Application of the notion of φ-object to the study of p-class groups and p-ramified torsion groups of abelian extensions

Georges Gras

APPLICATION OF THE NOTION OF φ-OBJECT TO THE STUDY OF p-CLASS GROUPS AND p-RAMIFIED TORSION GROUPS OF ABELIAN EXTENSIONS

GEORGES GRAS

ABSTRACT. Article based on the English translation, with many improvements, new results, and numerical illustrations, of our following original articles in French:

Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, *Publications Mathématiques de Besançon. Algèbre et théorie des nombres* **2***(1) (1976), 99 p.* https://doi.org/10.5802/pmb.a-10

Étude d'invariants relatifs aux groupes des classes des corps abéliens, *Astérisque* **41-42** *(1977), 35–53.* http://www.numdam.org/item?id=AST_1977__41-42__35_0

The "Main Conjecture", about the equality of Arithmetic and Analytic Invariants, that we revisit here, were stated in the papers mentioned above and given at the meeting: "Journées arithmétiques de Caen" (1976). These papers were written in french with illegible fonts due to the use of "typits", on typewriters, for mathematical symbols ! So they were largely ignored, as well as some aspects of Leopldt's papers on cyclotomy, written in Germain, in the 1950/1960's. Since that time, these abelian conjectures have been masterfully proven, essentially in the semi-simple case, then in general for relative class groups and Iwasawa's theory framework. The *non semi-simple real case*, was less understood because of a problematic definition of cyclotomic units (Leopoldt, Sinnott, etc.); but at the time, we proposed another more natural and canonical conjectural context, still unproved to our knowledge (see the important Remark 7.12).

Let $\mathscr{G} := \mathrm{Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$ be the Galois group of the maximal abelian extension $\mathbb{Q}^{\rm ab}$ of $\mathbb{Q}$ and denote by K any subfield of finite degree of $\mathbb{Q}^{\rm ab}$. The present article is divided into the following parts, after an Introduction giving a brief description about the story (rather prehistory) that led to the numerous proofs giving the "Main Theorem" on abelian fields:

(i) An algebraic part giving a systematic study of families $\mathbf{M}_K$, $K \subset \mathbb{Q}^{\rm ab}$, of $\mathbb{Z}[\mathscr{G}]$-modules and of the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_K := \mathbf{M}_K \otimes \mathbb{Z}_p$, including the non semi-simple case (i.e., $p \mid [K:\mathbb{Q}]$). This study leads to the definition of sub-modules $\mathscr{M}_\varphi^{\rm alg}$ (algebraic) and $\mathscr{M}_\varphi^{\rm ar}$ (arithmetic), indexed by the set of irreducible p-adic characters φ of $\mathscr{G}$ (leading to the notion of φ-objects).

The difference between $\mathscr{M}_\varphi^{\rm alg}$ (used in all the literature) and $\mathscr{M}_\varphi^{\rm ar}$ is that the first one relates to algebraic norms $\mathcal{V}_{k/k'} \in \mathbb{Z}[\mathrm{Gal}(k/k')]$ for their properties, while the second one uses arithmetic norms $\mathbf{N}_{k/k'}$, the gap being given by the relation $\mathcal{V}_{k/k'} = \mathbf{J}_{k/k'} \circ \mathbf{N}_{k/k'}$, where the transfer map $\mathbf{J}_{k/k'}$ is often non injective in p-extensions (see the corresponding definitions and the non semi-simple examples, given § 3.3, justifying our Definition 3.12 for the Main Conjecture). Moreover the "arithmetic" point of view allows more natural analytic formulas (as that of Theorem 3.15). See § 4.3 for the main properties of these families.

(ii) An arithmetic part where we apply the results on φ-objects to the p-class groups $\mathscr{H}_K$, for K real or imaginary, then to the torsion groups $\mathscr{T}_K$ of the Galois group of the maximal p-ramified abelian pro-p-extension of K real. For any rational character χ and any p-adic characters $\varphi \mid \chi$, we define the "Class Invariants" $m_\varphi^{\rm alg}(\mathscr{H})$ (algebraic), $m_\varphi^{\rm ar}(\mathscr{H})$, $m_\varphi^{\rm ar}(\mathscr{T})$ (arithmetic) and, in § 8.2, we define the corresponding "Analytic Invariants" $m_\varphi^{\rm an}(\mathscr{H})$, $m_\varphi^{\rm an}(\mathscr{T})$ suggested by the analytic formulas obtained for the arithmetic χ-components (Theorems 5.10, 7.10, 6.2), and we develop the problem of their comparison for even and odd p-adic characters φ.

We conjecture a new annihilation theorem for $\mathscr{H}_\varphi^{\rm ar}$, for any even φ (Conjecture 7.14).

Even if the conjectures are now largely proved in various ways, and extended to Iwasawa's theory statements, the case of *even p-adic characters in the non semi-simple case* seems largely unproved to day. So, the method of φ-objects may be useful to examine this case where the distinction between "algebraic" and "arithmetic" definitions is particularly crucial.

(iii) An illustration is given with cyclic cubic fields for $p \equiv 1 \pmod 3$, as well as a PARI program computing the above invariants, which was not possible in the 1970's.

Date: January 5, 2022.

2020 *Mathematics Subject Classification.* Primary 11R18, 11R29, 11R27 ; Secondary 11R37, 12Y05, 08-04.

Key words and phrases. abelian fields; p-adic characters; class groups and units; cyclotomic polynomials.

Contents

1. Introduction and brief historical survey

We translate, into english, and improve (with PARI programs and numerical illustrations), some parts of the original french versions of the papers [Gra1976, Gra1976/77], despite the fact that some arguments are now well-known, and that many progress have been done, to culminate with the Main Theorem on abelian fields, proving (essentially in the semi-simple case, then in general, for relative class groups and Iwasawa's theory framework), some of the conjectures that we stated in the 1970's.

However, the *non semi-simple real case* does not seem fully elucidated. Note that, in the literature, the word "Main Conjecture/Theorem" is related to the particular Iwasawa's theory statement.

1.1. **Main bibliographic reminders - Pioneering references.** It is not possible to give here all the story of such a subject, from Bernoulli–Kummer–Herbrand classical context, the initiating work of Iwasawa, Leopoldt, Greenberg, on the conjectures, then the deep results obtained by Ribet–Mazur–Wiles–Thaine–Rubin–Kolyvagin–Solomon–Greither–Coates–Sinnott, and others, on cyclotomy and p-adic **L**-functions, also giving the Iwasawa formulation of the Main Theorem (see e.g., [Gree1975], [Gree1977]), which is less precise than the expected results for finite extensions, but more conceptual in broader contexts (in fact, describing the similarity with the theory of p-adic **L**-functions, a more generalizable feature).

We refer, for a very nice story of pioneering works, to Ribet [Rib2008a, Rib2008b], for detailed proofs of Iwasawa Main Conjecture, to Washington's book [Was1997, Chap. 15] (following techniques initiated by Thaine, then Kolyvagin, Ribet, described in Lang's book [Lang1990]). A Bourbaki Seminar, by Bernadette Perrin-Riou [PR1990], gives a significant lecture, with an impressive bibliography, on the works of Kolyvagin, Rubin and others about the Main Conjectures for number fields and elliptic curves.

Finally, a proof of our conjectures for the relative p-class groups $\mathscr{H}^-$ and the real torsion groups $\mathscr{T}$ of the Galois groups of the maximal abelian p-ramified pro-p-extensions was given (by Solomon, for $\mathscr{H}^-$ and $p \neq 2$ [Sol1990, Theorem II.1], by Greither, for $\mathscr{H}^-$, $\mathscr{T}$ with $p \geq 2$, and $\mathscr{H}^+$ in a semi-simple context [Grei1992, Theorems A, B, C, 4.14, Corollary 4.15]). Let us mention especially the proof by Rubin [Rub1990], from Kolyvagin "Euler systems" [Kol2007] used in the above works.

Many complementary works about the orders or the annihilation of the $\mathscr{H}_\varphi$, for irreducible p-adic characters φ, were published before or after the decisive proofs (e.g., [Gra1977, Gil1977, Gra1979, Or1981, Or1986, BelNg2005, All2013, BelMar2014, All2017, Gra2018b]). Let us mention, for example, the (not very well-known) result of Oriat [Or1986, Theorem, p. 333] showing an algebraic link between the Main Conjectures, for $\mathscr{H}_\varphi$ and $\mathscr{H}_{\overline{\varphi}}$, in an abelian field containing μ_p and under some assumptions, where $\overline{\varphi}$ is the reflection of φ.

In the same way, it is hopeless to outline all generalizations giving "Main Conjectures" in other contexts than the absolute abelian case (e.g., [MazRub2011, CoLi2019, CoLi2020, BBDS2021]); an expository book may be [CS2006] for more recent works, but excluding the story of the origins of the Main Conjecture as explained in Solomon–Greither papers [Sol1990, Grei1992], Washington's book [Was1997], and Ribet's Lectures [Rib2008a, Rib2008b].

In another direction, we refer to enlargements of the algebraic/arithmetic aspects with p-adic characters in the area of metabelian Galois groups, with applications to class groups and units (see for instance [Jau1981, Théorème 1 and consequences], then [Jau1984],[Jau1986] in a class field theory context, [Lec2018, SchStu2019] in a geometric or Galois cohomology context), and the references of these papers. Due to the huge number of articles dealing with the concept of "Main Conjecture", some more recent (or not) articles may have escaped our notice and any information on this will be welcome.

1.2. **Introduction of Arithmetic Objects.** Nevertheless, these works deal with *algebraic definitions* of the φ-objects (for p-adic characters φ); that is to say, for $G := \mathrm{Gal}(K/\mathbb{Q})$ cyclic of order $g \equiv 0 \pmod p$, $\mathscr{H}_\varphi^{\mathrm{alg}} := \mathscr{H}_K \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\mu_g] = \{x \in \mathscr{H}_K,\ \nu_{K/k}(x) = 1, \text{ for all } k \subsetneq K\}$ for p-class groups ($\nu_{K/k}$ = algebraic norm), contrary to $\mathscr{H}_\varphi^{\mathrm{ar}} := \{x \in \mathscr{H}_K,\ \mathbf{N}_{K/k}(x) = 1, \text{ for all } k \subsetneq K\}$ (see § 2.2 for the main definitions and results). So the distinction between algebraic and arithmetic φ-components is not done in the literature. This does not matter for relative p-class groups $\mathscr{H}^-$ and torsion groups $\mathscr{T}$ since we will prove that the two notions coincide (Theorems 5.8, 6.1); so the case of these invariants can be considered as definitely solved, contrary to real p-class groups $\mathscr{H}^+$ in the non semi-simple case. We give numerical illustration showing the gap between the two notions (see § 3.3 for the two numerical examples given with $p = 3$).

If one replaces the p-class group $\mathscr{H}_K$ of a real abelian field K by the larger $\mathbb{Z}_p[\mathscr{G}]$-module $\mathscr{T}_K$ (torsion group of the Galois group of the maximal abelian p-ramified pro-p-extension of K), one gets easier annihilation theorems and a proof of the Main Conjecture for such invariants. Indeed, for them, the norm maps $\mathbf{N}_{k/k'}$ are surjective and the transfer maps $\mathbf{J}_{k/k'}$ are injective under Leopoldt's conjecture [Gra2005, Theorem IV.2.1], [Jau1986, Jau1998, Ng1986]; so this family behaves as the family of relative class groups, which allows obvious statements of the Main Conjecture and then their proofs with similar techniques, as done for instance in [Grei1992].

Moreover, $\mathscr{T}_K$ is closely related to the p-adic $\mathbf{L}$-functions "at $s=1$" [Coa1975] and a particularity of $\mathscr{T}_K$ is its interpretation by means of the three $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{H}_K^{\rm cyc}$, $\mathscr{R}_K$, $\mathscr{W}_K$; see [Gra2005, Lemma III.4.2.4], leading to the exact sequence (6.1) and the formula:

$$\#\mathscr{T}_K = \#\mathscr{H}_K^{\rm cyc} \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K,$$

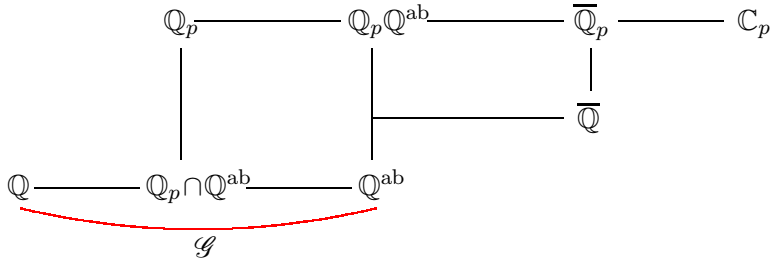
where $\mathscr{W}_K$ is an easy canonical invariant depending on local p-roots of unity, $\mathscr{R}_K$ is the normalized p-adic regulator [Gra2018a, Lemma 3.1], and $\mathscr{H}_K^{\rm cyc}$ a subgroup of $\mathscr{H}_K$ (equal to $\mathscr{H}_K$, except "the part" corresponding to the maximal unramified extension contained in the cyclotomic $\mathbb{Z}_p$-extension of K). The main invariant, besides the p-class group, is $\mathscr{R}_K$ whose order is (up to an obvious factor) the classical p-adic regulator given by the p-adic analytic formulas, from the pioneering work of Kubota–Leopoldt on p-adic $\mathbf{L}$-functions, then that of Amice–Fresnel–Barsky (see e.g., [Fre1965]), Coates, Ribet and many other; see a survey in [Gra1978/79a] and a lecture in [Rib1979] where is used the beginnings of the concept of p-adic pseudo-measures of Mazur, developed by Serre [Ser1978]). At this time was stated the Iwasawa formalism of the Main Conjecture by Greenberg [Gree1975, Gree1977] after Iwasawa [Iwa1964b] and annihilation theorems. We have discussed in [Gra2019, Gra2016] the behavior of $\mathscr{R}_K$ when $p \to \infty$

1.3. **Conclusion.** Let $K/\mathbb{Q}$ be a real abelian extension with a cyclic maximal p-sub-extension assumed to be non trivial (non semi-simple case); set $\mathscr{E} := \mathbf{E} \otimes \mathbb{Z}_p$, were $\mathbf{E}$ denotes groups of global units in K. It would remain to prove our conjecture [Gra1976/77] for the even p-adic characters φ, of $\mathrm{Gal}(K/\mathbb{Q})$, saying that $\#\mathscr{H}_\varphi^{\rm ar} = w_\varphi \cdot \#\widetilde{\mathscr{E}}_\varphi$ ($w_\varphi \in \{1, p\}$), $\widetilde{\mathscr{E}}_\varphi$ being the "φ-part", in the meaning of φ-objects, of $\widetilde{\mathscr{E}}_K := \mathscr{E}_K/\mathscr{E}_K^0 \cdot \mathscr{F}_K$, where $\mathscr{E}_K^0 \subseteq \mathscr{E}_K$ is generated by the $\mathscr{E}_k$ for all $k \subsetneq K$ and $\mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p$ is the group of Leopoldt's cyclotomic units (φ-version of the analytic formula of Theorem 7.10, Corollary 7.11, and Remark 7.12).

2. Abelian extensions

The idea of definition of the φ-objects owes a lot to the work of Leopoldt [Leo1954, Leo1962] and their writing in french by Oriat in [Or1975a, Or1975b]. Some outdated notations in [Gra1976, Gra1976/77, Gra1977] are modified, after changing ℓ into p (e.g., $\Omega_p \mapsto \overline{\mathbb{Q}}_p$, $\widehat{\Omega}_p \mapsto \mathbb{C}_p$, $\Gamma \mapsto \mathbb{Z}_p$) and new results are mentioned using additional references (References 9.3.2).

2.1. **Characters.** Let $\mathbb{Q}^{\rm ab}$ be the maximal abelian extension of $\mathbb{Q}$, contained in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ with the following diagram of inclusions ($\overline{\mathbb{Q}}_p$ is an algebraic closure of $\mathbb{Q}_p$ containing $\overline{\mathbb{Q}}$, $\mathbb{C}_p$ a completion of $\overline{\mathbb{Q}}_p$ and $\mathscr{G} := \mathrm{Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$):



Denote by Ψ the set of irreducible characters of $\mathscr{G}$, of degree 1 and finite order, with values in $\overline{\mathbb{Q}}_p$. We define the sets of irreducible p-adic characters Φ, for the given prime $p \geq 2$, the set $\mathscr{X}$ of irreducible rational characters and the corresponding sets of irreducible characters Ψ_K, Φ_K, $\mathscr{X}_K$, of the Galois group, $G_K := \mathrm{Gal}(K/\mathbb{Q})$, of a subfield K of $\mathbb{Q}^{\rm ab}$. The notation $\psi \mid \varphi \mid \chi$ (for $\psi \in \Psi$, $\varphi \in \Phi$, $\chi \in \mathscr{X}$) means that φ is a term of χ and ψ a term of φ.

Let $s \in \mathcal{G}$ be the complex conjugation and $\psi \in \Psi_K$; if $\psi(s) = 1$ (resp. $\psi(s) = -1$), we say that ψ is even (resp. odd) and we denote by Ψ_K^+ (resp. Ψ_K^-) the corresponding subsets of characters. Since $\Psi_K^\pm$ is stable by any conjugation, this defines $\Phi_K^\pm$, $\mathscr{X}_K^\pm$.

Let $\chi \in \mathscr{X}$ be an irreducible rational character. Denote by:

$$g_\chi,\ \ K_\chi,\ \ G_\chi,\ \ f_\chi,\ \ \mathbb{Q}(\mu_{g_\chi}),$$

the order of any $\psi \mid \chi$, the subfield of K fixed by $\mathrm{Ker}(\chi) := \mathrm{Ker}(\psi)$, $\mathrm{Gal}(K_\chi/\mathbb{Q})$, the conductor of K_χ, the field of values of the characters, respectively.

The set $\mathscr{X}$ has the following useful property which may be considered as an obvious "Main theorem" for rational components (see e.g., [Leo1954, Chap. I, § 1, 1]):

Theorem 2.1. *Let $K/\mathbb{Q}$ be a finite abelian extension and let $(A_\chi)_{\chi\in\mathscr{X}_K}$ and $(A'_\chi)_{\chi\in\mathscr{X}_K}$ be two families of numbers, indexed by the set $\mathscr{X}_K$ of irreducible rational characters of K. If for all subfields k of K, the equalities $\prod_{\chi\in\mathscr{X}_k} A'_\chi = \prod_{\chi\in\mathscr{X}_k} A_\chi$ are fulfilled, then $A'_\chi = A_\chi$ for all $\chi \in \mathscr{X}_K$.*

2.2. **Main definitions and results.** Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a family of finite $\mathbb{Z}[\mathcal{G}]$-modules, indexed with the set $\mathscr{K}$ of abelian extensions of $\mathbb{Q}$, and provided with the arithmetic norms $\mathbf{N}_{K/k}$ and transfer maps $\mathbf{J}_{K/k}$, for any $k \subseteq K$, where $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} = \nu_{K/k}$ (the algebraic norm in $\mathbb{Z}[\mathrm{Gal}(K/k)]$); we will give more well-known details in Section 3.1.

We associate with $\mathbf{M}$ the family of $\mathbb{Z}_p[\mathcal{G}]$-modules $\mathscr{M} := \mathbf{M} \otimes \mathbb{Z}_p$.

We define various χ-components $\mathbf{M}_\chi^{\mathrm{alg}}$, $\mathbf{M}_\chi^{\mathrm{ar}}$, $\mathscr{M}_\chi^{\mathrm{alg}}$, $\mathscr{M}_\chi^{\mathrm{ar}}$ (for $\chi \in \mathscr{X}$), and we define various φ-components $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi^{\mathrm{ar}}$ (for $\varphi \in \Phi$), as follows:

Let P_χ be the global g_χth cyclotomic polynomial and let P_φ be the local cyclotomic polynomial associated with $\varphi \mid \chi$ (so that $P_\chi = \prod_{\varphi|\chi} P_\varphi$ in $\mathbb{Z}_p[X]$). We define:

$$\mathbf{M}_\chi^{\mathrm{alg}} := \big\{x \in \mathbf{M}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\big\},\ \mathscr{M}_\chi^{\mathrm{alg}} := \mathbf{M}_\chi^{\mathrm{alg}} \otimes \mathbb{Z}_p,$$
$$\mathscr{M}_\varphi^{\mathrm{alg}} := \big\{x \in \mathscr{M}_\chi^{\mathrm{alg}},\ P_\varphi(\sigma_\chi)\cdot x = 1\big\},$$
$$\mathbf{M}_\chi^{\mathrm{ar}} := \{x \in \mathbf{M}_\chi^{\mathrm{alg}},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\},\ \mathscr{M}_\chi^{\mathrm{ar}} = \mathbf{M}_\chi^{\mathrm{ar}} \otimes \mathbb{Z}_p,$$
$$\mathscr{M}_\varphi^{\mathrm{ar}} := \{x \in \mathscr{M}_\varphi^{\mathrm{alg}},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}.$$

(i) Then we have the following results about the algebraic and arithmetic χ-components:

$\mathbf{M}_\chi^{\mathrm{alg}} = \big\{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\big\}$ (Theorem 3.8),

$\mathscr{M}_\chi^{\mathrm{alg}} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\mathrm{alg}}$ (Theorem 4.1),

$\mathscr{M}_\chi^{\mathrm{ar}} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\mathrm{ar}}$ (Theorem 4.4).

(ii) Assume that $K/\mathbb{Q}$ is cyclic and $\mathbf{M}_K$ finite.

(ii′) If, for all sub-extensions k/k' of $K/\mathbb{Q}$, the norm maps $\mathbf{N}_{k/k'}$ are surjective, then:

$\#\mathbf{M}_K = \prod_{\chi\in\mathscr{X}_K} \#\mathbf{M}_\chi^{\mathrm{ar}}$ (Theorem 3.15),

where $\mathscr{X}_K$ denotes the set of rational characters of K (i.e., such that $K_\chi \subseteq K$).

(ii″) Let K/K_0 be the maximal p-sub-extension of $K/\mathbb{Q}$; if, for all sub-extensions k/k' of K/K_0, the norm maps $\mathbf{N}_{k/k'}$ are surjective, then:

$\#\mathscr{M}_\chi^{\mathrm{ar}} = \prod_{\varphi|\chi} \#\mathscr{M}_\varphi^{\mathrm{ar}}$ (Theorem 4.4 for finite modules).

(ii‴) The above conditions of surjectivity of the norms are automatically fulfilled for the families $\mathbf{H}$, $\mathscr{H}$, $\mathscr{T}$.

(iii) Applying this to class groups $\mathbf{H}$ and torsion groups $\mathscr{T}$ of abelian p-ramification, we obtain:

(iii′) For all odd characters χ, we have:

$\mathbf{H}_\chi^{\mathrm{ar}} = \mathbf{H}_\chi^{\mathrm{alg}}$ and $\mathscr{H}_\varphi^{\mathrm{ar}} = \mathscr{H}_\varphi^{\mathrm{alg}}$, for all $\varphi \mid \chi$ (Theorem 5.8);

$\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi}\cdot w_\chi \cdot \prod\limits_{\psi\vert\chi}\big(-\frac{1}{2}\,\mathbf{B}_1(\psi^{-1})\big)$ (Theorem 5.10), in terms of Bernoulli numbers.

(iii″) For all even characters χ, we have:

$\mathbf{H}_\chi^{\rm ar} \subseteq \mathbf{H}_\chi^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar} \subseteq \mathscr{H}_\varphi^{\rm alg}$, for all $\varphi \mid \chi$ (see Examples 3.13, 3.14 for strict inclusions);

$\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot \big(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi}\cdot \mathbf{F}_{K_\chi}\big)$ (Theorem 7.10), in terms of cyclotomic units, where $\mathbf{E}^0_{K_\chi}$ is the subgroup of $\mathbf{E}_{K_\chi}$ generated by the $\mathbf{E}_k$ for all $k \subsetneq K_\chi$.

(iii‴) For all even characters χ, we have:

$\mathscr{T}_\chi^{\rm ar} = \mathscr{T}_\chi^{\rm alg}$ and $\mathscr{T}_\varphi^{\rm ar} = \mathscr{T}_\varphi^{\rm alg}$ for all $\varphi \mid \chi$ (Theorem 6.1);

$\#\mathscr{T}_\chi^{\rm ar} = w_\chi^{\rm cyc} \cdot \prod\limits_{\psi\vert\chi} \frac{1}{2}\,\mathbf{L}_p(1,\psi)$ (Theorem 6.2), in terms of p-adic $\mathbf{L}$-functions.

(iv) The Arithmetic Invariants of finite $\mathbb{Z}_p[\mathscr{G}]$ modules $\mathscr{M}_K$ are defined by means of the obvious algebraic writing of $\mathbb{Z}_p[\mu_{g_\chi}]$-modules (for the law defined via $\sigma\in\mathscr{G}\mapsto\psi(\sigma)$, for $\psi\mid\varphi$):

$$\mathscr{M}_\varphi^{\rm ar} \simeq \prod_{i\geq 1}\Big[\mathbb{Z}_p[\mu_{g_\chi}]\big/\mathfrak{p}_\varphi^{n^{\rm ar}_{\varphi,i}(\mathscr{M})}\Big],\ \ m_\varphi^{\rm ar}(\mathscr{M}) := \sum_i n^{\rm ar}_{\varphi,i}(\mathscr{M}),$$

where $\mathfrak{p}_\varphi$ is the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$, obtained as p-adic closure of a suitable $\mathfrak{p}\mid p$ of $\mathbb{Z}[\mu_{g_\chi}]$; the definition of the Analytic Invariants $m_\varphi^{\rm an}(\mathscr{M})$ comes directly from the formulas of $\#\mathscr{M}_\chi^{\rm ar}$ given above in (iii), taking into account the decompositions $\mathscr{M}_\chi^{\rm ar} = \bigoplus\limits_{\varphi\vert\chi}\mathscr{M}_\varphi^{\rm ar}$, whence the statement of the Main Conjecture "$m_\varphi^{\rm ar}(\mathscr{M}) = m_\varphi^{\rm an}(\mathscr{M})$, for all $\varphi\in\Phi$" (see Section 8, Conjecture 8.1).

3. Definition and study of the χ-object and φ-objects

We shall give, in this section, a general definition of θ-objects, θ being an irreducible character (rational or p-adic), the Galois modules which intervene in the definition of the θ-objects being not necessarily finite, as it is the case for unit groups; finally, the prime p is arbitrary and we shall emphasize on the non semi-simple framework.

3.1. **The Algebraic and Arithmetic $\mathscr{G}$-families.** Let $\mathscr{K}$ be the family of finite extensions K of $\mathbb{Q}$, contained in $\mathbb{Q}^{\rm ab}$, of Galois group G_K. We assume to have a family $\mathbf{M}$ of (multiplicative) $\mathbb{Z}[\mathscr{G}]$-modules, indexed by $\mathscr{K}$ (called, without more precision, a $\mathscr{G}$-family):

$$\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}},$$

and two families of maps, indexed by the set of sub-extensions K/k, $\mathbf{N}_{K/k}$ (arithmetic norms), $\mathbf{J}_{K/k}$ (arithmetic transfers). For all sub-extensions K/k, we define the algebraic norm:

$$\nu_{K/k} := \sum_{\sigma\in{\rm Gal}(K/k)}\sigma \in \mathbb{Z}[{\rm Gal}(K/k)].$$

If $\sigma\in\mathscr{G}$, we denote by σ_K the restriction of σ to K.

3.1.1. *Assumptions about the families* $(\mathbf{M}_K)_{K\in\mathscr{K}}$, $(\mathbf{N}_{K/k})_{K/k}$, $(\mathbf{J}_{K/k})_{K/k}$. We consider the three following conditions:

(a) For all $K\in\mathscr{K}$, all $x\in\mathbf{M}_K$ and all $\sigma\in\mathscr{G}$, x^σ (sometimes written $\sigma\cdot x$) only depends on the class of σ modulo ${\rm Gal}(\mathbb{Q}^{\rm ab}/K)$ (i.e., the $\mathbf{M}_K$'s are canonically $\mathbb{Z}[G_K]$-modules).

(b) For all sub-extension K/k, the arithmetic maps:

$$\mathbf{N}_{K/k}:\mathbf{M}_K\longrightarrow\mathbf{M}_k \quad\&\quad \mathbf{J}_{K/k}:\mathbf{M}_k\longrightarrow\mathbf{M}_K$$

are $\mathscr{G}$-module homomorphisms fulfilling the transitivity formulas $\mathbf{N}_{K/k}\circ\mathbf{N}_{L/K} = \mathbf{N}_{L/k}$ and $\mathbf{J}_{L/K}\circ\mathbf{J}_{K/k} = \mathbf{J}_{L/k}$, for all $k,K,L\in\mathscr{K}$, $k\subseteq K\subseteq L$.

(c) For all sub-extension K/k, we have, on $\mathbf{M}_K$:

$$\mathbf{J}_{K/k}\circ\mathbf{N}_{K/k} = \nu_{K/k}.$$

Definitions 3.1. *(i) If* $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ *only fulfills condition (a), we shall say that the family* $(\mathbf{M}, \nu)$ *is an algebraic* $\mathscr{G}$*-family; one may only use Galois theory in* K/k *and the algebraic norms* $\nu_{K/k} \in \mathbb{Z}[\mathrm{Gal}(K/k)]$.

(ii) If moreover, there exist two families $(\mathbf{N}_{K/k})$ *and* $(\mathbf{J}_{K/k})$ *(canonically associated with* $\mathbf{M}$*) fulfilling conditions (b) and (c), we shall say that the family* $(\mathbf{M}, \mathbf{N}, \mathbf{J})$ *is an arithmetic* $\mathscr{G}$*-family.*

Remark 3.2. Note that cohomology is only of algebraic nature since, for instance in the case of a cyclic extension K/k of Galois group $G =: \langle\sigma\rangle$, using the class group $\mathbf{H}_K$, we have:

$$\mathrm{H}^1(G, \mathbf{H}_K) = \mathrm{Ker}(\nu_{K/k})/\mathbf{H}_K^{1-\sigma}, \quad \mathrm{H}^2(G, \mathbf{H}_K) = \mathbf{H}_K^G/\nu_{K/k}(\mathbf{H}_K);$$

in general $\nu_{K/k}(\mathbf{H}_K)$ is not isomorphic to $\mathbf{N}_{K/k}(\mathbf{H}_K) \subseteq \mathbf{H}_k$, even if the arithmetic norm is surjective, since the transfer map $\mathbf{J}_{K/k}$ is often non-injective on class groups.

3.1.2. *Obvious properties of the arithmetic* $\mathscr{G}$*-families.*

Proposition 3.3. *For all* $K \in \mathscr{K}$, $\nu_{K/K}$, $\mathbf{N}_{K/K}$, $\mathbf{J}_{K/K}$ *are the identity,* id, *on* $\mathbf{M}_K$.

Proof. This is true for $\nu_{K/K}$; from condition (c), $\mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = \mathrm{id}$ and, from condition (b), $\mathbf{N}_{K/K}^2 = \mathbf{N}_{K/K}$ and $\mathbf{J}_{K/K}^2 = \mathbf{J}_{K/K}$ imply that $\mathbf{J}_{K/K} \circ \mathbf{N}_{K/K}^2 = \mathbf{N}_{K/K} = \mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = \mathrm{id}$ and $\mathbf{J}_{K/K}^2 \circ \mathbf{N}_{K/K} = \mathbf{J}_{K/K} = \mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = \mathrm{id}$. □

Proposition 3.4. *If the map* $\mathbf{N}_{K/k}$ *is surjective or if the map* $\mathbf{J}_{K/k}$ *is injective, then* $\mathbf{N}_{K/k} \circ \mathbf{J}_{K/k}$ *is the elevation to the power* $[K : k]$.

Proof. Assume $\mathbf{N}_{K/k}$ surjective. Let $x \in \mathbf{M}_k$, $x = \mathbf{N}_{K/k}(y)$, $y \in \mathbf{M}_K$; then we get $\mathbf{J}_{K/k}(x) = \mathbf{J}_{K/k} \circ \mathbf{N}_{K/k}(y) = \prod_{\tau\in\mathrm{Gal}(K/k)} y^\tau$ and $\mathbf{N}_{K/k} \circ \mathbf{J}_{K/k}(x) = \mathbf{N}_{K/k}(\prod_{\tau\in\mathrm{Gal}(K/k)} y^\tau) = \prod_{\tau\in\mathrm{Gal}(K/k)} (\mathbf{N}_{K/k}(y))^\tau$, but $\mathbf{N}_{K/k}(y) \in \mathbf{M}_k$, and the product is equal to $(\mathbf{N}_{K/k}(y))^{[K:k]} = x^{[K:k]}$.

Assume $\mathbf{J}_{K/k}$ injective. Then for all $x \in \mathbf{M}_k$, we have $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} \circ \mathbf{J}_{K/k}(x) = \nu_{K/k}(\mathbf{J}_{K/k}(x)) = \prod_{\tau\in\mathrm{Gal}(K/k)} (\mathbf{J}_{K/k}(x))^\tau = \prod_{\tau\in\mathrm{Gal}(K/k)} \mathbf{J}_{K/k}(x^\tau) = \mathbf{J}_{K/k}(x)^{[K:k]} = \mathbf{J}_{K/k}(x^{[K:k]})$, which leads to the identity $\mathbf{N}_{K/k} \circ \mathbf{J}_{K/k}(x) = x^{[K:k]}$. □

Examples 3.5. The most straightforward examples of such arithmetic $\mathscr{G}$-families are the following ones:

(i) $\mathbf{M}_K$ is the group $\mathbf{E}_K$ of units of K (for which the maps $\mathbf{J}_{K/k}$ are injective);

(ii) $\mathbf{M}_K$ is the class group $\mathbf{H}_K$ of K, or the p-class group $\mathscr{H}_K$ for a prime p.

(iii) $\mathbf{M}_K$ is the torsion group $\mathscr{T}_K$ of the Galois group of the maximal p-ramified abelian pro-p-extension of K.

These three cases are relative to the Galois action and the well-known maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$.

(iv) $\mathbf{M}_K := A[G_K]$, where A is a commutative ring; then $\mathbf{M}_K$ is a $A[\mathscr{G}]$-module if one puts $\sigma \cdot \Omega = \sigma_K \Omega$ (product in $A[G_K]$), for all $\Omega \in A[G_K]$ and $\sigma \in \mathscr{G}$. The maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$ are defined by A-linearity by $\mathbf{N}_{K/k}(\sigma_K) := \sigma_k$ and, for $\sigma_k \in G_k$, by $\mathbf{J}_{K/k}(\sigma_k) := \sum_{\tau\in\mathrm{Gal}(K/k)} \tau \cdot \sigma'_k = \nu_{K/k} \cdot \sigma'_k = \nu_{K/k}\sigma'_k$, where σ'_k is any extension of σ_k in G_K. So, for $\sigma_K \in G_K$, $\nu_{K/k}(\sigma_K) = \left(\sum_{\tau\in\mathrm{Gal}(K/k)} \tau\right) \cdot \sigma_K = \nu_{K/k}\sigma_K$.

3.2. **Definition of the $\mathscr{G}$-modules $\mathbf{M}_\chi^{\mathrm{alg}}$, $\mathbf{M}_\chi^{\mathrm{ar}}$, $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi^{\mathrm{ar}}$.** We shall assume in the sequel that $A \in \{\mathbb{Z},\ \mathbb{Z}_{(p)},\ \mathbb{Q},\ \mathbb{Z}_p,\ \mathbb{Q}_p\}$.

3.2.1. *Recalls on* Γ_κ*-conjugation* [Ser1998]. Let $\chi \in \mathscr{X}$. Let $P_\chi(X) \in \mathbb{Z}[X]$ be the g_χth global cyclotomic polynomial. Let κ_A be the field of quotients of A and let $\kappa_A(\mu_{g_\chi})/\kappa_A$ be the extension by the g_χth roots of unity; so, $\Gamma_{\kappa_A,\chi} := \mathrm{Gal}(\kappa_A(\mu_{g_\chi})/\kappa_A)$ is isomorphic to a subgroup of $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$.

One defines, as in [Ser1998], the Γ_{κ_A}-conjugation on Ψ by putting, for all $\tau \in \Gamma_{\kappa_A,\chi}$ and $\psi \in \Psi$, $\psi \mid \chi$, $\psi^\tau := \psi^a$, where $a \in \mathbb{Z}$ is a representative of τ in $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$. If σ_χ is a generator

of $G_\chi := G_{K_\chi}$, then the $\psi^\tau(\sigma_\chi)$ are the conjugates of $\psi(\sigma_\chi)$ in $\kappa_A(\mu_{g_\chi})/\kappa_A$. This defines the irreducible characters over κ_A (with values in A):

$$\theta = \sum_{\tau\in\Gamma_{\kappa_A,\,\chi}} \psi^\tau.$$

3.2.2. *Correspondence between characters and cyclotomic polynomials.* Let χ be an irreducible rational character. In $\kappa_A[X]$, P_χ splits into a product of irreducible distinct polynomials $P_{\chi,i}$; each $P_{\chi,i}$ splits into degree 1 polynomials over $\kappa_A(\mu_{g_\chi})$ and is of degree $[\kappa_A(\mu_{g_\chi}) : \kappa_A]$.

If $\zeta_i \in \mu_{g_\chi}$ is a root of $P_{\chi,i}$, the other roots are the ζ_i^τ for $\tau \in \Gamma_{\kappa_A,\chi}$; thus, these sets of roots are in one by one correspondence with the sets of the form $(\psi^\tau(\sigma_\chi))_{\tau\in\Gamma_{\kappa_A,\chi}}$, $\psi^\tau \mid \chi$, $\psi^\tau \in \Psi$ of order g_χ describing a representative set of characters for the Γ_{κ_A}-conjugation. One may index, *non-canonically*, the irreducible divisors of P_χ in $\kappa_A[X]$ by means of the characters θ obtained from the characters $\psi \in \Psi$ of orders g_χ and by choosing a generator σ_χ of G_χ. Put:

$$P_\theta := \prod_{\psi|\theta}(X - \psi(\sigma_\chi)) \in A[X]. \tag{3.1}$$

Thus $P_\chi = \prod_{\theta|\chi} P_\theta$; for $A = \mathbb{Z}_p$ we get the relation $P_\chi = \prod_{\varphi\in\Phi,\,\varphi|\chi} P_\varphi$, for $A = \mathbb{Z}$, P_χ is irreducible.

3.2.3. *Definition of the $\mathbb{Z}[\mu_{g_\chi}]$-modules $\mathbf{M}_\chi^{\rm alg}$ and the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{M}_\varphi^{\rm alg}$.* We fix a prime number p and consider Φ, the set of irreducible p-adic characters of $\mathscr{G}$.

Definition 3.6. *Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a $\mathscr{G}$-family and let $\mathscr{M} := \mathbf{M}\otimes\mathbb{Z}_p$ be the corresponding local $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules $(\mathscr{M}_K)_{K\in\mathscr{K}}$. Put, for $\chi \in \mathscr{X}$ and for $\varphi \mid \chi$, $\varphi \in \Phi$:*

$$\mathbf{M}_\chi^{\rm alg} := \big\{x \in \mathbf{M}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\big\} \text{ and } \mathscr{M}_\chi^{\rm alg} := \mathbf{M}_\chi^{\rm alg}\otimes\mathbb{Z}_p = \big\{x \in \mathscr{M}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\big\},$$
$$\mathscr{M}_\varphi^{\rm alg} := \big\{x \in \mathscr{M}_{K_\chi},\ P_\varphi(\sigma_\chi)\cdot x = 1\big\} = \big\{x \in \mathscr{M}_\chi^{\rm alg},\ P_\varphi(\sigma_\chi)\cdot x = 1\big\};$$

$\mathscr{M}_\varphi^{\rm alg}$ is a sub-$\mathbb{Z}_p[G_\chi]$-module of $\mathscr{M}_{K_\chi}$ (or of $\mathscr{M}_\chi^{\rm alg}$) and the elements of $\mathscr{M}_\varphi^{\rm alg}$ are called φ-objects (in the algebraic sense).

Since $\mathbb{Z}[G_\chi]/(P_\chi(\sigma_\chi)) \simeq \mathbb{Z}[X]/(X^{g_\chi}-1, P_\chi(X)) \simeq \mathbb{Z}[\mu_{g_\chi}]$, the $\mathscr{G}$-module $\mathbf{M}_\chi^{\rm alg}$ is canonically a $\mathbb{Z}[\mu_{g_\chi}]$-module; in the same way, since $\mathbb{Z}_p[G_\chi]/(P_\varphi(\sigma_\chi)) \simeq \mathbb{Z}_p[X]/(X^{g_\chi}-1, P_\varphi(X)) \simeq \mathbb{Z}_p[\mu_{g_\chi}]$, the $\mathscr{G}$-module $\mathscr{M}_\varphi^{\rm alg}$ is canonically a $\mathbb{Z}_p[\mu_{g_\chi}]$-module. The isomorphisms are realized via the maps deduced from $\sigma \mapsto \psi(\sigma)$ for all $\sigma \in G_\chi$ ($\psi \mid \chi$, $\psi \mid \varphi$, respectively); $\mathscr{M}_\varphi^{\rm alg}$ is the largest sub-module of $\mathscr{M}_\chi^{\rm alg}$ on which G_χ acts by $\psi \mid \varphi$.

From relation (3.1), the polynomials P_φ, irreducible over $\mathbb{Q}_p$, depend on the choice of the generator σ_χ of G_χ, but we have the following canonical property:

Lemma 3.7. *The Definitions 3.6 (of the $\mathbb{Z}[\mu_{g_\chi}]$-modules $\mathbf{M}_\chi^{\rm alg}$ and the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{M}_\varphi^{\rm alg}$) do not depend on the choice of σ_χ.*

Proof. Consider a p-adic character φ.

We have $P_\varphi(\sigma_\chi) = \prod_{\psi|\varphi}(\sigma_\chi - \psi(\sigma_\chi))$ and, for $a > 0$, $\gcd(a, g_\chi) = 1$, let $\sigma'_\chi =: \sigma_\chi^a$ another generator of G_χ giving $P'_\varphi(\sigma'_\chi) = \prod_{\psi|\varphi}(\sigma'_\chi - \psi(\sigma'_\chi))$; one must compare $P_\varphi(\sigma_\chi)$ and $P'_\varphi(\sigma'_\chi)$. Then, $P'_\varphi(\sigma_\chi^a) = \prod_{\psi|\varphi}(\sigma_\chi^a - \psi(\sigma_\chi^a)) = \prod_{\psi|\varphi}\big[(\sigma_\chi - \psi(\sigma_\chi))\times(\sigma_\chi^{a-1} + \cdots + \psi^{a-1}(\sigma_\chi))\big]$, and similarly, writing $1 \equiv a\,a^* \pmod{g_\chi}$, where $a^* > 0$ represents an inverse of a modulo g_χ, we have, from $\sigma_\chi = (\sigma_\chi^a)^{a^*}$, $P_\varphi(\sigma_\chi) = \prod_{\psi|\varphi}\big[(\sigma_\chi^a - \psi(\sigma_\chi^a))\times(\sigma_\chi^{a(a^*-1)} + \cdots + \psi^{a(a^*-1)}(\sigma_\chi))\big]$.

Since $P'_\varphi(\sigma'_\chi) \in P_\varphi(\sigma_\chi)\mathbb{Z}_p[G_\chi]$ and $P_\varphi(\sigma_\chi) \in P'_\varphi(\sigma'_\chi)\mathbb{Z}_p[G_\chi]$ the invariance of the definition of the φ-objects follows, as well as that of χ-objects since $P_\chi = \prod_{\varphi|\chi} P_\varphi$. □

3.2.4. *Another characterization of the χ-objects.* For any rational character $\chi \in \mathscr{X}$, we have defined $\mathbf{M}_\chi^{\rm alg}$ and $\mathscr{M}_\chi^{\rm alg}$, but there is, a priori, no obvious algebraic relation between $\mathscr{M}_\chi^{\rm alg}$ and the $\mathscr{M}_\varphi^{\rm alg}$'s of Definition 3.6 by means of local cyclotomic polynomials. A main result will be that $\mathscr{M}_\chi^{\rm alg}$ is the direct sum of them (Theorem 4.1).

We then have the following result, only valid for rational characters, but which will allow another definition of χ and φ-objects (that of "Arithmetic" objects):

Theorem 3.8. *Let $\mathbf{M}$ be a $\mathscr{G}$-family of finite or infinite $\mathbb{Z}[\mathscr{G}]$-modules and let (Definition 3.6) $\mathbf{M}_\chi^{\rm alg} = \{x \in \mathbf{M}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\}$. Then for any $\chi \in \mathscr{X}$ we have:*

$$\mathbf{M}_\chi^{\rm alg} = \{x \in \mathbf{M}_{K_\chi},\ \ \nu_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\},$$

whence $\mathscr{M}_\chi^{\rm alg} = \{x \in \mathscr{M}_{K_\chi}, \nu_{K_\chi/k}(x) = 1, \text{for all } k \subsetneq K_\chi\}$ (one may limit the norm conditions to $\nu_{K_\chi/k_\ell}(x) = 1$ for all prime divisors ℓ of $[K_\chi : \mathbb{Q}]$, where $k_\ell \subset K_\chi$ is such that $[K_\chi : k_\ell] = \ell$).

Proof. [1] We need three preliminary lemmas:

Lemma 3.9. *Let $n \geq 1$ and let q be an arbitrary prime number. Denote by P_n the nth cyclotomic polynomial in $\mathbb{Z}[X]$; then:*

(i) $P_n(X^q) = P_{nq}(X)$, if $q \mid n$;

(ii) $P_n(X^q) = P_{nq}(X)\,P_n(X)$, if $q \nmid n$;

(iii) For q prime and $k \geq 1$, $P_{q^k}(1) = q$. If $n > 1$ is not a prime power, $P_n(1) = 1$.

Proof. Obvious for (i), (ii) by means of comparison of the sets of roots of these polynomials and by induction for (iii). □

Lemma 3.10. *Let $n = \ell_1 \cdots \ell_t$, $t \geq 2$, the ℓ_i's being distinct prime numbers. Then for all pair (i,j), $i \neq j$, there exist A_i^j and A_j^i in $\mathbb{Z}[X]$, such that $A_i^j P_{\frac{n}{\ell_i}} + A_j^i P_{\frac{n}{\ell_j}} = 1$.*

Proof. This can be proved by induction on $t \geq 2$, the case $t = 1$ being empty.

If $t = 2$, $n = \ell_1\ell_2$, $P_{\frac{n}{\ell_2}} = P_{\ell_1} = X^{\ell_1-1} + \cdots + X + 1$, $P_{\frac{n}{\ell_1}} = P_{\ell_2} = X^{\ell_2-1} + \cdots + X + 1$. Let's call "geometric polynomial" any polynomial of the form $X^d + X^{d-1} + \cdots + X + 1$, $d \geq 0$ (including the polynomial 0).

Then if P and $Q \neq 0$ are geometric, the residue R of P modulo Q is geometric with residue $(P - R)Q^{-1} \in \mathbb{Z}[X]$; indeed, if $m \geq n$ and $m + 1 = q(n+1) + r$, $0 \leq r < n$, we get:

$$X^m + \cdots + X + 1 = (X^n + \cdots + X + 1) \times \left[X^{m+1-(n+1)} + X^{m+1-2(n+1)} + \cdots X^{m+1-q(n+1)}\right] + 1 + X + \cdots + X^{r-1}$$

(if $r \geq 1$, otherwise the residue R is 0). In particular, the gcd algorithm gives geometric polynomials; as the unique non-zero constant geometric polynomial is 1, it follows that if P and Q are co-prime polynomials in $\mathbb{Q}[X]$, $\gcd(P,Q) = 1$ and the Bézout relation takes place in $\mathbb{Z}[X]$, which is the case for the geometric polynomials P_{ℓ_1} and P_{ℓ_2}.

Suppose $t \geq 3$. Let ℓ_i, ℓ_j, q, be three distinct prime numbers dividing n and put $n' := \frac{n}{q}$; by induction, since ℓ_i and ℓ_j divide n', there exist polynomials $A_i'^j, A_j'^i$ in $\mathbb{Z}[X]$, such that:

$$A_i'^j(X) P_{\frac{n'}{\ell_i}}(X) + A_j'^i(X) P_{\frac{n'}{\ell_j}}(X) = 1,$$

thus, $A_i'^j(X^q) P_{\frac{n'}{\ell_i}}(X^q) + A_j'^i(X^q) P_{\frac{n'}{\ell_j}}(X^q) = 1$. But Lemma 3.9 (ii) gives:

$$P_{\frac{n'}{\ell_i}}(X^q) = P_{\frac{n}{\ell_i}}(X) P_{\frac{n'}{\ell_i}}(X) \quad \& \quad P_{\frac{n'}{\ell_j}}(X^q) = P_{\frac{n}{\ell_j}}(X) P_{\frac{n'}{\ell_j}}(X),$$

[1] With the contribution of a personal communication from Jacques Martinet, October 1968.

which yields the relation:

$$A_i'^{j}(X^q)P_{\frac{n}{\ell_i}}(X)P_{\frac{n'}{\ell_i}}(X)+A_j'^{i}(X^q)P_{\frac{n}{\ell_j}}(X)P_{\frac{n'}{\ell_j}}(X)=1.$$

We have proved the co-maximality, in $\mathbb{Z}[X]$, of any pair of ideals $(P_{\frac{n}{\ell_i}}(X))$, $(P_{\frac{n}{\ell_j}}(X))$, $i\neq j$ (the case $n=\ell$ giving the prime ideal $(P_\ell(X)\mathbb{Z}[X])$). □

Lemma 3.11. *Let $n>1$ of the form $\prod_{i=1}^{t}\ell_i^{a_i}$, $a_i\geq 1$; put $N_{n,\ell}(X):=\sum_{i=0}^{\ell-1}X^{\frac{n}{\ell}i}$ for any prime ℓ dividing n. Then there exist polynomials $A_\ell(X)\in\mathbb{Z}[X]$ such that $P_n(X)=\sum_{\ell\mid n}A_\ell(X)N_{n,\ell}(X)$ and $\big\langle N_{n,\ell}(X),\ \ell\mid n\big\rangle_{\mathbb{Z}[X]}=P_n(X)\mathbb{Z}[X]$.*

Proof. Assume by induction on n with t fixed that $P_n(X)=\sum_{\ell\mid n}A_\ell(X)N_{n,\ell}(X)$ and let q be a divisor of n; we have, from Lemma 3.9 (i), $P_{nq}(X)=P_n(X^q)=\sum_{\ell\mid n}A_\ell(X^q)N_{n,\ell}(X^q)$. Since we have $N_{n,\ell}(X^q)=\sum_{i=0}^{\ell-1}X^{\frac{n}{\ell}qi}=N_{nq,\ell}(X)$, we obtain that if the lemma is true for n, it is true for nq for all $q\mid n$. It follows that if the property is true for all square-free integers n, it is true for all $n>1$. So we may assume n square-free to prove the lemma by induction on t.

If $n=\ell_1$, $P_{\ell_1}(X)=X^{\ell_1-1}+\cdots+X+1=N_{\ell_1,\ell_1}(X)$ and the claim is obvious. If $n=\ell_1\ell_2\cdots\ell_t$, $t\geq 2$, with distinct primes, put $n_k=\frac{n}{\ell_k}$ for all k; by assumption:

$$P_{n_k}(X)=\sum_{1\leq s\leq t,\ s\neq k}A_s^k(X)N_{n_k,\ell_s}(X),$$

hence, $P_{n_k}(X^{\ell_k})=P_{n_k\ell_k}(X)\cdot P_{n_k}(X)=P_n(X)P_{n_k}(X)=\sum_{1\leq s\leq t\ s\neq k}A_s^k(X^{\ell_k})N_{n,\ell_s}(X)$; whence:

$$P_n(X)P_{n_k}(X)\in\big\langle N_{n,\ell}(X),\ \ell\mid n\big\rangle_{\mathbb{Z}[X]},\ \text{for all } k;$$

since $t\geq 2$, Lemma 3.10 applies and a Bézout relation in $\mathbb{Z}[X]$ between any two of the P_{n_k} (say P_{n_i} and P_{n_j}) yields $P_n(X)\times 1\in\langle N_{n,\ell}(X),\ \ell\mid n\rangle_{\mathbb{Z}[X]}$, whence the result.

We then have proved that the ideal generated, in $\mathbb{Z}[X]$, by the $N_{n,\ell}(X)$, $\ell\mid n$, contains $P_n(X)\mathbb{Z}[X]$. Let's see that $P_n(X)$ contains that ideal; it is sufficient to see that for all $\ell\mid n$, $N_{n,\ell}(X)=P_\ell(X^{\frac{n}{\ell}})$; any root of unity ζ_n of order n (i.e., root of $P_n(X)$), is a root of $N_{n,\ell}(X)$ since $\zeta_n^{\frac{n}{\ell}}=\zeta_\ell\neq 1$ and $\sum_{i=0}^{\ell-1}\zeta_\ell^i=0$; then $P_n(X)\mid N_{n,\ell}(X)$ in $\mathbb{Z}[X]$ (monic polynomials). □

We apply this to the $P_\chi(\sigma_\chi)=P_{g_\chi}(\sigma_\chi)$ and to the $N_{g_\chi,\ell}(\sigma_\chi)=\nu_{K_\chi/k_\ell}$, where k_ℓ is, for all $\ell\mid g_\chi$, the unique sub-extension of K_χ such that $[K_\chi:k_\ell]=\ell$.

The theorem immediately follows. □

3.2.5. *Application to the definition of $\mathbf{M}_\chi^{\rm ar}$.* Now we assume given an arithmetic $\mathscr{G}$-family $\mathbf{M}$, provided with norms $\mathbf{N}$ and transfer maps $\mathbf{J}$ with $\mathbf{J}\circ\mathbf{N}=\nu$.

Definition 3.12. *By analogy with the case of Theorem 3.8 giving, for χ-objects, the definition $\mathbf{M}_\chi^{\rm alg}:=\{x\in\mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x)=1,\ \text{for all } k\subsetneq K_\chi\}$, we define the arithmetic χ-objects:*

$$\mathbf{M}_\chi^{\rm ar}:=\{x\in\mathbf{M}_{K_\chi},\ \ \mathbf{N}_{K_\chi/k}(x)=1,\ \text{for all } k\subsetneq K_\chi\}\subseteq\mathbf{M}_\chi^{\rm alg}\quad\&\quad\mathscr{M}_\chi^{\rm ar}:=\mathbf{M}_\chi^{\rm ar}\otimes\mathbb{Z}_p$$

(one may limit the norm conditions to $\mathbf{N}_{K_\chi/k_\ell}(x)=1$ for all prime divisor ℓ of $[K_\chi:\mathbb{Q}]$, where k_ℓ is the subfield of K_χ such that $[K_\chi:k_\ell]=\ell$).

We have $\mathbf{M}_\chi^{\rm ar}=\mathbf{M}_\chi^{\rm alg}$ as soon as the $\mathbf{J}_{K_\chi/k}$'s are injective (for all $k\subsetneq K_\chi$ or simply the k_ℓ's).

In the case of an arithmetic $\mathscr{G}$-family $\mathbf{M}$, then $\mathbf{M}_\chi^{\rm ar}$ (resp. $\mathscr{M}_\chi^{\rm ar}$) is a sub-$\mathbb{Z}[\mu_{g_\chi}]$-module of $\mathbf{M}_\chi^{\rm alg}$ (resp. a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_\chi^{\rm alg}$). One verifies easily that if the norm maps $\mathbf{N}_{K_\chi/k}$ are surjective for all $k\subsetneq K_\chi$, then $\mathbf{M}_\chi^{\rm alg}/\mathbf{M}_\chi^{\rm ar}$ has exponent a divisor of $\prod_{\ell\mid g_\chi}\ell$.

3.3. **Comparison $\mathscr{M}^{\rm ar}$ versus $\mathscr{M}^{\rm alg}$.** In most papers, the notion of θ-component $\mathbf{M}_\theta$ (θ p-adic or rational) regarding the family $\mathbf{M}$ is, in an abelian field K of Galois group G:

$$\mathbf{M}_\theta := \mathbf{M} \otimes_{A[G]} A[\theta],$$

where $A[\theta]$ is the ring of values of θ over A (e.g., for $A = \mathbb{Z}_p$, $\theta \in \Phi$, $\theta \mid \chi$, $K = K_\chi$ one gets $A[\theta] = \mathbb{Z}_p[\mu_{g_\chi}]$).

As for the example of cohomology groups, this definition is only algebraic and not arithmetic. We shall compare this definition with Definition 3.12 considering irreducible p-adic characters. Let $\varphi \in \Phi$, $\varphi \mid \chi$; we have the classical algebraic definitions of the φ-objects attached to $\mathscr{M}$, that is to say ([Grei1992, Definition, p. 451], [PR1990, § 1.3]):

$$\widehat{\mathscr{M}_\varphi} := \mathscr{M} \otimes_{\mathbb{Z}_p[G_\chi]} \mathbb{Z}_p[\mu_{g_\chi}] \simeq \mathscr{M}/P_\varphi(\sigma_\chi)\cdot\mathscr{M}.$$

Another writing [Sol1990, § II.1, pp. 469–471], is to define $\widehat{\mathscr{M}^\varphi}$ as the largest sub-$\mathbb{Z}_p[G_\chi]$-module of $\mathscr{M}$, such that G_χ acts by ψ. Whence:

$$\widehat{\mathscr{M}^\varphi} := \{x \in \mathscr{M},\ \ P_\varphi(\sigma_\chi)\cdot x = 1\} = \mathscr{M}_\varphi^{\rm alg},$$

with the exact sequence $1 \to \widehat{\mathscr{M}^\varphi} = \mathscr{M}_\varphi^{\rm alg} \longrightarrow \mathscr{M} \longrightarrow P_\varphi(\sigma_\chi)\cdot\mathscr{M} \to 1$ giving the equalities $\#\widehat{\mathscr{M}_\varphi} = \#\widehat{\mathscr{M}^\varphi} = \#\mathscr{M}_\varphi^{\rm alg}$ for finite modules.

These definitions must be analyzed in a numerical point of view for arithmetic objects, as p-class groups; moreover, our forthcoming Definition 4.3 of the objects $\mathscr{M}_\varphi^{\rm ar} := \mathscr{M}_\chi^{\rm ar} \cap \mathscr{M}_\varphi^{\rm alg}$ (from the above Definition 3.12) introduces a second kind of experiments.

Indeed, the Main Theorem on abelian fields is concerned by algebraic definitions similar to $\widehat{\mathscr{M}_\varphi}$, but our conjectures given in the 1970's used the $\mathscr{M}_\varphi^{\rm ar}$ and new analytic formulas for $\#\mathscr{M}_\chi^{\rm ar}$ implying conjectural values for the $\#\mathscr{M}_\varphi^{\rm ar}$'s.

Of course, in the semi-simple case $p \nmid \#G_\chi$, $\mathscr{M} \simeq \mathscr{M}_\varphi \bigoplus \left[P_\varphi(\sigma_\chi)\cdot\mathscr{M}\right]$ whatever the definition, but, in the present paper, we are concerned by the non-trivial context when $g_\chi = [K_\chi : \mathbb{Q}]$ is a multiple of a non trivial power of p. Consider, for example, the following framework:

Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field and, for $p = 3$, let K be the compositum of k with a cyclic extension L of $\mathbb{Q}$ of 3-power degree; the field K is of the form K_χ for an irreducible rational character χ which is also irreducible 3-adic. We have given in [Gra2021b] many examples of capitulations of the 3-class group of k in K, giving $\mathscr{H}_\chi^{\rm ar} \subsetneqq \mathscr{H}_\chi^{\rm alg}$, as the two following ones:

Example 3.13. Let $k = \mathbb{Q}(\sqrt{4409})$ and let L be the degree 9 subfield of $\mathbb{Q}(\mu_{19})$; for convenience, put $k =: k_0$, $k_1 := L_1 k$ (resp. $k_2 := L_2 k$), where L_1 (resp. L_2) is the degree 3 (resp. 9) subfield of $\mathbb{Q}(\mu_{19})$. The prime 2 splits in k_0, is inert in k_2/k_0 and such that $\mathfrak{Q}_0 \mid 2$ in k_0 generates the class group $\mathscr{H}_{k_0}$ (cyclic of order 9); considering the extensions $\mathfrak{Q}_i = \mathbf{J}_{k_i/k_0}(\mathfrak{Q}_0)$ of $\mathfrak{Q}_0$ in k_i, we test its order in the class group $\mathscr{H}_{k_i}$ of k_i, $i = 1, 2$ (we are going to see that $\mathscr{H}_{k_i} \simeq \mathbb{Z}/9\mathbb{Z}$ for all i, which is supported by the fact that $\mathbf{N}_{k_2/k_0}(\mathfrak{Q}_2) = \mathfrak{Q}_0^9$ but $\mathbf{N}_{k_2/k_0}(\mathscr{H}_2) = \mathscr{H}_0$).

The following program is only for verification, the general one being given in [Gra2021b, § 4.2]:

```
{p=3;m=4409;P=x^2-m;ell=19;q=2;for(n=0,2,
R=polcompositum(P,polsubcyclo(ell,p^n))[1];kn=bnfinit(R,1);\\ Definition of kn, n=0,1,2
Fn=idealfactor(kn,q);Qn=component(Fn,1)[1];\\ Qn=ideal dividing 2 in kn (extension of Q0)
print("C",n,"=",kn.cyc,"  ",bnfisprincipal(kn,Qn)[1]))}
```

```
C0=[9]  [4]~                    C1=[9]  [6]~                    C2=[9]  [0]~
```

More precisely, $\mathsf{C0} = [9]$ denotes the class group of k_0 and $[4]^\sim$ means that the class of $\mathfrak{Q}_0 \mid 2$ is h_0^4, where h_0 is the generator (of order 9) given in `kn.cyc` by PARI; then $\mathsf{C1} = [9]$, $[6]^\sim$, is the similar data for k_1 in which we see a partial capitulation since the class of $\mathfrak{Q}_1 = \mathbf{J}_{k_1/k_0}(\mathfrak{Q}_0)$ becomes of order 3. Finally, $\mathsf{C2} = [9]$, $[0]^\sim$ shows the complete capitulation in k_2; the 18 large integers below are the coefficients, over an integral basis, of a generator of $\mathfrak{Q}_2 = \mathbf{J}_{k_2/k_0}(\mathfrak{Q}_0)$ in k_2:

```
Q2=[2,[-1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0]~,1,9,[0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0]~]

[[0]~,[-270476874595642910,323533824277028894,-236208800298303000,119737461690335806,
-255607858779215282,-198423813102857420,41058865020870414,-110028179006577678,
-44960079791821 4026,-4906665437527948,10274048566854232,4319852458093887,13258715755947394,
-6817941144899095,-15448507867705832,2623003974789062,-3264916449440532,-16606126998680345]~]
```

We use obvious notations for the characters defining the fields k_n, $n = 0, 1, 2$. Since arithmetic norms are surjective (here they are isomorphisms), the above computations prove that:

$$\nu_{k_2/k_1}(\mathscr{H}_{k_2}) = \mathbf{J}_{k_2/k_1} \circ \mathbf{N}_{k_2/k_1}(\mathscr{H}_{k_2}) = \mathbf{J}_{k_2/k_1}(\mathscr{H}_{k_1}) \simeq \mathbb{Z}/3\mathbb{Z},$$

since $\mathbf{N}_{k_2/k_1} \circ \mathbf{J}_{k_2/k_1}(\mathscr{H}_{k_1}) = \mathscr{H}_{k_1}^3$ (partial capitulation of $\mathscr{H}_{k_1} \simeq \mathbb{Z}/9\mathbb{Z}$). Whence:

$$\begin{cases} \mathscr{H}_{\chi_2}^{\rm ar} = \{x \in \mathscr{H}_{k_2},\ \mathbf{N}_{k_2/k_1}(x) = 1\} = 1, \\ \mathscr{H}_{\chi_2}^{\rm alg} = \{x \in \mathscr{H}_{k_2},\ P_{\chi_2}(\sigma_{\chi_2}) \cdot x = 1\} \\ \qquad\quad = \{x \in \mathscr{H}_{k_2},\ \nu_{k_2/k_1}(x) = 1\} = \mathscr{H}_{k_2}^3 \simeq \mathbb{Z}/3\mathbb{Z}. \end{cases}$$

We have $P_{\chi_2}(\sigma_\chi) = \sigma_\chi^6 + \sigma_\chi^3 + 1 = \nu_{k_2/k_1}$ (since L is principal, the norm ν_{k_2/L_2} does not intervene in the definition of the $\mathscr{H}^{\rm alg}$).

Similarly, we have $\nu_{k_1/k_0}(\mathscr{H}_{k_1}) = \mathbf{J}_{k_1/k_0} \circ \mathbf{N}_{k_1/k_0}(\mathscr{H}_{k_1}) = \mathbf{J}_{k_1/k_0}(\mathscr{H}_{k_0}) \simeq \mathbb{Z}/3\mathbb{Z}$ (partial capitulation of $\mathscr{H}_{k_0} \simeq \mathbb{Z}/9\mathbb{Z}$); whence:

$$\begin{cases} \mathscr{H}_{\chi_1}^{\rm ar} = \{x \in \mathscr{H}_{k_1},\ \mathbf{N}_{k_1/k_0}(x) = 1\} = 1, \\ \mathscr{H}_{\chi_1}^{\rm alg} = \{x \in \mathscr{H}_{k_1},\ \nu_{k_1/k_0}(x) = 1\} = \mathscr{H}_{k_0}^3 \simeq \mathbb{Z}/3\mathbb{Z}. \end{cases}$$

Thus, the forthcoming formula of Theorem 3.15 giving:

$$\#\mathscr{H}_{k_2} = \#\mathscr{H}_{\chi_0}^{\rm ar} \cdot \#\mathscr{H}_{\chi_1}^{\rm ar} \cdot \#\mathscr{H}_{\chi_2}^{\rm ar}$$

is of the form $\#\mathscr{H}_{k_2} = 9 \times 1 \times 1$, then $\#\mathscr{H}_{k_1} = 9 \times 1$; these formulas are not fulfilled in the algebraic sense, the product being $\#\mathscr{H}_{\chi_0}^{\rm alg} \cdot \#\mathscr{H}_{\chi_1}^{\rm alg} \cdot \#\mathscr{H}_{\chi_2}^{\rm alg} = 9 \times 3 \times 3 = 3^4$.

Now we intend to compute $\#\mathscr{H}_{\chi_1}^{\rm ar} = \#(\mathscr{E}_{k_1}/\mathscr{E}_{k_1}^0 \cdot \mathscr{F}_{k_1})$ (analytic formula of Theorem 7.10); in the general definition, $\mathscr{F}_k$ denotes the Leopoldt group of cyclotomic units of k, $\mathscr{E}_k^0$ the group of units generated by the units of the strict subfields of k.

We give numerical values of the units | e0 | of k_0, | ei | of L_1, | Ej | of k_1, and their logarithms; they are, respectively (standard PARI programs):

```
Units                                                  Logarithms
e0=664.00150602068057486397714386165380336808      6.49828441757729630972016
e1=0.28514248182978536439411987353066274134267     -1.25476628739511494204754
e2=4.50701864409297629866079992371567802 90259      1.50563588039686576534798
E1=0.28514248182978536439411987353066274134267     -1.25476628739511494204754
E2=0.22187616226319093426668005018505061559 91     -1.50563588039686576534798
E3=664.00150602068057486397714386165380336808      6.49828441757729630972016
E4=945628377316488.87204143428389231544006082      34.482870771982558197431847140626595088
E5=0.00257365190752746549299934631279513096 57     -5.96242941301396593243487767278611673020

Cyclotomic units:
{f=19*4409;z=exp(I*Pi/f);g1=lift(Mod(74956,f)^2);g2=lift(Mod(4410,f)^3);frob=1;
for(s=1,6,frob=lift(Mod(3*frob,f));Eta=1;for(k=1,(4409-1)/2,for(j=1,(19-1)/3,
as=lift(Mod(g1^k*g2^j*frob,f));if(as>f/2,next);Eta=Eta*(z^as-z^-as)));
print("Eta^s",s,"=",Eta," ",log(abs(real(Eta)))))}

Eta^s1=945628377316488.87204143428389215664559      34.482870771982558197431847140626595088
Eta^s2=2433718277092.68346630913000250376527 46     28.520441358968592264996969512765259527
Eta^s3=0.00257365190752746549299934631279469 73     -5.962429413013965932434877627861504 3514
Eta^s4=1.05749787547388046520632114968345 73 E-15   -34.482870771982558197431847140626932117
Eta^s5=4.10893902310911119828246133003785 55 E-13   -28.520441358968592264996969512765596690
Eta^s6=388.55293409150677930552045771356632326      5.962429413013965932434877627861167 3020
```

One obtains easily the following relations:

```
E1=e1,  E2=e2^-1,  E3=e0,  E_4^2=Eta^s,  E5^2=Eta^-1,
Eta^{s^2-s+1}=1  giving  Eta^(s^2)=E4^2.E5^2
Eta^{s^3+1}=1
```

Then, one gets $(\mathscr{E}_{k_1} : \mathscr{E}^0_{k_1} \cdot \mathscr{F}_{k_1}) = (\mathscr{E}_{k_1} : \mathscr{E}_{k_0} \cdot \mathscr{E}_{L_1} \cdot \mathscr{F}_{k_1}) = 1$ as expected since $\mathscr{H}^{\rm ar}_{\chi_1} = 1$. Moreover, we see that the conjugates of the cyclotomic units are not independent (see [Was1997, Chap. 8] giving such kind of relations), but, with our point of view, this does not matter since $\mathscr{E}^0_{k_1}$ is of $\mathbb{Z}_3$-rank 3 and $\mathscr{F}_{k_1}$ is of $\mathbb{Z}_3$-rank 2. Indeed, these relations lead to some difficulties in χ-formulas of the literature *only using larger groups of cyclotomic units* like Sinnott's cyclotomic units (see Remark 7.12 for more comments).

The computation of $(\mathscr{E}_{k_2} : \mathscr{E}^0_{k_2} \cdot \mathscr{F}_{k_2})$ is analogous but much longer.

To be complete, we must compute the more classical index of $\mathscr{F}_{k_0} =: \langle \eta_0 \rangle$ in $\mathscr{E}_{k_0}$:

```
{f=4409;z=exp(I*Pi/f);Eta0=1;g=znprimroot(f)^2;for(k=1,(f-1)/2,a=lift(g^k);if(a>f/2,next);
Eta0=Eta0*(z^a-z^-a)/(z^(3*a)-z^-(3*a)));print("Eta0=",Eta0," log(Eta0)=",log(abs(Eta0)))}

Eta0=3.985459685929 E-26     log(Eta0)=-58.484559758195
```

giving immediately $\mathsf{log(Eta0)} = -9 * \mathsf{log(e0)}$ from the above computation of $\mathsf{log(e0)}$; whence the equality $\#\mathscr{H}^{\rm ar}_{\chi_0} = (\mathscr{E}_{k_0} : \mathscr{E}^0_{k_0} \cdot \mathscr{F}_{k_0}) = (\mathscr{E}_{k_0} : \mathscr{F}_{k_0}) = 9$; obviously, the annihilator 9 of $\mathscr{E}_{k_0}/\mathscr{F}_{k_0}$ annihilates $\mathscr{H}^{\rm ar}_{\chi_0}$ (see Conjecture 7.14).

Example 3.14. Consider the same framework, replacing 19 by the prime 1747; one obtains the data showing, as before with $\mathfrak{Q}_0 \mid 2$, a partial capitulation of $\mathscr{H}_{k_0}$ in k_1 (but $\mathscr{H}_{k_1}$ is not cyclic):

```
C0=[9]        [4]~
C1=[9,3,3]    [6,0,0]~
```

One verifies that, in k_1, the ideal $\mathsf{Q_1} = [2, [-1,0,0,1,0,0]^\sim, 1, 3, [0,0,0,1,0,0]^\sim]$, extending that of k_0, is non-principal and such that its class is $\mathsf{h}_1^6\,\mathsf{h}_2^0\,\mathsf{h}_3^0$ on the PARI basis $\{\mathsf{h}_1, \mathsf{h}_2, \mathsf{h}_3\}$:

```
bnfisprincipal(K,[2, [-1,0,0,1,0,0]~,1,3,[0,0,0,1,0,0]~]) = [[6,0,0]~
```

but its 6-power $\mathsf{Q}_1^6 = [64,0,0,21,0,0;0,64,0,0,0,42;0,0,64,0,21,0;0,0,0,1,0,0;0,0,0,0,1,0;0,0,0,0,0,1]$ gives as expected the principality and an integer generator:

```
bnfisprincipal(K,[64,0,0,21,0,0;0,64,0,0,0,42;0,0,64,0,21,0;0,0,0,1,0,0;0,0,0,0,1,0;0,0,0,0,0,1])
=[[0,0,0]~,[821719075630487115396921 3,526028282779527429138218,-687786029075595676594134,
          251301709772155482917577,-210323764029679768881 26,-156093271274307529325 11]~]
```

The kernel of the arithmetic norm is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, thus:

$$\begin{cases} \mathscr{H}^{\rm ar}_{\chi_1} = \{x \in \mathscr{H}_{k_1},\ \mathbf{N}_{k_1/k_0}(x) = 1\} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ \mathscr{H}^{\rm alg}_{\chi_1} = \{x \in \mathscr{H}_{k_1},\ \nu_{k_1/k_0}(x) = 1\} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \end{cases}$$

since the transfer map applies $\mathscr{H}^{\rm ar}_{\chi_0} \simeq \mathbb{Z}/9\mathbb{Z}$ onto $\langle h_1^6 \rangle$.

The formula of Theorem 3.15 is, here, of the form $\#\mathscr{H}_{k_1} = \#\mathscr{H}^{\rm ar}_{\chi_1} \cdot \#\mathscr{H}^{\rm ar}_{\chi_0} = 9 \times 9$, since we have $\mathscr{H}^{\rm ar}_{\chi_0} = \mathscr{H}_{k_0}$ of order 9; of course a same formula with the $\mathscr{H}^{\rm alg}$'s does not exist since $\#\mathscr{H}^{\rm alg}_{\chi_1} \cdot \#\mathscr{H}^{\rm alg}_{\chi_0} = 27 \times 9$.

It would be useful to deepen these properties linking the notion of φ-objects (in both meanings) and capitulation of classes.

3.4. **Arithmetic computation of $\#\mathbf{M}_K$ and $\#\mathscr{M}_K$ for cyclic extensions.** Let $\mathbf{M}$ be an arithmetic $\mathscr{G}$-family where all the $\mathbb{Z}[\mathscr{G}]$-modules $\mathbf{M}_K$, $K \in \mathscr{K}$, are finite; then we can state:

Theorem 3.15. *Let $K/\mathbb{Q}$ be a cyclic extension and assume that for all sub-extension k/k' of $K/\mathbb{Q}$, the maps $\mathbf{N}_{k/k'}$ are surjective. Then one obtains the following formula:*

$$\#\mathbf{M}_K = \prod_{\chi \in \mathscr{X}_K} \#\mathbf{M}^{\rm ar}_\chi,$$

where $\mathbf{M}^{\rm ar}_\chi := \{x \in \mathbf{M}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}$ (Definition 3.12).

Assuming only the cyclicity of the p-Sylow subgroup of G_K, one obtains, for $\mathscr{M}_\chi^{\rm ar} := \mathbf{M}_\chi^{\rm ar} \otimes \mathbb{Z}_p$:

$$\#\mathscr{M}_K = \prod_{\chi \in \mathscr{X}_K} \#\mathscr{M}_\chi^{\rm ar}, \quad \textit{for that prime } p.$$

Proof. One may replace the $\mathbf{M}_k$, $k \subseteq K$, by the finite $\mathbb{Z}_p[G_K]$-modules $\mathscr{M}_k := \mathbf{M}_k \otimes \mathbb{Z}_p$, for all primes dividing $\#\mathbf{M}_K$, using the previous results, then globalizing at the end.

Two classical lemmas are necessary.

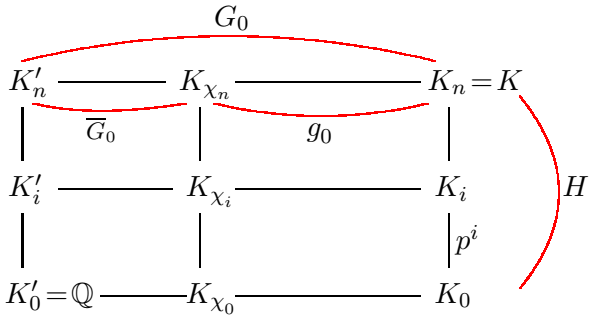
Lemma 3.16. *Assume that p does not divide $[k : k']$. If $\mathbf{N}_{k/k'} : \mathscr{M}_k \to \mathscr{M}_{k'}$ is surjective (resp. if $\mathbf{J}_{k/k'} : \mathscr{M}_{k'} \to \mathscr{M}_k$ is injective), then $\mathbf{J}_{k/k'}$ is injective (resp. $\mathbf{N}_{k/k'}$ is surjective).*

Proof. From Proposition 3.4, we know that $\mathbf{N}_{k/k'} \circ \mathbf{J}_{k/k'} = [k : k']$; whence the proofs since $[k : k']$ is invertible modulo p. □

Put $G_K = G_0 \times H$, where G_0 is a subgroup of prime-to-p order and H (cyclic of order p^n) is the p-Sylow subgroup of G_K. Let K_0 (resp. K'_n) be the field fixed by H (resp. G_0). The set of subfields of K is of the form:

$$\{K_{\chi_i},\ \chi_i \in \mathscr{X}_K,\ 0 \leq i \leq n\},$$

where χ_i is the rational character above $\psi_i := \psi_0\, \psi_{i,p}$, where $\psi_{i,p} \in \Psi_{K'_i}$ is of order p^i and $\psi_0 \in \Psi_{K_0}$; thus K_{χ_i} is the compositum of K_{χ_0} and K'_i. The characters ψ_0 (resp. $\psi_{i,p}$) will also be considered as characters of G_0 (resp. H). This leads to the diagram:



Let $\mathscr{M}^*_{K_{\chi_i}} = \mathrm{Ker}(\mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}})$, for $1 \leq i \leq n$, then put $\mathscr{M}^*_{K_{\chi_0}} := \mathscr{M}_{K_{\chi_0}}$. By assumption, we have the exact sequences of $\mathbb{Z}_p[G_K]$-modules:

$$1 \longrightarrow \mathscr{M}^*_{K_{\chi_i}} \longrightarrow \mathscr{M}_{K_{\chi_i}} \xrightarrow{\mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}}} \mathscr{M}_{K_{\chi_{i-1}}} \longrightarrow 1, \quad 1 \leq i \leq n. \tag{3.2}$$

One considers them as exact sequences of $\mathbb{Z}_p[G_0]$-modules. The idempotents of this algebra are those of $\mathbb{Q}[G_0]$ and are, for all $\chi_0 \in \mathscr{X}_{K_0}$, of the form:

$$e_{\chi_0} = \frac{1}{\#G_0} \sum_{\sigma \in G_0} \chi_0(\sigma^{-1})\, \sigma \in \mathbb{Z}_p[G_0].$$

From Leopoldt [Leo1954], [Leo1962, Chap. V, § 2], as the norm maps are surjective and the transfer maps injective, regarding the sub-extensions k/k' of prime-to-p degrees in $K/\mathbb{Q}$, we get the following canonical identifications:

Lemma 3.17. *Let $\mathscr{M}$ be an arithmetic $\mathscr{G}$-family whose elements $\mathscr{M}_K$ are $\mathbb{Z}_p[G_0 \times H]$-modules in the above sense. Then $\mathscr{M}_{K_i}^{e_{\chi_0}} \simeq \mathscr{M}_{K_{\chi_i}}^{e_{\chi_0}}$ and $(\mathscr{M}^*_{K_i})^{e_{\chi_0}} \simeq (\mathscr{M}^*_{K_{\chi_i}})^{e_{\chi_0}}$.*

Proof. For all i, we identifie $\mathrm{Gal}(K_i/K'_i)$ with G_0 acting by restriction and put $\overline{G}_0 := G_0/g_0$, where $g_0 := \mathrm{Gal}(K_n/K_{\chi_n})$. Thus, by abuse of notation, we identify $\nu_{K_i/K_{\chi_i}}$ with $\nu_{K_n/K_{\chi_n}} =: \nu_{g_0}$; moreover, since the degree of these extensions are prime to p, we may identify $\mathbf{N}_{K_i/K_{\chi_i}}$ with $\mathbf{N}_{K_n/K_{\chi_n}} =: \mathbf{N}_{g_0}$, and $\mathbf{J}_{K_i/K_{\chi_i}}$ with $\mathbf{J}_{K_n/K_{\chi_n}} =: \mathbf{J}_{g_0}$. Thus $\mathbf{N}_{g_0}$ is surjective and $\mathbf{J}_{g_0}$ injective.

One computes that $e_{\chi_0} = \dfrac{\nu_{g_0}}{\#g_0}\, \overline{e}_{\chi_0}$, where $\overline{e}_{\chi_0} := \dfrac{1}{\#\overline{G}_0} \displaystyle\sum_{\overline{\sigma} \in \overline{G}_0} \chi_0(\overline{\sigma}^{-1})\, \sigma \in \mathbb{Z}_p[G_0]$; but we have:

$$\nu_{g_0}(\mathscr{M}_{K_i}) = \mathbf{J}_{g_0} \circ \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathscr{M}_{K_{\chi_i}}; \tag{3.3}$$

whence $\mathscr{M}_{K_i}^{e_{\chi_0}} \simeq \mathscr{M}_{K_{\chi_i}}^{\overline{e}_{\chi_0}}$.

Similarly, we shall obtain $(\mathscr{M}_{K_i}^*)^{e_{\chi_0}} \simeq \mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*)^{\overline{e}_{\chi_0}} \simeq (\mathscr{M}_{K_{\chi_i}}^*)^{\overline{e}_{\chi_0}}$. For this, it suffices to verify that, for all $i \geq 1$, $\mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*) = \mathscr{M}_{K_{\chi_i}}^*$. The inclusion $\mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*) \subseteq \mathscr{M}_{K_{\chi_i}}^*$ being obvious, let $x \in \mathscr{M}_{K_{\chi_i}}^*$; we have $x = \mathbf{N}_{g_0}(y)$, $y \in \mathscr{M}_{K_i}$, and $1 = \mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}} \circ \mathbf{N}_{g_0}(y) = \mathbf{N}_{g_0} \circ \mathbf{N}_{K_i/K_{i-1}}(y)$. Let $z := \mathbf{N}_{K_i/K_{i-1}}(y)$, we have $\mathbf{N}_{g_0}(z) = 1$; applying $\mathbf{J}_{K_{i-1}/K_{\chi_{i-1}}}$, one gets $\nu_{g_0}(z) = 1$; but we have, as for (3.3), $\nu_{g_0}(\mathscr{M}_{K_{i-1}}) \simeq \mathscr{M}_{K_{\chi_{i-1}}}$ (or apply $\mathbf{N} \circ \nu$ in $K_{i-1}/K_{\chi_{i-1}}$ of prime-to-p degree); whence $z = 1$, $y \in \mathscr{M}_{K_i}^*$ and $x \in \mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*)$. □

From [Leo1954, Chap. I, § 1, 2; formula (6), p. 21] or our previous norm computations since $p \nmid \#G_0$, we have the relations (surjectivity of the norms and Lemma 3.16):

$$\mathscr{M}_{K_{\chi_i}}^{\overline{e}_{\chi_0}} = \{x \in \mathscr{M}_{K_{\chi_i}},\ \ \mathbf{N}_{K_{\chi_i}/k}(x) = 1 \text{ for all } k,\ \ K_i' \subseteq k \subsetneqq K_{\chi_i}\},$$

$$\mathscr{M}_{K_{\chi_i}}^{*\,\overline{e}_{\chi_0}} = \{x \in \mathscr{M}_{K_{\chi_i}}^*,\ \ \mathbf{N}_{K_{\chi_i}/k}(x) = 1 \text{ for all } k,\ \ K_i' \subseteq k \subsetneqq K_{\chi_i}\}.$$

From the norm definitions of $(\mathscr{M}_{K_{\chi_i}}^{\mathrm{ar}})_{\chi_0}$ and from $\mathscr{M}_{K_{\chi_i}}^* := \{x \in \mathscr{M}_{K_{\chi_i}},\ \ \mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}}(x) = 1\}$, it follows that $(\mathscr{M}_{K_{\chi_i}}^*)^{\overline{e}_{\chi_0}} = \mathscr{M}_{\chi_i}^{\mathrm{ar}}$, for all $i \geq 1$.

In the finite case, this yields, using the above, the exact sequence (3.2) and $\mathscr{M}_{K_0}^* = \mathscr{M}_{K_0}$:

$$\prod_{i=0}^{n} \#\mathscr{M}_{K_{\chi_i}}^{*\,\overline{e}_{\chi_0}} = \#\mathscr{M}_{K_0}^{*\,\overline{e}_{\chi_0}} \prod_{i=1}^{n} \frac{\#\mathscr{M}_{K_i}^{\overline{e}_{\chi_0}}}{\#\mathscr{M}_{K_{i-1}}^{\overline{e}_{\chi_0}}} = \#\mathscr{M}_K^{\overline{e}_{\chi_0}}, \qquad \prod_{\chi \in \mathscr{X}_K} \#\mathscr{M}_\chi^{\mathrm{ar}} = \prod_{\chi_0} \#\mathscr{M}_K^{\overline{e}_{\chi_0}} = \#\mathscr{M}_K. \tag{3.4}$$

Which ends the proof of the theorem. □

The assumption on the surjectivity of the norms is fulfilled for class groups (resp. p-class groups), as soon as $K/\mathbb{Q}$ (resp. the maximal p-sub-extension of $K/\mathbb{Q}$) is cyclic; the same observation holds for the family $\mathscr{T}$.

4. Semi-simple decomposition of the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_\chi^{\mathrm{alg}}$

Let $\mathscr{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules provided with norms and transfer maps as usual. From $\psi \in \Psi$ given, there exists unique ψ_0, $\psi_p \in \Psi$ such that $\psi = \psi_0\,\psi_p$, ψ_0 of prime-to-p order and ψ_p of p-power order. We restrict the study to $K := K_\chi$ for the rational character χ above ψ, so that, from the previous § 3.4, G_K becomes $G_\chi = G_0 \times H$ of order $g_\chi = g_{\chi_0} \cdot p^n$.

We shall use what we call the "semi-simple idempotents" of $\mathbb{Z}_p[G_\chi]$:

$$e^{\varphi_0} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\,\sigma \in \mathbb{Z}_p[G_0], \qquad e^{\chi_0} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \chi_0(\sigma^{-1})\,\sigma \in \mathbb{Z}_{(p)}[G_0], \tag{4.1}$$

where φ_0 (resp. χ_0) is the p-adic (resp. rational) character over ψ_0.

4.1. **Study of the algebra $\mathscr{A}_\chi := \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$.** This algebra occurs naturally because the $\mathscr{M}_\chi^{\mathrm{alg}}$ are, by definition, $\mathbb{Z}_p[G_\chi]$-modules annihilated by $P_\chi(\sigma_\chi)$, then modules over $\mathscr{A}_\chi$; this algebra is an integral domain if and only if p does not split in $\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}$. We shall see that it is semi-simple even when G_χ is not of prime-to-p order.

Theorem 4.1. *Let $\mathscr{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules. For all $\chi \in \mathscr{X}$ we get the decomposition:*

$$\mathscr{M}_\chi^{\mathrm{alg}} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\mathrm{alg}}.$$

The sub-$\mathscr{A}_\chi$-modules $\mathscr{M}_\varphi^{\mathrm{alg}}$ (Definition 3.6) coincide with the sub-modules $(\mathscr{M}_\chi^{\mathrm{alg}})^{e^{\varphi_0}}$, where the $e^{\varphi_0} \in \mathbb{Z}_p[G_0]$ are the semi-simple idempotents (4.1) associated to φ_0 above the component ψ_0 of prime-to-p order of $\psi \mid \chi$. More generaly, if $\mathscr{M}_\chi'$ is a sub-$\mathscr{A}_\chi$-module of $\mathscr{M}_\chi^{\mathrm{alg}}$, then $\mathscr{M}_\chi' = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi'$, where $\mathscr{M}_\varphi' := (\mathscr{M}_\chi')^{e^{\varphi_0}} = \{x' \in \mathscr{M}_\chi',\ \ P_\varphi \cdot x' = 1\}$. These modules $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi'$ are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules by means of the choice of $\psi \mid \varphi$.

Proof. One may suppose that $g_\chi \equiv 0 \pmod p$, otherwise we are in the semi-simple case and the proof is obvious [Or1975a, Part II].

Let φ_1 and φ_2 be two distinct p-adic characters dividing χ (if $\chi = \varphi$ is p-adic irreducible, the result is trivial). Put $P_{\varphi_1} =: Q_1$, $P_{\varphi_2}(X) =: Q_2$ (cf. § 3.2.2 for the definition of P_φ).

Lemma 4.2. *There exist $U_1, U_2 \in \mathbb{Z}_p[X]$ such that $U_1Q_1 + U_2Q_2 = 1$.*

Proof. Since the distinct polynomials Q_1 and Q_2 are irreducible in $\mathbb{Q}_p[X]$, one may write a Bézout relation in $\mathbb{Z}_p[X]$:

$$U_1Q_1 + U_2Q_2 = p^k, \ \ k \geq 1,$$

choosing U_1 (resp. U_2) of degree less than the degree of Q_2 (resp. Q_1); moreover, since Q_1 and Q_2 are monic, one may suppose that (for instance) the coefficients of U_2 are not all divisible by p, otherwise, necessarily $U_1 \equiv 0 \pmod p$ and one can decrease k.

Let D_χ be the decomposition group of p in $\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}$ and let $\zeta \in \mu_{g_\chi}$ be a root of Q_1 (ζ is of order g_χ and the other roots are the ζ^a for Artin symbols $\sigma_a \in D_\chi$); we then have:

$$U_2(\zeta)\, Q_2(\zeta) = p^k \text{ in } \mathbb{Z}[\mu_{g_\chi}]; \tag{4.2}$$

but $Q_2(X) = \prod_{\sigma_a \in D_\chi}(X - \zeta_1^a)$, where $\zeta_1 =: \zeta^c$, for some $\sigma_c \notin D_\chi$; thus:

$$Q_2(\zeta) = \prod_{\sigma_a \in D_\chi}(\zeta - \zeta_1^a) = \prod_{\sigma_a \in D_\chi}(\zeta - \zeta^{ac}) = \prod_{\sigma_a \in D_\chi}\big[\,\zeta(1 - \zeta^{ac-1})\,\big].$$

Recall that $g_\chi = g_{\chi_0}p^n$, $n \geq 1$, and that g_{χ_0} since χ is not an irreducible p-adic character. Then $1-\zeta^{ac-1}$ is non invertible in $\mathbb{Z}_p[\mu_{g_\chi}]$ if and only if $ac-1 \equiv 0 \pmod{g_{\chi_0}}$, which implies $\sigma_a\sigma_c \in D_\chi$ since $\mathrm{Gal}(\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}(\mu_{g_{\chi_0}})) \subseteq D_\chi$ because of the total ramification of p in the p-extension, but $\sigma_a \in D_\chi$ implies $\sigma_c \in D_\chi$ (absurd). So $Q_2(\zeta)$ is a p-adic unit, whence, from (4.2):

$$U_2(\zeta) \equiv 0 \pmod{p^k}, \ k \geq 1.$$

Denote by $\mathfrak{p}$ the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$ and let $\overline{F}_p := \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}$ be the residue field; for any $P \in \mathbb{Z}_p[X]$, let $\overline{P}$ be its image in $\mathbb{F}_p[X]$ and let $\overline{\zeta}$ be the image of ζ in $\overline{F}_p$. We have:

$$\overline{Q}_1 = (\overline{Q}_0)^e, \tag{4.3}$$

where $e = p^{n-1}(p-1)$ (ramification index of p in $\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}$) and where $\overline{Q}_0$ is irreducible in $\mathbb{F}_p[X]$ (that is to say the irreducible polynomial of $\overline{\zeta}$).

With these notations, any polynomial $P \in \mathbb{Z}_p[X]$ such that $P(\zeta) \equiv 0 \pmod{\mathfrak{p}}$ is such that $\overline{P} \in \overline{Q}_0\,\mathbb{F}_p[X]$; in particular, it is the case of $\overline{U}_2$, so we will have, in $\mathbb{F}_p[X]$ (since $\overline{U}_2 \neq 0$ in $\mathbb{F}_p[X]$ by assumption), $\overline{U}_2 = \overline{A}\,(\overline{Q}_0)^\alpha$, $\alpha \geq 1$, $\overline{A} \neq 0$, $\overline{Q}_0 \nmid \overline{A}$. We may assume that A, $Q_0 \in \mathbb{Z}_p[X]$ have same degrees as their images in $\mathbb{F}_p[X]$. This yields:

$$U_2 = A\,Q_0^\alpha + pB,\ B \in \mathbb{Z}_p[X],$$

thus $U_2(\zeta) = A(\zeta)\,Q_0^\alpha(\zeta) + p\,B(\zeta) \equiv 0 \pmod{p^k}$, whence $A(\zeta)\,Q_0^\alpha(\zeta) \equiv 0 \pmod p$. But $A(\zeta)$ is a p-adic unit (since $\overline{Q}_0 \nmid \overline{A}$), which gives:

$$Q_0^\alpha(\zeta) \equiv 0 \pmod p. \tag{4.4}$$

Let's show that $\alpha \geq e$; the unique case where, possibly, $p \mid g_\chi$ and $e = 1$ is the case $p = 2$, $n = 1$; this case trivially gives $\alpha \geq e$. Consider the g_{χ_0}th cyclotomic polynomial. Assuming $e > 1$, we have $P_{g_{\chi_0}}(\zeta) = \prod_{a \in (\mathbb{Z}/g_{\chi_0}\mathbb{Z})^*}(\zeta - \zeta^{p^n a}) = \prod_a[\,\zeta(1 - \zeta^{p^n a - 1})\,]$; but $\zeta^{p^n a-1}$ is of p-power order if and only if $p^n a \equiv 1 \pmod{g_{\chi_0}}$; taking into account the domain of a, this defines a unique value a_0 such that $p^n a_0 \equiv 1 \pmod{g_{\chi_0}}$, whence $p^n a_0 \not\equiv 1 \pmod{pg_{\chi_0}}$ and $1 - \zeta^{p^n a_0 - 1} \in \mathfrak{p} \setminus \mathfrak{p}^2$, thus the fact that $P_{g_{\chi_0}}(\zeta) \in \mathfrak{p} \setminus \mathfrak{p}^2$; it follows, from $P_{g_{\chi_0}} = C\,Q_0^\beta + pD$, $\beta \geq 1$, $C, D \in \mathbb{Z}_p[X]$, $C(\zeta) \not\equiv 0 \pmod{\mathfrak{p}}$, that $P_{g_{\chi_0}}(\zeta) \equiv C(\zeta)\,Q_0^\beta(\zeta) \pmod{\mathfrak{p}^e}$, thus $Q_0^\beta(\zeta) \in \mathfrak{p} \setminus \mathfrak{p}^2$ since $e > 1$. This implies $\beta = 1$ and $Q_0(\zeta) \in \mathfrak{p} \setminus \mathfrak{p}^2$.

The congruence (4.4), written $Q_0^{\alpha}(\zeta) \equiv 0 \pmod{\mathfrak{p}^e}$, implies $\alpha \geq e$ and $U_2 = A'\,Q_0^e + p\,B$, where $A' := A\,Q_0^{\alpha-e}$; but we also have from (4.3):

$$Q_1 = Q_0^e + p\,T,\ T \in \mathbb{Z}_p[X],$$

hence:

$$U_2 = A'\,(Q_1 - p\,T) + p\,B = A'\,Q_1 + p\,S,\ S \in \mathbb{Z}_p[X].$$

Since $A \neq 0$ by assumption, since $A' \neq 0$ is monic, U_2 is of degree larger or equal to that of Q_1 (absurd). In conclusion, $\overline{U}_2 = 0$, contrary to the assumption $k \geq 1$ in (4.2). □

Give now some properties of the system of idempotents of $\mathscr{A}_\chi = \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$.

Let $\{\varphi_1, \ldots, \varphi_{g_p}\}$ be the set of distinct p-adic characters dividing χ (thus, $g_p \mid \phi(g_{\chi_0})$ is the number of prime ideals dividing p in $\mathbb{Q}(\mu_{g_{\chi_0}})/\mathbb{Q}$, so that, only the case $g_p = 1$ is trivial for the Main Conjecture); from the property of co-maximality, given by Lemma 4.2, one may write:

$$\mathbb{Z}_p[X]/P_\chi(X) = \mathbb{Z}_p[X]\Big/\Big(\prod_{u=1}^{g_p} Q_u(X)\Big) \simeq \prod_{u=1}^{g_p} \mathbb{Z}_p[X]/\big(Q_u(X)\big) \simeq (\mathbb{Z}_p[G_\chi])^{g_p}. \tag{4.5}$$

There exist elements $e_{\varphi_u}(X) \in \mathbb{Z}_p[X]$, whose images modulo $P_\chi(X)$ constitute an exact system of orthogonal idempotents of $\mathbb{Z}_p[X]/(P_\chi(X))$. Whence a classical system of orthogonal idempotents of $\mathbb{Z}_p[G_\chi]$ given by the $e_{\varphi_u}(\sigma_\chi)$.

Since $(\mathscr{M}_\chi^{\rm alg})^{P_\chi(\sigma_\chi)} = 1$, we obtain (in the algebraic meaning):

$$\mathscr{M}_\chi^{\rm alg} = \bigoplus_{u=1}^{g_p} (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_u}(\sigma_\chi)}. \tag{4.6}$$

It remains to verify that:

$$(\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_u}(\sigma_\chi)} = \mathscr{M}_{\varphi_u}^{\rm alg} = \{x \in \mathscr{M}_\chi^{\rm alg},\ P_{\varphi_u}(\sigma_\chi)\cdot x = 1\}.$$

If $x \in (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_u}(\sigma_\chi)}$, $x = y^{e_{\varphi_u}(\sigma_\chi)}$, $y \in \mathscr{M}_\chi^{\rm alg}$ and $x^{P_{\varphi_u}(\sigma_\chi)} = y^{e_{\varphi_u}(\sigma_\chi)P_{\varphi_u}(\sigma_\chi)}$; but we have $e_{\varphi_u}(\sigma_\chi)\,P_{\varphi_u}(\sigma_\chi)) \equiv 0 \pmod{P_\chi(\sigma_\chi)}$, whence $y^{e_{\varphi_u}(\sigma_\chi)\,P_{\varphi_u}(\sigma_\chi)} = 1$ since $y \in \mathscr{M}_\chi^{\rm alg}$, and $x \in \mathscr{M}_{\varphi_u}^{\rm alg}$. If $x \in \mathscr{M}_{\varphi_u}^{\rm alg}$, then $x^{P_{\varphi_u}(\sigma_\chi)} = 1$; writing $x = \prod_{j=1}^{g_p} x^{e_{\varphi_v}(\sigma_\chi)}$, we get $e_{\varphi_v}(\sigma_\chi) \equiv \delta_{u,v} \pmod{P_{\varphi_u}(\sigma_\chi)}$, thus $e_{\varphi_v}(\sigma_\chi) \equiv 0 \pmod{P_{\varphi_u}(\sigma_\chi)}$ for $v \neq u$ and $x^{e_{\varphi_v}(\sigma_\chi)} = 1$, for $v \neq u$. Whence $x = x^{e_{\varphi_u}(\sigma_\chi)}$.

In the algebra $\mathscr{A}_\chi = \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$, we obtain two systems of idempotents, that is to say, the images in $\mathscr{A}_\chi$ of the $e_{\varphi_{u,0}}$, where $\varphi_{u,0}$ is above the component $\psi_{u,0}$, of prime-to-p order, of ψ_u, and that of the $e_{\varphi_u}(\sigma_\chi)$ corresponding to φ_u. Fixing the character $\varphi_u =: \varphi$ above $\psi =: \psi_0\,\psi_p$ and its non p-part φ_0 above ψ_0, we consider both:

$$e^{\varphi} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\,\sigma \tag{4.7}$$

and $e_\varphi(\sigma_\chi)$ defined as follows by means of polynomial relations in $\mathbb{Z}[X]$ deduced from (4.5):

$$e_\varphi(\sigma_\chi) = \Lambda_\varphi(\sigma_\chi)\cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(\sigma_\chi), \text{ such that } \Lambda_\varphi(X)\cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(X) \equiv 1 \pmod{P_\varphi(X)}; \tag{4.8}$$

we denote $e_\varphi(\sigma_\chi)$ simply by e_φ, which is legitimate by Lemma 3.7.

To verify that $(\mathscr{M}_\chi^{\rm alg})^{e^\varphi} = (\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$, it suffices to show that e^φ and e_φ correspond to the same simple factor of the algebra $\mathscr{A}_\chi$. For this, we remark that the homomorphism defined, for the fixed character φ, by $\sigma_\chi \mapsto \psi(\sigma_\chi)$, $\psi \mid \varphi$, induces a surjective homomorphism $\mathscr{A}_\chi \longrightarrow \mathbb{Z}_p[\mu_{g_\chi}]$ whose kernel is equal to $\bigoplus_{\varphi' \neq \varphi} \mathscr{A}_\chi e_{\varphi'}$.

Thus, to show that $\mathscr{A}_\chi e^\varphi = \mathscr{A}_\chi e_\varphi$, it suffices to show that $\psi(e^\varphi) \neq 0$; but, from (4.7), e^φ is a sum of the idempotents $e_{\psi_0'} = \frac{1}{g_{\chi_0}} \sum_{\sigma_0 \in G_0} \psi_0'(\sigma_0)\sigma_0^{-1}$, where $\psi_0' \mid \varphi_0$. It follows, since $\psi = \psi_0\,\psi_p$, that $\psi(\sigma_0) = \psi_0(\sigma_0)$ and then:

$$\psi(e_{\psi_0'}) = \frac{1}{g_{\chi_0}} \sum_{\sigma_0 \in G_0} \psi_0'(\sigma_0)\psi(\sigma_0)^{-1} = \frac{1}{g_{\chi_0}} \sum_{\sigma_0 \in G_0} \psi_0'(\sigma_0)\psi_0(\sigma_0)^{-1},$$

which is zero for all ψ_0' except $\psi_0'=\psi_0$ where $\psi(e_{\psi_0})=1$. Whence $\psi(e^{\varphi})\neq 0$.

Let $\mathscr{M}_\chi^{\rm alg}$ as $\mathscr{A}_\chi$-module; on may write (from (4.6)):

$$\mathscr{M}_\chi^{\rm alg}=\bigoplus_{\varphi\vert\chi}(\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$$

and we know that $(\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$ coincides with the sub-module $(\mathscr{M}_\chi^{\rm alg})^{e^\varphi}=\mathscr{M}_\varphi^{\rm alg}$ (Definition (4.7)); then, due to the properties of the e_φ (defined by (4.8)):

$$(\mathscr{M}_\chi^{\rm alg})^{e_\varphi}=\{x\in\mathscr{M}_\chi^{\rm alg},\ \ P_\varphi(\sigma_\chi)\cdot x=1\}=\mathscr{M}_\varphi^{\rm alg}.$$

We shall denote by e_φ any of these two semi-simple p-adic idempotents e^φ or e_φ.

If $\mathscr{M}_\chi'$ is a sub-$\mathscr{A}_\chi$-module of $\mathscr{M}_\chi^{\rm alg}$, then $\mathscr{M}_\varphi':=(\mathscr{M}_\chi')^{e_\varphi}=\{x'\in\mathscr{M}_\chi',\ P_\varphi(\sigma_\chi)\cdot x'=1\}$. Since $\mathscr{A}_\chi\, e_\varphi\simeq\mathbb{Z}_p[\mu_{g_\chi}]$, $\mathscr{M}_\varphi^{\rm alg}$ and $\mathscr{M}_\varphi'$ are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

This finishes the proof of Theorem 4.1. □

4.2. **Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\rm ar}$.** From Definition 3.12, one has:

$$\mathscr{M}_\chi^{\rm ar}:=\{x\in\mathscr{M}_{K_\chi},\ \ \mathbf{N}_{K_\chi/k}(x)=1,\ \text{for all } k\subsetneq K_\chi\}.$$

This invites to give the following arithmetic definitions, especially for numerical experiments and to avoid intricate computations, with idempotents, to get $(\mathscr{M}_\chi^{\rm ar})^{e_\varphi}$:

Definition 4.3. *Let $\mathscr{M}$ be an arithmetic family of $\mathbb{Z}_p[\mathscr{G}]$-modules. For any $\varphi\mid\chi$, $\chi\in\mathscr{X}$, we define an arithmetic $\mathbb{Z}_p[\mu_{g_\chi}]$-module of φ-object by putting:*

$$\mathscr{M}_\varphi^{\rm ar}:=\mathscr{M}_\varphi^{\rm alg}\cap\mathscr{M}_\chi^{\rm ar}=\{x\in\mathscr{M}_\varphi^{\rm alg},\ \ \mathbf{N}_{K_\chi/k}(x)=1,\ \textit{for all } k\subsetneq K_\chi\}=(\mathscr{M}_\chi^{\rm ar})^{e_\varphi},$$

where e_φ is defined by (4.7) or (4.8); $\mathscr{M}_\varphi^{\rm ar}$ is a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_\varphi^{\rm alg}$.

So, we have the arithmetic version of Theorem 4.1:

Theorem 4.4. *Let $\mathscr{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules. Then we get the decomposition:*

$$\mathscr{M}_\chi^{\rm ar}=\bigoplus_{\varphi\vert\chi}\mathscr{M}_\varphi^{\rm ar},\ \ \textit{for all } \chi\in\mathscr{X}.$$

To summarize the results that we have obtained, we can state (from Theorems 3.15, 4.1, 4.4, using Definitions 3.6, 3.12, 4.3):

4.3. **Summary of the main results.** Let $\mathscr{M}$ be an arithmetic family of $\mathbb{Z}_p[\mathscr{G}]$-modules with the norm and transfer maps $\mathbf{N}_{k/k'}$ and $\mathbf{J}_{k/k'}$ for any $k',k\in\mathscr{K}$, $k'\subseteq k$. Let χ be an irreducible rational character and let φ be an irreducible p-adic character dividing χ.

(i) Let σ_χ be a generator of $G_\chi:=G_{K_\chi}$ and let $g_\chi:=\#G_\chi$; put:

$\mathscr{M}_\chi^{\rm alg}:=\big\{x\in\mathscr{M}_{K_\chi},\ \ P_\chi(\sigma_\chi)\cdot x=1\big\}$, where P_χ is the g_χth global cyclotomic polynomial,

$\mathscr{M}_\varphi^{\rm alg}:=\big\{x\in\mathscr{M}_{K_\chi},\ \ P_\varphi(\sigma_\chi)\cdot x=1\big\}$, where $P_\varphi\mid P_\chi$ is the local φ-cyclotomic polynomial,

$\mathscr{M}_\chi^{\rm ar}:=\{x\in\mathscr{M}_\chi^{\rm alg},\ \ \mathbf{N}_{K_\chi/k}(x)=1,\ \text{for all } k\subsetneq K_\chi\}$,

$\mathscr{M}_\varphi^{\rm ar}:=\big\{x\in\mathscr{M}_\varphi^{\rm alg},\ \ \mathbf{N}_{K_\chi/k}(x)=1,\ \text{for all } k\subsetneq K_\chi\big\}=\mathscr{M}_\chi^{\rm ar}\cap\mathscr{M}_\varphi^{\rm alg}$.

Then we have:

$$\mathscr{M}_\chi^{\rm alg}=\bigoplus_{\varphi\vert\chi}\mathscr{M}_\varphi^{\rm alg}\quad\&\quad\mathscr{M}_\chi^{\rm ar}=\bigoplus_{\varphi\vert\chi}\mathscr{M}_\varphi^{\rm ar}.$$

(ii) Assume that the maximal p-sub-extension K/K_0, of $K/\mathbb{Q}$, is cyclic and such that for all sub-extensions k/k' of K/K_0, the norms $\mathbf{N}_{k/k'}$ are surjective. Then, if $\mathscr{M}_K$ is finite:

$$\#\mathscr{M}_K=\prod_{\chi\in\mathscr{X}_K}\#\mathscr{M}_\chi^{\rm ar}=\prod_{\varphi\in\Phi_K}\#\mathscr{M}_\varphi^{\rm ar}.$$

5. Application to relative class groups of abelian extensions

5.1. **Arithmetic definition of relative class groups.** The class groups of the number fields $K \in \mathscr{K}$ lead to the algebraic and arithmetic $\mathscr{G}$-families to which we will apply the previous results using first odd characters χ giving $\mathbf{H}_\chi^{\rm alg}$ and $\mathbf{H}_\chi^{\rm ar}$, respectively. The case of even characters requires some deepening of Leopoldt's results [Leo1954]; it will be considered in the next section.

For $K \in \mathscr{K}$, we denote by $\mathbf{H}_K$ the class group of K in the ordinary sense. If K is imaginary, with maximal real subfield K^+, we define the relative class group of K:

$$(\mathbf{H}_K^{\rm ar})^- := \{h \in \mathbf{H}_K,\ \ \mathbf{N}_{K/K^+}(h) = 1\} \tag{5.1}$$

(the notation $\mathbf{H}^{\rm ar}$ recalls that the definition of the minus part uses the arithmetic norm and not the algebraic one $\nu_{K/K^+} = 1 + s$, s being the complex conjugation).

It is classical to put $\mathbf{H}_K^+ := \mathbf{H}_{K^+}$; since K/K^+ is ramified for the real infinite places of K^+, class field theory implies that $\mathbf{N}_{K/K^+}$ is surjective for class groups in the ordinary sense, giving the exact sequence $1 \to (\mathbf{H}_K^{\rm ar})^- \longrightarrow \mathbf{H}_K \xrightarrow{\mathbf{N}_{K/K^+}} \mathbf{H}_{K^+} = \mathbf{H}_K^+ \to 1$ and the formula:

$$\#\mathbf{H}_K = \#(\mathbf{H}_K^{\rm ar})^- \cdot \#\mathbf{H}_K^+. \tag{5.2}$$

For the prime p fixed, we denote by $\mathscr{H}_K$ (resp. $(\mathscr{H}_K^{\rm ar})^-$, $\mathscr{H}_K^+ := \mathscr{H}_{K^+}$), the p-Sylow subgroup of $\mathbf{H}_K$ (resp. $(\mathbf{H}_K^{\rm ar})^-$, $\mathbf{H}_K^+$). For the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{H}_K$, we introduce the $\mathscr{A}_\chi$-modules $\mathscr{H}_\chi^{\rm alg}$ and $\mathscr{H}_\chi^{\rm ar}$ for $\chi \in \mathscr{X}$, and the φ-components (Definitions 3.6, 3.12, 4.3) which are $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

5.2. **Proof of the equality $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$, for all $\chi \in \mathscr{X}^-$.** To prove this equality, and the equalities $\mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg}$, $\varphi \mid \chi$, it is sufficient to consider, for any $p \geq 2$, the p-Sylow subgroups $\mathscr{H}_{K_\chi}$, and the χ-components $\mathscr{H}_\chi^{\rm alg}$, $\mathscr{H}_\chi^{\rm ar}$, for $\chi \in \mathscr{X}^-$.

Lemma 5.1. *Assume that $\mathscr{H}_\chi^{\rm ar} \subsetneq \mathscr{H}_\chi^{\rm alg}$. Then there exists a unique sub-extension $K_{\chi'}$ of K_χ, such that $[K_\chi : K_{\chi'}] = p$ (i.e., if $\psi \mid \chi$ then χ' is above $\psi' = \psi^p$), and a class $h \in \mathscr{H}_\chi^{\rm alg}$ such that $h' := \mathbf{N}_{K_\chi/K_{\chi'}}(h)$ fulfills the following properties, :*

(i) For all prime $\ell \neq p$ dividing g_χ, $\nu_{K_{\chi'}/k'_\ell}(h') = 1$, where k'_ℓ is the unique sub-extension of $K_{\chi'}$ such that $[K_{\chi'} : k'_\ell] = \ell$ (empty condition if g_χ is a p-power);

(ii) $\mathbf{J}_{K_\chi/K_{\chi'}}(h') = 1$;

(iii) h' is of order p in $\mathscr{H}_{K_{\chi'}}$.

Proof. Indeed, if $[K_\chi : \mathbb{Q}]$ is prime to p, we are in the semi-simple case (for the algebra $\mathbb{Z}_p[G_\chi]$) and $\mathscr{H}_\chi^{\rm alg} = \mathscr{H}_\chi^{\rm ar}$ since in that case the maps $\mathbf{N}$ are surjective and the maps $\mathbf{J}$ are injective. So we assume that $p \mid [K_\chi : \mathbb{Q}]$, whence the existence and unicity of $K_{\chi'}$.

Let $h \in \mathscr{H}_\chi^{\rm alg}$, $h \notin \mathscr{H}_\chi^{\rm ar}$, and let $h' := \mathbf{N}_{K_\chi/K_{\chi'}}(h)$. Let $\ell \mid g_\chi$, $\ell \neq p$.

(i) We have the following diagram where k_ℓ is the unique sub-extension of K_χ such that $[K_\chi : k_\ell] = \ell$ and then $k'_\ell = k_\ell \cap K_{\chi'}$:

$$\begin{array}{ccc} k_\ell & \overset{\ell}{\text{———}} & K_\chi \quad h \\ \Big| p & & \Big| p \\ k'_\ell & \overset{\ell}{\text{———}} & K_{\chi'} \quad h' := \mathbf{N}_{K_\chi/K_{\chi'}}(h) \end{array}$$

We have $\nu_{K_\chi/k_\ell}(h) = 1$ since $h \in \mathscr{H}_\chi^{\rm alg}$; applying $\mathbf{N}_{K_\chi/K_{\chi'}}$, we get $\nu_{K_{\chi'}/k'_\ell}(h') = 1$.

(ii) We have $\mathbf{J}_{K_\chi/K_{\chi'}}(h') = \mathbf{J}_{K_\chi/K_{\chi'}} \circ \mathbf{N}_{K_\chi/K_{\chi'}}(h) = \nu_{K_\chi/K_{\chi'}}(h) = 1$ since $h \in \mathscr{H}_\chi^{\rm alg}$.

(iii) Since the class h' capitulates in K_χ, its order is 1 or p. Suppose that $h' = 1$; for $\ell \neq p$, the maps $\mathbf{J}_{K_\chi/k_\ell}$ and $\mathbf{J}_{K_{\chi'}/k'_\ell}$ are injective, so $\mathbf{N}_{K_\chi/k_\ell}(h) = \mathbf{N}_{K_{\chi'}/k'_\ell}(h') = 1$, for all $\ell \neq p$ dividing g_χ; since moreover $h' = \mathbf{N}_{K_\chi/K_{\chi'}}(h) = 1$, this yields by definition $h \in \mathscr{H}_\chi^{\rm ar}$ (absurd). □

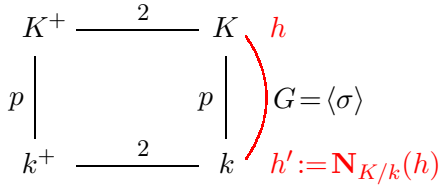
Lemma 5.2. *Let K/k be a cyclic extension of degree p and Galois group $G =: \langle\sigma\rangle$. Let $\mathbf{E}_k$ and $\mathbf{E}_K$ be the unit groups of k and K, respectively. Consider the transfer map $\mathbf{J}_{K/k} : \mathscr{H}_k \to \mathscr{H}_K$; then $\mathrm{Ker}(\mathbf{J}_{K/k})$ is isomorphic to a subgroup of $\mathrm{H}^1(G, \mathbf{E}_K) \simeq \mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ (where $\mathbf{E}_K^* = \mathrm{Ker}(\nu_{K/k})$). The group $\mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ is of exponent 1 or p.*

Proof. Let $\mathbf{Z}_k$ and $\mathbf{Z}_K$ be the rings of integers of k and K, respectively; let $\mathscr{A}_k(\mathfrak{a}) \in \mathscr{H}_k$, with $\mathfrak{a}\mathbf{Z}_K =: (\alpha)\mathbf{Z}_K$, $\alpha \in K^\times$. We then have $\alpha^{1-\sigma} =: \varepsilon \in \mathbf{E}_K^*$. The map, which associates with $\mathscr{A}_k(\mathfrak{a}) \in \mathrm{Ker}(\mathbf{J}_{K/k})$ the class of ε modulo $\mathbf{E}_K^{1-\sigma}$, is obviously injective.

If $\varepsilon \in \mathbf{E}_K^*$, then $1 = \varepsilon^{1+\sigma+\cdots+\sigma^{p-1}} = \varepsilon^{p+(\sigma-1)\Omega}$, $\Omega \in \mathbb{Z}[G]$; whence $\varepsilon^p \in \mathbf{E}_K^{1-\sigma}$. □

5.2.1. *Study of the case $p \neq 2$.* We are in the context of Lemma 5.1. Put $K := K_\chi$ and $k := K_{\chi'}$; then K/k is of degree p and the class $h' = \mathbf{N}_{K/k}(h) \in \mathscr{H}_k$ is of order p and capitulates in K. Assume that K is imaginary (i.e., χ is odd, thus $h \in (\mathscr{H}_K^{\mathrm{ar}})^-$); if K/k is of degree $p \neq 2$, then k is also imaginary and $h' \in (\mathscr{H}_k^{\mathrm{ar}})^-$.

We introduce the maximal real subfields, giving the diagram:



Lemma 5.3. *Let μ_K^* be the p-torsion sub-group of $\mathbf{E}_K^*$, that is to say the set of p-roots of unity ζ of K such that $\mathbf{N}_{K/k}(\zeta) = 1$. Then the image of $(\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, by the map $\mathrm{Ker}(\mathbf{J}_{K/k}) \to \mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ of Lemma 5.2, is contained in the image of μ_K^* modulo $\mathbf{E}_K^{1-\sigma}$.*

Proof. Let q be the map $\mathbf{E}_K^* \to \mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$. Denote by $x \mapsto \overline{x}$ the complex conjugation in K. If $h' \in (\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, then $\mathbf{N}_{k/k^+}(h') = 1$ and $\nu_{k/k^+}(h') = h'\overline{h'} = 1$; if $h' = \mathscr{A}_k(\mathfrak{a})$ we then have $\mathfrak{a}\overline{\mathfrak{a}} = a\mathbf{Z}_k$, $a \in k^\times$, and $\mathfrak{a}\mathbf{Z}_K\overline{\mathfrak{a}}\mathbf{Z}_K = a\mathbf{Z}_K$, with $\mathfrak{a}\mathbf{Z}_K = (\alpha)\mathbf{Z}_K$ and $\overline{\mathfrak{a}}\mathbf{Z}_K = (\overline{\alpha})\mathbf{Z}_K$, $\alpha \in K^\times$ (since $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ become principal in K), which yields relations of the form $\alpha^{1-\sigma} = \varepsilon$, $\overline{\alpha}^{1-\sigma} = \overline{\varepsilon}$, $\varepsilon, \overline{\varepsilon} \in \mathbf{E}_K^*$. From the relation $\mathfrak{a}\overline{\mathfrak{a}} = a\mathbf{Z}_k$, one obtains, in K, $\alpha\overline{\alpha} = \eta a$, $\eta \in \mathbf{E}_K$, then $\alpha^{1-\sigma}\overline{\alpha}^{1-\sigma} = \eta^{1-\sigma}$, giving $\varepsilon\overline{\varepsilon} = \eta^{1-\sigma}$.

From [Has1952, Satz 24], $\varepsilon = \varepsilon^+\zeta$, $\varepsilon^+ \in \mathbf{E}_{K^+}$, $\zeta \in \mu_K$. So $q(\varepsilon\overline{\varepsilon}) = q(\varepsilon^{+2}) = 1$. Since p is odd and $\mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ of exponent divisor of p, $\varepsilon^+ \in \mathbf{E}_K^{1-\sigma}$; since $\varepsilon \in \mathbf{E}_K^*$, we have $\zeta \in \mathbf{E}_K^*$, whence $q(\varepsilon) = q(\zeta) \in q(\mu_K^*) = \mu_K^*/(\mathbf{E}_K^{1-\sigma} \cap \mu_K^*)$. □

Lemma 5.4. *The group $q(\mu_K^*)$ (of order 1 or p) is of order p if and only if $\mu_K^* = \langle\zeta_1\rangle$ and $\mathbf{E}_K^{1-\sigma} \cap \langle\zeta_1\rangle = 1$, where ζ_1 is of order p.*

Proof. A direction being obvious, assume that $q(\mu_K^*) = \mu_K^*/(\mathbf{E}_K^{1-\sigma} \cap \mu_K^*)$ is of order p and let ζ be a generator of μ_K^* (necessarily, $\zeta \neq 1$). If $\zeta \in k$, then $\mathbf{N}_{K/k}(\zeta) = \zeta^p$, so $\zeta^p = 1$ and $\zeta = \zeta_1 \in k$.

If $\zeta \notin k$, $K = k(\zeta)$; it follows that $\zeta_1 \in k$ and $\zeta^p \in k$ (since $[K : k] = [\mathbb{Q}(\zeta) : k \cap \mathbb{Q}(\zeta)] = p$), thus K/k is a Kummer extension of the form $K = k(\sqrt[p]{\zeta_r})$, ζ_r of order p^r, $r \geq 1$, $\zeta = \zeta_{r+1}$, and $\zeta^{1-\sigma} = \zeta_1$, giving $\mathbf{N}_{K/k}(\zeta) = \zeta^p = 1$, hence $\zeta = \zeta_1 \in k$ (absurd). So we have $\zeta = \zeta_1 \in k$ and $\mathbf{E}_K^{1-\sigma} \cap \mu_K^* \subseteq \langle\zeta_1\rangle$. Thus, $q(\mu_K^*)$ being of order p, necessarily $\mathbf{E}_K^{1-\sigma} \cap \mu_K^* = 1$. □

Lemma 5.5. *If $(\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) \neq 1$, this group is of order p and K/k is a Kummer extension of the form $K = k(\sqrt[p]{a})$, $a \in k^\times$, $a\mathbf{Z}_k = \mathfrak{a}^p$, the ideal $\mathfrak{a}$ of k being non-principal (such a Kummer extension is said "of class type").*

Proof. If $h' \in (\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, $h' := \mathscr{A}_k(\mathfrak{a}) \neq 1$, this means that $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$, $\alpha \in K^\times$; so $\alpha^{1-\sigma} = \varepsilon$, $\varepsilon \in \mathbf{E}_K^*$; from Lemma 5.4, $q(\varepsilon) = q(\zeta_1)^\lambda$, hence $\varepsilon = \zeta_1^\lambda\eta^{1-\sigma}$, $\eta \in \mathbf{E}_K$, whence $\alpha^{1-\sigma} = \zeta_1^\lambda\eta^{1-\sigma}$ and in the equality $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$ one may suppose α chosen modulo $\mathbf{E}_K$ such that $\alpha^{1-\sigma} = \zeta_1^\lambda$; moreover we have $\lambda \not\equiv 0 \pmod p$, otherwise α should be in k and $\mathfrak{a}$ should be principal. Thus $\alpha^{1-\sigma} = \zeta_1'$ of order p, and $\alpha^p = a \in k^\times$, whence $K = k(\alpha)$ is the Kummer extension $k(\sqrt[p]{a})$; we have $a\mathbf{Z}_K = \mathfrak{a}^p\mathbf{Z}_K$, hence $a\mathbf{Z}_k = \mathfrak{a}^p$, since extension of ideals is injective. □

We shall show now that the context of Lemma 5.5 is not possible for a cyclic extension $K/\mathbb{Q}$, which will apply to $K_\chi/\mathbb{Q}$.

Since $K = k(\sqrt[p]{a})$, with $a\mathbf{Z}_k = \mathfrak{a}^p$, only the prime ideals dividing p can ramify in K/k.

Consider the following decomposition of the extension $K/\mathbb{Q}$ for $p \neq 2$, with K/K_0 and $K'/\mathbb{Q}$ cyclic of p-power degree p^n, K/K' and $K_0/\mathbb{Q}$ of prime-to-p degree:

$$\begin{array}{ccc} K' & \text{———} & K = k(\sqrt[p]{a}) \\ | & & | \, p \\ k' & \text{———} & k \\ | & & | \, p^{n-1} \\ \mathbb{Q} & \text{———} & K_0 \end{array}$$

Let ℓ be a prime number totally ramified in $K'/\mathbb{Q}$ (such a prime does exist since $G_{K'} \simeq \mathbb{Z}/p^n\mathbb{Z}$); this prime is then totally ramified in K/K_0, hence in K/k; this implies $\ell = p$ and p is the unique ramified prime in $K'/\mathbb{Q}$.

This identifies the extension $K'/\mathbb{Q}$; its conductor is p^{n+1}, $n \geq 1$, since $p \neq 2$, and K' is the unique sub-extension of degree p^n of $\mathbb{Q}(\mu_{p^{n+1}})$ and k' the unique sub-extension of degree p^{n-1} of $\mathbb{Q}(\mu_{p^n})$ (in other words, K' is contained in the cyclotomic $\mathbb{Z}_p$-extension); as $\zeta_1 \in k$, one has $\mu_{p^n} \subset k$, $\mu_{p^{n+1}} \subset K$ and $\mu_{p^{n+1}} \not\subset k$, so $K = k(\zeta) = k(\sqrt[p]{\zeta^p})$, ζ of order p^{n+1}.

It suffices to apply Kummer theory which shows that $k(\sqrt[p]{a}) = k(\sqrt[p]{\zeta^p})$ implies $a = \zeta^{\lambda p} b^p$, with $p \nmid \lambda$ and $b \in k^\times$; so $a\mathbf{Z}_k = b^p\mathbf{Z}_k = \mathfrak{a}^p$, whence $\mathfrak{a} = b\mathbf{Z}_k$ principal (absurd).

So in the case $p \neq 2$, for $K/\mathbb{Q}$ imaginary cyclic, and K/k cyclic of degree p, we have the relation $(\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) = 1$ (injectivity of $\mathbf{J}_{K/k}$ on the relative p-class group).

5.2.2. *Case $p = 2$.* The extension $K/\mathbb{Q}$ is still imaginary cyclic and in that case k is necessarily equal to K^+ and σ is the complex conjugation s.

From [Has1952, Satz 24] the "index of units" Q_K^- is trivial in the cyclic case; thus for all $\varepsilon \in \mathbf{E}_K^*$, $\varepsilon = \varepsilon^+\zeta$, $\varepsilon^+ \in k$, ζ root of unity of 2-power order; then $\mathbf{N}_{K/k}(\varepsilon) = 1$ yields $\varepsilon^{+2} = 1$, thus $\varepsilon^+ = \pm 1$ and $\varepsilon = \zeta' = \pm\zeta$; since $K/\mathbb{Q}$ is cyclic (whence $\mathbb{Q}(\zeta)/\mathbb{Q}$ cyclic), we shall have $\varepsilon \in \{1, -1, i, -i\}$.

Recall that $h' = \mathbf{N}_{K/k}(h) \in \mathrm{Ker}(\mathbf{J}_{K/k})$, $h' = \mathscr{C}\ell_k(\mathfrak{a}) \neq 1$, with $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$ and $\alpha^{1-\sigma} = \varepsilon \in \mathbf{E}_K^*$. One may assume $\varepsilon \in \{-1, i, -i\}$ ($\varepsilon \neq 1$ since $\alpha \notin k^\times$):

(i) Case $\varepsilon = -1$. Then $\alpha^{1-\sigma} = -1$, $\alpha^2 =: a \in k^\times$, $\alpha \notin k^\times$, and we get the Kummer extension $K = k(\sqrt{a})$ with $a\mathbf{Z}_k = \mathfrak{a}^2$, $\mathfrak{a}$ non-principal (Kummer extension of class type).

(ii) Case $\varepsilon = \pm i$. Then $\alpha^{1-\sigma} = \pm i$ with $-1 = (\pm i)^{1-\sigma}$; one may assume $\alpha^{1-\sigma} = i$. This yields $\alpha^2 i^{-1} \in k^\times$. Put $\alpha^2 = ic$, $c \in k^\times$; it follows $\mathfrak{a}^2\mathbf{Z}_K = \alpha^2\mathbf{Z}_K = c\mathbf{Z}_K$, hence $\mathfrak{a}^2 = c\mathbf{Z}_k$.

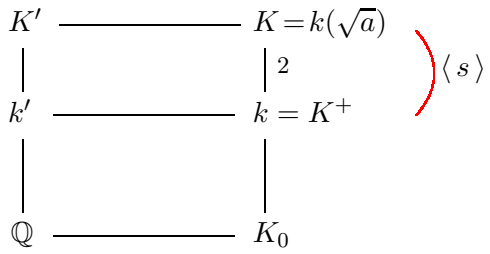
Let τ be a generator of G_K; one has $\alpha^{2\tau} = i^\tau c^\tau = -ic^\tau = -c^{\tau-1}\alpha^2$, hence $\alpha^{2\tau} = \alpha^2 d$, $d := -c^{\tau-1} \in k^\times$; we obtain $(\alpha\mathbf{Z}_K)^{2\tau} = (\alpha\mathbf{Z}_K)^2 d\mathbf{Z}_K$, thus $\mathfrak{a}^{2\tau}\mathbf{Z}_K = \mathfrak{a}^2\mathbf{Z}_K d\mathbf{Z}_K$ giving $\mathfrak{a}^{2\tau} = \mathfrak{a}^2 d\mathbf{Z}_k$.

If $d \in k^{\times 2}$, $d = e^2$, $e \in k^\times$, and $\mathfrak{a}^\tau \sim \mathfrak{a}$ saying that h' is an invariant class in $k/\mathbb{Q}$.

If $d \notin k^{\times 2}$, the relation $\alpha^{2\tau} = \alpha^2 d$ shows that $d = (\alpha^{\tau-1})^2 \in K^{\times 2}$; from Kummer theory, since $K = k(\sqrt{d}) = k(i)$, one obtains $d = -\delta^2$, $\delta \in k^\times$, and $\mathfrak{a}^{2\tau} = \mathfrak{a}^2\delta^2\mathbf{Z}_K$, still giving $\mathfrak{a}^\tau = \mathfrak{a} \cdot \delta\mathbf{Z}_k$ and an invariant class in $k/\mathbb{Q}$.

But K is the direct compositum over $\mathbb{Q}$ of $k = K^+$ and $\mathbb{Q}(i)$ and must be cyclic, so $[k : \mathbb{Q}]$ is necessarily odd and an invariant class in $k/\mathbb{Q}$ is of odd order giving the principality of $\mathfrak{a}$ in k (absurd). So, only the case (i) is a priori possible.

Consider the following diagram, with K/K_0 and $K'/\mathbb{Q}$ cyclic of 2-power order, then K/K' and $K_0/\mathbb{Q}$ of odd degree:



where we recall that $a\mathbf{Z}_k = \mathfrak{a}^2$ with $\mathfrak{a}$ non-principal and $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$, $\alpha \in K^\times$. Similarly, since K/k is only ramified at 2, then K/K_0 and $K'/\mathbb{Q}$ are totally ramified at 2, the conductor of K' is a power of 2, say 2^{r+1}, $r \geq 1$ (K' is an imaginary cyclic subfield of $\mathbb{Q}(\mu_{2^{r+1}})$).

The Kummer extension K'/k' is 2-ramified of the form $K' = k'(\sqrt{a'})$, $a' \in k'^\times$. So we have $a'\mathbf{Z}_{k'} = \mathfrak{a}'^2$ or $a'\mathbf{Z}_{k'} = \mathfrak{a}'^2\mathfrak{p}'$, where $\mathfrak{p}' \mid 2$ in k'. But all the subfields of $\mathbb{Q}(\mu_{2^\infty})$ have a trivial 2-class group; thus, one may suppose that a' is, up to $k'^{\times 2}$, a unit or an uniformizing parameter of k'. Then $K = k(\sqrt{a'})$ is not of class type (absurd); so $h' = 1$.

We have obtained:

Proposition 5.6. *For any imaginary cyclic extension $K/\mathbb{Q}$ and for any relative extension K/k, of prime degree $p \geq 2$, we have $(\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) = 1$ if $p \neq 2$ (in other words the relative classes of k do not capitulate in K), then $\mathrm{Ker}(\mathbf{J}_{K/K^+}) = 1$ if $p = 2$ (the real 2-classes of $k = K^+$ do not capitulate in K).*

Using the order formula (5.2), we get:

Corollary 5.7. *We have $\mathbf{J}_{K/K^+}(\mathscr{H}_{K^+}) \simeq \mathscr{H}_K^+ := \mathscr{H}_{K^+} = \mathbf{N}_{K/K^+}(\mathscr{H}_K)$ and the direct sum $\mathscr{H}_K = (\mathscr{H}_K^{\rm ar})^- \oplus \mathbf{J}_{K/K^+}(\mathscr{H}_{K^+})$.*

We then have obtained the following result about the relative class groups:

Theorem 5.8. *Let K be an imaginary cyclic field of maximal real subfield K^+. Let p be any prime number, and $\mathscr{H} = \mathbf{H} \otimes \mathbb{Z}_p$. Define:*

$$(\mathscr{H}_K^{\rm ar})^- := \{h \in \mathscr{H}_K,\, \mathbf{N}_{K/K^+}(h) = 1\} \quad \& \quad (\mathscr{H}_K^{\rm alg})^- := \{h \in \mathscr{H}_K,\, \nu_{K/K^+}(h) = 1\}.$$

We have $\mathscr{H}_K^{\rm ar} = \mathscr{H}_K^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg}$ for all $\varphi \in \Phi_K^-$. Whence $(\mathbf{H}_K^{\rm ar})^- = (\mathbf{H}_K^{\rm alg})^-$.

Proof. For all subfield k of K with $[K : k] = p$, $\mathbf{J}_{K/k}$ is injective on $(\mathscr{H}_k^{\rm ar})^-$ if $p \neq 2$ and $\mathbf{J}_{K/K^+}$ is injective on $\mathscr{H}_{K^+}$ for $p = 2$; so $\nu_{K/k} = \mathbf{J}_{K/k} \circ \mathbf{N}_{K/k}$ yields $(\mathscr{H}_K^{\rm ar})^- = (\mathscr{H}_K^{\rm alg})^-$ from Definition 3.12, then $(\mathbf{H}_K^{\rm ar})^- = (\mathbf{H}_K^{\rm alg})^-$ by globalization. □

We shall write simply $\mathbf{H}_K^-$ for the two notions "alg" and "ar" in the cyclic case.

Using Theorem 4.1 we may write for instance $\#\mathscr{H}_\chi^{\rm alg} = \#\mathscr{H}_\chi^{\rm ar} = \prod\limits_{\varphi \mid \chi} \#\mathscr{H}_\varphi^{\rm ar}$, for all $\chi \in \mathscr{X}^-$.

Corollary 5.9. *Let $K/\mathbb{Q}$ be an imaginary cyclic extension. Then $\#\mathbf{H}_K^+ = \prod_{\chi \in \mathscr{X}_K^+} \#\mathbf{H}_\chi^{\rm ar}$, and $\#\mathbf{H}_K^- = \prod_{\chi \in \mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm ar}$.*

Proof. To apply Theorem 3.15, we shall prove that all the arithmetic norms are surjective in any sub-extension k/k' of $K/\mathbb{Q}$; we do this for each p-class group; so the proof of the surjectivity is only necessary in the sub-extensions k/k' of p-power degree; then we use the fact that this property holds as soon as k/k' is totally ramified at some place.

Consider K as direct compositum $K'K_0$, over $\mathbb{Q}$, where K/K_0 and $K'/\mathbb{Q}$ are cyclic of p-power degree and where K/K' and $K_0/\mathbb{Q}$ are of prime-to-p degree. Let ℓ be a prime number totally ramified in $K'/\mathbb{Q}$; thus ℓ is totally ramified in any sub-extension k/k' of $K'/\mathbb{Q}$ (and in K/K_0). So Theorem 3.15 implies $\#\mathbf{H}_K = \prod\limits_{\chi \in \mathscr{X}_K} \#\mathbf{H}_\chi^{\rm ar}$.

From (5.2), we have $\#\mathbf{H}_K = \#\mathbf{H}_K^- \cdot \#\mathbf{H}_K^+$ and we can also apply Theorem 3.15 to the maximal real subfield K^+ of K, giving $\#\mathbf{H}_K^+ = \prod_{\chi \in \mathscr{X}_K^+} \#\mathbf{H}_\chi^{\rm ar}$, whence the formulas taking into account the relation $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$ for odd characters (Theorem 5.8). □

5.3. **Computation of $\#\mathbf{H}_\chi^{\rm ar}$ for $\chi \in \mathscr{X}^-$.** For an arbitrary imaginary extension $K/\mathbb{Q}$, we have (e.g., from [Has1952, p. 12] or [Was1997, Theorem 4.17]) the formula:

$$\#\mathbf{H}_K^- = Q_K^- w_K^- \prod_{\psi \in \Psi_K^-} \big(-\tfrac{1}{2}\, \mathbf{B}_1(\psi^{-1}) \big), \ \text{ with } \ \mathbf{B}_1(\psi^{-1}) := \frac{1}{f_\chi} \sum_{a \in [1, f_\chi[} \psi^{-1}(\sigma_a)\, a,$$

where w_K^- is the order of the group of roots of unity of K and Q_K^- the index of units; from [Has1952, Satz 24], $Q_K^- = 1$ when $K/\mathbb{Q}$ is cyclic. We then have the following result:

Theorem 5.10. *Let $\chi \in \mathscr{X}^-$ and recall that $\mathbf{H}_\chi^{\rm ar} := \{x \in \mathbf{H}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,$ for all $k \subsetneq K_\chi\}$. Let g_χ be the order of χ and f_χ its conductor; then:*

$$\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi \mid \chi} \big(-\tfrac{1}{2}\, \mathbf{B}_1(\psi^{-1}) \big),$$

where $\alpha_\chi = 1$ (resp. $\alpha_\chi = 0$) if g_χ is a 2-power (resp. if not), and where w_χ is as follows:

(i) $w_\chi = 1$ if K_χ is not an imaginary cyclotomic field;

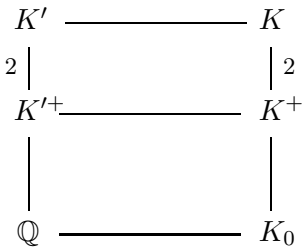
(ii) $w_\chi = p$ if $K_\chi = \mathbb{Q}(\mu_{p^n})$, $p \geq 2$ prime, $n \geq 1$.

Proof. We use [Or1975b, Proposition III (g)] or [Leo1954, Chap. I, § 1 (4)] recalled in Theorem 2.1; it is sufficient to prove that for any imaginary cyclic extension $K/\mathbb{Q}$:

$$\#\mathbf{H}_K^- = \prod_{\chi \in \mathscr{X}_K^-} \big(2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi \mid \chi} \big(-\tfrac{1}{2}\, \mathbf{B}_1(\psi^{-1}) \big) \big),$$

the expected equality will come from Theorem 5.8, taking into account the relation $\#\mathbf{H}_K^- = \prod_{\chi \in \mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm ar}$. So, it remains to prove that $\prod_{\chi \in \mathscr{X}_K^-} \big(2^{\alpha_\chi} \cdot w_\chi\big) = w_K^-$.

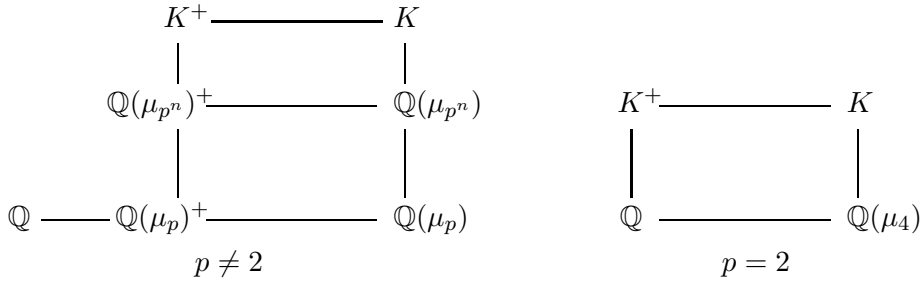
Consider the following diagram:



where K/K_0 and $K'/\mathbb{Q}$ are cyclic of 2-power degree and where K/K' and $K_0/\mathbb{Q}$ are of odd degree. As K^+ and K'^+ are real, then all the α_χ are zero, except when g_χ is a 2-power, hence for the unique χ_0 defining K' for which $\alpha_\chi = 1$; whence $\prod_{\chi \in \mathscr{X}_K^-} 2^{\alpha_\chi} = 2$.

If K does not contain any cyclotomic field (different from $\mathbb{Q}$), then $w_K^- = 2$, moreover, all the w_χ are trivial and the required equality holds in that case.

So, let $\mathbb{Q}(\mu_{p^n})$, $n \geq 1$, be the largest cyclotomic field contained in K; this yields two possibilities:



In the case $p \neq 2$, one has $\prod_{\chi \in \mathscr{X}_K^-} w_\chi = p^n$ (due to the n odd characters defined by the $\mathbb{Q}(\mu_{p^i})$, $1 \leq i \leq n$), and for $p = 2$ this gives $\prod_{\chi \in \mathscr{X}_K^-} w_\chi = 2$; whence the result (cf. [Has1952, Chap. III, § 33, Theorem 34 and others]). □

Remark 5.11. For any imaginary extension K, $\#\mathbf{H}_K^- = \frac{Q_K^- w_K^-}{2^{n_K^-}} \prod_{\chi \in \mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm alg}$, where n_K^- is the number of imaginary cyclic sub-extensions of K of 2-power degree, and where w_K^- is the 2-part of w_K (resp. $\frac{1}{2}w_K$) if $\mathbb{Q}(\mu_4) \not\subset K$ (resp. $\mathbb{Q}(\mu_4) \subset K$). See [Gra1976, Remarque II 2, p. 32].

5.4. **Annihilation theorem for relative p-class groups.** Before significant improvements, by means of Stickelberger's elements, leading to the construction of p-adic measures, to index formulas and annihilators of various invariants of an abelian field, Iwasawa [Iwa1962a] proves the following formula for the cyclotomic fields $K = \mathbb{Q}(\mu_{p^n})$, $p \neq 2$, $n \geq 1$, of Galois group G_K:

$$\#\mathbf{H}_K^- = \big(\mathbb{Z}[G_K]^- : \mathbf{B}_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K]^-\big),$$

where $\mathbb{Z}[G_K]^- := \{\Omega \in \mathbb{Z}[G_K],\ (1+s)\cdot\Omega = 0\}$, s being the complex conjugation, and $\mathbf{B}_K := \frac{1}{p^n} \sum_{a \in [1, p^n[,\, p \nmid a} a\, \sigma_a^{-1}$, where $\sigma_a \in G_K$ denotes the corresponding Artin automorphism.

One can verify that this formula does not generalize for arbitrary abelian imaginary extension $K/\mathbb{Q}$ (see the counterexample given in [Gra1976, p. 33]). Many contributions have appeared (e.g., [Leo1962, Gil1975, Coa1975, Gra1978, All2013, All2017, GreiKuč2020]; for more precise formulas, see [Sin1980], [Was1997, § 6.2, § 15.1], among many other). Nevertheless, we gave in [Gra1976] another definition in the spirit of the φ-objects which succeeded to give a correct formula (we shall make the same remark for the index formulas given via cyclotomic units in the real case).

5.4.1. *General definition of Stickelberger's elements.* Let $K \in \mathscr{K}$, $K \neq \mathbb{Q}$. Let $f_K =: f > 1$ be the conductor of K and let $\mathbb{Q}(\mu_f)$ be the corresponding cyclotomic field. Define the more suitable writing of the Stickelberger element:

$$\mathbf{B}_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f} \left(\frac{a}{f} - \frac{1}{2}\right) \cdot \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$$

(in the summation, the integers a are prime to f and the Artin symbols are taken over $\mathbb{Q}$). Note that the part $\sum_{a=1}^{f} \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ is the algebraic norm $\nu_{\mathbb{Q}(\mu_f)/\mathbb{Q}}$ which does not modify the image of $\mathbf{B}_{\mathbb{Q}(\mu_f)}$ by ψ, for $\psi \in \Psi$, $\psi \neq 1$.

We shall use two arithmetic $\mathscr{G}$-families: the $\mathscr{G}$-family $\mathbf{M}$, for which $\mathbf{M}_K = \mathbb{Z}[G_K]$ and the $\mathscr{G}$-family $\mathbf{S}$ defined by:

$$\mathbf{S}_K := \mathbf{B}_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K], \text{ where } \mathbf{B}_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = -\sum_{a=1}^{f} \left(\frac{a}{f} - \frac{1}{2}\right)\left(\frac{K}{a}\right)^{-1}. \tag{5.3}$$

Lemma 5.12. *For any integer c prime to $2f$, let $\mathbf{B}_K^c := \left(1 - c\left(\frac{K}{c}\right)^{-1}\right)\cdot \mathbf{B}_K$; then $\mathbf{B}_K^c \in \mathbb{Z}[G_K]$.*

Proof. We have $\mathbf{B}_K^c = \frac{-1}{f}\sum_a \left[a\left(\frac{K}{a}\right)^{-1} - ac\left(\frac{K}{a}\right)^{-1}\left(\frac{K}{c}\right)^{-1}\right] + \frac{1-c}{2}\sum_a \left(\frac{K}{a}\right)^{-1}$. Let $a'_c \in [1, f]$ be the unique integer such that $a'_c \cdot c \equiv a \pmod f$ and put:

$$a'_c \cdot c = a + \lambda_a(c) f, \quad \lambda_a(c) \in \mathbb{Z};$$

using the bijection $a \mapsto a'_c$ in the summation of the second term in between $[\ ]$ and the relation $\left(\frac{K}{a'_c}\right)\left(\frac{K}{c}\right) = \left(\frac{K}{a}\right)$, this yields:

$$\begin{aligned}\mathbf{B}_K^c &= \frac{-1}{f}\Big[\sum_a a\left(\frac{K}{a}\right)^{-1} - \sum_a a'_c \cdot c\left(\frac{K}{a'_c}\right)^{-1}\left(\frac{K}{c}\right)^{-1}\Big] + \frac{1-c}{2}\sum_a\left(\frac{K}{a}\right)^{-1}\\ &= \frac{-1}{f}\sum_a\Big[a - a'_c\cdot c\Big]\left(\frac{K}{a}\right)^{-1} + \frac{1-c}{2}\sum_a\left(\frac{K}{a}\right)^{-1}\\ &= \sum_a\Big[\lambda_a(c) + \frac{1-c}{2}\Big]\left(\frac{K}{a}\right)^{-1} \in \mathbb{Z}[G_K].\end{aligned}$$

We have moreover the relations $\lambda_{f-a}(c) + \frac{1-c}{2} = -\big(\lambda_a(c) + \frac{1-c}{2}\big)$ which proves that:

$$\mathbf{B}_K^c = \mathbf{B}_K'^c \cdot (1-s),\ \ \mathbf{B}_K'^c \in \mathbb{Z}[G_K], \tag{5.4}$$

useful in the case $p = 2$ and giving $\mathbf{N}_{K/K^+}(\mathbf{B}_K^c) = 0$. □

Definition 5.13. *Let K be an imaginary abelian field. Put $\mathfrak{A}_K := \{\Omega \in \mathbb{Z}[G_K],\ \Omega\,\mathbf{B}_K \in \mathbb{Z}[G_K]\}$ ($\mathfrak{A}_K$ is an ideal of $\mathbb{Z}[G_K]$ and $\mathbf{S}_K := \mathbf{B}_K \cdot \mathfrak{A}_K$ (cf. (5.3)). We denote by $\Lambda_K \in \mathfrak{A}_K$ the least rational integer such that $\Lambda_K \mathbf{B}_K \in \mathbb{Z}[G_K]$ (thus $\Lambda_K \mid 2f$, where f is the conductor of K).*

For $K = K_\chi$, $\chi \in \mathscr{X}^-$, we put $\mathfrak{A}_{K_\chi} =: \mathfrak{A}_\chi$ and $\Lambda_{K_\chi} =: \Lambda_\chi$.

Since we will only use images by $\psi \in \Psi^-$ of elements of $\mathbb{Q}[G_K]$, we can neglect, by abuse, the term $\sum_{a=1}^{f}\frac{1}{2}\left(\frac{K}{a}\right)^{-1}$ in some reasonings and computations, using $\frac{1}{f}\sum_{a=1}^{f} a\left(\frac{K}{a}\right)^{-1}$ instead of $\mathbf{B}_K$.

Note that for any odd c prime to f, $\left(1 - c\left(\frac{K}{c}\right)^{-1}\right)\cdot\sum_{a=1}^{f}\frac{1}{2}\left(\frac{K}{a}\right)^{-1} \in \mathbb{Z}[G_K]$ and that such considerations only concerns the case $p = 2$ when f is an odd prime power with $[\mathbb{Q}(\mu_f) : K]$ odd (see Example 5.20 with $K = \mathbb{Q}(\mu_{47})$).

Lemma 5.14. *Let α_σ be the coefficient of $\sigma \in G_K$ in the writing of $\sum_{a=1}^{f} a\left(\frac{K}{a}\right)^{-1}$ on the canonical basis G_K of $\mathbb{Z}[G_K]$ (in particular, we have $\alpha_1 = \sum_{a,\ \sigma_{a|_K}=1} a$). Then $\alpha_\sigma \equiv c\,\alpha_1 \pmod f$, where c is a representative modulo f such that $\sigma_c = \sigma^{-1}$. Thus, we have $\Lambda_K = \frac{f}{\gcd(f,\alpha_1)}$.*

Proof. The first claim is obvious and Λ_K is the least integer Λ such that $\frac{\Lambda\cdot\alpha_1}{f} \in \mathbb{Z}$, since $\Lambda\sum_{a=1}^{f}\frac{a}{f}\left(\frac{K}{a}\right)^{-1} \in \mathbb{Z}[G_K]$ if and only if $\frac{\Lambda\cdot\alpha_\sigma}{f} \in \mathbb{Z}$ for all $\sigma \in G_K$, thus, for instance, for $\sigma = 1$. □

Proposition 5.15. *(i) The ideal $\mathfrak{A}_K$ of $\mathbb{Z}[G_K]$ is a free $\mathbb{Z}$-module; a $\mathbb{Z}$-basis is given by the set $\big\{\cdots, \left(\frac{K}{a}\right) - a, \cdots;\ \Lambda_K\big\}$, for the representatives a of $(\mathbb{Z}/f\mathbb{Z})^\times \setminus \{1\}$.*

(ii) If $K/\mathbb{Q}$ is cyclic, then $\mathfrak{A}_K$ is the ideal of $\mathbb{Z}[G_K]$ generated by $\left(\frac{K}{c}\right) - c$ and Λ_K, where $\left(\frac{K}{c}\right)$ is any generator of G_K.

Proof. See [Gra1976, p. 35–36]. □

5.4.2. *Study of the algebraic $\mathscr{G}$-families* $\mathbf{M}_K := \mathbb{Z}[G_K]$, $\mathbf{S}_K := \mathbf{B}_K\mathfrak{A}_K$. We then have:

$$\begin{aligned}&\mathbf{M}_{K_\chi} = \mathbb{Z}[G_\chi], && \mathbf{S}_{K_\chi} = \mathbf{B}_{K_\chi}\,\mathfrak{A}_\chi,\\ &\mathbf{M}_\chi = \{\Omega \in \mathbb{Z}[G_\chi],\ P_\chi\cdot\Omega = 0\}, && \mathbf{S}_\chi = \mathbf{B}_{K_\chi}\mathfrak{A}_\chi \cap \mathbf{M}_\chi\end{aligned}$$

($\mathbf{M}_\chi$ and $\mathbf{S}_\chi$ are ideals of $\mathbf{M}_{K_\chi}$).

Lemma 5.16. *We have $\mathbf{M}_\chi = \prod_{\ell|g_\chi}(1-\sigma_\chi^{g_\chi/\ell})\,\mathbb{Z}[G_\chi]$. The image of $\mathbf{M}_\chi$, by $\psi : \mathbb{Z}[G_\chi] \to \mathbb{Z}[\mu_{g_\chi}]$, is isomorphic to the ideal $\mathfrak{a}_\chi := \prod_{\ell|g_\chi}\big(1-\psi(\sigma_\chi)^{g_\chi/\ell}\big)\mathbb{Z}[\mu_{g_\chi}]$; in this isomorphism, $\mathbf{S}_\chi$ corresponds to an ideal $\mathfrak{b}_\chi$ multiple of $\mathfrak{a}_\chi$.*

Proof. See [Gra1976, Lemmes II.8 and II.9, pp. 37/39]. □

The computation of $\mathfrak{b}_\chi$ needs to recall the norm action on Stickelberger's elements; because of the similarity of the result for the norm action on cyclotomic numbers, we recall, without proof, the following well-known formulas:

Lemma 5.17. *Let $f>1$ and $m \mid f$, $m>1$, be any modulus; let $\mathbb{Q}(\mu_f)$, $\mathbb{Q}(\mu_m) \subseteq \mathbb{Q}(\mu_f)$, be the corresponding cyclotomic fields. Let $\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)} : \mathbb{Q}[G_{\mathbb{Q}(\mu_f)}] \to \mathbb{Q}[G_{\mathbb{Q}(\mu_m)}]$. Let:*

$$\mathbf{B}_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f} \Big(\frac{a}{f}-\frac{1}{2}\Big) \cdot \Big(\frac{\mathbb{Q}(\mu_f)}{a}\Big)^{-1} \quad \& \quad \mathbf{C}_{\mathbb{Q}(\mu_f)} := 1-\zeta_f.$$

We have:

$$\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = \prod_{p\mid f,\ p\nmid m} \Big(1-\Big(\frac{\mathbb{Q}(\mu_m)}{p}\Big)^{-1}\Big) \cdot \mathbf{B}_{\mathbb{Q}(\mu_m)},$$

$$\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(\mathbf{C}_{\mathbb{Q}(\mu_f)}) = \big(\mathbf{C}_{\mathbb{Q}(\mu_m)}\big)^{\Omega}, \quad \Omega := \prod_{p\mid f,\ p\nmid m} \Big(1-\Big(\frac{\mathbb{Q}(\mu_m)}{p}\Big)^{-1}\Big).$$

We can conclude by the following statements [Gra1976, Théorèmes II.5, II.6]:

Theorem 5.18. *Let $\chi \in \mathscr{X}^-$ and let $\psi \mid \chi$ defining the law of $\mathbb{Z}[\mu_{g_\chi}]$-module for the χ-objects. Then $\mathbf{H}_\chi^{\rm alg} = \mathbf{H}_\chi^{\rm ar}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1}) \cdot (\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}[\mu_{g_\chi}]$, where $\sigma_a := \big(\frac{K}{a}\big)$ is any generator of G_K (cf. Lemma 5.14, Proposition 5.15).*
The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ is the unit ideal except if $K_\chi \neq \mathbb{Q}(\mu_4)$ is an extension of $\mathbb{Q}(\mu_p)$ of p-power degree and if $\Lambda_\chi \equiv 0 \pmod p$, in which case, this ideal is a prime ideal $\mathfrak{p}_\chi \mid p$ in $\mathbb{Q}(\mu_{g_\chi})$. If $K_\chi = \mathbb{Q}(\mu_4)$, this ideal is the ideal (4).

Theorem 5.19. *For $\varphi \in \Phi^-$ and $\psi \mid \varphi$, the $\mathbb{Z}_p[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi^{\rm alg} = \mathscr{H}_\varphi^{\rm ar}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1}) \cdot (\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$, where σ_a is any generator of G_K.*
The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$ is the unit ideal except if $K_\chi \neq \mathbb{Q}(\mu_4)$ is an extension of $\mathbb{Q}(\mu_p)$ of p-power degree, if $\Lambda_\chi \equiv 0 \pmod p$ and if $\lambda = 1$ in the writing $\psi = \omega^\lambda \cdot \psi_p$ (where ω is the Teichmüller character and ψ_p of p-power order), in which case, this ideal is the prime ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$. If $K_\chi = \mathbb{Q}(\mu_4)$, this ideal is the ideal (4).

Example 5.20. Let $K := K_\chi$ be the field $\mathbb{Q}(\mu_{47})$, of degree $g_\chi = 46$. From Theorem 5.10, we have $\#\mathbf{H}_\chi = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi\mid\chi} \big(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$ with in that case $\alpha_\chi = 0$ and $w_\chi = 47$ and where by definition $-\frac{1}{2}\mathbf{B}_1(\psi^{-1}) = -\frac{1}{2}\sum_{a=1}^{46}\big(\frac{a}{47}-\frac{1}{2}\big)\psi^{-1}(\sigma_a) = -\frac{1}{2}\sum_{a=1}^{46}\frac{a}{47}\,\psi^{-1}(\sigma_a)$. The following program computes $\#\mathbf{H}_\chi = 47 \cdot \mathbf{N}_{\mathbb{Q}(\mu_{46})/\mathbb{Q}}\big(-\frac{1}{2}\sum_{a=1}^{46}\frac{a}{47}\,\psi^{-1}(\sigma_a)\big)$:

```
{P=polcyclo(46);g=lift(znprimroot(47));A=0;for(n=0,45,a=lift(Mod(g,47)^n);
A=A+x^n*(1/47*a-1/2));B=Mod(-1/2*A,P);print(47*norm(B))}
139
```

Note that $-\frac{47}{2}\mathbf{B}_1(\psi^{-1})$ is, with PARI polynomial writing $x=\zeta_{46}$, the integer:

```
4*x^21+25*x^20+9*x^19+26*x^18-19*x^17+11*x^16-22*x^15+x^14-24*x^13+10*x^12
+6*x^11+16*x^10-21*x^9+20*x^8+8*x^7+7*x^6-4*x^5+14*x^4-12*x^3+3*x^2+14*x+27
```

Whence $\#\mathbf{H}_\chi = 139$ and $\mathbf{H}_\chi \simeq \mathbb{Z}[\mu_{46}]/\mathfrak{p}_{139}$. Since $\Lambda_\chi = 47$, the ideal $\mathfrak{A}_K$ is $\big(\sigma_a - a, 47\big)$, with for instance $a=5$ (Lemma 5.14), and $\mathfrak{A}_K \cdot \frac{1}{2}\mathbf{B}_K$ annihilates $\mathbf{H}_\chi$; since the image of $\mathfrak{A}_K \cdot \frac{1}{2}\mathbf{B}_K$ is the ideal $\big(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big) = \mathfrak{p}_{139}$, *the annihilator* of $\mathbf{H}_\chi$ is $\mathfrak{p}_{139}$. But this ideal is not principal in $\mathbb{Q}(\mu_{46})$ (from [Gra1978/79b]); PARI checking:

```
{L=bnfinit(polcyclo(46));F=idealfactor(L,139);print(bnfisprincipal(L,component(F,1)[1])[1])}
[2]~
```

showing that its class is the square of the PARI generating class. More precisely, the class group of $\mathbb{Q}(\mu_{46}) = \mathbb{Q}(\mu_{23})$ is equal to 3; then any $\mathfrak{q}_{47} \mid 47$ or $\mathfrak{q}_{139} \mid 139$ generates this class group.

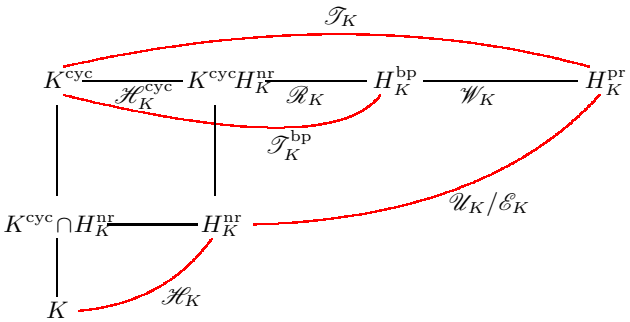
In [Gra1978, Chap. IV, § 2], [Gra1978/79b, Théorèmes 1, 2, 3], we have given improvements of the annihilation for 2-class groups but it is difficult to say if the case $p = 2$ is optimal or not. By way of example, we cite the following [Gra1978, Théorème IV1] under the above context:

Theorem 5.21. *Let $\chi \in \mathscr{X}^-$ and let $\psi \mid \varphi \mid \chi$ for $p = 2$ with $\psi = \psi_0\,\psi_2$ and $\psi_0 \neq 1$ of even order. Put $K := K_\chi$. The $\mathbb{Z}_2[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi/\mathbf{J}_{K/K^+}(\mathscr{H}_{\varphi'}^+)$ is annihilated by $\big(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$, where $\mathscr{H}_\varphi^+ := \{x \in \mathscr{H}_{K^+},\ P_{\varphi'}(\sigma_\chi)\cdot x = 1\}$ with $\varphi' \in \Phi^+$ is above $\psi' := \psi_0\,\psi_2^2$.*

Note that this result does not imply that $\mathscr{H}_\varphi$ is annihilated by $\big(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$.

6. Application to torsion groups of abelian p-ramification

Let K be a real abelian field and let $\mathscr{T}_K$ be the torsion group of the Galois group of the maximal p-ramified abelian pro-p-extension $H_K^{\rm pr}$ of K. Since Leopoldt's conjecture holds for abelian fields, we have $\mathscr{T}_K = {\rm Gal}(H_K^{\rm pr}/K^{\rm cyc})$, where $K^{\rm cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension of K.



Then $H_K^{\rm nr}$ is the p-Hilbert class field, $H_K^{\rm bp}$ the Bertrandias–Payan field and $\mathscr{T}_K^{\rm bp} := {\rm Gal}(H_K^{\rm bp}/K^{\rm cyc})$ is called the Bertrandias–Payan module (see [Ng1986, Section 4], [Jau1990, Section 2 (b)]). The diagram is related to the exact sequence (we denote by K_v the completion of K at the place v):

$$1 \to \mathscr{W}_K \longrightarrow {\rm tor}_{\mathbb{Z}_p}\big(\mathscr{U}_K/\mathscr{E}_K\big) \xrightarrow{\log_p} \mathscr{R}_K := {\rm tor}_{\mathbb{Z}_p}\big(\log_p\big(\mathscr{U}_K\big)/\log_p(\mathscr{E}_K)\big) \to 0, \tag{6.1}$$

where $\mathscr{W}_K := \big(\oplus_{v\mid p}\,\mu_p(K_v)\big)/\mu_p(K)$, $\mathscr{U}_K$ denotes the group of local units at p and $\mathscr{E}_K = \mathbf{E}_K \otimes \mathbb{Z}_p$ is identified with its diagonal image in $\mathscr{U}_K$ (see [Gra2005, § III.2, (c), Fig. 2.2; Lemma III.4.2.4] and [Gra2018a]).

6.1. **Order of $\mathscr{T}_K$.** The order of this $\mathbb{Z}_p[\mathscr{G}]$-module is well known and given, analytically, by the residue at $s = 1$ of the p-adic ζ-function of K, whence by the values at $s = 1$ of p-adic $\mathbf{L}$-functions of the non-trivial characters of K (after [Coa1975, Appendix]); see for instance [Gra2019, § 3.4, formula (3.8)] for analytic context. In conclusion we can write:

$$\#\mathscr{T}_K = \#\mathscr{H}_K^{\rm cyc}\cdot\#\mathscr{R}_K\cdot\#\mathscr{W}_K \sim [K\cap\mathbb{Q}^{\rm cyc}:\mathbb{Q}]\cdot\prod_{\psi\neq 1}\tfrac{1}{2}\,\mathbf{L}_p(1,\psi). \tag{6.2}$$

Since the arithmetic family of these $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{T}_K$ follows the most favorable properties (surjectivity of the norms for real fields K, injectivity of the transfer maps), we can state, in a similar context as for Theorems 5.8:

Theorem 6.1. *For all $\chi \in \mathscr{X}^+$ (resp. $\varphi \in \Phi^+$), we have:*

$$\mathscr{T}_\chi^{\rm ar} = \mathscr{T}_\chi^{\rm alg} = \{x \in \mathscr{T}_{K_\chi},\ P_\chi\cdot x = 1\} = \{x \in \mathscr{T}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \textit{for all } k \subsetneq K_\chi\}$$

(resp. $\mathscr{T}_\varphi^{\rm ar} = \mathscr{T}_\varphi^{\rm alg} = \{x \in \mathscr{T}_{K_\chi},\ P_\varphi\cdot x = 1\} = \{x \in \mathscr{T}_\chi,\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \textit{for all } k \subsetneq K_\chi\}$).

Moreover, if $K/\mathbb{Q}$ is real cyclic, we then have:

$$\#\mathscr{T}_K = \prod_{\chi\in\mathscr{X}_K}\#\mathscr{T}_\chi^{\rm ar} = \prod_{\varphi\in\Phi_K}\#\mathscr{T}_\varphi^{\rm ar}.$$

We denote simply $\mathscr{T}_\chi$ (resp. $\mathscr{T}_\varphi$) these components in the analytic and arithmetic senses. In the analytic point of view, we have the analogue of Theorems 5.10 and 7.10 (see some p-adic formulas about $\mathbf{L}_p$-functions, from classical papers, as for instance [KL1964, AF1972, Gra1978/79a] and a broad presentation in [Was1997, Theorems 5.18, 5.24]):

Theorem 6.2. *Let $\chi \in \mathscr{X}^+ \setminus \{1\}$. Then $\#\mathscr{T}_\chi = w_\chi^{\rm cyc} \cdot \prod\limits_{\psi\mid\chi} \frac{1}{2}\,\mathbf{L}_p(1,\psi)$, where $w_\chi^{\rm cyc}$ is as follows, from analytic formula (6.2):*

(i) $w_\chi^{\rm cyc} = 1$ if K_χ is not a subfield of $\mathbb{Q}^{\rm cyc}$;

(ii) $w_\chi^{\rm cyc} = p$ if K_χ is a subfield of $\mathbb{Q}^{\rm cyc}$.

6.2. **Annihilation theorem for $\mathscr{T}_K$.** An annihilator of $\mathscr{T}_K$ is given by the following statement [Gra2018b, Theorem 5.5] which does not assume any hypothesis on K and p and gives again the known results (e.g., [Or1981]):

Theorem 6.3. *Let K be any real abelian field of conductor f_K. Let $c \in \mathbb{Z}$ be prime to $2pf_K$. Let f_n be the conductor of $L_n := K\mathbb{Q}(\mu_{qp^n})$, n large enough, where $q = p$ or 4 as usual. For all $a \in [1, f_n]$, prime to f_n, let a'_c be the unique integer in $[1, f_n]$ such that $a'_c \cdot c \equiv a \pmod{f_n}$ and put $a'_c \cdot c - a = \lambda_a^n(c)\, f_n$, $\lambda_a^n(c) \in \mathbb{Z}$. Let s be the complex conjugation. Then:*

$$\mathbf{A}_{K,n}(c) := \sum_{a=1}^{f_n} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big) =: \mathbf{A}'_{K,n}(c)\cdot(1+s_\infty),\ \text{where}\ \mathbf{A}'_{K,n}(c) = \sum_{a=1}^{f_n/2} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big).$$

Let $\mathbf{A}_K(c) := \lim\limits_{n\to\infty} \Big[\sum\limits_{a=1}^{f_n} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big)\Big] =: \mathbf{A}'_K(c)\cdot(1+s_\infty)$; we then have:

(i) For $p \neq 2$, $\mathbf{A}'_K(c)$ annihilates the $\mathbb{Z}_p[G_K]$-module $\mathscr{T}_K$.

(ii) For $p = 2$, the annihilation is true for $2\cdot\mathbf{A}_K(c)$ and $4\cdot\mathbf{A}'_K(c)$.

Remark 6.4. In practice, when the exponent p^e of $\mathscr{T}_K$ is known, one can take $n = n_0 + e$, where $n_0 \geq 0$ is defined by $[K \cap \mathbb{Q}^{\rm cyc} : \mathbb{Q}] =: p^{n_0}$, and use the annihilators $\mathbf{A}_{K,n}(c)$, $\mathbf{A}'_{K,n}(c)$. When $K = K_\chi$, the annihilator limit $\mathbf{A}_{K_\chi}(c)$ is related to p-adic $\mathbf{L}$-functions via the formula:

$$\psi(\mathbf{A}_{K_\chi}(c)) = (1-\psi(c))\cdot\mathbf{L}_p(1,\psi), \quad \text{for } \psi \mid \chi.$$

In the case where g_χ is not a p-power, one can choose c such that $1-\psi(c)$ be invertible giving $\psi(\mathbf{A}_{K_\chi}(c)) \sim \mathbf{L}_p(1,\psi)$; otherwise, if $g_\chi = p^n$, $n \geq 1$, $\psi(\mathbf{A}_{K_\chi}(c)) \sim \pi_\chi \mathbf{L}_p(1,\psi)$, where π_χ is an uniformizing parameter in $\mathbb{Q}_p(\mu_{p^n})$.

This annihilation theorem is the analog of Theorem 5.19, using Bernoulli's numbers, linked to $\mathbf{L}_p(0,\omega\psi^{-1})$, instead of $\mathbf{L}_p(1,\psi)$.

7. Application to class groups of real abelian extensions

Denote by $\mathbf{E}$ the $\mathscr{G}$-family for which $\mathbf{E}_K$, $K \in \mathscr{K}$, is the group of absolute value of the global units of K, the Galois action being defined by $|\varepsilon|^\sigma = |\varepsilon^\sigma|$ for any unit ε and any $\sigma \in \mathscr{G}$. The $\mathbf{E}_K$ are free $\mathbb{Z}$-modules.

7.1. **The Leopoldt χ-units.** In [Leo1954] Leopoldt defined unit groups, $\mathbf{E}_\chi$, that we shall call (as in [Or1975b]) the group of χ-units for rational characters $\chi \in \mathscr{X}^+ \setminus \{1\}$; from the definition of χ-objects and the results of the previous sections we can write:

$$\mathbf{E}_\chi = \{|\varepsilon| \in \mathbf{E}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot|\varepsilon| = 1\} = \{|\varepsilon| \in \mathbf{E}_{K_\chi},\ \nu_{K_\chi/k}(|\varepsilon|) = 1, \text{ for all } k \subsetneq K_\chi\}. \tag{7.1}$$

Definition 7.1. *Denote by $\mathbf{E}^0$ the $\mathscr{G}$-family such that $\mathbf{E}^0_K$ is the subgroup of $\mathbf{E}_K$ generated by the $\mathbf{E}_k$ for the subfields $k \subsetneq K$ (or simply the subfields k_ℓ such that $[K_\chi : k_\ell] = \ell \mid [K_\chi : \mathbb{Q}]$).*

Lemma 7.2. *We have $\mathbf{E}^0_{K_\chi}\cdot\mathbf{E}_\chi = \mathbf{E}^0_{K_\chi} \oplus \mathbf{E}_\chi$, for all $\chi \in \mathscr{X}^+$.*

Proof. One knows that $\bigoplus\limits_{\theta\in\mathscr{X}_K} \mathbf{E}_\theta$ is of finite index Q_K in $\mathbf{E}_K$ for any real K (cf. [Leo1954, Chap. 5, § 4]). Let $|\varepsilon| \in \mathbf{E}^0_{K_\chi} \cap \mathbf{E}_\chi$; there exist strict subfields $k_1, \ldots, k_t$ of K_χ such that $|\varepsilon| = |\varepsilon_1|\cdots|\varepsilon_t|$, $|\varepsilon_i| \in \mathbf{E}_{k_i}$ and an integer $n \geq 1$ such that $|\varepsilon_i^n| \in \bigoplus\limits_{\theta_i\in\mathscr{X}_{k_i}} \mathbf{E}_{\theta_i}$, for all i (in particular, $\chi \notin \mathscr{X}_{k_i}$); we then have $|\varepsilon^n| \in \Big(\bigoplus\limits_{\theta\in\mathscr{X}_{K_\chi}\ \theta\neq\chi} \mathbf{E}_\theta\Big) \bigcap \mathbf{E}_\chi = \{1\}$, which implies $|\varepsilon| = 1$. □

Definition 7.3. *Let K be any real abelian field. Put $Q_K = \left(\mathbf{E}_K : \bigoplus_{\chi\in\mathscr{X}_K} \mathbf{E}_\chi\right)$, where $\mathbf{E}_\chi$ is the group of χ-units (7.1), and, for all $\chi \in \mathscr{X}_K^+$, put $Q_\chi = \left(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \oplus \mathbf{E}_\chi\right)$.*

The main following computations are also available in [Leo1954, Leo1962] and [Or1975b].

Lemma 7.4. *We have, for all cyclic real field K, $Q_K = \prod_{\chi\in\mathscr{X}_K} Q_\chi$.*

Proof. This may be proved locally; for this, we use the $\mathscr{G}$-family $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$, for any prime p, and the $\mathscr{E}_\chi$ as above. Then one uses, inductively, Lemma 7.2 with characters $\psi \mid \varphi \mid \chi$, written as $\psi = \psi_0\,\psi_p$ (ψ_0 of prime-to-p order, ψ_p of order p^n, $n \geq 0$). See the details in [Gra1976, pp. 72–75]. □

Definition 7.5. *Let ϕ be the Euler totient function and put, for all character $\chi \in \mathscr{X}^+$:*

$q_\chi = \prod_{\ell\mid g_\chi} \ell^{\frac{\phi(g_\chi)}{\ell-1}}$, *if g_χ is not the power of a prime number,*

$q_\chi = \ell^{\frac{\phi(g_\chi)}{\ell-1}-1} = \ell^{\ell^{n-1}-1}$, *if g_χ is a prime power ℓ^n, $n \geq 1$,*

$q_1 = 1$.

For any real abelian field K, set $q_K = \left(\frac{g^{g-2}}{\prod_{\chi\in\mathscr{X}_K} d_\chi}\right)^{\frac{1}{2}}$, where $g := [K : \mathbb{Q}]$ and d_χ is the discriminant of $\mathbb{Q}(\mu_{g_\chi})$.

Lemma 7.6. *We have, for all cyclic real field K, $q_K = \prod_{\chi\in\mathscr{X}_K} q_\chi$.*

Proof. From [Has1952, § 15, p. 34, (2), p. 35]; see [Gra1976, pp. 76–77] for more details. □

7.2. **The Leopoldt cyclotomic units.** For the main definitions and properties of cyclotomic units, see [Leo1954, § 8 (1)], [Or1975a].

Definitions 7.7. *(i) Let $\chi \in \mathscr{X}^+$ of conductor f_χ; we define the "cyclotomic numbers":*

$$\mathbf{C}_\chi := \prod_{a\in A_\chi} (\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a}),$$

where $\zeta_{2f_\chi} := \exp\left(\frac{i\pi}{f_\chi}\right)$, and A_χ is a half-system of representatives of $(\mathbb{Z}/f_\chi\mathbb{Z})^\times$.

(ii) Let K be a real abelian field and let $\mathbf{C}_K$ be the multiplicative group generated by the conjugates of $|\mathbf{C}_\chi|$, for all $\chi \in \mathscr{X}_K$. Then we define the group of cyclotomic units:

$$\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K \quad \& \quad \mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p.$$

Recall that $\mathbf{C}_\chi^2 \in K_\chi$ and that any conjugate $\mathbf{C}'_\chi$ of $\mathbf{C}_\chi$ is such that $\frac{\mathbf{C}'_\chi}{\mathbf{C}_\chi}$ is a unit of K_χ. If f_χ is not a prime power, then $\mathbf{C}_\chi$ is a unit.

Lemma 7.8. *The $\mathbb{Z}[G_K]$-modules $\mathbf{C}_K$ and $\mathbf{F}_K = \mathbf{C}_K \cap \mathbf{E}_K$ are free $\mathbb{Z}$-modules; the families defined by $\mathbf{C}_K$ and $\mathbf{F}_K$ are $\mathscr{G}$-families with the arithmetic norms and transfers.*

Proof. In particular, for conductors f and $m \mid f$, we have, for the norms, the formula given in Lemma 5.17, $\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(|\mathbf{C}_{\mathbb{Q}(\mu_f)}|) = |\mathbf{C}_{\mathbb{Q}(\mu_m)}|^\Omega$, where $\Omega = \prod_{q\mid f,\, q\nmid m} \left(1 - \left(\frac{\mathbb{Q}(\mu_m)/\mathbb{Q}}{q}\right)\right)$, which generates all the norm formulas in $\mathbb{Q}^{\rm ab}/\mathbb{Q}$. □

7.3. **Arithmetic computation of $\#\mathbf{H}_\chi^{\rm ar}$ and $\#\mathscr{H}_\chi^{\rm ar}$ for $\chi \in \mathscr{X}^+$.** Using Leopoldt's formula [Leo1954, Satz 21, § 8 (4)] and Propositions 7.4, 7.6, we obtain (see [Gra1976, Théorème III.1]):

Proposition 7.9. *For all $\chi \in \mathscr{X}^+ \setminus \{1\}$, $\#\mathbf{H}_\chi^{\rm ar} = \frac{Q_\chi}{q_\chi} \cdot (\mathbf{E}_\chi : \mathbf{C}_\chi^{\Delta_\chi})$, where $\Delta_\chi = \prod_{\ell\mid g_\chi} \left(1 - \sigma_\chi^{g_\chi/\ell}\right)$.*

We get the relation $\#\mathbf{H}_\chi^{\rm ar} = \frac{1}{q_\chi}\left(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \oplus \mathbf{C}_\chi^{\Delta_\chi}\right)$ interpreting Q_χ [Gra1976, Corollaire III.1].

To interpret the coefficient q_χ, we have replaced the Leopoldt group $\mathbf{C}_\chi^{\Delta_\chi}$ of cyclotomic units by the larger group $\mathbf{F}_{K_\chi} := \mathbf{C}_{K_\chi} \cap \mathbf{E}_{K_\chi}$ deduced from $\mathbf{C}_{K_\chi}$; see the long proof [Gra1976, Chap. III, § 3] giving the final result interpreting the coefficient q_χ and giving the analog of Theorem 5.10 for the real class groups.

Let $\mathbf{E}_{K_\chi}$ be the group of absolute values of units of K_χ, $\mathbf{E}^0_{K_\chi}$ the subgroup of $\mathbf{E}_{K_\chi}$ generated by the $\mathbf{E}_k$ for all the subfields $k \subsetneq K$ (Definition 7.1) and let $\mathbf{F}_{K_\chi} = \mathbf{C}_{K_\chi} \cap \mathbf{E}_{K_\chi}$ (Definition 7.7).

Theorem 7.10. *Let $\chi \in \mathscr{X}^+ \setminus \{1\}$ and let $\mathbf{H}^{\rm ar}_\chi := \{x \in \mathbf{H}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}$. Let g_χ be the order of χ and f_χ its conductor. Then:*

$$\#\mathbf{H}^{\rm ar}_\chi = w_\chi \cdot \big(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \cdot \mathbf{F}_{K_\chi}\big) \quad \& \quad \#\mathscr{H}^{\rm ar}_\chi = w_\chi \cdot \big(\mathscr{E}_{K_\chi} : \mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi}\big),$$

where w_χ is defined as follows:

(i) Case g_χ non prime power. Then $w_\chi = 1$;

(ii) Case $g_\chi = p^n$, $p \neq 2$ prime, $n \geq 1$:

(ii′) Case $f_\chi = \ell^k$, ℓ prime, $k \geq 1$. Then $w_\chi = 1$;

(ii″) Case f_χ non prime power. Then $w_\chi = p$;

(iii) Case $g_\chi = 2^n$, $n \geq 1$:

(iii′) Case $f_\chi = \ell^k$, ℓ prime, $k \geq 1$. Then $w_\chi = 1$;

(iii″) Case f_χ non prime power. Then $w_\chi \in \{1, 2\}$.

Proof. For the ugly proof see [Gra1976, Théorème III.2, pp. 78–85]. □

Corollary 7.11. *In the semi-simple case $p \nmid g_\chi$, we obtain $\#\mathscr{H}_\chi = \big(\mathscr{E}_\chi : \mathscr{F}_\chi\big)$ and, conjecturally, $\#\mathscr{H}_\varphi = \big(\mathscr{E}_\varphi : \mathscr{F}_\varphi\big)$, where $\mathscr{E}_\chi$ (resp. $\mathscr{F}_\chi$) $= \{x \in \mathscr{E}_{K_\chi}$ (resp. $\mathscr{F}_{K_\chi}$), $P_\chi(\sigma_\chi) \cdot x = 1\}$.*

Proof. In the semi-simple case, for any $\mathbb{Z}_p[G_K]$-module $\mathscr{M}_K$, $\mathscr{M}_\chi = \mathscr{M}_K^{e_\chi}$, with the usual idempotent; thus, $\widetilde{\mathscr{E}}_\chi = \widetilde{\mathscr{E}}_\chi^{e_\chi} = \mathscr{E}_{K_\chi}^{e_\chi}/(\mathscr{E}^0_{K_\chi})^{e_\chi} \cdot \mathscr{F}_{K_\chi}^{e_\chi} = \mathscr{E}_\chi/\mathscr{F}_\chi$ since $(\mathscr{E}^0_{K_\chi})^{e_\chi} = 1$. □

Remarks 7.12. (i) This point of view, which appears to have been ignored, seems more convenient than formulas using Sinnott's cyclotomic units together with the $\mathscr{H}_\chi^{\rm alg}$, especially in the non semi-simple case. Indeed, compare with [Grei1992, Theorem 4.14] using instead $\mathscr{H}_\chi^{\rm alg}$ (only in the semi-simple context of the relations (3.4)) and Sinnott's cyclotomic units, more elaborate than classical Leopoldt's units (Definition 7.7), but which give rise to intricate index formulas. Moreover, as we have mentioned in [Gra1976/77, Remark III.1], an analytic formula for $\#\mathscr{H}_\chi^{\rm alg}$, $\chi \in \mathscr{X}^+$, does not seem obvious (if any) because of capitulation aspects (see the numerical examples of § 3.3). We hope that this theorem suggests a new statement of the Main Conjecture, especially in the non semi-simple case (see § 8.2).

(ii) We remark that $\widetilde{\mathbf{E}}_\chi := \mathbf{E}_{K_\chi}/\mathbf{E}^0_{K_\chi} \cdot \mathbf{F}_{K_\chi}$ and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi}$ are χ-objects since, for any non trivial norm, $\mathbf{N}_{K_\chi/k}(\mathbf{E}_{K_\chi}) \subseteq \mathbf{E}^0_{K_\chi}$ and $\mathbf{N}_{K_\chi/k}(\mathscr{E}_{K_\chi}) \subseteq \mathscr{E}^0_{K_\chi}$. Then $\widetilde{\mathscr{E}}_\chi = \bigoplus\limits_{\varphi|\chi} \widetilde{\mathscr{E}}_\varphi$, where the φ-components are (using the semi-simple idempotent e_φ):

$$\widetilde{\mathscr{E}}_\varphi = (\widetilde{\mathscr{E}}_\chi)^{e_\varphi} = \{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ \ P_\varphi \cdot \widetilde{x} = 1\};$$

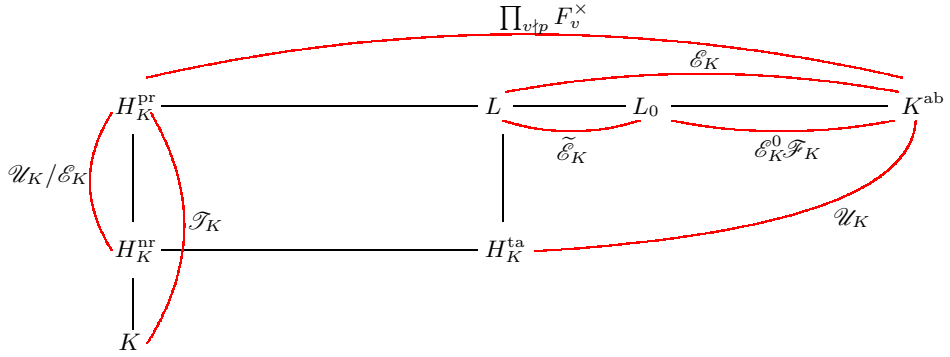
they are canonical with the classical Leopoldt definition of cyclotomic units, and independent of the problems raised by the splitting, in sub-extensions of K_χ, of ramified primes for Sinnott's cyclotomic units.

7.4. **Class field theory and regulators.** Let $K \in \mathscr{K}$ (denoting essentially a real field K_χ in what follows). To simplify the diagrams and the statements, we assume to be in the most common case where $\mathscr{W}_K = 1$ and $K \cap \mathbb{Q}^{\rm cyc} = \mathbb{Q}$, which gives the relations $\mathscr{T}_K = \mathscr{T}_K^{\rm bp}$ (Diagram of Section 6) and $\#\mathscr{T}_K \sim \prod_{\psi \in \mathscr{X}_K} \frac{1}{2}\, \mathbf{L}_p(1, \psi)$ (relation (6.2)).

The Galois group $\mathscr{T}_K$ may be compared with a "cyclotomic regulator" $\mathscr{R}_K^{\rm cyc}$ as follows.

For this purpose, the diagram of the maximal abelian pro-p-extension $K^{\rm ab}$ of K is necessary (from [Gra2005, III.4 (d) & Diagram III.4.4.1] with our present notations), where $H_K^{\rm ta}$ is the maximal tamely ramified abelian pro-p-extension of K and $F_v^\times$ the p-Sylow subgroup of the multiplicative group of the residue field of the tame place v; let L be the compositum $H_K^{\rm pr}H_K^{\rm ta}$.

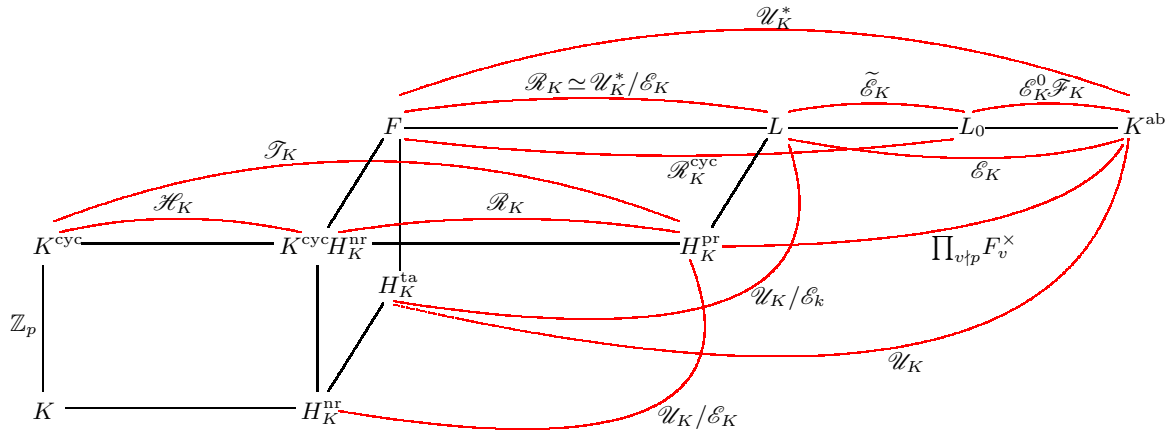
Class field theory interprets $\mathrm{Gal}(K^{\rm ab}/L)$ as the $\mathbb{Z}_p$-module $\mathscr{E}_K$ and $\mathrm{Gal}(K^{\rm ab}/H_K^{\rm ta})$ as the $\mathbb{Z}_p$-module $\mathscr{U}_K$ as follows:



We put $\mathscr{U}_K^* := \{u \in \mathscr{U}_K,\ \mathbf{N}_{K/\mathbb{Q}}(u) = \pm 1\}$; since K is real, $\mathscr{E}_K$ is of finite index in $\mathscr{U}_K^*$ and one has the relation $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{U}_K/\mathscr{E}_K) = \mathscr{U}_K^*/\mathscr{E}_K \simeq \mathscr{R}_K$ implying that F is fixed by $\mathscr{U}_K^*$ and that $F \cap H_K^{\rm pr} = K^{\rm cyc}H_K^{\rm nr}$ (recall, from [Gra2021a, § 2 & Figure 3], the exact sequence $1 \to \mathscr{R}_K^{\rm ram} \to \mathscr{R}_K \to \mathscr{R}_K^{\rm nr} \to 1$, so that a sub-extension of L/F may be unramified).

Which yields the more complete diagram, where F is the compositum of $H_K^{\rm ta}$ with $K^{\rm cyc}H_K^{\rm nr}$, and where we suppose that $K^{\rm cyc} \cap H_K^{\rm nr} = K$ to simplify; we have moreover:

$$\mathrm{Gal}(F/K^{\rm cyc}H_K^{\rm nr}) \simeq \mathrm{Gal}(H_K^{\rm ta}/H_K^{\rm nr}) \simeq \mathrm{Gal}(L/H_K^{\rm pr}) \simeq \big(\textstyle\prod_{v\nmid p}F_v^\times\big)/\mathscr{E}_K.$$



Define (under the assumptions $\mathscr{W}_K = 1$ and $K \cap \mathbb{Q}^{\rm cyc} = \mathbb{Q}$):

$$\mathscr{R}_K^{\rm cyc} := \mathrm{tor}_{\mathbb{Z}_p}(\mathscr{U}_K/\mathscr{E}_K^0\cdot\mathscr{F}_K) = \mathscr{U}_K^*/\mathscr{E}_K^0\cdot\mathscr{F}_K \simeq \log_p(\mathscr{U}_K^*)/\log_p(\mathscr{E}_K^0\cdot\mathscr{F}_K),$$

which yields, for $\chi \neq 1$, the $\mathbb{Z}_p[G_\chi]$-modules isomorphism:

$$\mathscr{R}_{K_\chi} \simeq \mathscr{R}_{K_\chi}^{\rm cyc}/\widetilde{\mathscr{E}}_\chi. \tag{7.2}$$

We then have $\mathscr{R}_K^{\rm cyc} = \mathrm{Gal}(L_0/F)$, where L_0 is the subfield of $K^{\rm ab}$ fixed by $\mathscr{E}_K^0\mathscr{F}_K$. For the Artin maps defining the above Galois pro-p-groups, see [Gra2005, § III.4.4.5.1]

Remarks 7.13. Let $\chi \in \mathscr{X}^+ \setminus \{1\}$ and assume to simplify that $\mathscr{W}_K = 1$, $w_\chi = 1$, $K \cap \mathbb{Q}^{\rm cyc} = \mathbb{Q}$ and $K^{\rm cyc} \cap H_K^{\rm nr} = K$.

(i) Theorem 7.10 and isomorphism (7.2) give:

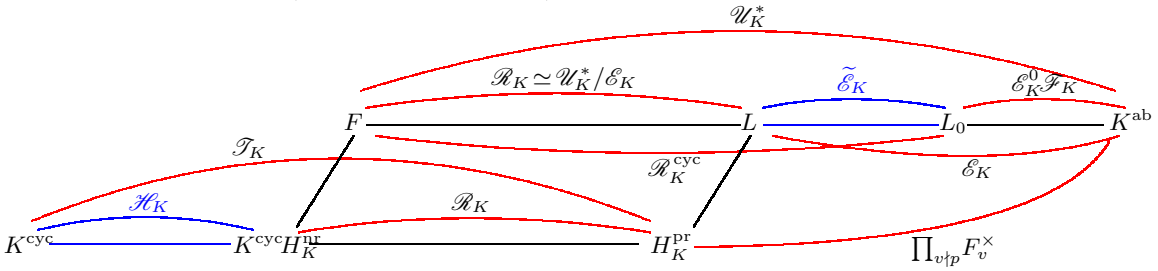
$$\#\mathscr{T}_\chi = \#\mathscr{R}_\chi^{\rm cyc} \quad \& \quad \#\widetilde{\mathscr{E}}_\chi = \frac{\#\mathscr{R}_{K_\chi}^{\rm cyc}}{\#\mathscr{R}_{K_\chi}} = \#\mathscr{H}_\chi^{\rm ar}.$$

Of course the $\mathscr{A}_\chi$-modules $\mathscr{T}_\chi$ and $\mathscr{R}_\chi^{\rm cyc}$ (resp. $\widetilde{\mathscr{E}}_\chi$ and $\mathscr{H}_\chi^{\rm ar}$) are not necessarily isomorphic and this is due essentially to the structure of $\mathscr{H}_\chi$ as shown by the following table giving only cyclic cubic fields K such that $\mathscr{R}_K$ is of maximal 7-rank 2 and $\mathscr{T}_K$ of 7-rank ≥ 3 implying $\mathscr{H}_K \neq 1$; give a short excerpt (no example of 7-rank ≥ 4 exists in the interval considered):

```
x^3+x^2-39666*x-2582719      Structure of the 7-torsion group: [7,7,7]
x^3+x^2-43300*x-3411104      Structure of the 7-torsion group: [49,7,7]
x^3+x^2-13226*x-508479       Structure of the 7-torsion group: [343,7,7]
x^3+x^2-427660*x-31551829    Structure of the 7-torsion group: [2401,7,7]
x^3+x^2-2033484*x-966131001  Structure of the 7-torsion group: [49,49,7]
```

(ii) By nature, the $\mathbb{Z}_p$-modules $\mathscr{R}_{K_\chi}$ and $\mathscr{R}_{K_\chi}^{\rm cyc}$ are of p-rank limited by $[K_\chi : \mathbb{Q}] - 1$ and the p-ranks of their φ-components, $\varphi \neq 1$, are less or equal to the order of the decomposition group of p in $\mathbb{Q}(\mu_{g_\chi})$.

(iii) The sub-diagram, given by the extension $K^{\rm ab}/K^{\rm cyc}$, opens perhaps an access way for an interpretation of the Main Conjecture for even characters in the non semi-simple case, or at least an annihilation theorem (see Conjecture 7.14) in the spirit of Thaine's theorem:



7.5. **Annihilation conjecture for real p-class groups.** Before any proof of the conjectural equality $\#\mathscr{H}_\varphi^{\rm ar} = \#\widetilde{\mathscr{E}}_\varphi = \#(\mathscr{E}_{K_\chi}/\mathscr{E}_{K_\chi}^0\cdot\mathscr{F}_{K_\chi})_\varphi$ (giving again the Main Theorem for $\varphi \in \Phi_K^+$), it will be interesting to prove that any annihilator of $\widetilde{\mathscr{E}}_\varphi$ annihilates $\mathscr{H}_\varphi^{\rm ar}$, which will be more precise than the annihilators of $\mathscr{T}_\varphi$ (see Theorem 6.3, Remarks 6.4, 7.13).

To our knowledge, the best known annihilation theorem of real p-class groups is Thaine's Theorem [Th1988], [Was1997, Theorem 15.2] saying that any annihilator of $\mathscr{E}_{K_\chi}/\mathscr{F}'_{K_\chi}$ (for a classical definition of the group of cyclotomic units $\mathscr{F}'_{K_\chi}$) is an annihilator of $\mathscr{H}_{K_\chi}$. But Thaine's Theorem only concerns the semi-simple case.

Mention also annihilation theorems by Solomon [Sol1992], which are not optimal because of vanishing of Euler factors; this is discussed in [Gra2018b].

Conjecture 7.14. *Let $\chi \in \mathscr{X}^+\backslash\{1\}$. Any element of $\mathbb{Z}[\mu_{g_\chi}]$, annihilating $\widetilde{\mathbf{E}}_\chi := \mathbf{E}_{K_\chi}/\mathbf{E}_{K_\chi}^0\cdot\mathbf{F}_{K_\chi}$, annihilates $\mathbf{H}_\chi^{\rm ar}$.*

For this, we will prove the following lemma, giving some prerequisites on the subject, and some numerical computations.

Lemma 7.15. *Let $\mathbf{M}_{K_\chi}$ be a torsion-free monogenic $\mathbb{Z}[G_\chi]$-module (i.e., $\mathbb{Z}$-free and $\mathbb{Z}[G_\chi]$-generated by a single element). Let $\mathbf{M}'_{K_\chi}$ be a sub-module of $\mathbf{M}_{K_\chi}$, such that $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$ is finite and annihilated by $P_\chi(\sigma_\chi)\,\mathbb{Z}[G_\chi]$. Then $(\mathscr{M}_{K_\chi}/\mathscr{M}'_{K_\chi})^{e_\varphi} := ((\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi})\otimes\mathbb{Z}_p)^{e_\varphi} \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{\lambda_\varphi}$ for all $\varphi \mid \chi$.*

Proof. By assumptions, $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$ is a finite monogenic $\mathbb{Z}[\mu_{g_\chi}]$-module, whence of the form $\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A}$, with a non-zero ideal $\mathfrak{A}$; so $\mathscr{M}_{K_\chi}/\mathscr{M}'_{K_\chi} \simeq (\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A})\otimes\mathbb{Z}_p$, giving:

$$\mathscr{M}_{K_\chi}/\mathscr{M}'_{K_\chi} \simeq \bigoplus\nolimits_{\varphi\mid\chi}\big[\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{\lambda_\varphi}\big],$$

with the usual correspondence between prime ideals $\mathfrak{p} \mid p$ and p-adic characters $\varphi \mid \chi$; whence the claim. □

It is well-known that there exists in $|E_{K_\chi}|$ a unit $|\varepsilon|$ generating, with its conjugates, a subgroup E of $|E_{K_\chi}|$ of prime-to-p finite index (Minkowski unit). Then $\mathbf{M} := \mathbb{Z}[G_\chi] \cdot |\varepsilon|$ is monogenic and torsion-free.

Let $\mathbf{M}'_{K_\chi} := \mathbf{E}^0_{K_\chi} \mathbf{F}_{K_\chi}$. Then, taking into account orders, monogenicity and the fact that $(P_\chi(\sigma_\chi))$ annihilates $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$, Lemma 7.15 is coherent with an annihilation theorem of the $\mathscr{H}_\varphi^{\mathrm{ar}}$'s since, from the results of § 7.4, $\mathscr{H}_\chi^{\mathrm{ar}}$ is a quotient of $\mathscr{R}_\chi^{\mathrm{cyc}}$.

Example 7.16. We consider, for $p = 7$, the cubic field $K = K_\chi$ of conductor $f = 2557$ defined by the polynomial $P = x^3 + x^2 - 852\,x + 9281$; then $\mathscr{H}_K \simeq \mathbb{Z}/7\mathbb{Z}$, $\mathscr{T}_K \simeq \mathbb{Z}/7^2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $\mathscr{E}_K/\mathscr{F}_K \simeq \mathbb{Z}[j]/(1-2j)\mathbb{Z}[j] \simeq \mathbb{Z}[j]/\mathfrak{p}$ for a prime $\mathfrak{p} \mid 7$.

The following program computes the annihilator $\mathbf{A}_K(c)$ of $\mathscr{T}_K$; it may be easily used for other examples, defining the three classes $\sigma^k \cdot \mathrm{Gal}(\mathbb{Q}(\mu_{fp^N})/K)$, $k = 0, 1, 2$, giving the annihilator $\mathbf{A}_K(c) = A_0 + A_1\sigma + A_2\sigma^2$, then $\beta := A_0 - A_2 + (A_1 - A_2)\,j$, yielding $\mathfrak{p}_1^u \cdot \mathfrak{p}_2^v$ in $\mathbb{Z}[\mu_3]$:

```
{p=7;f=2557;N=3;pN=p^N;fpN=f*pN;e=eulerphi(fpN);
g=znprimroot(f);lg=lift(Mod((1-lift(g))/f,pN));g=Mod(lift(g)+lg*f,fpN);g3=g^3;
G=znprimroot(pN);lG=lift(Mod((1-lift(G))/pN,f));G=Mod(lift(G)+lG*pN,fpN);
c=lift(znprimroot(f));cm=Mod(c,fpN)^-1;A0=0;A1=0;A2=0;
for(k=1,(f-1)/3,for(j=1,e,A=g3^k*G^j;gA=g*A;ggA=g^2*A;
a=lift(A);aa=lift(A*cm);la=(aa*c-a)/fpN;A0=A0+la*A^-1;
a=lift(gA);aa=lift(gA*cm);la=(aa*c-a)/fpN;A1=A1+la*A^-1;
a=lift(ggA);aa=lift(ggA*cm);la=(aa*c-a)/fpN;A2=A2+la*A^-1));
print(Mod(lift(A0),pN)," ",Mod(lift(A1),pN)," ",Mod(lift(A2),pN))}

Mod(51,343) Mod(203,343) Mod(195,343)
```

Modulo 7^3, one obtains $A_0 = 51$, $A_1 = 203$, $A_2 = 195$; since we can compute modulo the norm $1+\sigma+\sigma^2$, this yields for instance the ideal $(19+18j) = \mathfrak{p}^3$. Whence $\mathscr{T}_K \simeq \mathbb{Z}[j]/(1-2j)^3\mathbb{Z}[j]$ (as $\mathbb{Z}$-module, $\mathscr{T}_K$ is given by $\langle\,\overline{7}\,\rangle \oplus \langle\,\overline{31+j}\,\rangle$, whose components are of order 7^2 and 7, respectively). One verifies that $\mathscr{R}_K \simeq (1-2j)\mathbb{Z}[j]/(1-2j)^3\mathbb{Z}[j]$ and that $\mathscr{H}_K \simeq \mathbb{Z}[j]/(1-2j)\mathbb{Z}[j]$ is, indeed, annihilated by $(1-2j)$.

8. Invariants (Algebraic, Arithmetic, Analytic) – Main Conjecture

In the sequel, we fix an irreducible character $\chi \in \mathscr{X}$ (of order g_χ, of conductor f_χ). We apply the previous results to the families $\mathscr{H}_\varphi^{\mathrm{alg}}$, $\mathscr{H}_\varphi^{\mathrm{ar}}$ and $\mathscr{T}_\varphi$, for any $\varphi \mid \chi$, $\varphi \in \Phi$.

8.1. **Definitions of Algebraic and Arithmetic Invariants $m^{\mathrm{alg}}(\mathscr{M})$, $m^{\mathrm{ar}}(\mathscr{M})$.** Write simply that $\mathscr{H}_\varphi^{\mathrm{alg}}$, $\mathscr{H}_\varphi^{\mathrm{ar}}$ and $\mathscr{T}_\varphi^{\mathrm{ar}} = \mathscr{T}_\varphi^{\mathrm{alg}}$ are finite $\mathbb{Z}_p[\mu_{g_\chi}]$-modules whatever $\varphi \in \Phi = \Phi^+ \cup \Phi^-$; thus:

$$\mathscr{H}_\varphi^{\mathrm{alg}} \simeq \prod_{i\geq 1} \mathbb{Z}_p[\mu_{g_\chi}] \Big/ \mathfrak{p}_\varphi^{n_{\varphi,i}^{\mathrm{alg}}(\mathscr{H})},\ \mathscr{H}_\varphi^{\mathrm{ar}} \simeq \prod_{i\geq 1} \mathbb{Z}_p[\mu_{g_\chi}] \Big/ \mathfrak{p}_\varphi^{n_{\varphi,i}^{\mathrm{ar}}(\mathscr{H})},\ \mathscr{T}_\varphi \simeq \prod_{i\geq 1} \mathbb{Z}_p[\mu_{g_\chi}] \Big/ \mathfrak{p}_\varphi^{n_{\varphi,i}^{\mathrm{ar}}(\mathscr{T})},$$

where $\mathfrak{p}_\varphi$ is the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$, the $n_{\varphi,i}$ being decreasing integers up to 0. Put:

$$\begin{aligned} m_\varphi^{\mathrm{alg}}(\mathscr{H}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{alg}}(\mathscr{H}), \qquad & m_\chi^{\mathrm{alg}}(\mathscr{H}) &:= \sum_{\varphi\mid\chi} m_\varphi^{\mathrm{alg}}(\mathscr{H}), \\ m_\varphi^{\mathrm{ar}}(\mathscr{H}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{H}), \qquad & m_\chi^{\mathrm{ar}}(\mathscr{H}) &:= \sum_{\varphi\mid\chi} m_\varphi^{\mathrm{ar}}(\mathscr{H}), \\ m_\varphi^{\mathrm{ar}}(\mathscr{T}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{T}), \qquad & m_\chi^{\mathrm{ar}}(\mathscr{T}) &:= \sum_{\varphi\mid\chi} m_\varphi^{\mathrm{ar}}(\mathscr{T}). \end{aligned} \tag{8.1}$$

Whence the order formulas for $\varphi \in \Phi = \Phi^+ \cup \Phi^-$:

$$\#\mathscr{H}_\varphi^{\mathrm{alg}} = p^{\varphi(1)\, m_\varphi^{\mathrm{alg}}(\mathscr{H})}, \quad \#\mathscr{H}_\varphi^{\mathrm{ar}} = p^{\varphi(1)\, m_\varphi^{\mathrm{ar}}(\mathscr{H})}, \quad \#\mathscr{T}_\varphi = p^{\varphi(1)\, m_\varphi^{\mathrm{ar}}(\mathscr{T})}.$$

8.2. **Definitions of of Analytic Invariants $m^{\rm an}(\mathscr{M})$.** We may define, in view of the statement of the Main Conjecture, the following Analytic Invariants $m_\varphi^{\rm an}$, from the expressions given with rational characters, where $\mathrm{val}_p(\bullet)$ denote the usual p-adic valuation; the purpose is to satisfy the necessary relations implied by Theorems 3.15, 4.1 about arithmetic components:

$$\sum_{\varphi|\chi} m_\varphi^{\rm ar}(\mathscr{M}) = \sum_{\varphi|\chi} m_\varphi^{\rm an}(\mathscr{M}),$$

for any family $\mathscr{M} \in \{\mathscr{H}^-, \mathscr{H}^+, \mathscr{T}\}$ and any $\chi \in \mathscr{X}$ (cf. Theorems 5.10, 7.10, 6.2).

8.2.1. *Case $\varphi \in \Phi^-$ for class groups.* Here, Algebraic and Arithmetic Invariants coincide. The definitions given in [Gra1976, Gra1976/77, Gra1977] were:

(i) Case $p \neq 2$ (conjecture proven by Solomon [Sol1990, Theorem II.1]).

(i′) K_χ is not of the form $\mathbb{Q}(\mu_{p^n})$, $n \geq 1$; then:

$$m_\varphi^{\rm an}(\mathscr{H}^-) := \mathrm{val}_p\Big(\prod_{\psi|\varphi}\big(-\tfrac{1}{2}\mathbf{B}_1(\psi^{-1})\big)\Big),$$

(i″) $K_\chi = \mathbb{Q}(\mu_{p^n})$, $n \geq 1$; let $\psi = \omega^\lambda \cdot \psi_p$, ψ_p of order p^{n-1} (where ω is the Teichmüller character); then:

$$m_\varphi^{\rm an}(\mathscr{H}^-) := \mathrm{val}_p\Big(\prod_{\psi|\varphi}\big(-\tfrac{1}{2}\mathbf{B}_1(\psi^{-1})\big)\Big), \text{ if } \lambda \neq 1,$$
$$m_\varphi^{\rm an}(\mathscr{H}^-) := 0, \text{ if } \lambda = 1.$$

(ii) Case $p = 2$ (conjecture proven by Greither [Grei1992, Theorem B], when g_χ is not a 2-power and f_χ is odd).

(ii′) g_χ is not a 2-power; then:

$$m_\varphi^{\rm an}(\mathscr{H}^-) := \mathrm{val}_2\Big(\prod_{\psi|\varphi}\big(-\tfrac{1}{2}\mathbf{B}_1(\psi^{-1})\big)\Big).$$

(ii″) g_χ is a 2-power; then:

$$m_\varphi^{\rm an}(\mathscr{H}^-) := \mathrm{val}_2\Big(\prod_{\psi|\varphi}\big(-\tfrac{1}{2}\mathbf{B}_1(\psi^{-1})\big)\Big), \text{ if } K_\chi \neq \mathbb{Q}(\mu_4),$$
$$m_\varphi^{\rm an}(\mathscr{H}^-) := 0, \text{ if } K_\chi = \mathbb{Q}(\mu_4).$$

8.2.2. *Case $\varphi \in \Phi^+$, $\varphi \neq 1$, for class groups.* From Definition 7.7 and Theorem 7.10, we consider, for any cyclic field K, where we recall that $\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K$:

$$\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p, \quad \mathscr{E}_K^0 := \mathbf{E}_K^0 \otimes \mathbb{Z}_p, \quad \mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p, \quad \widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi} =: \bigoplus_{\varphi|\chi} \widetilde{\mathscr{E}}_\varphi,$$

where: $\widetilde{\mathscr{E}}_\varphi = \{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ P_\varphi(\sigma_\chi)\cdot\widetilde{x} = 1\} = \widetilde{\mathscr{E}}_\chi^{e_\varphi}$, in terms of the semi-simple idempotents of the algebra $\mathscr{A}_\chi := \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$. Since $\widetilde{\mathscr{E}}_\varphi$ is, for $\varphi \neq 1$, a free $\mathbb{Z}_p[\mu_{g_\chi}]$-modules of rank 1, we define $m_\varphi^{\rm an}(\mathscr{H}^+)$ by means of the relation:

$$\widetilde{\mathscr{E}}_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{m_\varphi^{\rm an}(\mathscr{H}^+)}, \quad m_\varphi^{\rm an}(\mathscr{H}^+) \geq 0.$$

Consider the relation $\#\mathscr{H}_\chi^{\rm ar} = w_\chi \cdot (\mathscr{E}_{K_\chi} : \mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi}) = w_\chi \prod_{\varphi|\chi} \#\widetilde{\mathscr{E}}_\varphi$ of Theorem 7.10; we remark that $w_\chi = p$ occurs only when g_χ is a p-power, in which case p is totally ramified in $\mathbb{Q}(\mu_{g_\chi})$ and $\varphi = \chi$ (which defines $w_\varphi = w_\chi$). So, we may define $m_\varphi^{\rm an}(\mathscr{H}^+)$ and w_φ as follows (the corresponding conjecture is proven by Greither [Grei1992, Theorem 4.14, Corollary 4.15], essentially in a semi-simple context (it is indeed that of the relations (3.4) which shall not give each $\#\mathscr{H}_\varphi^{\rm ar}$ compared with $\widetilde{\mathscr{E}}_\varphi$) and using Sinnott's definition of cyclotomic units):

(i) Case g_χ non prime power. Then $w_\varphi = 1$ and:

$$m_\varphi^{\rm an}(\mathscr{H}^+) := \mathrm{val}_p(\#\widetilde{\mathscr{E}}_\varphi).$$

(ii) Case $g_\chi = p^n$, $p \neq 2$ prime, $n \geq 1$:

(ii′) Case $f_\chi = \ell^k$, ℓ prime, $k \geq 1$. Then $w_\varphi = 1$ and :

$$m_\varphi^{\rm an}(\mathscr{H}^+) := \mathrm{val}_p(\#\widetilde{\mathscr{E}}_\varphi),$$

(ii″) Case f_χ non prime power. Then $w_\varphi = p$ and

$m_\varphi^{\rm an}(\mathscr{H}^+) := {\rm val}_p(\#\widetilde{\mathscr{E}}_\varphi) + 1$.

(iii) Case $g_\chi = 2^n$, $n \geq 1$:

(iii′) Case $f_\chi = \ell^k$, ℓ prime, $k \geq 1$. Then $w_\varphi = 1$ and:

$m_\varphi^{\rm an}(\mathscr{H}^+) := {\rm val}_p(\#\widetilde{\mathscr{E}}_\varphi)$,

(iii″) Case f_χ non prime power. Then $w_\varphi \in \{1, 2\}$ and:

$m_\varphi^{\rm an}(\mathscr{H}^+) \in \{{\rm val}_p(\#\widetilde{\mathscr{E}}_\varphi), {\rm val}_p(\#\widetilde{\mathscr{E}}_\varphi) + 1\}$.

8.2.3. *Case $\varphi \in \Phi^+$ for p-torsion groups.* From Theorem 6.2, we define $m_\varphi^{\rm an}(\mathscr{T})$ as follows (conjecture proven by Greither [Grei1992, Theorem C], when g_χ is not a 2-power):

(i) Case where g_χ and f_χ are not p-powers. Then:

$m_\varphi^{\rm an}(\mathscr{T}) := {\rm val}_p\Big(\prod_{\psi|\varphi} \frac{1}{2}\,\mathbf{L}_p(1, \psi)\Big)$.

(ii) Case where $g_\chi \neq 1$ and f_χ are p-powers. Then:

$m_\varphi^{\rm an}(\mathscr{T}) := {\rm val}_p\Big(\prod_{\psi|\varphi} \frac{1}{2}\,\mathbf{L}_p(1, \psi)\Big) + 1$.

8.3. **The Main Conjecture – Motivations and Statement.** The conjectures we have given in [Gra1976, Gra1976/77, Gra1977] where simply equality of Arithmetic and Analytic Invariants, due to numerical observations, Theorems 5.10, 6.2, 7.10, with the specific property of the p-adic characters given by Theorem 4.4, and the fact that counterexamples would introduce a curious gap between an elementary context (abelian characters) and a deep one (class field theory), a gap which is not in the general philosophy of algebraic number theory.

Moreover, the annihilation properties of Theorems 5.18, 5.19, 5.21, 6.3, enforce the conjectures as well as reflection theorems that were given, after the Leopoldt's Spiegelungsatz, in [Gra1998] or [Gra2005, Theorem II.5.4.5] giving a more suitable comparison, for instance between $\mathscr{H}_\varphi$ and $\mathscr{T}_{\omega\varphi^{-1}}$, $\varphi \in \Phi^-$, where ω is the Teichmüller character. See also [Or1981, Or1986] for similar informations and complements.

Conjecture 8.1. *For any abelian p-adic irreducible character $\varphi \in \Phi = \Phi^+ \cup \Phi^-$, we have:*

$$m_\varphi^{\rm ar}(\mathscr{H}^+) = m_\varphi^{\rm an}(\mathscr{H}^+)\ (\varphi \in \Phi^+), \quad m_\varphi^{\rm ar}(\mathscr{H}^-) = m_\varphi^{\rm an}(\mathscr{H}^-)\ (\varphi \in \Phi^-), \quad m_\varphi^{\rm ar}(\mathscr{T}) = m_\varphi^{\rm an}(\mathscr{T})\ (\varphi \in \Phi^+).$$

A main justification of such equalities comes from the easy Theorem 2.1 since, from the analytic Definitions 8.2 and the arithmetic expressions that we recall:

(i) Theorem 5.10 giving $\mathbf{H}_\chi^{\rm ar} = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi|\chi} \big(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$, for $\chi \in \mathscr{X}^-$,

(ii) Theorem 6.2 giving $\#\mathscr{T}_\chi = w_\chi^{\rm cyc} \cdot \prod_{\psi|\chi} \frac{1}{2}\,\mathbf{L}_p(1, \psi)$, for $\chi \in \mathscr{X}^+$,

(iii) Theorem 7.10 giving $\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot (\mathbf{E}_{K_\chi} : \mathbf{E}_{K_\chi}^0 \cdot \mathbf{F}_{K_\chi})$, for $\chi \in \mathscr{X}^+$,

we indeed satisfy, for any family $\mathscr{M} \in \{\mathscr{H}^-, \mathscr{H}^+, \mathscr{T}\}$, to the following equalities:

$$\sum_{\varphi|\chi} m_\varphi^{\rm ar}(\mathscr{M}) = \sum_{\varphi|\chi} m_\varphi^{\rm an}(\mathscr{M}).$$

Remark 8.2. It would remain the problem of giving the orders, $\#\mathscr{H}_\chi^{\rm alg}$ and $\#\mathscr{H}_\varphi^{\rm alg}$, for which no analytic formula does appear clearly in the non semi-simple real case; for instance, in Example 3.13 for $p = 3$, $\chi_i = \varphi_i$ $(i \in \{1, 2\})$ are the characters of the fields k_i of degrees 6 and 18, respectively, in the compositum K of $k_0 = \mathbb{Q}(\sqrt{4409})$ with the degree 9 field of conductor 19, one gets $\mathscr{H}_{\chi_i}^{\rm alg} \simeq \mathbb{Z}/3\mathbb{Z}$ while $\mathscr{H}_{\chi_i}^{\rm ar} = 1$, as predicted by the conjecture and checked numerically. In the Example 3.14, one finds $\mathscr{H}_{\chi_1}^{\rm alg} \simeq (\mathbb{Z}/3\mathbb{Z})^3$ while $\mathscr{H}_{\chi_1}^{\rm ar} \simeq (\mathbb{Z}/3\mathbb{Z})^2$.

8.4. **Finite Iwasawa's theory in p-cyclic extensions.** For more details and an application to classical Iwasawa's theory for real abelian fields, in the spirit of Greenberg's conjecture [Gree1976], see [Gra1976, Chap. IV]; nevertheless, *the results hold in arbitrary cyclic extensions.* As usual, considering an irreducible character $\chi \in \mathscr{X}^+$ and $\psi \mid \varphi \mid \chi$, we put $\psi = \psi_0 \cdot \psi_p$, ψ_0 of order g_0 prime to p and ψ_p of p-power order; then if $G_\chi = G_0 \times H$ in an obvious way, we denote by e_φ the semi-simple idempotents attached to $\mathbb{Z}_p[G_\chi]$, that is to say, $e_\varphi := \frac{1}{g_0} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\, \sigma$, for φ_0 above ψ_0.

To use the properties of $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi} = \oplus_{\varphi \mid \chi} \widetilde{\mathscr{E}}_\varphi$, we note that $(\mathscr{E}^0_{K_\chi})^{e_\varphi} \simeq \mathscr{E}^{e_\varphi}_{K_{\chi'}}$, giving $\widetilde{\mathscr{E}}_\varphi \simeq \mathscr{E}^{e_\varphi}_{K_\chi}/\mathscr{E}^{e_\varphi}_{K_{\chi'}} \cdot \mathscr{F}^{e_\varphi}_{K_\chi}$, then the isomorphism $\mathscr{E}^{e_\varphi}_{K_\chi}/\mathscr{E}^{e_\varphi}_{K_{\chi'}} \simeq \mathbb{Z}_p[\mu_{g_\chi}]$ (see [Gra1976, Lemma IV.1]), and the following principle:

Theorem 8.3. *Let $\chi \in \mathscr{X}^+$ be such that $g_\chi = g_0 \cdot p^n$, $p \nmid g_0$, $n \geq 2$. Let χ' (resp. χ'') be the rational character such that $[K_\chi : K_{\chi'}] = [K_{\chi'} : K_{\chi''}] = p$; to simplify, set $K := K_\chi$, $K' := K_{\chi'}$, $K'' := K_{\chi''}$. Assume that $\mathbf{N}_{K/K'}(\mathscr{F}_K) = \mathscr{F}_{K'}$.*[2] *Let $\mathfrak{p}_\varphi$ be the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$; put:*

$$\mathscr{F}^{e_\varphi}_K/\mathscr{F}^{e_\varphi}_K \cap \mathscr{E}^{e_\varphi}_{K'} \simeq \mathfrak{p}^A_\varphi, \quad A \geq 0;$$

in the isomorphism $\mathscr{E}^{e_\varphi}_{K'}/\mathscr{E}^{e_\varphi}_{K''} \simeq \mathbb{Z}_p[\mu_{g_\chi/p}]$, put:

$$\mathscr{F}^{e_\varphi}_{K'}/\mathscr{F}^{e_\varphi}_{K'} \cap \mathscr{E}^{e_\varphi}_{K''} \simeq \mathfrak{p}^a_{\varphi'} \simeq \mathfrak{p}^{pa}_\varphi, \ a \geq 0 \quad \& \quad \mathbf{N}_{K/K'}(\mathscr{E}^{e_\varphi}_K)/\mathbf{N}_{K/K'}(\mathscr{E}^{e_\varphi}_K) \cap \mathscr{E}^{e_\varphi}_{K''} \simeq \mathfrak{p}^b_{\varphi'} \simeq \mathfrak{p}^{p\,b}_\varphi, \ b \geq 0.$$

(i) If $a < p^{n-2}(p-1)$, then $A = a - b$.

(ii) If $a \geq p^{n-2}(p-1)$, then $A \geq p^{n-2}(p-1) - b$.

Theorem 8.4. *Let $\chi \in \mathscr{X}^-$ be such that $g_\chi = g_0 \cdot p^n$, $p \nmid g_0$, $n \geq 2$. Let χ' be the rational character such that $[K_\chi : K_{\chi'}] = p$ and put $K := K_\chi$, $K' := K_{\chi'}$. Assume that the Stickelberger elements $\mathbf{B}_K$, $\mathbf{B}_{K'}$ are p-integers in $\mathbb{Z}_p[G_K]$ and that $\mathbf{N}_{K/K'}(\mathbf{B}_K) = \mathbf{B}_{K'}$ (see Footnote 2). Put:*

$$\mathbf{B}_1(\psi^{-1})\mathbb{Z}_p[\mu_{g_\chi}] = \mathfrak{p}^A_\varphi, \ A \geq 0 \quad \& \quad \mathbf{B}_1(\psi^{-p})\mathbb{Z}_p[\mu_{g_\chi/p}] = \mathfrak{p}^{p\,a}_\varphi, \ a \geq 0.$$

(i) If $a < p^{n-2}(p-1)$, then $A = a$.

(ii) If $a \geq p^{n-2}(p-1)$, then $A \geq p^{n-2}(p-1)$.

This allows to prove again Iwasawa's formula in the case $\mu = 0$ [Gra1976, Theorems IV.1, IV.2, Remark IV.4] and gives an algorithm to study the p-class groups in the first layers.

To simplify, let k be a real base field such that $G_0 := G_k$ is of prime-to-p order, and let $k^{\rm cyc} = \bigcup_{n \geq 0} k_n$ be its cyclotomic $\mathbb{Z}_p$-extension. The condition $\mu = 0$ of Iwasawa's theory is here equivalent to the existence (for all the semi-simple component defined by the characters of G_0) of n (corresponding to a character χ_{n+1} of order $g_0\, p^{n+1}$) such that $a_n < p^{n-2}(p-1)$ (case (i) of the Theorem 8.3); then the sequence $\#\mathscr{H}_{\chi_n}$ becomes constant giving the λ-invariant and the relation $\mathscr{E}_{k_n} = \mathbf{N}_{k_{n+1}/k_n}(\mathscr{E}_{k_{n+1}}) \cdot \mathscr{E}_{k_{n-1}}$ for $n \gg 0$; we then have $p^\lambda = (\mathscr{E}_{k_n} : \mathscr{E}^0_{k_n}\, \mathscr{F}_{k_n})$ for $n \gg 0$. More precisely we have (with obvious notations) $p^{\lambda_\varphi} = (\mathscr{E}^{e_\varphi}_{k_n} : \mathscr{E}^{e_\varphi}_{k_{n-1}}\, \mathscr{F}^{e_\varphi}_{k_n})$ for $n \gg 0$.

This methodology does exist in terms of p-adic **L**-functions for real and imaginary abelian fields (see [Gra1978/79a, Chap. V]).

Recall that Greenberg's conjecture [Gree1976] for a totally real base field (i.e., $\lambda = \mu = 0$) is equivalent to the property that the norms $\mathbf{N}_{k_m/k_n} : \mathscr{H}_{k_m} \longrightarrow \mathscr{H}_{k_n}$, $m \geq n \gg 0$ are isomorphisms (see other equivalent conditions in [Gra2019, Corollary 3.4]).

Corollary 8.5. *In an analytic context, Greenberg's conjecture is equivalent to $\mathscr{E}_{k_n} = \mathscr{E}^0_{k_n} \cdot \mathscr{F}_{k_n}$ for all $n \gg 0$ (cf. Definitions 7.1 and 7.7 yielding $\mathscr{E}^0_{k_n}$ and the group $\mathscr{F}_{k_n}$ of Leopoldt cyclotomic units computed from the field $\mathbb{Q}(\mu_{f_n})$, where f_n is the conductor of k_n).*

[2] See Lemma 5.17 giving the ramification conditions. In particular, it is the case when K and K' have the same set of ramified places, whence in the cyclotomic $\mathbb{Z}_p$-extension of a real number field k of prime-to-p degree.

9. Numerical illustrations with cyclic cubic fields

For $\chi \in \mathscr{X}^+$ and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi}$, we have $\#\mathscr{H}^{\rm ar}_\chi = w_\chi \cdot \#\widetilde{\mathscr{E}}_\chi$ (Theorem 7.10), and for any $\varphi \mid \chi$ we have, conjecturally, $\#\mathscr{H}^{\rm ar}_\varphi = w_\varphi\, \#\widetilde{\mathscr{E}}_\varphi$, $w_\varphi \in \{1, p\}$, $\widetilde{\mathscr{E}}_\varphi = \{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ \ P_\varphi \cdot \widetilde{x} = 1\}$, and:

$$\widetilde{\mathscr{E}}_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{m^{\rm an}_\varphi(\mathscr{H})},\ m^{\rm an}_\varphi(\mathscr{H}) \geq 0, \qquad \mathscr{H}^{\rm ar}_\varphi \simeq \bigoplus_{i=1}^{r_\varphi} \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{m^{\rm ar}_{\varphi,i}(\mathscr{H})},\ m^{\rm ar}_{\varphi,i}(\mathscr{H}) \geq 0,$$

for a decreasing sequence $(m^{\rm ar}_{\varphi,i}(\mathscr{H}))_i$ giving $m^{\rm an}_\varphi(\mathscr{H}) = \sum_{i=1}^{r_\varphi} m^{\rm ar}_{\varphi,i}(\mathscr{H})$ to be compared with $m^{\rm ar}_\varphi(\mathscr{H})$.

We intend to see more precisely what happens for these analytic and arithmetic invariants since the above equality defining $m^{\rm an}_\varphi(\mathscr{H})$ can be fulfilled in various ways. We will examine the case of the cyclic cubic fields $K = K_\chi$ for primes $p \equiv 1 \pmod 3$ giving two p-adic characters $\varphi \mid \chi$; in that case, $\mathscr{E}^0_K = 1$ and $\#\mathscr{H}^{\rm ar}_\varphi = (\mathscr{E}_K : \mathscr{F}_K)$.

For example, for $p = 7$, the possible structures, for the $\mathbb{Z}[j]$-module $\mathbf{E}_K/\mathbf{F}_K$, are of the form $\mathbb{Z}[j]/\big[(-2+j)^{m_1} \cdot (3+j)^{m_2} \cdot \mathfrak{a}\big]$, ($m_1, m_2 \geq 0$ and $\mathfrak{a}$ prime to 7), giving the two φ-components $\mathbb{Z}_7[j]/(-2+j)^{m_1}$ and $\mathbb{Z}_7[j]/(3+j)^{m_2}$ for the $\widetilde{\mathscr{E}}_\varphi$'s.

9.1. **Description of the computations.** The part of the PARI [Pari2016] program computing all the cyclic cubic fields is that given in [Gra2019, § 6.1].

A crucial fact, without which the checking of the φ-components of the G_K-modules $\mathscr{E}_K/\mathscr{F}_K$ and $\mathscr{H}_K$ could be misleading, is the definition of a generator σ of G_K giving the correct conjugation, both for the fundamental units, the cyclotomic ones and the elements of the class group; this is not so easy even if a conjugation does exist for the data given by $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P})$ from the explicit instructions $\mathsf{G} = \mathsf{nfgaloisconj}(\mathsf{P})$, giving x^σ under the form $g(x)$, $g \in \mathbb{Q}[X]$, for a root x of the defining polynomial P, and $\mathsf{nfgaloisapply}$ acting on any PARI object.

Thus it is not too difficult to find, from $\mathsf{K.fu}$ giving a $\mathbb{Z}$-basis of E_K, a "Minkowski unit" ε and its conjugate ε^σ such that $\langle \varepsilon, \varepsilon^\sigma \rangle_{\mathbb{Z}} = E_K$; indeed, for the numerical evaluation of $\varepsilon(x)$ and $\varepsilon(g(x))$, at a root $\rho \in \mathbb{R}$ of P, we only have a set $\{\rho_1, \rho_2, \rho_3\}$ given in a random order by $\mathsf{polroot}(\mathsf{P})$. Any change of root gives an inconsequential permutation $(\varepsilon, \varepsilon^\sigma) \mapsto (\varepsilon^\tau, \varepsilon^{\tau\sigma})$, $\tau \in G_K$.

For security, we test $\mathsf{Reg_1}/\mathsf{Reg} = 1$ where $\mathsf{Reg_1}$ is the regulator computed with the root ρ and where $\mathsf{Reg} = \mathsf{K.reg}$ is the true regulator given by PARI.

Then we must write the Leopoldt cyclotomic unit η of K of conductor f (Definition 7.7) under the form $\eta = \varepsilon^{\alpha + \beta\,\sigma}$, $\alpha, \beta \in \mathbb{Z}$, which is easy as soon as we have η and η^σ. But η is computed by means of the analytic expression of $|\mathbf{C}| = \prod_{a \in [1, f/2[,\, \sigma_{a|_K} = 1} |\zeta_{2f}^a - \zeta_{2f}^{-a}|$, as product of the $|\zeta_{2f}^a - \zeta_{2f}^{-a}|$ for the prime-to-f integers $a < f/2$ such that the Artin symbol $\sigma_a = \big(\frac{Q(\mu_f)/\mathbb{Q}}{a}\big)$ is in G_K (which is tested using a prime $q_a \equiv a \pmod f$ giving $\sigma_{a|_K} = 1$ if and only if q_a splits in K).

If f is prime, $\zeta_{2f} - \zeta_{2f}^{-1}$ generates the prime ideal above p; thus, $\pi := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\zeta_{2f} - \zeta_{2f}^{-1}) = \pm\mathbf{C}^2$ is such that $\pi^3 = f \cdot \eta'$, $\eta' \in \mathbf{E}_K$, whence $\pi^{3\,(1-\sigma)} = \eta'^{1-\sigma} = \eta^6 := (\mathbf{C}^{1-\sigma})^6$ (Proposition 7.9); the program computes $3\log(\mathbf{C}) - \frac{1}{2}\log(f)$ so that we must divide the regulator RegC by 3 and multiply $\alpha + j\,\beta$ by $\frac{1-j}{3}$ in that case.

If f is composite, we have $\eta = \mathbf{C}$ obtained via the half-system and the class number is the product of the index of units by $w_\chi = 3$ (Theorem 7.10), so this appear in the results (e.g., for the first example $f = 13 \cdot 97$, $P = x^3 + x^2 - 420x - 1728$, $\mathsf{classgroup} = [21]$ and $\mathsf{Index}\ [\mathsf{E_K} : \mathsf{C_K}] = 7$, but $\alpha + j\,\beta = -3 - 2j$ of norm 7; for $f = 3^2 \cdot 307$, $P = x^3 - 921x - 10745$, $\mathsf{classgroup} = [21, 3]$ and $\mathsf{Index}\ [\mathsf{E_K} : \mathsf{C_K}] = 21$, but $\alpha + j\,\beta = -5 - j$ of norm 21).

To define the correct conjugation $\zeta_{2f} \mapsto \zeta_{2f}^\sigma =: \zeta_{2f}^q$, for some prime q, we use the fundamental property of Frobenius automorphisms giving $y^{{\rm Frob}(q)} \equiv y^q \pmod q$, for any integer y of K, if q is inert in $K/\mathbb{Q}$; using $x^\sigma = g(x)$, we test the congruence $g(x) - x^q \pmod q$ to decide if $\sigma = {\rm Frob}(q)$ or ${\rm Frob}(q)^2$, in which case $\zeta_{2f}^\sigma = \zeta_{2f}^q$ or $\zeta_{2f}^{q^2}$, giving easily the conjugate η^σ.

9.2. **The general PARI program.** The program is the following and we explain, with some examples, how to use the numerical results checking the Main Conjecture (of course, now, the Main Theorem); hmin = p^{vp} means that the program only computes fields with p-class groups CKp of order at least p^{vp}, and bf, Bf define an interval for the conductors f.

Other indications are given in the text of the program (if necessary, the program can be copy and past at https://www.dropbox.com/s/k6v3bh6z957bdy9/Program.tex?dl=0):

```
\p 50
{p=7; \\ Take any prime p congruent to 1 modulo 3
bf=2;Bf=10^6;hmin=p^2;
\\ Arithmetic of Q(j), j^2+j+1=0:
S=y^2+y+1;kappa=bnfinit(S);Y=idealfactor(kappa,p);
P1=component(Y,1)[1];P2=component(Y,1)[2]; \\ Decomposition (p)=P1*P2 in Z[j]
\\ Iteration over the conductors f in [bf,Bf]:
for(f=bf,Bf,vf=valuation(f,3);if(vf!=0 & vf!=2,next);
F=f/3^vf;if(core(F)!=F,next);F=factor(F);Div=component(F,1);
d=matsize(F)[1];for(j=1,d,D=Div[j];if(Mod(D,3)!=1,break));
\\ Computation of solutions a and b such that f=(a^2+27*b^2)/4:
\\ Iteration over b, then over a:
for(b=1,sqrt(4*f/27),if(vf==2 & Mod(b,3)==0,next);A=4*f-27*b^2;
if(issquare(A,&a)==1,
\\ computation of the corresponding defining polynomial P:
if(vf==0,if(Mod(a,3)==1,a=-a);P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);
if(vf==2,if(Mod(a,9)==3,a=-a);P=x^3-f/3*x-f*a/27);
K=bnfinit(P,1); \\ PARI definition of the cubic field K
\\ Test on the p-class number #CKp regarding hmin:
if(Mod(K.no,hmin)==0,print();
G=nfgaloisconj(P); \\ Definition of the Galois group G
\\ Frob = Artin symbol defining the PARI generator sigma=G[2]:
forprime(q=2,10^4,if(Mod(f,q)==0,next);
Pq=factor(P+O(q));if(matsize(Pq)[1]==1,Frob=q;break));X=x^Frob-G[2];
if(valuation(norm(Mod(X,P)),Frob)==0,Frob=lift(Mod(Frob^2,f)));
E=K.fu;Reg=K.reg; \\ Group of units, Regulator
\\ We certify that a suitable PARI unit is a Z[G]-generator of E_K:
E1=lift(E[1]);E2=lift(nfgaloisapply(K,G[2],E[1]));
Root=polroots(P);Rho=real(Root[1]); \\  Selecting a root of P
e1= abs(polcoeff(E1,0)+polcoeff(E1,1)*Rho+polcoeff(E1,2)*Rho^2);
e2= abs(polcoeff(E2,0)+polcoeff(E2,1)*Rho+polcoeff(E2,2)*Rho^2);
l1=log(e1);l2=log(e2);Reg1=l1^2+l1*l2+l2^2;quot=Reg1/Reg;
print(quot); \\ This quotient must be equal to 1
\\ Computation of the cyclotomic units C1,C2=sigma(C1):
z=exp(I*Pi/f);C1=1;C2=1;
\\ Case of a prime conductor f using (Z/fZ)^* cyclic):
if(isprime(f)==1,g=znprimroot(f)^3;
\\ Description of a half-system:
for(k=1,(f-1)/6,gk=lift(g^k);sgk=lift(Mod(gk*Frob,f));
C1=C1*(z^gk-z^-gk);C2=C2*(z^sgk-z^-sgk));
L1=3*log(abs(C1))-log(f)/2;L2=3*log(abs(C2))-log(f)/2; \\ Logarithms of C1,C2
\\ computation of the cyclotomic regulator and of the index Quot=(E:F):
RegC=L1^2+L1*L2+L2^2;Quot=1/3*RegC/Reg); \\ Division by 3 of RegC
\\ Case of a composite conductor:
if(isprime(f)==0,for(aa=1,(f-1)/2,if(gcd(aa,f)!=1,next);
\\ Search of a prime qa congruent to a modulo f, split in K:
qa=aa;while(isprime(qa)==0,qa=qa+f);if(matsize(idealfactor(K,qa))[1]==1,next);
\\ The Artin symbol of aa fixes K:
C1=C1*(z^aa-z^-aa);C2=C2*(z^(Frob*aa)-z^-(Frob*aa)));
L1=log(abs(C1));L2=log(abs(C2)); \\ Logarithms of C1,C2
\\ computation of the cyclotomic regulator and of the index Quot=(E:F):
RegC=L1^2+L1*L2+L2^2;Quot=RegC/Reg);
\\ printing of the basic data of K:
print("P=",P," f=",f,"=",factor(f)," (a,b)=","(",a,",",b")",
" class group=",K.cyc,"  sigma=",Frob);print("Index [E_K:C_K]=",Quot);
\\ Annihilator alpha+sigma.beta of the quotient E/C:
```

```
alpha=((log(e1)+log(e2))*L1+log(e2)*L2)/Reg;beta=(log(e2)*L1-log(e1)*L2)/Reg;
if(isprime(f)==1, \\ In the prime case one multiply alpha+j.beta by (1-j)/3
alpha0=(alpha+beta)/3;beta0=(-alpha+2*beta)/3;alpha=alpha0;beta=beta0);
\\ Writing of alpha and beta as reals for checking:
print("(alpha,beta)=","(",alpha,", ",beta,")");
\\ Computation of alpha and beta as integers:
alpha=sign(alpha)*floor(abs(alpha)+10^-6);beta=sign(beta)*floor(abs(beta)+10^-6);
\\ Class group structure (r = global rank;rp = p-rang;expo = exposant of CKp)
\\ vp = valuations of CKp, ve = valuation of the exponent expo of CKp:
CK=K.clgp;r=matsize(CK[2])[2];CKp=List;EKp=List;rp=0;vp=0;ve=0;for(i=1,r,
ei=CK[2][i];vi=valuation(ei,p);if(vi>0,rp=rp+1;vp=vp+vi;ve=max(ve,vi));expo=p^ve;
\\ The rp following ideals Ai generate the p-class group CKp:
Ai=idealpow(K,CK[3][i],ei/p^vi);listput(CKp,Ai,i);listput(EKp,p^vi,i));
\\ Computation of the matrices h and sh of Ai and sAi on the PARI basis of CK
L0=List;for(i=1,r,listput(L0,0,i));LH=List;LsH=List;
for(i=1,rp,Ai=CKp[i];h=bnfisprincipal(K,Ai)[1];
sAi=nfgaloisapply(K,G[2],Ai);sh=bnfisprincipal(K,sAi)[1];
print("h=",h,", ","sigma(h)=",sh);listput(LH,h,i);listput(LsH,sh,i));
\\ Determination of the Pi-valuations of (alpha+j.beta), i=1,2:
Z=Mod(alpha+y*beta,S);w1=idealval(kappa,Z,P1);w2=idealval(kappa,Z,P2);
print(w1,"  ",w2,"  P1 and P2-valuations for alpha+j*beta");
\\ Galois structure of CKp; computation of the phi-components:
if(rp==1,
u=lift(LsH[1][1]*Mod(LH[1][1],expo)^-1);
YY=Mod(y-u,S);v1=idealval(kappa,YY,P1);v2=idealval(kappa,YY,P2);
v1=min(v1,ve);v2=min(v2,ve);print(v1,"  ",v2,"  P1 and P2-valuations for H"));
if(rp==2,
\\ Computation of ci(mod expo) such that Pi=(ci+j),i=1,2 (phi-annihilators):
Sp=lift(factor(S+O(p^ve)));Sp1=component(Sp,1)[1];Sp2=component(Sp,1)[2];
c1=polcoeff(Sp1,0);c2=polcoeff(Sp2,0);
\\ Coefficients of the classes LH[1],LsH[1],LH[2],LsH[2], on the PARI basis of CK
H1=LH[1];A1=H1[1];B1=H1[2];sH1=LsH[1];C1=sH1[1];D1=sH1[2];
H2=LH[2];A2=H2[1];B2=H2[2];sH2=LsH[2];C2=sH2[1];D2=sH2[2];
\\ Computation of the determinants of the relations:
Delta1=((C1+c1*A1)*(D2+c1*B2)-(D1+c1*B1)*(C2+c1*A2));Delta1=lift(Mod(Delta1,expo));
Delta2=((C1+c2*A1)*(D2+c2*B2)-(D1+c2*B1)*(C2+c2*A2));Delta2=lift(Mod(Delta2,expo));
print(Delta1,"  ",Delta2,"   Determinants: Delta1,Delta2");
\\ Computation of the relations defining the phi-components:
r11x=C1+c1*A1;r11y=C2+c1*A2;
r12x=D1+c1*B1;r12y=D2+c1*B2;
r11x=lift(Mod(r11x,expo));r11y=lift(Mod(r11y,expo));
r12x=lift(Mod(r12x,expo));r12y=lift(Mod(r12y,expo));
r21x=C1+c2*A1;r21y=C2+c2*A2;
r22x=D1+c2*B1;r22y=D2+c2*B2;
r21x=lift(Mod(r21x,expo));r21y=lift(Mod(r21y,expo));
r22x=lift(Mod(r22x,expo));r22y=lift(Mod(r22y,expo));
print("R11=",r11x,"*X+",r11y,"*Y","  R12=",r12x,"*X+",r12y,"*Y");
print("R21=",r21x,"*X+",r21y,"*Y","  R22=",r22x,"*X+",r22y,"*Y"));
\\ Structure of the torsion group Tp of p-ramification:
n=6; \\ Choose any n, large enough, such that p^(n+1) annihilates Tp:
LTp=List;Kpn=bnrinit(K,p^n);Hpn=Kpn.cyc;dim=component(matsize(Hpn),2);
for(k=2,dim,c=component(Hpn,k);if(Mod(c,p)==0,listput(LTp,p^valuation(c,p),k)));
print("Structure of the ",p,"-torsion group: ",LTp)))))}
```

9.3. **Numerical examples.** Since the approximations are in general very good (with precision \p 50), we have suppressed useless decimals in the numerical results for integers computed and given as real numbers. But for some conductors, the precision \p 100 may be necessary, because of a fundamental unit close to 0 (e.g., $f = 21193, 30223$). For $f = 42667$, \p 100 does not compute correctly and \p 150 gives a nice result for α and β; but we see that, for this example,

```
e_1=3062171948818717694.348000505806    &    e_2=1.221295564694 E-69,
```

which explains what happens.

Note that, according to the PARI version used, numerical data for generators of class groups may vary and propagate in some computations, but without any trouble for final results.

9.3.1. *Galois structure of $\mathscr{E}_K/\mathscr{F}_K$.* Let ε be the $\mathbb{Z}[G]$-generator of $\mathbf{E}_K$ and let η that of the subgroup $\mathbf{F}_K$ of Leopoldt's cyclotomic units; thus we have $\eta = \varepsilon^{\alpha+\beta\,\sigma}$ and obtain the isomorphism:

$$\mathbf{E}_K/\mathbf{F}_K \simeq \mathbb{Z}[j]/(\alpha + j\,\beta)\mathbb{Z}[j],$$

where j is root of $\mathsf{S} := \mathsf{y}^2 + \mathsf{y} + 1$.

In all the sequel, from a factorization $p = (r_1 + j\,r_1')\cdot(r_2 + j\,r_2') =: \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[j]$, we associate, for the exponent p^e, the two annihilators $c_i + \sigma$ such that $(c_i + j) = \mathfrak{p}_i^e$ (up to a prime-to-p ideal); this preserves the definition of the φ_1 and φ_2-components. For instance, for $p = 7$, $\mathfrak{p}_1 := (-2+j)\mathbb{Z}[j]$ and $\mathfrak{p}_2 := (3 + j)\mathbb{Z}[j]$; writing $(\alpha + j\,\beta) =: \mathfrak{p}_1^u \cdot \mathfrak{p}_2^v \cdot \mathfrak{a}$, $\mathfrak{a}$ prime to 7, we get immediately the two φ-components of $\mathscr{E}_K/\mathscr{F}_K$ (e.g., if $e = 2$, the two annihilators are $19+j$ and $-18+j$, respectively; for $p = 13$, we get $23 + j$ and $-22 + j$).

9.3.2. *Galois structure of $\mathscr{H}_K$.* Recall that the instruction $\mathsf{bnfisprincipal(K, Ideal)[1]}$ gives the matrix of components, of the class of Ideal, on the basis $\{h_1, \ldots, h_r\}$ given by $\mathsf{K.clgp}$ (in CK) and the fact that $\mathsf{0}$ at the place i means that the corresponding component of $\mathsf{cl(Ideal)}$ on h_i is trivial.

We first replace the PARI basis of $\mathbf{H}_K$ by a basis $\{h_1, \ldots, h_{r_p}\}$ of $\mathscr{H}_K$ (where $r_p \le r$ is the p-rank). The Galois action on the h_i is computed using the instructions:

$$\mathsf{h = bnfisprincipal(K, Ai)[1]; sAi = nfgaloisapply(K, G[2], Ai); sh = bnfisprincipal(K, sAi)[1];}$$

where $\mathsf{G[2]}$ gives the σ-conjugate; so the Galois structure of $\mathscr{H}_K$ becomes linear algebra from the matrices given by the program, via the relations $h = \prod_{i=1}^{r_p} h_i^{a_i}$ (in h) and $h^\sigma = \prod_{i=1}^{r_p} h_i^{b_i}$ (in sh).

(a) **Case of 7-rank** $r_7 = 1$. This case is obvious, writing $h = h_1^a$, $h^\sigma = h_1^b$; we write $P_{\varphi_1} \equiv c_1 + y \pmod{7^e}$ and $P_{\varphi_2} \equiv c_2 + y \pmod{7^e}$, where 7^e is the exponent of $\mathscr{H}_K$; we obtain $h^{c_1+\sigma} = h_1^{c_1 a + b}$ and $h^{c_2+\sigma} = h_1^{c_2 a + b}$; so $\mathscr{H}_K = \mathscr{H}_{\varphi_1}$ (resp. $\mathscr{H}_{\varphi_2}$) if and only if $c_1 a + b \equiv 0 \pmod{7^e}$ (resp. $c_2 a + b \equiv 0 \pmod{7^e}$). In fact the program computes $-a^* b + j$, where a^* is inverse of a modulo 7^e, and write $(-a^* b + j) = \mathfrak{p}_i^u$ for the suitable $i \in \{1, 2\}$.

The Galois actions are to be read in columns; for instance, the valuations:

$$\mathsf{v \quad 0 \qquad P1\ and\ P2 - valuations\ for\ alpha + j * beta\ (resp.\ H)}$$

in a line gives the structures $\mathbb{Z}[j]/\mathfrak{p}_1^v \cdot \mathfrak{p}_2^0$ for "$\mathscr{M} = \mathscr{E}/\mathscr{F}$ (resp. $\mathscr{H}$)", whence $\mathscr{M}_{\varphi_1} \simeq \mathbb{Z}[j]/\mathfrak{p}_1^v$, $\mathscr{M}_{\varphi_2} = 1$, and so on.

Denote by $\widetilde{\mathscr{E}}$ the family $\mathscr{E}/\mathscr{F}$. The first examples with $r_7 = 1$ are:

```
P=x^3+x^2-104*x+371  f=313=Mat([313,1])  (a,b)=(35,1)
Class group=[7]  sigma=4
(alpha,beta)=(-3.000000000000,-2.000000000000), Index [E_K:C_K]=7.000000000000
h=[1]~,  sigma(h)=[2]~
1  0    P1 and P2-valuations for alpha+j*beta
1  0    P1 and P2-valuations for  H
Structure of the 7-torsion group: List([7,7])
```

We have $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathscr{H}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_1 \simeq \mathbb{F}_7$ and the conjugation $h^\sigma = h^2$, giving the annihilator $(-2 + j) = \mathfrak{p}_1$ as expected; whence the two columns given by the program. We deduce that $\mathscr{T}_K = \mathscr{H}_K \bigoplus \mathscr{R}_K$.

```
P=x^3+x^2-2450*x-1089  f=7351=Mat([7351,1])  (a,b)=(-1,33)
Class group=[49]  sigma=4
(alpha,beta)=(5.000000000000,8.000000000000), Index [E_K:C_K]=49.000000000000
h=[1]~,  sigma(h)=[30]~
2  0    P1 and P2-valuations for alpha+j*beta
2  0    P1 and P2-valuations for  H
Structure of the 7-torsion group: List([2401])
```

We have $(\alpha+j\,\beta)=(5+8j)$, thus the annihilator $(19+j)=\mathfrak{p}_1^2$; then $h^\sigma=h^{30}$ gives (modulo 7^2) the same annihilator. The two φ_2-components are of course trivial.

Since $\mathscr{T}_K\simeq\mathbb{Z}/7^4\mathbb{Z}$, we deduce $\mathscr{R}_K=\mathscr{T}_K^{7^2}$ and $\mathscr{H}_K\simeq\mathscr{T}_K/\mathscr{R}_K\simeq\mathbb{Z}/7^2\mathbb{Z}$.

The first field such that $\mathscr{H}_K\simeq\mathbb{Z}/7^3\mathbb{Z}$ is the following:

```
P=x^3+x^2-77006*x-34225  f=231019=Mat([231019,1])  (a,b)=(-1,185)
Class group=[343]  sigma=4
(alpha,beta)=(19.000000000000,18.000000000000), Index [E_K:C_K]=343.000000000000
h=[1]~,  sigma(h)=[18]~
0  3   P1 and P2-valuations for alpha+j*beta
0  3   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([343,7])
```

The annihilator of $\mathscr{H}_K$ is $(-18+j)=\mathfrak{p}_2^3$. The structures are similar with the φ_2-components since $(19+18j)=\mathfrak{p}_2^3$. In that case, $\mathscr{T}_K=\mathscr{H}_K\bigoplus\mathscr{R}_K$ with $\mathscr{H}_K\simeq\mathbb{Z}/7^3\mathbb{Z}$ and $\mathscr{R}_K\simeq\mathbb{Z}/7\mathbb{Z}$.

(b) **Case of 7-rank** $r_7=2$ This case depends on the matrices giving the data:

$$\mathsf{h}=[\mathsf{a},\mathsf{b}],\ \mathsf{sigma}(\mathsf{h})=[\mathsf{c},\mathsf{d}]\quad\&\quad\mathsf{h}'=[\mathsf{a}',\mathsf{b}'],\ \mathsf{sigma}(\mathsf{h}')=[\mathsf{c}',\mathsf{d}'];$$

this means that the corresponding generating classes h, h', fulfill the relations (regarding the basis $\{h_1,h_2\}$ of the class group) $h=h_1^a\cdot h_2^b$ and $h^\sigma=h_1^c\cdot h_2^d$, then $h'=h_1^{a'}\cdot h_2^{b'}$ and $h^\sigma=h_1^{c'}\cdot h_2^{d'}$. Thus we compute the conditions $H^{c_i+\sigma}=1$, $i=1,2$, for $H:=h^x\cdot h'^y$; this gives the relations R11, R21 of the program (the relations R12, R22 are checked by security since they must be proportional to the previous ones); whence the arrangement of lines when the conjecture holds. The program computes the corresponding determinants of the relation (Determinants Delta1 Delta2); this is superfluous but have been computed (but not printed) for verification.

```
P=x^3+x^2-3422*x-1521  f=10267=Mat([10267,1])  (a,b)=(-1,39)
Class group=[7,7]  sigma=2
(alpha,beta)=(-7.000000000000,-7.000000000000), Index [E_K:C_K]=49.000000000000
h=[1,0]~, sigma(h)=[0,1]~
h=[0,1]~, sigma(h)=[6,6]~
1  1   P1 and P2-valuations for alpha+j*beta
R11=3*X+6*Y  R12=1*X+2*Y
R21=5*X+6*Y  R22=1*X+4*Y
Structure of the 7-torsion group: List([49,7])
```

This case means that $\widetilde{\mathscr{E}}_K\simeq\mathbb{Z}[j]/(7)$, giving the two non trivial φ-components of order 7.

The relations, for $\mathscr{H}_K$, reduce to $\mathsf{R11}=3*\mathsf{X}+6*\mathsf{Y}$ and $\mathsf{R21}=5*\mathsf{X}+6*\mathsf{Y}$. Thus $\mathscr{H}_K=\mathscr{H}_{\varphi_1}\cdot\mathscr{H}_{\varphi_2}\simeq\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$. Since $\mathscr{T}_K\simeq\mathbb{Z}/7^2\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$, $\mathscr{R}_K\simeq\mathbb{Z}/7\mathbb{Z}$, and $\mathscr{R}_K=\mathscr{T}_K^7$.

```
P=x^3+x^2-55296*x-1996812  f=165889=[19,1;8731,1]  (a,b)=(-322,144)
Class group=[294,2,2,2] sigma=25
(alpha,beta)=(-32.000000000000,-20.000000000000), Index [E_K:C_K]=784.000000000000
h=[6,0,0,0]~, sigma(h)=[108,1,0,0]~
0  2   P1 and P2-valuations for alpha+j*beta
0  2   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([49])
```

Here $\mathscr{R}_K=1$ and $\mathscr{T}_K=\mathscr{H}_K\simeq\mathbb{Z}_7[j]/\mathfrak{p}_2^2$.

```
P=x^3+x^2-453576*x+117425873  f=1360729=Mat([1360729,1])  (a,b)=(2333,1)
Class group=[98,14]  sigma=2
(alpha,beta)=(42.000000000000,28.000000000000), Index [E_K:C_K]=1372.000000000000
h=[1,0]~, sigma(h)=[44,11]~
h=[0,1]~, sigma(h)=[7,11]~
2  1   P1 and P2-valuations for alpha+j*beta
R11=14*X+7*Y  R12=11*X+30*Y
R21=26*X+7*Y  R22=11*X+42*Y
Structure of the 7-torsion group: List([49,7,7])
```

We have $(\alpha+\beta j)=2\cdot 7(3+2j)$ giving the annihilator $\mathfrak{p}_1^2\mathfrak{p}_2$ which is also the annihilator of $\mathscr{H}_K$. The structure is $\mathscr{T}_K=\mathscr{H}_K\bigoplus\mathscr{R}_K$.

```
P=x^3+x^2-884540*x-393129  f=2653621=Mat([2653621,1])  (a,b)=(-1,627)
Class group=[686,14]  sigma=2
(alpha,beta)=(-112.000000000000,-70.000000000000), Index [E_K:C_K]=9604.000000000000
h=[2,0]~, sigma(h)=[36,2]~
h=[0,2]~,  sigma(h)=[0,4]~
1    3   P1 and P2-valuations for alpha+j*beta
R11=74*X+0*Y  R12=2*X+42*Y
R21=0*X+0*Y  R22=2*X+311*Y
Structure of the 7-torsion group: List([343,49])
```

In that case, $\mathscr{T}_K\simeq Z/7^3\mathbb{Z}\times\mathbb{Z}/7^2\mathbb{Z}$ and $\mathscr{R}_K\simeq(\mathbb{Z}/7^3\mathbb{Z})^0\times(7\,\mathbb{Z}/7^2\mathbb{Z})$ in an obvious meaning.

(c) **Larger 7-ranks**. If the order 7^3, with 7-rank 1 or 2, is rather frequent for the 7-class group, we find, after several days of computer, only three examples of 7-rank 3 in the interval $f\in[7,50071423]$; they are obtained with the conductors $f=14376321,39368623,43367263$, giving interesting structures (use precision \p 100).

The least field with 7-rank 3 is the following:

```
P=x^3-4792107*x+4022175142  f=14376321=[3,2;1597369,1]  (a,b)=(-7554,128)
Class group=[21,7,7]  sigma=5
(alpha,beta)=(-7.000000000000,-21.000000000000), Index [E_K:C_K]=343.000000000000
h =[3,0,0]~, sigma(h) =[15, 4, 0]~
h'=[0,1,0]~, sigma(h')=[3, 1, 0]~
h"=[0,0,1]~, sigma(h")=[6, 5, 2]~
2   1   P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([7,7,7])
```

The ideals generating the 3 independent classes are given by K.clgp:

```
[12, [6, 2], [[5, 3, 2; 0, 1, 0; 0, 0, 1], [25, 20, 23; 0, 5, 4; 0, 0, 1]]]
```

Using the above information giving α and β, we obtain, for $\widetilde{\mathscr{E}}_K=\mathscr{E}_K/\mathscr{F}_K$:

$$\widetilde{\mathscr{E}}_K\simeq(\mathbb{Z}[j]/7\cdot(3+2j))\otimes\mathbb{Z}_7\simeq(\mathbb{Z}[j]/\mathfrak{p}_1^2\,\mathfrak{p}_2)\otimes\mathbb{Z}_7\simeq\mathbb{Z}_7[j]/\mathfrak{p}_1^2\oplus\mathbb{Z}_7[j]/\mathfrak{p}_2,$$

where $\mathfrak{p}_1=(-2+j)$ and $\mathfrak{p}_2=(3+j)$. Using the annihilators $19+\sigma\pmod{7^2}$ and $31+\sigma\pmod{7^2}$, we get the φ-components $\widetilde{\mathscr{E}}_{\varphi_1}\simeq\mathbb{Z}_7[j]/\mathfrak{p}_1^2$ and $\widetilde{\mathscr{E}}_{\varphi_2}\simeq\mathbb{Z}_7[j]/\mathfrak{p}_2$.

To obtain the two φ-components of $\mathscr{H}_K=\mathscr{T}_K$, we put $H=h^xh'^yh''^z$ and we determine the solutions of the two relations$H^{P_{\varphi_i}(\sigma)}=1$, that is to say, $H^{-2+\sigma}=1$ and $H^{3+\sigma}=1$. We then obtain the systems (considered modulo 7 since the exponent of $\mathscr{H}_K$ is 7):

$$\begin{cases}2x+3y-z=0\\4x-y+5z=0\end{cases}\text{ expressing }H^{-2+\sigma}=1\quad\&\quad\begin{cases}3x+3y+6z=0\\4x+4y+5z=0\\z=0,\end{cases}\text{ expressing }H^{3+\sigma}=1.$$

Since the first system is of rank 1 and the second one of rank 2, they are equivalent to:

$$2x+3y-z=0\ (\text{for }H^{-2+\sigma}=1)\quad\&\quad x+y=0\ \&\ z=0\ (\text{for }H^{3+\sigma}=1).$$

Which gives, considering the $\mathbb{F}_7$-dimensions given by the systems:

$$\mathscr{H}_{\varphi_1}\simeq\mathbb{Z}_7[j]/\mathfrak{p}_1\times\mathbb{Z}_7[j]/\mathfrak{p}_1\quad\&\quad\mathscr{H}_{\varphi_1}\simeq\mathbb{Z}_7[j]/\mathfrak{p}_2.$$

We have indeed equalities for the orders of the φ-components relative to $\widetilde{\mathscr{E}}_K$ and $\mathscr{H}_K$, respectively, but of course with different structures of $\mathbb{Z}_7[j]$-modules since we obtain $\widetilde{\mathscr{E}}_{\varphi_1}\simeq\mathbb{Z}_7[j]/\mathfrak{p}_1^2$.

The two other examples are similar and the analysis is left to the reader:

```
P=x^3+x^2-13122874*x-7765825411  f=39368623=[7,1;79,1;71191,1]  (a,b)=(-5323,2187)
class group=[21,21,7]   sigma=4
(alpha,beta)=(28.000000000000,-7.000000000000)  Index [E_K:C_K]=1029.000000000000
h =[3,0,0]~, sigma(h) =[3,9,0]~
h'=[0,3,0]~,  sigma(h')=[18,15,0]~
```

```
h"=[0,0,1]~,  sigma(h")=[15,6,4]~
1   2  P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([7,7,7])
```

```
P=x^3+x^2-14455754*x-16977480367  f=43367263=[43,1;1008541,1]  (a,b)=(-10567,1513)
class group=[273,7,7]  sigma=2
(alpha,beta)=(42.000000000000,77.000000000000)  Index [E_K:C_K]=4459.000000000000
h =[39,0,0]~, sigma(h) =[0,5,1]~
h'=[0,1,0]~,   sigma(h')=[156,6,5]~
h"=[0,0,1]~,   sigma(h")=[0,0,2]~
2   1  P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([49,7,7])
```

(d) **Larger primes** p. Let's give, without comments, some examples for $p = 13, 19, 31$:

```
p=13
P=x^3+x^2-15196*x-726047  f=45589=Mat([45589,1])  (a,b)=(-427,1)
Class group=[169]  sigma=2
(alpha,beta)=(15.000000000000,8.000000000000), Index [E_K:C_K]=169.000000000000
h=[1]~, sigma(h)=[146]~
2  0   P1 and P2-valuations for alpha+j*beta
2  0   P1 and P2-valuations for  H
Structure of the 13-torsion group: List([169])
```

```
P=x^3+x^2-65862*x-6527689  f=197587=[13,1;15199,1]  (a,b)=(-889,1)
Class group=[507]  sigma=4
(alpha,beta)=(7.000000000000,15.000000000000), Index [E_K:C_K]=169.000000000000
h=[3]~, sigma(h)=[66]~
0  2   P1 and P2-valuations for alpha+j*beta
0  2   P1 and P2-valuations for  H
Structure of the 13-torsion group: List([169])
```

```
P=x^3+x^2-186520*x-18424064  f=559561=Mat([559561,1])  (a,b)=(-886,232)
Class group=[13,13]  sigma=3
(alpha,beta)=(1.108047223073 E-68,13.000000000000), Index [E_K:C_K]=169.000000000000
h=[1,0]~, sigma(h)=[3,0]~
h=[0,1]~, sigma(h)=[8,9]~
1  1   P1 and P2-valuations for alpha+j*beta
R11=7*X+8*Y  R12=0*X+0*Y
R21=0*X+8*Y  R22=0*X+6*Y
Structure of the 13-torsion group: List([13,13])
```

```
P=x^3+x^2-238516*x-7579519  f=715549=Mat([715549,1])  (a,b)=(-283,321)
Class group=[13,13]  sigma=2
(alpha,beta)=(7.000000000000,-8.000000000000), Index [E_K:C_K]=169.000000000000
h=[1,0]~, sigma(h)=[9,0]~
h=[0,1]~,  sigma(h)=[0,9]~
0  2   P1 and P2-valuations for alpha+j*beta
R11=0*X+0*Y  R12=0*X+0*Y
R21=6*X+0*Y  R22=0*X+6*Y
Structure of the 13-torsion group: List([13,13])

p=19
P=x^3-137271*x+45757  f=411813=[3,2;45757,1]  (a,b)=(-3,247)
Class group=[1083]  sigma=2
(alpha,beta)=(-21.000000000000,-5.000000000000) Index [E_K:C_K]=361.000000000000
h=[3]~, sigma(h)=[204]~
0  2   P1 and P2-valuations for alpha+j*beta
0  2   P1 and P2-valuations for  H
Structure of the 19-torsion group: List([361])

P=x^3+x^2-162636*x+25190561  f=487909=[31,1;15739,1]  (a,b)=(1397,1)
Class group=[57,19]  sigma=2
(alpha,beta)=(19.000000000000,4.195145162776 E-69) Index [E_K:C_K]=361.000000000000
h=[3,0]~, sigma(h)=[51,16]~
h=[0,1]~,  sigma(h)=[3,1]~
1  1   P1 and P2-valuations for alpha+j*beta
```

```
R11=18*X+3*Y  R12=16*X+9*Y
R21=11*X+3*Y  R22=16*X+13*Y
Structure of the 19-torsion group: List([19,19])

p=31
P=x^3+x^2-63804*x+6181931  f=191413=Mat([191413,1])  (a,b)=(875,1)
class group=[31,31]  sigma=4
(alpha,beta)=(31.000000000000,-4.108428504342 E-69)  Index [E_K:C_K]=961.000000000000
h=[1,0]~,   sigma(h) =[30,30]~
h'=[0,1]~, sigma(h')=[1,0]~
1  1  P1 and P2-valuations for alpha+j*beta
R11=5*X+1*Y  R12=30*X+6*Y
R21=25*X+1*Y  R22=30*X+26*Y
Structure of the 31-torsion group: List([31,31])

P=x^3+x^2-76004*x-8090239  f=228013=Mat([228013,1])  (a,b)=(-955,1)
class group=[961]  sigma=2
(alpha,beta)=(-11.000000000000,-35.000000000000)  Index [E_K:C_K]=961.000000000000
h=[1]~, sigma(h)=[439]~
2  0  P1 and P2-valuations for alpha+j*beta
2  0  P1 and P2-valuations for H
Structure of the 31-torsion group: List([961])
```

The above program for cyclic cubic fields may be used to make statistics about the repartition of the various structures of class groups $\mathscr{H}_\varphi$ and quotients $\widetilde{\mathscr{E}}_\varphi = (\mathscr{E}_K/\mathscr{F}_K)^{e_\varphi}$, $\varphi \in \{\varphi_1, \varphi_2\}$.

Some probabilistic approaches, taking into account the relations between these invariants, due to the Main Theorem, may confirm (or not) the classical Cohen–Lenstra–Malle–Martinet heuristics on p-class groups; indeed, heuristics on the p-class groups must be equivalent to heuristics on the quotients $\widetilde{\mathscr{E}}_\varphi$. We left this as a question, as well as *a proof of the Main Conjecture in the non semi-simple real case* using the statement with arithmetic φ-objects, especially to prove that for all $\chi \in \mathscr{X}^+$ (where $w_\varphi \in \{1, p\}$ is defined § 8.2.2):

$$\#\mathscr{H}_\varphi = w_\varphi \cdot \#(\mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi}\mathscr{F}_{K_\chi})^{e_\varphi}, \text{ for all } \varphi \mid \chi.$$

References

[Gra1976] G. Gras, Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, Publications Mathématiques de Besançon. Algèbre et théorie des nombres, vol. 2 (1976), article no. 1, 99 pp. 2, 4, 24, 25, 26, 29, 30, 34, 35, 36
https://doi.org/10.5802/pmb.a-10

[Gra1976/77] G. Gras, Étude d'invariants relatifs aux groupes des classes des corps abéliens, Journées Arithmétiques de Caen (1976), Astérisque (1977), no. 41-42, 19 pp. 2, 4, 30, 34, 35
http://www.numdam.org/item/?id=AST_1977__41-42__35_0

Original references (1976)

[Coa1975] J. Coates, p-adic L-functions and Iwasawa's theory, Durham symposium in algebraic number theory, Sept. 1975. 4, 24, 27
https://dokumen.pub/p-adic-l-functions-and-iwasawas-theory.html

[Gil1975] R. Gillard, Relations de Stickelberger, Séminaire de théorie des nombres de Grenoble, Tome 4 (1974-1975), Exposé no. 1, 10 pp. 24
http://www.numdam.org/item/?id=STNG_1974-1975__4__A1_0

[Has1952] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin (1952). 20, 21, 23, 24, 29

[Iwa1962a] K. Iwasawa, A class number formula for cyclotomic fields, Ann. of Math., Second Series **76**(1) (1962), 171–179. 24
https://doi.org/10.2307/1970270

[Leo1954] H.W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsche Akad. Wiss. Berlin, Math. **2** (1954), 47 pp. 4, 5, 14, 15, 19, 23, 28, 29

[Leo1962] H.W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, Jour, für die reine und ang. Math. **209** (1962), 54–71. 4, 14, 24, 29

[KL1964] T. Kubota und H.W. Leopoldt, Eine p-adische Theorie der Zetawerte I, Jour, für die reine und ang. Math. **214/215** (1964), 328–339. 27
http://eudml.org/doc/150624

[Or1975a] B. Oriat, Quelques caractères utiles en arithmétique, Publications Mathématiques de Besançon (1975), no. 4, 27 pp. 4, 16, 29
https://doi.org/10.5802/pmb.a-4

[Or1975b] B. Oriat, Sur l'article de Leopoldt "Über Einheintengruppe und Klassenzahl reeller abelscher Zahlkörper", Publications Mathématiques de Besançon (1975), no. 5, 35 pp. 4, 23, 28, 29
https://doi.org/10.5802/pmb.a-5

[Ser1998] J.-P. Serre, *Représentations linéaires des groupes finis*, cinquième édition corrigée et augmentée de nouveaux exercices, Coll. Méthodes, Hermann 1998. 7

Additional references (2021/2022)

[AF1972] Y. Amice, J. Fresnel, Fonctions zêta p-adiques des corps de nombres abéliens réels, Acta Arithmetica, **20**(4) (1972), 353–384. http://matwbn.icm.edu.pl/ksiazki/aa/aa20/aa2043.pdf 27

[All2013] T. All, On p-adic annihilators of real ideal classes, J. Number Theory **133**(7) (2013), 2324–2338. 3, 24
https://doi.org/10.1016/j.jnt.2012.12.013

[All2017] T. All, Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups, Acta Arithmetica **178** (2017), 273–299. 3, 24
https://doi.org/10.4064/aa8537-2-2017

[BBDS2021] D. Bullach, D. Burns, A. Daoud, S. Seo, Dirichlet L-series at $s = 0$ and the scarcity of Euler systems (2021). 3
https://arxiv.org/abs/2111.14689

[BelMar2014] J-R. Belliard, A. Martin, Annihilation of real classes (2014), 10 pp. 3
http://jrbelliard.perso.math.cnrs.fr/BM1.pdf

[BelNg2005] J-R. Belliard, T. Nguyen Quang Do, On modified circular units and annihilation of real classes, Nagoya Math. J. **177** (2005), 77–115. 3
https://doi.org/10.1017/S0027763000009065

[BP1972] F. Bertrandias, J-J. Payan, Γ-extensions et invariants cyclotomiques, Ann. Sci. Ec. Norm. Sup. 4e série, **5**(4) (1972), 517–548. https://doi.org/10.24033/asens.1236

[CoLi2019] J. Coates, Y. Li, Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication II (2019). 3
https://arxiv.org/pdf/1904.05756

[CoLi2020] J. Coates, Y. Li, Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication, Proceedings of the London Math. Soc. **121**(6) (2020), 1531–1578. 3
https://doi.org/10.1112/plms.12379

[CS2006] J. Coates, R. Sujatha, *Cyclotomic Fields and Zeta Values*, Springer 2006. 3
https://doi.org/10.1007/978-3-540-33069-1_6

[Fre1965] J. Fresnel, Nombres de Bernoulli et fonctions L p-adiques, Séminaire Delange–Pisot–Poitou (Théorie des nombres) **7**(2) (1965-1966), Exposé no. 14, 1–15. 4
http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A3_0

[Gil1977] R. Gillard, Sur le groupe des classes des extensions abéliennes réelles, Séminaire Delange-Pisot-Poitou (Théorie des nombres) **18**(1) (1976-1977), Exposé no. 10, 6 pp. 3
http://www.numdam.org/item/SDPP_1976-1977__18_1_A8_0/

[GreiKuč2020] C. Greither, R. Kučera, Washington units, semispecial units, and annihilation of class groups, manuscripta mathematica **166** (2021), 277–286. 24
https://doi.org/10.1007/s00229-020-01241-y

[Gra1977] G. Gras, Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Annales de l'Institut Fourier **27**(1) (1977), 1–66. 3, 4, 34, 35
https://doi.org/10.5802/aif.641

[Gra1978] G. Gras, Sommes de Gauss sur les corps finis, Publications Mathématiques de Besançon. Algèbre et théorie des nombres (1978), no. 1, article no. 2, 72 pp. 24, 27
https://doi.org/10.5802/pmb.a-16

[Gra1978/79a] G. Gras, Sur la construction des fonctions L p-adiques abéliennes, Séminaire Delange–Pisot–Poitou (Théorie des nombres) **20**(2) (1978–1979), Exposé no. 22, 1–20. 4, 27, 36
http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A1_0

[Gra1978/79b] G. Gras, Sur l'annulation en 2 des classes relatives des corps abéliens, C.R. Math. Rep. Acad. Sci. Canada **1**(2) (1979), 107–110. 26, 27
https://mr.math.ca/article/sur-lannulation-en-2-des-classes-relatives-des-corps-abeliens/

[Gra1979] G. Gras, Annulation du groupe des ℓ-classes généralisées d'une extension abélienne réelle de degré premier à ℓ, Annales de l'institut Fourier **29**(1) (1979), 15–32. 3
http://www.numdam.org/item?id=AIF_1979__29_1_15_0

[Gra1998] G. Gras, Théorèmes de réflexion, J. Théorie Nombres Bordeaux **10**(2) (1998), 399–499. 35
http://www.numdam.org/item/JTNB_1998__10_2_399_0/

[Gra2005] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). 4, 27, 31, 35

[Gra2016] G. Gras, Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, Canadian Journal of Mathematics **68**(3) (2016), 571–624. 4
https://doi.org/10.4153/CJM-2015-026-3; english translation: https://arxiv.org/abs/1701.02618

[Gra2018a] G. Gras, The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator, Int. J. of Number Theory **14**(2) (2018), 329–337. 4, 27
https://doi.org/10.1142/S1793042118500203

[Gra2018b] G. Gras, Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{G}_{K,S}^{\mathrm{ab}})$ for real abelian extensions $K/\mathbb{Q}$, Communications in Advanced Mathematical Sciences **1**(1) (2018), 5–34. 3, 28, 32
https://dergipark.org.tr/tr/download/article-file/543993

[Gra2019] G. Gras, Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem, Math. Comp. **88**(318) (2019), 1929–1965. 4, 27, 36, 37
https://doi.org/10.1090/mcom/3395

[Gra2021a] G. Gras, Algorithmic complexity of Greenberg's conjecture, Arch. Math. **117** (2021), 277–289. 31
https://doi.org/10.1007/s00013-021-01618-9

[Gra2021b] G. Gras, On the λ-stability of p-class groups along cyclic p-towers of a number field (preprint 2021). https://arxiv.org/abs/2103.01565 11

[Gree1975] R. Greenberg, On p-adic L-functions and cyclotomic fields, Nagoya Mathematical Journal **56** (1975), 61–77. 3, 4
https://doi.org/10.1017/S002776300001638X

[Gree1977] R. Greenberg, On p-adic L-functions and cyclotomic fields. II, Nagoya Mathematical Journal **67** (1977), 139–158. 3, 4
https://doi.org/10.1017/S0027763000022583

[Gree1976] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98**(1) (1976), 263–284. 36
https://doi.org/10.2307/2373625

[Grei1992] C. Greither, Class groups of abelian fields, and the main conjecture, Annales de l'Institut Fourier **42**(3) (1992), 449–499. 3, 4, 11, 30, 34, 35
https://doi.org/10.5802/aif.1299

[Iwa1964b] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan **16**(1) (1964), 42–82. 4
https://doi.org/10.2969/jmsj/01610042

[Jau1981] J-F. Jaulent, Unités et classes dans les extensions métabéliennes de degré $n\ell^s$ sur un corps de nombres algébriques, Annales de l'Institut Fourier **31**(1) (1981), pp. 39–62. 3
https://doi.org/10.5802/aif.816

[Jau1984] J-F. Jaulent, Représentations ℓ-adiques et invariants cyclotomiques, Publications Mathématiques de Besançon. Algèbre et théorie des nombres (1984), no. 3, 41 p. 3
https://doi.org/10.5802/pmb.a-39

[Jau1986] J-F. Jaulent, L'arithmétique des ℓ-extensions (Thèse d'état), Publications Mathématiques de Besançon (1986), vol. 1, no. 1, 1–357. 3, 4
https://doi.org/10.5802/pmb.a-42

[Jau1990] J-F. Jaulent, La théorie de Kummer et le K_2 des corps de nombres, J. Théorie Nombres Bordeaux **2**(2) (1990), 377–411. http://www.numdam.org/item/?id=JTNB_1990__2_2_377_0 27

[Jau1998] J-F. Jaulent, Théorie ℓ-adique globale du corps de classes, J. Théorie Nombres Bordeaux **10**(2) (1998), 355–397. 4
https://doi.org/10.5802/jtnb.233

[Kol2007] V.A. Kolyvagin, *Euler Systems*. In: Cartier P., Katz N.M., Manin Y.I., Illusie L., Laumon G., Ribet K.A. (eds), The Grothendieck Festschrift. Modern Birkhäuser Classics. Birkhäuser, Boston, MA. 3
https://doi.org/10.1007/978-0-8176-4575-5_11

[Lec2018] E. Lecouturier, On the Galois structure of the class group of certain Kummer extensions, J. London Math. Soc. **98**(1) (2018), 35–58. https://doi.org/10.1112/jlms.12123 3

[Lang1990] S. Lang, *Cyclotomic fields I and II*, Graduate Texts in Mathematics **121**, With an appendix by Karl Rubin (Combined 2nd ed.), Berlin, New York, Springer–Verlag. 3
https://link.springer.com/content/pdf/bbm%3A978-1-4612-0987-4%2F1.pdf

[MazRub2011] B. Mazur, K. Rubin, Refined class number formulas and Kolyvagin systems, Compositio Mathematica **147**(1) (2011), 56–74. https://doi.org/10.1112/S0010437X1000494X 3

[Ng1986] T. Nguyen Quang Do, Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens, Ann. Inst. Fourier **36**(2) (1986), 27–46. 4, 27
https://doi.org/10.5802/aif.1045

[Or1981] B. Oriat, Annulation de groupes de classes réelles, Nagoya Math. J. **81** (1981), 45–56. 3, 28, 35
https://projecteuclid.org/download/pdf_1/euclid.nmj/1118786304

[Or1986] B. Oriat, Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens, Acta Arithmetica **46** (1986), 331–354. 3, 35
https://doi.org/10.4064/aa-46-4-331-354

[Pari2016] The PARI Group, *PARI/GP, version* `2.9.0`, Université de Bordeaux (2016). 37

[PR1990] B. Perrin-Riou, *Travaux de Kolyvagin et Rubin*, Séminaire Bourbaki : volume 1989/90, exposés 715–729, Astérisque **189–190** (1990), Exposé no. 717, 38 p. 3, 11
http://www.numdam.org/item/SB_1989-1990__32__69_0/

[Rib1979] K.A. Ribet, Fonctions L p-adiques et théorie d'Iwasawa (rédigé par P. Satgé d'après un cours de K. Ribet 1977-78), Publications mathématiques d'Orsay 1979. 4
https://www.imo.universite-paris-saclay.fr/~biblio/cours-m2/Fonctions_L_p-adiques_et_theorie_Iwasawa.pdf

[Rib2008a] K.A. Ribet, Bernoulli numbers and ideal classes, SMF, Gazette **118** (2008). 3
https://www.dropbox.com/s/1uir9crhidorejy/smf.Ribet.pdf?dl=0

[Rib2008b] K.A. Ribet, Modular constructions of unramified extensions and their relation with a theorem of Herbrand (Class groups and Galois representations), ENS., J. Herbrand centennaire 2008. 3
https://math.berkeley.edu/~ribet/herbrand.pdf

[Rub1990] K. Rubin, The main conjecture, Appendix to *Cyclotomic fields I and II* by S. Lang GTM 121, Springer-Verlag 1990, pp. 397–419. 3
https://link.springer.com/content/pdf/bbm%3A978-1-4612-0987-4%2F1.pdf

[SchStu2019] K. Schaefer, E. Stubley, Class groups of Kummer extensions via cup products in Galois cohomology, Trans. Amer. Math. Soc., **372** (2019), 6927-6980. https://doi.org/10.1090/tran/7746 3

[Ser1978] J-P. Serre, Sur le résidu de la fonction zêta p-adique d'un corps de nombres, C.R. Acad. Sci. Paris, **287**(Série I) (1978), 183–188. 4

[Sin1980] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. **62** (1980), 181–234. 24
https://doi.org/10.1007/BF01389158

[Sol1990] D. Solomon, On the class groups of imaginary abelian fields, Annales de l'Institut Fourier **40**(3) (1990), 467–492. 3, 11, 34
https://doi.org/10.5802/aif.1221

[Sol1992] D. Solomon, On a construction of p-units in abelian fields, Invent. Math. **109**(2) (1992), 329–350.http://eudml.org/doc/144024 32

[Th1988] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. second series **128**(1) (1988), 1–18. http://www.jstor.org/stable/1971460 32

[Was1997] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997. 3, 13, 23, 24, 27, 32

Address: Villa la Gardette, 4, chemin Château Gagnière, F–38520, Le Bourg d'Oisans (Isère)
http://orcid.org/0000-0002-1318-4414
Email address: g.mn.gras@wanadoo.fr