cyc_n) & & \end{array} \tag{5.5}$$

An easy diagram chase shows that $\mathrm{Ker}(\alpha_{[0,1]}) \cong \mathrm{Ker}(\psi)$. In order to study $\mathrm{Ker}(\psi)$, observe that ψ appears in the sequence

$$0 \to \hat{H}^0(G_{n,m}, \mathcal{B}_n^1) \to \hat{H}^{-1}(G_{n,m}, \langle \eta_n \rangle) \xrightarrow{\psi} \hat{H}^{-1}(G_{n,m}, U_n^1) \ , \tag{5.6}$$

because $\hat{H}^{-1}(G_{n,m}, Cyc_n) = \hat{H}^{-1}(G_{n,m}, \langle \eta_n \rangle)$ by Lemma 3.1, while Corollary **??** gives $\hat{H}^{-1}(G_{n,m}, U_n) = \hat{H}^{-1}(G_{n,m}, U_n^1)$. Morever, again by Corollary 4.3, $\hat{H}^0(G_{n,m}, U_n^1) = 0$ and (5.6) is exact, thus giving

$$\mathrm{Ker}(\alpha_{[0,1]}) \cong \hat{H}^0(G_{n,m}, \mathcal{B}_n^1) \cong \mathbb{Z}_p / L_p(1, \chi) \ , \tag{5.7}$$

the last isomorphisms being Lemma 4.4.
Having determined $\mathrm{Ker}(\alpha_{[0,1]})$, the exactness of (5.1) together with Corollary 4.3 (and Lemma 4.4) show immediately that

$$\mathrm{Coker}(\alpha_{[1,0]}) \cong \hat{H}^0(G_{n,m}, \mathcal{B}_0) \cong \mathbb{Z}_p / L_p(1, \chi) \ . \tag{5.8}$$

Since the orders of A_n and B_n coincide for $n \gg 0$, and since these groups are isomorphic to $\hat{H}^q(G_{n,m}, Q_n)$ and $\hat{H}^q(G_{n,m}, B_n)$ respectively (see (3.4) and (5.3)), the equalities of orders

$$|\mathrm{Ker}(\alpha_{[0,1]})| = |\mathrm{Coker}(\alpha_{[0,1]})| \quad \text{and} \quad |\mathrm{Ker}(\alpha_{[1,0]})| = |\mathrm{Coker}(\alpha_{[1,0]})|$$

hold. By (5.7) and (5.8), the four groups have the same order, equal to $|L_p(1, \chi)|_p^{-1}$.
We are left with the structure of $\mathrm{Ker}(\alpha_{[1,0]})$ and $\mathrm{Coker}(\alpha_{[0,1]})$. The map $\alpha_{[1,0]}$ is the composition

$$\hat{H}^{-1}(G_{n,m}, Q_n) \xrightarrow{\tilde{\beta}} \hat{H}^0(G_{n,m}, \mathcal{O}_n^\times) \longrightarrow \hat{H}^0(G_{n,m}, B_n) \tag{5.9}$$
$$\alpha_{[1,0]}$$

and $\mathrm{Ker}(\alpha_{[1,0]}) \supseteq \mathrm{Ker}(\tilde{\beta}) = \Pi_n$, the last identification coming from Lemma 2.1. Combining Corollary 4.6 with the computation of the order of $\mathrm{Ker}(\alpha_{[1,0]})$ performed above, the inclusion cannot be strict, and $\mathrm{Ker}(\alpha_{[1,0]})$ is cyclic of the prescribed order. Looking at $\mathrm{Ker}(\alpha_{[1,0]})$ and at $\mathrm{Coker}(\alpha_{[0,1]})$ as subgroups of $\hat{H}^{-1}(G_{n,m}, \mathcal{B}_n)$ as in (5.1), and knowing the structure of this last module by Lemma 4.3, shows that $\mathrm{Coker}(\alpha_{[0,1]})$ is cyclic, too. □

Now we can single out from the proof a precise description of the kernels of the maps $\alpha_{[1,0]}$ and $\alpha_{[0,1]}$ when seen as maps

$$\alpha_{[i,j]} : A_n \to B_n$$

by combining (3.4) and (5.3). Before stating the next result, observe that, by Lemma (3.1), $\hat{H}^{-1}(G_{n,m}, Cyc_n) \cong \hat{H}^{-1}(G_{n,m}, \langle\eta_n\rangle)$, while (3.2) and (3.3) show that $\hat{H}^{-1}(G_{n,m}, \langle\eta_n\rangle) \cong \hat{H}^{-1}(G_{n,m}, I_{G_n}) \cong \hat{H}^0(G_{n,m}, \mathbb{Z}_p)$. It is clear that these isomorphisms are not only $G_{n,m}$-linear, but also G_n-linear: therefore $\hat{H}^{-1}(G_{n,m}, Cyc_n)$ has trivial G_n-action.

Corollary 5.2. *With the same hypothesis as in the theorem,*

$$\mathrm{Ker}(\alpha_{[0,1]}) = \mathrm{Ker}(\alpha_{[1,0]}) = \Pi_n \ .$$

Proof. While proving the theorem we found $\mathrm{Ker}(\alpha_{[1,0]}) = \Pi_n$, and we now focus on $\mathrm{Ker}(\alpha_{[0,1]})$. We already know it is cyclic: looking again at (5.5) we find $\mathrm{Ker}(\alpha_{[0,1]}) \subseteq \mathrm{Im}\big(\hat{H}^{-1}(G_{n,m}, Cyc_n)\big) \subseteq \hat{H}^{-1}(G_{n,m}, \mathcal{O}_n^\times)^{G_n}$: since the isomorphisms $\hat{H}^0(G_{n,m}, Q_n) \cong A_n$ are G_n-linear, we get $\mathrm{Ker}(\alpha_{[0,1]}) \subseteq A_n^{G_n}$. As in the proof of Corollary (4.6), the assumption $\lambda = 0$ is equivalent to $\Pi_n = X^\Gamma$ and $X^\Gamma = A_n^{G_n}$ if n is big enough; putting all together, we have $\mathrm{Ker}(\alpha_{[0,1]}) \subseteq \Pi_n$. Since they have the same order thanks to Corollary 4.6 together with Theorem 5.1, the inclusion turns into an equality. □

Remark. As the above Corollary shows, there are indeed two maps $\alpha_{[0,1]}$ and $\alpha_{[1,0]}$ sitting in an exact sequence

$$0 \longrightarrow \Pi_n \longrightarrow A_n \xrightarrow{\alpha} B_n \longrightarrow \mathcal{B}_0/\eta_0 \longrightarrow 0 \ ,$$

where α can be either of them. This is the same as in the non-split case, where both $\alpha_{[0,1]}$ and $\alpha_{[1,0]}$ give an isomorphism $A_n \cong B_n$ for $n \gg 0$ if $\lambda = 0$ (see [KS95]).

References

[BNQD01] J.-R. Belliard and T. Nguyen Quang Do, *Formules de classes pour les corps abéliens réels*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 4, 903–937.

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[FW79] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[Gil79a] Roland Gillard, *Remarques sur les unités cyclotomiques et les unités elliptiques*, J. Number Theory **11** (1979), no. 1, 21–48.

[Gil79b] ———, *Unités cyclotomiques, unités semi-locales et $\mathbf{Z}_l$-extensions.II*, Ann. Inst. Fourier (Grenoble) **29** (1979), no. 4, viii, 1–15.

[Gre76] Ralph Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284.

[Gre77] ———, *On p-adic L-functions and cyclotomic fields. II*, Nagoya Math. J. **67** (1977), 139–158.

[Iwa60] Kenkichi Iwasawa, *On local cyclotomic fields*, J. Math. Soc. Japan **12** (1960), 16–21.

[Iwa73] ———, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[KS95] James S. Kraft and René Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), no. 1-2, 135–155, Special issue in honour of Frans Oort.

[Kuz96] L. V. Kuz′min, *On formulas for the class number of real abelian fields*, Izv. Ross. Akad. Nauk Ser. Mat. **60** (1996), no. 4, 43–110.

[Lan90] Serge Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000.

[Oza97] Manabu Ozaki, *On the cyclotomic unit group and the ideal class group of a real abelian number field. I, II*, J. Number Theory **64** (1997), no. 2, 211–222, 223–232.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Sch90] René Schoof, *The structure of the minus class groups of abelian number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 185–204.

[Sin81] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980/81), no. 2, 181–234.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

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

On Fake $\mathbb{Z}_p$-extensions of Number Felds

Luca Caputo and Filippo Alberto Edoardo Nuccio

July 7th, 2008

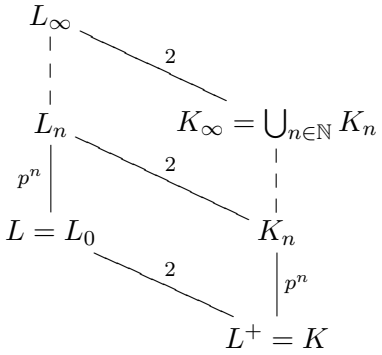
Abstract

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

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

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 $\psi_1, \ldots, \psi_{(q-1)/2}$ 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 $0 \leqslant h \leqslant q-1$, 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 $0 < a \leqslant q-1$,

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

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

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

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 $s \in \mathbb{C} \smallsetminus \{1\}$. *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 $\operatorname{Re} s > 1$,

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

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

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

by Lemma 2.2.
Now we consider ζ_k: we have

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

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

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

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

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

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

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

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

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

and[2]

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

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 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

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

[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.

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)

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

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

$$(E_F : E_k E_{k'}) = \frac{2^{n-1} q R_k^2 (\mathcal{O}_L^\times : \mathcal{O}_K^\times)}{Q R_K R_F (\mathrm{tor}_{\mathbb{Z}}\mathcal{O}_F^\times : \mathrm{tor}_{\mathbb{Z}}(\mathcal{O}_k^\times \mathcal{O}_{k'}^\times))}$$

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*

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

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

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

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

$$0 \to A[N_{G_n}] \to A \to N_{G_n} A \to 0 \tag{25}$$

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

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

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

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

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

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

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

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

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 $\mathrm{coker}(k_n)$ 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 $\mathrm{coker}(k_n)$.

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)

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

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

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

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 $\mathfrak{P}_{i,1}, \ldots, \mathfrak{P}_{i,s}$ 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 $j = 1, \ldots, s$, 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 $\{\mathrm{Frob}(\mathfrak{P}_{i,j}, M_\infty/L_\infty)\}_{i=1,2;\, j=1,\ldots,s}$: 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). □

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*

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

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)

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

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

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

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

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

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

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

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

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

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