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. English translation, with many improvements and numerical experiments, of the main parts 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 and for relative classes, but in the non semi-simple real one we proposed another more natural conjectural context, still unproved to our knowledge.

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 some families $\mathbf{M}_K$ ($K \subset \mathbb{Q}^{\rm ab}$) of $\mathbb{Z}[\mathscr{G}]$-modules ($\mathscr{G} := {\rm Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$) and to 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 $\mathscr{G}$. The elements of $\mathscr{M}_\varphi^{\rm alg}$ and $\mathscr{M}_\varphi^{\rm ar} \subseteq \mathscr{M}_\varphi^{\rm alg}$ are called 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 uses algebraic norms $\mathcal{N}_{k/k'} \in \mathbb{Z}[{\rm Gal}(k/k')]$ while the second one uses arithmetic norms $\mathbf{N}_{k/k'}$, in subextensions of $K/\mathbb{Q}$, for their definitions, the gap being given by the relation $\mathcal{N}_{k/k'} = \mathbf{J}_{k/k'} \circ \mathbf{N}_{k/k'}$, where the transfer map $\mathbf{J}_{k/k'}$ is very often non injective in p-extensions (see the examples given in § 2.4). Moreover the "arithmetic" point of view allows more natural analytic formulas (as that of Theorem 2.16).

(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 § 7.2, we define the corresponding "Analytic Invariants" $m_\varphi^{\rm an}(\mathscr{H})$, $m_\varphi^{\rm an}(\mathscr{T})$ suggested by the new analytic formulas obtained for the χ-components (Theorems 3.10, 5.10, 6.2), and we develop the problem of their comparison for even and odd p-adic characters φ.

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; for instance there is an easy annihilation theorem for $\mathscr{T}_\varphi$ but not for $\mathscr{H}_\varphi^{\rm ar}$ in the real case. So, the method of φ-objects may be useful to examine this case where the distinction between "algebraic" and "arithmetic" definitions is particularly crucial. Some questions remain open and are discussed, especially the role of the various versions of cyclotomic units (Leopoldt, Sinnott, etc.) in the real case (see the important Remark 5.11).

(iii) An illustration of the semi-simple case is given for cyclic cubic fields with $p \equiv 1 \pmod 3$, as well as a PARI program computing the above invariants with some statistics and precisions beyond the expected results of the Main Theorem, which was not possible in the 1970's.

Date: December 5, 2021.

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 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, among other results, some of the conjectures that we have stated in the 1970's.

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 $\mathbf{L}$-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.

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), finally, for 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, to Solomon (for $\mathscr{H}^-$ and $p \neq 2$ [Sol1990, Theorem II.1]), and to Greither (for $\mathscr{H}^-$, $\mathscr{T}$ with $p \geq 2$, $\mathscr{H}^+$ in the semi-simple case [Grei1992, Theorems A, B, C, 4.14, Corollary 4.15]). Let us mention especially the proof by Rubin [Rub1990], from Kolyvagin "Euler systems" used in the above works.

Many complementary works about the orders or the annihilation of the $\mathscr{H}_\varphi$ 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 not possible 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, excluding the story; the origins of the Main Conjecture are explained in Solomon–Greither papers [Sol1990, Grei1992], Ribet's Lectures [Rib2008a, Rib2008b] and Washington's book.

In another direction, we refer to enlargements of the algebraic/arithmetic aspects in the area of metabelian Galois groups, with applications to class groups and units (see for instance [Jau1981, Jau1984, Jau1986] in a class field theory context, [Lec2018, SchStu2019] in a more 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.

Nevertheless, all these works deal with the *algebraic definitions* of the φ-objects (for p-adic characters φ) and for the corresponding analytic definitions; so the distinction between algebraic and arithmetic φ-components (of class groups $\mathscr{H}$, p-torsion groups $\mathscr{T}$, etc.) 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 3.8, 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 § 2.4 and the two numerical examples given for $p = 3$).

If one replaces the p-class group $\mathscr{H}$ 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 $\mathscr{H}_K^{\mathrm{c}}$, $\mathscr{R}_K$, $\mathscr{W}_K$; see [Gra2005, Lemma III.4.2.4], leading to the exact sequence (9.1) and the formula:

$$\#\mathscr{T}_K = \#\mathscr{H}_K^{\mathrm{c}} \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K,$$

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 $\mathscr{H}_K^{\mathrm{c}}$ 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); finally the p-adic regulator $\mathscr{R}_K^{\mathrm{c}}$ of the cyclotomic units gives, in the semi-simple case, an index $\mathscr{R}_K^{\mathrm{c}}/\mathscr{R}_K$ closely related to $\mathscr{H}_K$, so that we get the formula $\#\mathscr{T}_K = \#\mathscr{R}_K^{\mathrm{c}}$, up to a standard factor.

The main invariant, besides the p-class group, is the $\mathscr{G}$-module $\mathscr{R}_K$ 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] and [Gra2016] the behavior of $\mathscr{R}_K$ when $p \to \infty$

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]. We may give an overview of the relations that exist between the two notions of φ-objects and some of their properties, as follows, where we use obvious definitions (from Section **??**) of abelian characters (a character denoted ψ is irreducible of degree 1, φ is the p-adic character above ψ, χ is the rational character above φ whose kernel in $\mathrm{Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$ fixes the field K_χ; then $G_\chi = \langle \sigma_\chi \rangle = \mathrm{Gal}(K_\chi/\mathbb{Q})$ is of order g_χ, the order of ψ, so $K_\chi/\mathbb{Q}$ is cyclic of degree g_χ).

Main definitions and results. *Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a family of finite $\mathbb{Z}[\mathscr{G}]$-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 $k \subseteq K$, and where $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} = \nu_{K/k}$ (the algebraic norm in $\mathbb{Z}[\mathrm{Gal}(K/k)]$); see more details in Section* **??**.

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

We define various χ-components $\mathbf{M}_\chi^{\rm alg}$, $\mathbf{M}_\chi^{\rm ar}$, $\mathscr{M}_\chi^{\rm alg}$, $\mathscr{M}_\chi^{\rm ar}$, of the $\mathbf{M}_{K_\chi}$'s and the corresponding φ-components $\mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}_\varphi^{\rm ar}$, of the $\mathscr{M}_\chi$'s, as follows:

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

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

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

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

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

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

$$\mathbf{M}_\chi^{\rm alg} = \big\{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\big\}\ \text{(Theorem 2.9)},$$

$$\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi\mid\chi} \mathscr{M}_\varphi^{\rm alg}\ \text{(Theorem 2.19)},$$

$$\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi\mid\chi} \mathscr{M}_\varphi^{\rm ar}\ \text{(Theorem 2.23)}.$$

(ii) Assume that $K/\mathbb{Q}$ is cyclic and $\mathbf{M}_K$ finite. If, for all sub-extensions k/k' of $K/\mathbb{Q}$, the norm maps $\mathbf{N}_{k/k'}$ are surjective, then:

$$\#\mathbf{M}_K = \prod_{\chi\in\mathscr{X}_K} \#\mathbf{M}_\chi^{\rm ar}\ \text{(Theorem 2.16)},$$

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

$$\#\mathscr{M}_\chi^{\rm ar} = \prod_{\varphi\mid\chi} \#\mathscr{M}_\varphi^{\rm ar}\ \text{(from Theorem 2.23)},$$

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

(iii′) For odd characters χ, we have:

$$\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}\ \text{and}\ \mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg},\ \text{for all } \varphi \mid \chi\ \text{(Theorem 3.8)};$$

$$\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi}\cdot w_\chi \cdot \prod_{\psi\mid\chi}\big(-\tfrac{1}{2}\,\mathbf{B}_1(\psi^{-1})\big)\ \text{(Theorem 3.10), in terms of Bernoulli numbers.}$$

(iii″) For χ even, we have:

$$\mathbf{H}_\chi^{\rm ar} \subseteq \mathbf{H}_\chi^{\rm alg}\ \text{and}\ \mathscr{H}_\varphi^{\rm ar} \subseteq \mathscr{H}_\varphi^{\rm alg},\ \text{for all } \varphi \mid \chi,\ \text{with possible strict inclusions;}$$

$$\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot \big(\mathbf{E}_{K_\chi} : \mathbf{E}_{K_\chi}^0 \oplus \mathbf{F}_{K_\chi}\big)\ \text{(Theorem 5.10), in terms of cyclotomic units, where } \mathbf{E}_{K_\chi}^0 \text{ is the subgroup of } \mathbf{E}_{K_\chi} \text{ generated by the } \mathbf{E}_k \text{ for all } k \subsetneq K_\chi.$$

(iii‴) For χ even, we have:

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

$\#\mathscr{T}_\chi = w_\chi^{\rm c} \cdot \prod_{\psi \mid \chi} \frac{1}{2}\, \mathbf{L}_p(1, \psi)$ *(Theorem 6.2), in terms of p-adic* $\mathbf{L}$*-functions.*

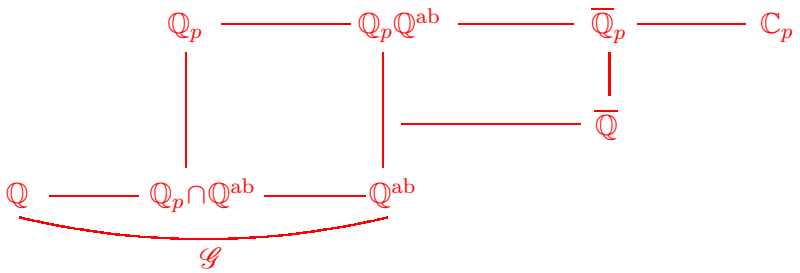
For the definitions of the Arithmetic and Analytic Invariants, $m_\varphi^{\rm ar}$, $m_\varphi^{\rm an}$, then the statement of the Main Conjecture on equalities $m_\varphi^{\rm ar} = m_\varphi^{\rm an}$, for all $\varphi \in \Phi$, see Section 7, Conjecture 7.1.

2. Definition and general study of the φ-objects

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 some new results are mentioned using additional references.

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.

2.1. **Abelian extensions of $\mathbb{Q}$ – 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 $\overline{\mathbb{Q}}$, and $\mathbb{C}_p$ a completion of $\overline{\mathbb{Q}}_p$):



Put $\mathscr{G} := {\rm Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$ and 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 p-adic characters Φ, for the given prime $p \geq 2$, the set $\mathscr{X}$ of rational characters and the corresponding sets of irreducible characters Ψ_K, $\mathscr{X}_K$, Φ_K, 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 $s \in \mathscr{G}$ 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 ${\rm Ker}(\chi) := {\rm Ker}(\psi)$, ${\rm Gal}(K_\chi/\mathbb{Q})$, the conductor of K_χ, the field of values of the characters, respectively.

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

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

and two families of arithmetic maps, indexed by the set of sub-extensions K/k:

$$\mathbf{N}_{K/k} \text{ (arithmetic norms)}, \quad \mathbf{J}_{K/k} \text{ (arithmetic transfers)}.$$

For K/k, we put:

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

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

2.2.1. *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 only depends on the class of σ modulo ${\rm Gal}(\mathbb{Q}^{\rm ab}/K)$ (i.e., the $\mathbf{M}_K$'s are canonically ${\rm Gal}(K/\mathbb{Q})$-modules).

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

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

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

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

Remark 2.3. Note that cohomology is only of algebraic nature since, for instance in the case of cyclic extension K/k of Galois group $G =: \langle\sigma\rangle$, using the class group $\mathbf{H}_K$, we have:

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

in general $\mathbf{H}_K^G$ is not isomorphic to $\mathbf{H}_k$ (think to Chevalley's formula giving $\#\mathbf{H}_K^G$) and $\nu_{K/k}(\mathbf{H}_K)$ is not isomorphic to $\mathbf{N}_{K/k}(\mathbf{H}_K)$ since the transfer map $\mathbf{J}_{K/k}$ is in general non-injective, so that ${\rm Ker}(\nu_{K/k})$ on $\mathbf{H}_K$ may be different from ${\rm Ker}(\mathbf{N}_{K/k})$.

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

Proposition 2.4. *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 (iii), $\mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = {\rm id}$ and, from (ii), $\mathbf{N}_{K/K}^2 = \mathbf{N}_{K/K}$ and $\mathbf{J}_{K/K}^2 = \mathbf{J}_{K/K}$ imply that $\mathbf{J}_{K/K} \circ \mathbf{N}_{K/K}^2 = \mathbf{N}_{K/K} = \mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = {\rm id}$ and $\mathbf{J}_{K/K}^2 \circ \mathbf{N}_{K/K} = \mathbf{J}_{K/K} = \mathbf{J}_{K/K} \circ \mathbf{N}_{K/K} = {\rm id}$. □

Proposition 2.5. *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 $\mathbf{J}_{K/k}(x) = \mathbf{J}_{K/k}\circ\mathbf{N}_{K/k}(y) = \prod_{\tau\in{\rm Gal}(K/k)} y^\tau$ and $\mathbf{N}_{K/k}\circ\mathbf{J}_{K/k}(x) = \mathbf{N}_{K/k}(\prod_{\tau\in{\rm Gal}(K/k)} y^\tau) = \prod_{\tau\in{\rm Gal}(K/k)} (\mathbf{N}_{K/k}(y))^\tau$, 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 $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} \circ \mathbf{J}_{K/k}(x) = \nu_{K/k}(\mathbf{J}_{K/k}(x)) = \prod_{\tau\in{\rm Gal}(K/k)} (\mathbf{J}_{K/k}(x))^\tau = \prod_{\tau\in{\rm Gal}(K/k)} \mathbf{J}_{K/k}(x^\tau) = \mathbf{J}_{K/k}(x)^{[K:k]} = \mathbf{J}_{K/k}(x^{[K:k]})$, which leads to $\mathbf{N}_{K/k}\circ \mathbf{J}_{K/k}(x) = x^{[K:k]}$. □

Examples 2.6. 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, for a given prime p, the torsion group $\mathscr{T}_K$ of the Galois group of the maximal p-ramified abelian pro-p-extension of K.

In these three cases the law is the Galois action and the maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$ are well known in algebraic number theory.

(iv) $\mathbf{M}_K := A[\mathrm{Gal}(K/\mathbb{Q})]$, where A is a commutative ring; then $\mathbf{M}_K$ is a $\mathscr{G}$-module if one puts $\sigma \cdot \Omega = \sigma_K \Omega$ (product in $A[\mathrm{Gal}(K/\mathbb{Q})]$), for all $\Omega \in A[\mathrm{Gal}(K/\mathbb{Q})]$ 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 $\sigma_k \in \mathrm{Gal}(k/\mathbb{Q})$, by $\mathbf{J}_{K/k}(\sigma_k) := \sum_{\tau \in \mathrm{Gal}(K/k)} \tau \cdot \sigma'_k = \nu_{K/k} \cdot \sigma'_k$, where σ'_k is any extension of σ_k in $\mathrm{Gal}(K/\mathbb{Q})$. So, for $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$, $\nu_{K/k}(\sigma_K) = \left(\sum_{\tau \in \mathrm{Gal}(K/k)} \tau\right) \cdot \sigma_K = \nu_{K/k} \cdot \sigma_K$. The maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$ are, respectively, surjective and injective, whatever $K, k \in \mathscr{K}$, $k \subseteq K$, and the map $\mathbf{N}_{K/k}$ is an homomorphism of A-algebras, while $\mathbf{J}_{K/k}$ is only an homomorphism of A-modules.

2.3. **Definition of the sub-modules $\mathbf{M}_\chi^{\mathrm{alg}}$, $\mathbf{M}_\chi^{\mathrm{ar}}$, $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi^{\mathrm{ar}}$.** Let A be a sub-ring of $\overline{\mathbb{Q}}_p$. We shall assume in the sequel that A is a Dedekind ring with finite residue field such that $A[\zeta]$ is a Dedekind ring for any root of unity ζ (e.g., $A = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$).

2.3.1. *Recalls on Γ_κ-conjugation* [Ser1998]. Let $\chi \in \mathscr{X}$. Let P_χ be the g_χth global cyclotomic polynomial seen in $A[X]$. Let κ_A be the field of quotients of A in $\overline{\mathbb{Q}}_p$ and let $\kappa_A(\mu_{g_\chi})/\kappa_A$ be the extension by the g_χth roots of unity; recall that $\mathrm{Gal}(\kappa_A(\mu_{g_\chi})/\kappa_A)$ is isomorphic to a subgroup of $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$. Put:

$$\Gamma_{\kappa_A,\chi} := \mathrm{Gal}(\kappa_A(\mu_{g_\chi})/\kappa_A).$$

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 $G_\chi := \mathrm{Gal}(K_\chi/\mathbb{Q})$, 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):

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

2.3.2. *Correspondence between abelian 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 $\kappa_A(\mu_{g_\chi})$. Each $P_{\chi,i}$ 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 to 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:

$$P_\theta := \prod_{\psi \mid \theta} (X - \psi(\sigma_\chi)) \in A[X]. \tag{2.1}$$

Thus $P_\chi = \prod_{\theta \mid \chi} P_\theta$, and for $A = \mathbb{Z}_p$ we get the relation $P_\chi = \prod_{\varphi \in \Phi,\, \varphi \mid \chi} P_\varphi$.

2.3.3. *Definition of the modules $\mathscr{M}_\varphi^{\mathrm{alg}}$.* We fix a prime number p and consider Φ, the set of irreducible p-adic characters of $\mathscr{G}$.

Definition 2.7. *Let* $\mathbf{M}$ *be a* $\mathcal{G}$*-family and let* $\mathscr{M} := \mathbf{M} \otimes \mathbb{Z}_p$ *be the corresponding local* $\mathcal{G}$*-family of* $\mathbb{Z}_p[\mathcal{G}]$*-modules* $\mathscr{M}_K$*. 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);* $\mathscr{M}_\varphi^{\rm alg}$ *is the largest sub-module of* $\mathscr{M}_\chi^{\rm alg}$ *on which* G_χ *acts by* ψ*.*

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* $\mathcal{G}$*-module* $\mathscr{M}_\varphi^{\rm alg}$ *is canonically a* $\mathbb{Z}_p[\mu_{g_\chi}]$*-module; the isomorphism is realized via the map deduced from* $\sigma \mapsto \psi(\sigma)$ *for all* $\sigma \in G_\chi$*.*

From relation (2.1), 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 2.8. *The sub-modules* $\mathscr{M}_\varphi^{\rm alg}$ *do not depend on the choice of* σ_χ *but only of* φ*.*

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

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. □

2.3.4. *Case of rational characters.* For any irreducible rational character χ, we have defined:

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

but there is, a priori, no obvious relation between $\mathscr{M}_\chi^{\rm alg}$ and the $\mathscr{M}_\varphi^{\rm alg}$'s of Definition 2.7 by means of local cyclotomic polynomials.

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" χ and φ-objects):

Theorem 2.9. *Let* $\mathbf{M}$ *be a* $\mathcal{G}$*-family of finite or infinite* $\mathbb{Z}[\mathcal{G}]$*-modules. Then for any* $\chi \in \mathscr{X}$ *we have* $\mathbf{M}_\chi^{\rm alg} = \big\{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\big\}$ *(one may limit the norm conditions to* $\nu_{K_\chi/k_q}(x) = 1$ *for all prime divisors* q *of* $[K_\chi : \mathbb{Q}]$*, where* $k_q \subset K_\chi$ *is such that* $[K_\chi : k_q] = q$*).*

Proof. [1] We need three preliminary lemmas:

Lemma 2.10. *Let* $n \geq 1$ *and let* q *be an arbitrary prime number. Denote by* P_n *the* n*th 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 2.11. *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* $A_i^j P_{\frac{n}{\ell_i}} + A_j^i P_{\frac{n}{\ell_j}} = 1$*.*

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

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 2.10 (ii) gives:

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

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 2.12. *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 number ℓ dividing n. Then there exist polynomials $A_\ell(X) \in \mathbb{Z}[X]$ such that $P_n(X) = \sum_{\ell|n} A_\ell(X)N_{n,\ell}(X)$ and $\langle N_{n,\ell}(X),\ \ell \mid n\rangle_{\mathbb{Z}[X]} = P_n(X)\mathbb{Z}[X]$.*

Proof. Assume by induction on n with t fixed that $P_n(X) = \sum_{\ell|n} A_\ell(X)N_{n,\ell}(X)$ and let q be a divisor of n; we have, from Lemma 2.10 (i), $P_{nq}(X) = P_n(X^q) = \sum_{\ell|n} A_\ell(X^q)N_{n,\ell}(X^q)$. 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:

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

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

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

since $t \geq 2$, Lemma 2.11 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. □

2.3.5. *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 2.13. *By analogy to the case of Theorem 2.9 giving the algebraic relation* $\mathbf{M}_\chi^{\rm alg} := \{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}$, *we define the arithmetic* χ*-object:*

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

(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 shall have $\mathbf{M}_\chi^{\rm ar} = \mathbf{M}_\chi^{\rm alg}$ as soon as the restrictions of the maps $\mathbf{J}_{K_\chi/k}$ to the sub-modules $\mathbf{N}_{K_\chi/k}(\mathbf{M}_{K_\chi})$ are injective (for all $k \subsetneq K_\chi$ or simply for the k_ℓ's).

In the case of an arithmetic $\mathscr{G}$-family, $\mathbf{M}_\chi^{\rm ar}$ is a sub-$\mathbb{Z}[\mu_{g_\chi}]$-module of $\mathbf{M}_\chi^{\rm alg}$. 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 $\prod_{\ell \mid g_\chi} \ell$.

2.4. **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 $A = \mathbb{Z}_p$, $\theta \in \Phi$, $\theta \mid \chi$, $K = K_\chi$ and $A[\theta] = \mathbb{Z}_p[\mu_{g_\chi}]$).

As for the example of cohomology groups, this definition is only algebraic and not arithmetic. We shall compare this definition with Definition 2.13 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]:

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

Another writing [Sol1990, § II.1, pp. 469–471], is to define $\widehat{\mathscr{M}^\varphi}$ as the largest sub-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 $1 \to \widehat{\mathscr{M}^\varphi} = \mathscr{M}_\varphi^{\rm alg} \to \mathscr{M} \to P_\varphi(\sigma_\chi) \cdot \mathscr{M} \to 1$ 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 definition of the objects $\mathscr{M}_\varphi^{\rm ar} \subseteq \mathscr{M}_\varphi^{\rm alg}$ 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 $\#\mathscr{M}_\chi^{\rm ar}$.

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 this paper, we are concerned with the non-trivial context when $g_\chi = [K_\chi : \mathbb{Q}]$ is a multiple of a non trivial p-power. 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 a cyclic extension L of $\mathbb{Q}$ of 3-power degree with k; 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 [Gra2021] many examples of capitulations of the 3-class group of k in K, giving $\mathscr{H}_\varphi^{\rm ar} \subsetneq \mathscr{H}_\varphi^{\rm alg}$, as the two following ones:

Example 2.14. 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 following program is only for verification, the general one being given in [Gra2021, § 4.2]. 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 $\mathbf{H}_{k_0}$ (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 $\mathbf{H}_{k_i}$ of k_i, $i = 1, 2$ (we are going to see that $\mathbf{H}_{k_i} \simeq \mathbb{Z}/9\mathbb{Z}$ for all i, which is supported by the fact that $\mathbf{N}_{k_2/k_0}(\mathfrak{Q}_2) = \mathfrak{Q}_0^9$ but $\mathbf{N}_{k_2/k_0}(\mathscr{H}_2) = \mathscr{H}_0$):

```
{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, C0 = [9] denotes the class group of k_0 and [4]~ 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 C1 = [9], [6]~, 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, C2 = [9], [0]~ 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,[-1,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0]~,1,9,[0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0]~]

[[0]~,[-270476874595642910,323533824277028894,-236208800298303000,119737461690335806,
-55560785877921528 2,-19842381310285742 0,4105888650208704 14,-11002817900657767 8,
-4496007979182140 26,-490666543752794 8,1027404856685423 2,431985245809388 7,13258715755947394,
-681794114489909 5,-15448507867705832,2623003974789062,-3264916449440532,-16606126998680345]~]
```

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

$$\begin{aligned} \mathscr{H}_{\chi_2}^{\rm ar} &= \{x \in \mathscr{H}_{k_2},\ \mathbf{N}_{k_2/k_1}(x) = 1\} = 1, \\ \mathscr{H}_{\chi_2}^{\rm alg} &= \{x \in \mathscr{H}_{k_2},\ P_{\chi_2}(\sigma_{\chi_2}) \cdot x = 1\} = \{x \in \mathscr{H}_{k_2},\ \nu_{k_2/k_1}(x) = 1\} = \mathscr{H}_{k_2}^3. \end{aligned} \tag{2.2}$$

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:

$$\mathscr{H}_{\chi_1}^{\rm alg} = \mathscr{H}_{k_1}^3 \quad \text{and} \quad \mathscr{H}_{\chi_1}^{\rm ar} = 1.$$

Thus, the forthcoming formula of Theorem 2.16 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 $\#\mathscr{H}_{\chi_1}^{\rm ar} = \#(\mathscr{E}_{k_1}/\mathscr{E}_{k_1}^0 \oplus \mathscr{F}_{k_1})$ (analytic formula of Theorem 5.10); 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 | ei | of L_1, | e0 | of k_0, | Ej | of k_1, and their logarithms; they are, respectively (standard PARI programs):

```
Unities                                                  Logarithms

e1=0.285142481829785364394119873530627413426 7     -1.2547662873951149420 4754
e2=4.507018644092976298660799923715678029025 9      1.5056358803968657653 4798

e0=664.00150602068057486397714386165380336808       6.4982844175772963097 2016

E1=0.285142481829785364394119873530627413426 7     -1.2547662873951149420 4754
E2=0.221876162263190934266680050185050615599 1     -1.5056358803968657653 4798
E3=664.00150602068057486397714386165380336808       6.4982844175772963097 2016
E4=945628377316488.87204143428389231544006082       34.48287077191825581974 318
E5=0.00257365190752746549299934631279513096 57     -5.96242941301396593243 20487
```

```
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       34.48287077191825581974 318471406265950 88
Eta^s2=2433718277092.68346630913000250376527 46      28.52044135896859226499696951276525952 7
Eta^s3=0.00257365190752746549299934631279469 73     -5.96242941301396593243 48776278615043514
Eta^s4=1.05749787547388046520632114968345 73 E-15   -34.48287077191825581974 318471406269321 17
Eta^s5=4.10893902310911119828246133003785 55 E-13   -28.52044135896859226499696951276559669 0
Eta^s6=388.55293409150677930552045771356632326       5.96242941301396593243 48776278611673020
```

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 $(\mathscr{E}_{k_1} : \mathscr{E}_{k_1}^0 \oplus \mathscr{F}_{k_1}) = 1$ as expected since $\mathscr{H}_{\chi_1}^{\rm ar} = 1$. 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 ($\mathscr{E}_{k_1}^0$ 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 5.11 for more comments).

The computation of $(\mathscr{E}_{k_2} : \mathscr{E}_{k_2}^0 \oplus \mathscr{F}_{k_2})$ 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 $\#\mathscr{H}_{\chi_0}^{\rm ar} = (\mathscr{E}_{k_0} : \mathscr{E}_{k_0}^0 \oplus \mathscr{F}_{k_0}) = (\mathscr{E}_{k_0} : \mathscr{F}_{k_0}) = 9$.

Example 2.15. 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]~,[-109314239520681583852491868090391 25/703657534464269024161568,
          -183317981458710599286692619444 67/703657534464269024161568,
          -351695176307469407115167997574 49/439785959040168140100 98,
           204725511770566909682809143731071/703657534464269024161568,
           894673913338308496518130829619/439785959040168140100 98,
          -201678908467111394367611629238 79/140731506892853804832 3136]~]
```

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]~,[82171907563048711539692 13,52602828277952742913821 8,-68778602907559567659413 4,
          25130170977215548291757 7,-21032376402967976888126,-15609327127430752932511]~]
```

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

$$\mathscr{H}_{\chi_1}^{\mathrm{ar}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \text{ while } \mathscr{H}_{\chi_1}^{\mathrm{alg}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

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

The formula of Theorem 2.16 is, here, of the form:

$$\#\mathscr{H}_{k_1} = \#\mathscr{H}_{\chi_1}^{\mathrm{ar}} \cdot \#\mathscr{H}_{\chi_0}^{\mathrm{ar}} = 9 \times 9,$$

since we have $\mathscr{H}_{\chi_0}^{\mathrm{ar}} = \mathscr{H}_{k_0}$ of order 9; of course a same formula with the $\mathscr{H}^{\mathrm{alg}}$'s does not exist since $\#\mathscr{H}_{\chi_1}^{\mathrm{alg}} \cdot \#\mathscr{H}_{\chi_0}^{\mathrm{alg}} = 27 \times 9$.

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

2.5. **Computation of $\#\mathbf{M}_K$ for cyclic extensions.** Let $\mathbf{M}$ be an arithmetic $\mathscr{G}$-family where the $\mathbb{Z}[\mathscr{G}]$-modules $\mathbf{M}_K$ are finite (as, for instance, the class groups of abelian fields); then we can state:

Theorem 2.16. *Let $K/\mathbb{Q}$ be a cyclic extension; one assumes that $\mathbf{M}_K$ is finite and 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 indexed by the irreducible rational characters of K:*

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

Proof. One may assume, for the proof, that we replace the $\mathbf{M}_k$, $k \subseteq K$, by the finite $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_k := \mathbf{M}_k \otimes \mathbb{Z}_p$, for all primes $p \mid \#\mathbf{M}_K$, using the previous results, then globalizing at the end. Moreover, if one is only interested by a localization at a specific prime p, it suffices to assume that the p-Sylow subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. Two classical lemmas are necessary.

Lemma 2.17. *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).*

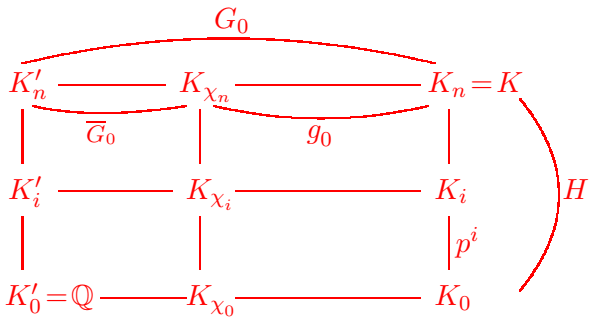
Proof. From Proposition 2.5, we know that $\mathbf{N}_{k/k'} \circ \mathbf{J}_{k/k'} = [k : k']$; whence the proofs since $[k : k']$ is invertible modulo p. □

Put $\mathrm{Gal}(K/\mathbb{Q}) = G_0 \times H$, where G_0 is a subgroup of prime-to-p order and H (cyclic of order p^n) is the p-Sylow subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. 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 $\psi_i := \psi_{i,0}\,\psi_{i,p}$, where $\psi_{i,p}$ is of order p^i and $\psi_{i,0} \in \Psi_{K_0}$; thus K_{χ_i} is the compositum of K_{χ_0} and K_i', where K_{χ_0} correspond to $\psi_{0,0}$ and K_i' to $\psi_{i,p}$ (K_i' is

of degree p^i over $\mathbb{Q}$). This leads to the diagram:



Let $\mathscr{M}^*_{K_{\chi_i}} = \mathrm{Ker}(\mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}})$, for $1 \le i \le n$, then put $\mathscr{M}^*_{K_{\chi_0}} := \mathscr{M}_{K_{\chi_0}}$. We have the exact sequences of $\mathrm{Gal}(K/\mathbb{Q})$-modules:

$$1 \longrightarrow \mathscr{M}^*_{K_{\chi_i}} \longrightarrow \mathscr{M}_{K_{\chi_i}} \xrightarrow{\mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}}} \mathscr{M}_{K_{\chi_{i-1}}} \longrightarrow 1, \quad 1 \le i \le n. \tag{2.3}$$

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 2.18. *Let $\mathscr{M}$ be an arithmetic $\mathscr{G}$-family whose elements are $\mathbb{Z}_p[G]$-modules, where $G = G_0 \times H$. 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 $\nu_{K_n/K_{\chi_n}}$ (denoted ν_{g_0}); moreover, since the degree of these extensions are prime to p, we may identify $\mathbf{N}_{K_i/K_{\chi_i}}$ with $\mathbf{N}_{K_n/K_{\chi_n}}$ (denoted $\mathbf{N}_{g_0}$) and $\mathbf{J}_{K_i/K_{\chi_i}}$ with $\mathbf{J}_{K_n/K_{\chi_n}}$ (denoted $\mathbf{J}_{g_0}$). 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:

$$\nu_{g_0}(\mathscr{M}_{K_i}) = \mathbf{J}_{g_0} \circ \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathscr{M}_{K_{\chi_i}}; \tag{2.4}$$

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 $i \ge 1$, $\mathbf{N}_{g_0}(\mathscr{M}^*_{K_i}) = \mathscr{M}^*_{K_{\chi_i}}$.

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 (2.4), $\nu_{g_0}(\mathscr{M}_{K_{i-1}}) \simeq \mathscr{M}_{K_{\chi_{i-1}}}$ (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 2.17):

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

It follows, from the norm definitions of $(\mathscr{M}^{\mathrm{ar}}_{K_{\chi_i}})_{\chi_0}$ and $\mathscr{M}^*_{K_{\chi_i}}$, that $(\mathscr{M}^*_{K_{\chi_i}})^{\overline{e}_{\chi_0}} = \mathscr{M}^{\mathrm{ar}}_{\chi_i}$ for all $i \ge 1$.

In the finite case, this yields, using the above, the exact sequence (2.3) and $\mathscr{M}^*_{K_0} = \mathscr{M}_{K_0}$:

$$\prod_{\chi\in\mathscr{X}_K} \#\mathscr{M}^{\rm ar}_\chi = \prod_{\chi_0}\prod_{i=0}^{n} \#(\mathscr{M}^*_{K_{\chi_i}})^{\overline{e}_{\chi_0}} = \prod_{i=0}^{n}\prod_{\chi_0} \#(\mathscr{M}^*_{K_i})^{\overline{e}_{\chi_0}}$$
$$= \prod_{i=0}^{n} \#\mathscr{M}^*_{K_i} = \#\mathscr{M}^*_{K_0} \prod_{i=1}^{n} \frac{\#\mathscr{M}_{K_i}}{\#\mathscr{M}_{K_{i-1}}} = \#\mathscr{M}_{K_n} = \#\mathscr{M}_K.$$

Which ends the proof of the theorem (note that the assumption on the surjectivity of the norms is fulfilled if and only if all intermediate extensions k/k' are totally ramified, which will be the case in cyclic extensions $K/\mathbb{Q}$). □

2.6. **Local decomposition of the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_\chi$.** 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 § 2.5, $\mathrm{Gal}(K/\mathbb{Q})$ becomes $G_\chi = G_0 \times H$ of order $g_\chi = g_{\chi_0}\cdot p^n$. We define, what we call the "tame idempotents" of $\mathbb{Z}_p[G_\chi]$:

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

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

Theorem 2.19. *Let $\mathscr{M}$ be a family of $\mathbb{Z}_p[\mathscr{G}]$-modules. Let $\chi \in \mathscr{X}$; for any $\psi \mid \chi$, put $\psi = \psi_0\psi_p$ (ψ_0 of prime-to-p order, ψ_p of p-power order). Then we get the decomposition:*

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

In this decomposition, the sub-modules $\mathscr{M}^{\rm alg}_\varphi$ (Definition 2.7) coincide with the sub-modules $(\mathscr{M}^{\rm alg}_\chi)^{e^{\varphi_0}}$, where $e^{\varphi_0} \in \mathbb{Z}_p[G_0]$ is the tame idempotent associated to φ_0 above ψ_0.

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. § 2.3.2 for the definition of P_φ).

Lemma 2.20. *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:

$$U_2(\zeta)\,Q_2(\zeta) = p^k \text{ in } \mathbb{Z}[\mu_{g_\chi}]; \tag{2.5}$$

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:

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

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 (2.5):

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

Denote by $\mathfrak{p}_\chi$ the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$ and let $\overline{F}_p := \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\chi$ 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:

$$\overline{Q}_1 = (\overline{Q}_0)^e, \tag{2.6}$$

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 $P(\zeta) \equiv 0 \pmod{\mathfrak{p}_\chi}$ 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:

$$Q_0^\alpha(\zeta) \equiv 0 \pmod{p}. \tag{2.7}$$

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 $p^n a_0 \not\equiv 1 \pmod{p g_{\chi_0}}$ and $1 - \zeta^{p^n a_0 - 1} \in \mathfrak{p}_\chi \setminus \mathfrak{p}_\chi^2$, thus the fact that $P_{g_{\chi_0}}(\zeta) \in \mathfrak{p}_\chi \setminus \mathfrak{p}_\chi^2$; it follows, from $P_{g_{\chi_0}} = C\,Q_0^\beta + pD$, $\beta \geq 1$, $C, D \in \mathbb{Z}_p[X]$, $C(\zeta) \not\equiv 0 \pmod{\mathfrak{p}_\chi}$, that $P_{g_{\chi_0}}(\zeta) \equiv C(\zeta)\,Q_0^\beta(\zeta) \pmod{\mathfrak{p}_\chi^e}$, thus $Q_0^\beta(\zeta) \in \mathfrak{p}_\chi \setminus \mathfrak{p}_\chi^2$ since $e > 1$. This implies $\beta = 1$ and $Q_0(\zeta) \in \mathfrak{p}_\chi \setminus \mathfrak{p}_\chi^2$.

The congruence (2.7), written $Q_0^\alpha(\zeta) \equiv 0 \pmod{\mathfrak{p}_\chi^e}$, 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 (2.6):

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

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 (2.5). □

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 2.20, one may write:

$$\mathbb{Z}_p[X]/P_\chi(X) = \mathbb{Z}_p[X]\Big/\Big(\prod_{u=1}^{g_p} Q_u(X)\Big) \simeq \prod_{u=1}^{g_p} \mathbb{Z}_p[X]/\big(Q_u(X)\big) \simeq (\mathbb{Z}_p[G_\chi])^{g_p}. \tag{2.8}$$

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):

$$\mathscr{M}_\chi^{\rm alg} = \bigoplus_{u=1}^{g_p} (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_u}(\sigma_\chi)}. \tag{2.9}$$

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 have $e_{\varphi_v}(\sigma_\chi) \equiv \delta_{u,v} \pmod{P_{\varphi_u}(\sigma_\chi)}$, 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 $\mathscr{A} := \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$ we obtain two systems of idempotents, that is to say, the images in $\mathscr{A}$ 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 tame part φ_0 above ψ_0, we consider both:

$$e^{\varphi_0} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\,\sigma \tag{2.10}$$

and $e_\varphi(\sigma_\chi)$ defined as follows by means of polynomial relations in $\mathbb{Z}[X]$ deduced from (2.8):

$$e_\varphi(\sigma_\chi) = \Lambda_\varphi(\sigma_\chi) \cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(\sigma_\chi), \text{ such that } \Lambda_\varphi(X) \cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(X) \equiv 1 \pmod{P_\varphi(X)}. \tag{2.11}$$

we denote them e^{φ_0} and e_φ, respectively.

To verify that $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}} = (\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$, it suffices to show that e^{φ_0} and e_φ correspond to the same simple factor of the algebra $\mathscr{A}$. 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 $\mathscr{A} \longrightarrow \mathbb{Z}_p[\mu_{g_\chi}]$ whose kernel is equal to $\bigoplus_{\varphi' \neq \varphi} \mathscr{A} e_{\varphi'}$.

Thus, to show that $\mathscr{A} e^{\varphi_0} = \mathscr{A} e_\varphi$, it suffices to show that $\psi(e^{\varphi_0}) \neq 0$; but, from (2.10), e^{φ_0} 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 $\psi(e^{\varphi_0}) \neq 0$.

This finishes the proof of the theorem. □

Remark 2.21. Let $\mathscr{M}_\chi^{\rm alg}$ as $\mathbb{Z}_p[G_\chi]$-module annihilated by $P_\chi(\sigma_\chi)$; on may write (from relation (2.9)) $\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi \mid \chi} (\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$ and we know that $(\mathscr{M}_\chi^{\rm alg})^{e_\varphi}$ coincides with the sub-module $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}} = \mathscr{M}_\varphi^{\rm alg}$ (cf. Definition (2.10)); then, due to the properties of the e_φ, one obtains:

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

where e_φ is defined by (2.11).

From Definition 2.13, one has $\mathscr{M}_\chi^{\rm ar} := \{x \in \mathscr{M}_{K_\chi},\ \ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneqq K_\chi\}$. 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 2.22. *Let $\mathscr{M}$ be an arithmetic family of $\mathbb{Z}_p[\mathscr{G}]$-modules; we define an arithmetic φ-object by putting:*

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

where e_φ is defined by (2.11).

So, we have the arithmetic version of Theorem 2.19:

Theorem 2.23. *Let $\mathscr{M}$ be a family of $\mathbb{Z}_p[\mathscr{G}]$-modules. Then we get the decomposition:*

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

To summarize the results that we have obtained, we can state (from Theorems 2.16, 2.19, 2.23, using Definitions 2.7, 2.13, 2.22):

Main Theorem 2.24. *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.*

Let σ_χ be a generator of $G_\chi:=\mathrm{Gal}(K_\chi/\mathbb{Q})$ and $g_\chi:=\#G_\chi$; 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,*

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

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

Then we have:

$$\mathscr{M}_\chi^{\rm alg}=\bigoplus_{\varphi\mid\chi}\mathscr{M}_\varphi^{\rm alg}\ \text{ and }\ \mathscr{M}_\chi^{\rm ar}=\bigoplus_{\varphi\mid\chi}\mathscr{M}_\varphi^{\rm ar}.$$

Assume $K/\mathbb{Q}$ abelian with a cyclic p-Sylow subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, such that for all sub-extensions k/k' of $K/\mathbb{Q}$ of p-power degree, the norm map $\mathbf{N}_{k/k'}$ is surjective; then, if $\mathscr{M}_K$ is finite:

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

3. Application to relative class groups of abelian extensions

3.1. **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:

$$(\mathbf{H}_K^{\rm ar})^-:=\{h\in\mathbf{H}_K,\ \ \mathbf{N}_{K/K^+}(h)=1\}\tag{3.1}$$

(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:

$$\#\mathbf{H}_K=\#(\mathbf{H}_K^{\rm ar})^-\cdot\#\mathbf{H}_K^+.\tag{3.2}$$

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 sub-modules $\mathscr{H}_\chi^{\rm alg}$ and $\mathscr{H}_\chi^{\rm ar}$ for $\chi\in\mathscr{X}$, and the φ-components (Definitions 2.7, 2.13, 2.22); they are $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

3.2. **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 3.1. *Assume that $\mathscr{H}_\chi^{\rm ar}\subsetneqq\mathscr{H}_\chi^{\rm alg}$. 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 $k'_\ell = k_\ell \cap K_{\chi'}$:

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

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 3.2. *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 $\varepsilon^p \in \mathbf{E}_K^{1-\sigma}$. □

3.2.1. *Study of the case $p \neq 2$.* We are in the context of Lemma 3.1. 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 $h \in (\mathscr{H}_K^{\rm ar})^-$); if K/k is of degree $p \neq 2$, then k is also imaginary and $h' \in (\mathscr{H}_k^{\rm ar})^-$.

We introduce the maximal real subfields, giving the diagram:

$$\begin{array}{ccc} K^+ & \overset{2}{\longrightarrow} & K \quad h \\ p \Big| & & \Big| p \quad \big) G = \langle\sigma\rangle \\ k^+ & \underset{2}{\longrightarrow} & k \quad h' := \mathbf{N}_{K/k}(h) \end{array}$$

Lemma 3.3. *Let μ_K^* be the p-torsion 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 $(\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, by the map $\mathrm{Ker}(\mathbf{J}_{K/k}) \to \mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ of Lemma 3.2, 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 $h' \in (\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, 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 3.4. *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 $\mathbf{E}_K^{1-\sigma} \cap \mu_K^* = 1$. □

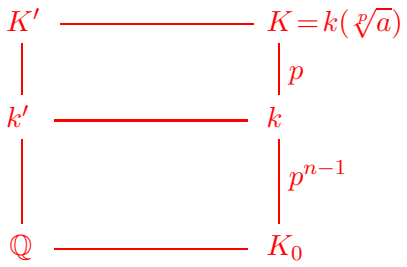
Lemma 3.5. *If $(\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) \neq 1$, this group is of order p and K/k is a Kummer extension of the form $K = k(\sqrt[p]{a})$, $a \in k^\times$, $a\mathbf{Z}_k = \mathfrak{a}^p$, the ideal $\mathfrak{a}$ of k being non-principal (such a Kummer extension is said "of class type").*

Proof. If $h' \in (\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, $h' := \mathscr{C}\ell_k(\mathfrak{a}) \neq 1$, 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 3.4, $q(\varepsilon) = q(\zeta_1)^\lambda$, 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 3.5 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:



Let ℓ be a prime number totally ramified in $K'/\mathbb{Q}$ (such a prime does exist since $\mathrm{Gal}(K'/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$); 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 $(\mathscr{H}_k^{\rm ar})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) = 1$ (injectivity of $\mathbf{J}_{K/k}$ on the relative p-class group).

3.2.2. *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 $\mathfrak{a}^2 = c\mathbf{Z}_k$.

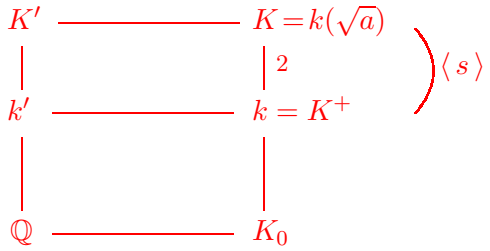
Let τ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$; one has $\alpha^{2\tau} = i^\tau c^\tau = -ic^\tau = -c^{\tau-1}\alpha^2$, hence $\alpha^{2\tau} = \alpha^2 d$, $d := -c^{\tau-1} \in k^\times$; we obtain $(\alpha\mathbf{Z}_K)^{2\tau} = (\alpha\mathbf{Z}_K)^2 d\mathbf{Z}_K$, thus $\mathfrak{a}^{2\tau}\mathbf{Z}_K = \mathfrak{a}^2\mathbf{Z}_K d\mathbf{Z}_K$ 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 3.6. *For any imaginary cyclic extension $K/\mathbb{Q}$ and for any relative extension K/k, of prime degree $p \geq 2$, we have $(\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) = 1$ 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 (3.2), we get:

Corollary 3.7. *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 $\mathscr{H}_K = (\mathscr{H}_K^{\mathrm{ar}})^- \oplus \mathbf{J}_{K/K^+}(\mathscr{H}_{K^+})$.*

We then have obtained the following result about the relative classes:

Theorem 3.8. *Let K be an imaginary cyclic field of maximal real subfield K^+. Let p any fixed prime, and let $(\mathscr{H}_K^{\rm ar})^- := \{h \in \mathscr{H}_K,\, \mathbf{N}_{K/K^+}(h) = 1\}$, $(\mathscr{H}_K^{\rm alg})^- := \{h \in \mathscr{H}_K,\, \nu_{K/K^+}(h) = 1\}$. We have $\mathscr{H}_K^{\rm ar} = \mathscr{H}_K^{\rm alg}$, then $\mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg}$ 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 2.13, 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 2.19 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 3.9. *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 2.16, 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 2.16 implies $\#\mathbf{H}_K = \prod\limits_{\chi \in \mathscr{X}_K} \#\mathbf{H}_\chi^{\rm ar}$.

From (3.2), we have $\#\mathbf{H}_K = \#\mathbf{H}_K^- \cdot \#\mathbf{H}_K^+$ and we can also apply Theorem 2.16 to the maximal real subfield K^+ of K, giving $\#\mathbf{H}_K^+ = \prod\limits_{\chi \in \mathscr{X}_K^+} \#\mathbf{H}_\chi^{\rm ar}$, whence the formulas taking into account the relation $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$ for odd characters (Theorem 3.8). □

3.3. **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:

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

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 3.10. *Recall that $\mathbf{H}_\chi^{\rm ar} := \{x \in \mathbf{H}_{K_\chi},\, \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}$ and let $\chi \in \mathscr{X}^-$. 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;

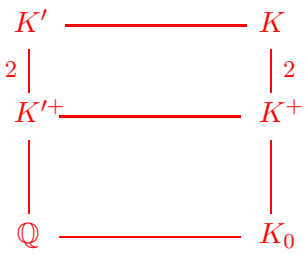
(ii) $w_\chi = p$ if $K_\chi = \mathbb{Q}(\mu_{p^n})$, $p \geq 2$ prime, $n \geq 1$.

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 3.8, taking into account the relation $\#\mathbf{H}_K^- = \prod\limits_{\chi \in \mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm ar}$. So, it remains to prove that $\prod\limits_{\chi \in \mathscr{X}_K^-} \big(2^{\alpha_\chi} \cdot w_\chi \big) = w_K^-$.

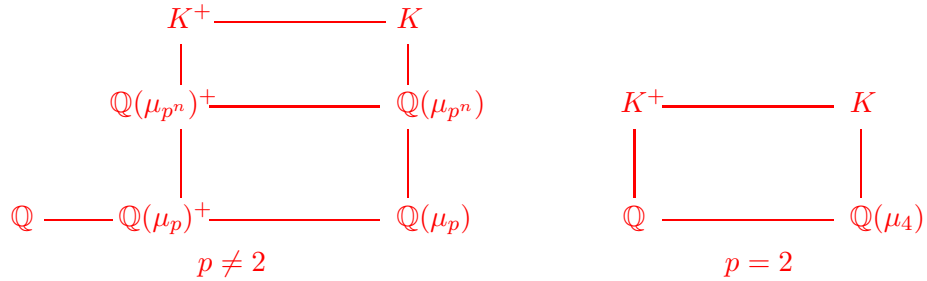
Consider the following diagram:



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 3.11. For any imaginary extension K, $\#\mathbf{H}_K^- = \frac{Q_K^- w_K^-}{2^{n_K^-}} \prod_{\chi\in\mathscr{X}_K^-} \#\mathbf{H}_\chi^{\mathrm{alg}}$, 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].

4. Annihilation of $\mathbf{H}_K^-$ – Generalization of Iwasawa's results

This part was written before some improvements given by means of Stickelberger's elements for the annihilation of relative class groups and the construction of p-adic measures, then by means of index formulas with cyclotomic units in the context of real class groups.

In [Iwa1962a], Iwasawa 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).

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:

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

(in the summation, the integers a are prime to f and the Artin symbols are taken over $\mathbb{Q}$). Note that the part $\sum\limits_{a=1}^{f} \Big(\frac{\mathbb{Q}(\mu_f)}{a}\Big)^{-1}$ is the algebraic norm $\mathcal{V}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}$ which does not modify the image 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:

$$\mathbf{S}_K := \mathbf{B}_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K], \text{ where } \mathbf{B}_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = -\sum_{a=1}^{f} \Big(\frac{a}{f} - \frac{1}{2}\Big)\Big(\frac{K}{a}\Big)^{-1}. \tag{4.1}$$

Lemma 4.1. *For any odd integer c prime to f and, by restriction of $\mathbf{B}_{\mathbb{Q}(\mu_f)}$ to K, let $\mathbf{B}_K^c := \Big(1 - c\Big(\frac{K}{c}\Big)^{-1}\Big) \cdot \mathbf{B}_K$; then $\mathbf{B}_K^c \in \mathbb{Z}[G_K]$.*

Proof. We have $\mathbf{B}_K^c = \frac{-1}{f} \sum\limits_a \Big[a\Big(\frac{K}{a}\Big)^{-1} - ac\Big(\frac{K}{a}\Big)^{-1}\Big(\frac{K}{c}\Big)^{-1}\Big] + \frac{1-c}{2} \sum\limits_a \Big(\frac{K}{a}\Big)^{-1}$.

Let $a'_c \in [1, f]$ be the unique integer such that $a'_c \cdot c \equiv a \pmod f$ and put:

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

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

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

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:

$$\mathbf{B}_K^c = \mathbf{B}_K'^c \cdot (1 - s), \ \ \mathbf{B}_K'^c \in \mathbb{Z}[G_K], \tag{4.2}$$

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

Definition 4.2. *Put $\mathfrak{A}_K := \{\Omega \in \mathbb{Z}[G_K],\ \Omega\,\mathbf{B}_K^c \in \mathbb{Z}[G_K]\}$ ($\mathfrak{A}_K$ is an ideal of $\mathbb{Z}[G_K]$ and then $\mathbf{S}_K := \mathbf{B}_K^c \cdot \mathfrak{A}_K$ (cf. (4.1)). Let $\Lambda_K \geq 1$ be the least rational integer such that $\Lambda_K \mathbf{B}_K^c \in \mathbb{Z}[G_K]$ (thus $\Lambda_K \mid f$). For $K = K_\chi$, we put $\mathfrak{A}_{K_\chi} =: \mathfrak{A}_\chi$ and $\Lambda_{K_\chi} =: \Lambda_\chi$.*

Lemma 4.3. *Let α_σ be the coefficient of $\sigma \in G_K$ in the writing of $\mathbf{B}_K$ on the canonical basis G_K of $\mathbb{Z}[G_K]$ (in particular, we have $\alpha_1 = \sum\limits_{a,\ \sigma_a|_K = 1} a$). 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 $\Lambda_K = \dfrac{f}{\gcd(f, \alpha_1)}$.*

Proof. The first claim is obvious and Λ_K is the least integer Λ such that $\dfrac{\Lambda \cdot \alpha_1}{f} \in \mathbb{Z}$, since $\Lambda_K \mathbf{B}_K \in \mathbb{Z}[G_K]$ if and only if $\dfrac{\Lambda_K \cdot \alpha_\sigma}{f} \in \mathbb{Z}$ for all $\sigma \in G_K$, thus, for instance, for $\sigma = 1$. □

Proposition 4.4. *(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 $\{\cdots, \left(\frac{K}{a}\right) - a, \cdots ;\ \Lambda_K\}$, 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 $\left(\frac{K}{a}\right) - a$, and Λ_K, where $\left(\frac{K}{a}\right)$ is any generator of G_K.

Proof. See [Gra1976, p. 35–36]. □

4.2. **Study of the algebraic $\mathscr{G}$-families $\mathbf{M}_K := \mathbb{Z}[G_K]$, $\mathbf{S}_K := \mathbf{B}_K \cdot \mathfrak{A}_K$.** 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 4.5. *We have $\mathbf{M}_\chi = \Big(\prod_{\ell \mid g_\chi} (1 - \sigma_\chi^{g_\chi/\ell})\Big)\mathbb{Z}[G_\chi]$. The image of $\mathbf{M}_\chi$, by $\psi : \mathbb{Z}[G_\chi] \to \mathbb{Z}[\mu_{g_\chi}]$, is isomorphic to the ideal $\mathfrak{a}_\chi := \prod_{\ell \mid g_\chi} \big(1 - \psi(\sigma_\chi)^{g_\chi/\ell}\big)\mathbb{Z}[\mu_{g_\chi}]$; 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 proofs for the norm action on cyclotomic numbers, we recall, without proof, the following well-known formulas:

Lemma 4.6. *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 $\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)} : \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})]$. Let*

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

We have:

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

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

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

Theorem 4.7. *For all $\chi \in \mathscr{X}^-$, the $\mathbb{Z}[\mu_{g_\chi}]$-module $\mathbf{H}_\chi^{\mathrm{alg}} = \mathbf{H}_\chi^{\mathrm{ar}}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1}) \cdot (\psi(a) - a, \Lambda_\chi)$ of $\mathbb{Z}[\mu_{g_\chi}]$, $\psi \mid \chi$ (cf. Lemma 4.3, Proposition 4.4).*

The ideal $(\psi(a) - a, \Lambda_\chi)$ 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 4.8. *For all $\varphi \in \Phi^-$, the $\mathbb{Z}_p[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi^{\mathrm{alg}} = \mathscr{H}_\varphi^{\mathrm{ar}}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1}) \cdot (\psi(a) - a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$, $\psi \mid \varphi$.*

The ideal $(\psi(a) - a, \Lambda_\chi)$ 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 4.9. Let $K := K_\chi$ be the field $\mathbb{Q}(\mu_{47})$, of degree $g_\chi = 46$. From Theorem 3.10, we have $\mathbf{H}_\chi = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi \mid \chi} \big(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$ where $-\frac{1}{2}\mathbf{B}_1(\psi^{-1}) = -\frac{1}{2}\sum_{a=1}^{47} \big(\frac{a}{47} - \frac{1}{2}\big)\psi^{-1}(a)$, $\alpha_\chi = 0$ and $w_\chi = 47$. The following program computes $\#\mathbf{H}_\chi$:

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

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 $\big((\frac{K}{a}) - a, 47\big)$, for a suitable a (Lemma 4.3), 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),1);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.

In [Gra1978, Chap. IV, § 2] and in [Gra1978/79b, Theorèmes 1, 2, 3], we have given some improvements of the annihilation for 2-class groups but it is difficult to say if the case $p = 2$ is optimal or not without numerical studies. By way of example, we can cite the following [Gra1978/79b, Théorème IV1] under the above context ($\psi \mid \varphi \mid \chi$, $\psi = \psi_0\,\psi_2$ and $\psi_0 \neq 1$):

Theorem 4.10. *The $\mathbb{Z}_2[\mu_{g_\chi}]$-module $\mathscr{H}_{K_\chi}^{e^{\varphi_0}}/\mathbf{J}_{K_\chi/K_\chi^+}(\mathscr{H}_{K_\chi^+}^{e^{\varphi_0}})$ is annihilated by $\big(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big)$, where e^{φ_0} is the corresponding tame idempotent.*

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

5. 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.

5.1. **Reminders on 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 $\chi \in \mathscr{X}^+$; from the definition of χ-objects and the results of the previous sections we can write:

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

Definition 5.1. *Denote by $\mathbf{E}^0$ the $\mathscr{G}$-family such that $\mathbf{E}_K^0$ is the subgroup of $\mathbf{E}_K$ generated by the $\mathbf{E}_k$ for all the subfields $k \subsetneq K$.*

Lemma 5.2. *We have $\mathbf{E}_{K_\chi}^0 \cdot \mathbf{E}_\chi = \mathbf{E}_{K_\chi}^0 \oplus \mathbf{E}_\chi$, for all $\chi \in \mathscr{X}^+$.*

Proof. One knows that $\bigoplus_{\theta \in \mathscr{X}_K} \mathbf{E}_\theta$ is of finite index Q_K in $\mathbf{E}_K$ for any real K (cf. [Leo1954, Chap. 5, § 4]). Let $|\varepsilon| \in \mathbf{E}_{K_\chi}^0 \cap \mathbf{E}_\chi$; 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 $|\varepsilon_i^n| \in \bigoplus_{\theta_i \in \mathscr{X}_{k_i}} \mathbf{E}_{\theta_i}$, for all i (in particular, $\chi \notin \mathscr{X}_{k_i}$); we then have $|\varepsilon^n| \in \Big(\bigoplus_{\theta \in \mathscr{X}_{K_\chi}\ \theta \neq \chi} \mathbf{E}_\theta\Big) \bigcap \mathbf{E}_\chi = \{1\}$, which implies $|\varepsilon| = 1$. □

Definition 5.3. *Let K be any real abelian field. Put $Q_K = \Big(\mathbf{E}_K : \bigoplus_{\chi \in \mathscr{X}_K} \mathbf{E}_\chi\Big)$ and, for all $\chi \in \mathscr{X}_K^+$, put $Q_\chi = \big(\mathbf{E}_{K_\chi} : \mathbf{E}_{K_\chi}^0 \oplus \mathbf{E}_\chi\big)$.*

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

Lemma 5.4. *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 define 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 5.2 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]. □

Definitions 5.5. *(i) 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, $n \geq 1$,*

$q_1 = 1$.

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

Lemma 5.6. *We have, for all cyclic real field K, $q_K = \prod\limits_{\chi \in \mathscr{X}_K} q_\chi$.*

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

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

Definitions 5.7. *(i) Let f_χ be the conductor of the field K_χ, $\chi \in \mathscr{X}^+$, $\zeta_{2f_\chi} := \exp\left(\frac{i\pi}{f_\chi}\right)$, and:*

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

where A_χ denotes a half-system of representatives of $\mathrm{Gal}(\mathbb{Q}(\mu_{f_\chi})/\mathbb{Q})$.

(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 put:

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

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 5.8. *The $\mathscr{G}$-module $\mathbf{C}_K$ is a free $\mathbb{Z}$-module; the families defined by $\mathbf{C}_K$, $\mathbf{F}_K = \mathbf{C}_K \cap \mathbf{E}_K$ and $\mathscr{F}_K$ 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 4.6, $\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(|\mathbf{C}_{\mathbb{Q}(\mu_f)}|) = |\mathbf{C}_{\mathbb{Q}(\mu_m)}|^\Omega$, where $\Omega = \prod\limits_{q \mid f,\, q \nmid m} \left(1 - \left(\frac{\mathbb{Q}(\mu_m)/\mathbb{Q}}{q}\right)\right)$, which generates all the norm formulas in $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$. □

5.3. **Computation of $\#\mathbf{H}_\chi^{\mathrm{ar}}$ for $\chi \in \mathscr{X}^+$.** Using Leopoldt's formula [Leo1954, Satz 21, § 8 (4)] and Propositions 5.4, 5.6, we obtain (see [Gra1976, Théorème III.1]):

Proposition 5.9. *For all $\chi \in \mathscr{X}^+$, $\#\mathbf{H}_\chi^{\mathrm{ar}} = \frac{Q_\chi}{q_\chi} \cdot (\mathbf{E}_\chi : \mathbf{C}_\chi^{\Delta_\chi})$, where $\Delta_\chi = \prod\limits_{\ell \mid g_\chi} \left(1 - \sigma_\chi^{g_\chi/\ell}\right)$. We then get the relation $\#\mathbf{H}_\chi^{\mathrm{ar}} = \frac{1}{q_\chi}\left(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \oplus \mathbf{C}_\chi^{\Delta_\chi}\right)$ interpreting the coefficient Q_χ (see [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 $\mathbf{F}_{K_\chi}$ 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 3.10 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 5.1) and let $\mathbf{F}_{K_\chi} = \mathbf{C}_{K_\chi} \cap \mathbf{E}_{K_\chi}$ (Definition 5.7).

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

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

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]. □

Remark 5.11. The local index $\big(\mathscr{E}_{K_\chi} : \mathscr{E}^0_{K_\chi} \oplus \mathscr{F}_{K_\chi}\big)$, deduced from that of Theorem 5.10, where $\mathbf{E}^0_{K_\chi} = \langle\, \mathbf{E}_k \,\rangle_{k \subsetneq K_\chi}$, gives, for $\mathscr{H} = \mathbf{H} \otimes \mathbb{Z}_p$, the formula:

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

and 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 $\mathscr{H}_\chi^{\rm alg}$ and Sinnott's cyclotomic units, more elaborate than classical Leopoldt's ones (Definition 5.7), but which give rise to intricate index formulas. As we have observed in [Gra1976/77, Remark III.1], a formula for $\#\mathscr{H}_\chi^{\rm alg}$ does not seem obvious because of capitulation aspects (see the numerical examples of § 2.4).

This point of view, which appears to have been ignored, seems much better suited for a proof of the Main Conjecture, especially in the non semi-simple case (see § 7.2), since the φ-components of $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \oplus \mathscr{F}_{K_\chi}$ are canonical with the classical Leopoldt definition of cyclotomic units, moreover independent of the problems raised by the splitting, in sub-extensions of K_χ, of ramified primes for Sinnott's cyclotomic units. For the non semi-simple case, we shall use the $\mathbb{Z}_p[G_\chi]$-module $\widetilde{\mathscr{E}}_\chi$ which is such that $\widetilde{\mathscr{E}}_\chi = \bigoplus\limits_{\varphi \mid \chi} \widetilde{\mathscr{E}}_\varphi$ as usual.

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 $\mathscr{T}_K = {\rm Gal}(H_K^{\rm pr}/K\mathbb{Q}^{\rm c})$, where $\mathbb{Q}^{\rm c}$ is the cyclotomic $\mathbb{Z}_p$-extension.

The order of this group is well known and given by the residue at $s = 1$ of the p-adic ζ-function of K, whence by the values at $s = 1$ of the p-adic $\mathbf{L}$-functions of the non-trivial characters of K (after [Coa1975, Appendix]; see for instance [Gra2019, § 3.4, formula (3.8)] and its references for analytic context, then [Gra2018a] for arithmetic interpretation given by the formula $\#\mathscr{T}_K = \#\mathscr{H}_K^{\rm c} \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K$ recalled in the Introduction):

$$\#\mathscr{T}_K \sim [K \cap \mathbb{Q}^{\rm c} : \mathbb{Q}] \cdot \prod_{\psi \neq 1} \tfrac{1}{2}\, \mathbf{L}_p(1, \psi). \tag{6.1}$$

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 transfers), we can state, in a similar context as for Theorems 3.8:

Theorem 6.1. *For all* $\chi \in \mathscr{X}^+$ *(resp.* $\varphi \in \Phi^+$*), we have:* $\mathscr{T}_\chi^{\rm ar} = \mathscr{T}_\chi^{\rm alg}$ *(resp.* $\mathscr{T}_\varphi^{\rm ar} = \mathscr{T}_\varphi^{\rm alg}$*); so we denote simply* $\mathscr{T}_\chi$ *(resp.* $\mathscr{T}_\varphi$*) these components. Moreover, if* $K/\mathbb{Q}$ *is real cyclic, we then have* $\#\mathscr{T}_K = \prod\limits_{\chi \in \mathscr{X}_K} \#\mathscr{T}_\chi = \prod\limits_{\varphi \in \Phi_K} \#\mathscr{T}_\varphi$.

In the analytic point of view, we have the analogue of Theorems 3.10 and 5.10:

Theorem 6.2. *Let $\mathscr{T}_\chi := \{x \in \mathscr{T}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneq K_\chi\}$ for any $\chi \in \mathscr{X}^+$. Let g_χ be the order of $\chi \in \mathscr{X}^+$, $\chi \neq 1$ (otherwise $\mathscr{T}_1 = \mathscr{T}_\mathbb{Q} = 1$), and let f_χ be its conductor; then:*

$$\#\mathscr{T}_\chi = w_\chi^{\mathrm{c}} \cdot \prod_{\psi|\chi} \tfrac{1}{2}\, \mathbf{L}_p(1,\psi),$$

where w_χ^{c} is as follows from formula (6.1):

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

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

In terms of annihilation of $\mathscr{T}_K$, we have the following statement [Gra2018b, Theorem 5.5] which does not assume any hypothesis on K and p and gives again the known results of annihilation (e.g., [Or1981] generalizing to the non semi-simple case and improving our results: *G. Gras, Annulation du groupe des ℓ-classes generalisées d'une extension abélienne réelle de degré premier à ℓ, Ann. Inst. Fourier,* **29***(1) (1979), 15–32.* https://doi.org/10.5802/aif.725):

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.*

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

Let $\mathscr{A}_K(c) := \lim_{n\to\infty} \Big[\sum_{a=1}^{f_n} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big)\Big] =: \mathscr{A}'_K(c) \cdot (1 + s_\infty)$.

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

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

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 $[K \cap \mathbb{Q}^{\mathrm{c}} : \mathbb{Q}] =: p^{n_0}$, and use the annihilators $\mathscr{A}_{K,n}(c)$, $\mathscr{A}'_{K,n}(c)$, the annihilator limit $\mathscr{A}_K(c)$ being related to p-adic $\mathbf{L}$-functions of primitive characters $\widetilde{\psi}$ associated to the Galois characters $\psi \in \Psi_K$ as follows:

$$\psi(\mathscr{A}_K(c)) = (1 - \psi(c)) \cdot \mathbf{L}_p(1,\psi) = (1 - \psi(c)) \cdot \prod_{\ell \nmid f_K,\, \ell \nmid p f_{\widetilde{\psi}}} \big(1 - \widetilde{\psi}(\ell)\ell^{-1}\big)\, \mathbf{L}_p(1,\widetilde{\psi}).$$

Of course, if $n_0 = 0$, since $\mathscr{H}_K$ is a quotient of $\mathscr{T}_K$, the element $\mathscr{A}_K(c)$ annihilates $\mathscr{H}_K$, as well as the normalized regulator $\mathscr{R}_K$; then the above expression $\psi(\mathscr{A}_K(c))$ annihilates $\mathscr{H}_\varphi^{\mathrm{alg}}$.

7. 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 $\varphi \mid \chi$, $\varphi \in \Phi$.

7.1. **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 $\mathscr{T}_\varphi$ are finite $\mathbb{Z}_p[\mu_{g_\chi}]$-modules whatever $\varphi \in \Phi = \Phi^+ \cup \Phi^-$; thus:

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

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

$$\begin{aligned}
m_\varphi^{\mathrm{alg}}(\mathscr{H}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{alg}}(\mathscr{H}), & m_\chi^{\mathrm{alg}}(\mathscr{H}) &:= \sum_{\varphi|\chi} \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{alg}}(\mathscr{H}),\\
m_\varphi^{\mathrm{ar}}(\mathscr{H}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{H}), & m_\chi^{\mathrm{ar}}(\mathscr{H}) &:= \sum_{\varphi|\chi} \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{H}),\\
m_\varphi^{\mathrm{ar}}(\mathscr{T}) &:= \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{T}), & m_\chi^{\mathrm{ar}}(\mathscr{T}) &:= \sum_{\varphi|\chi} \sum_{i\geq 1} n_{\varphi,i}^{\mathrm{ar}}(\mathscr{T}).
\end{aligned} \tag{7.1}$$

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

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

7.2. **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 2.16, 2.19 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 3.10, 5.10, 6.2).

7.2.1. *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 (where ω is the Teichmüller character):

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

(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}; 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:

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

$$m_\varphi^{\rm an}(\mathscr{H}^-) := 0, \text{ if } K_\chi = \mathbb{Q}(\mu_4).$$

7.2.2. *Case $\varphi \in \Phi^+$, $\varphi \neq 1$, for class groups.* From Definition 5.7 and Theorem 5.10, we consider, for any cyclic field K, where we recall that $\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K$:

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

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

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

Consider the relation $\#\mathscr{H}_\chi^{\rm ar} = w_\chi \cdot (\mathscr{E}_{K_\chi} : \mathscr{E}_{K_\chi}^0 \oplus \mathscr{F}_{K_\chi}) = w_\chi \prod_{\varphi|\chi} \#\widetilde{\mathscr{E}}_\varphi$ of Theorem 5.10; 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 $\varphi = \chi$. So, we may define $m_\varphi^{\rm an}(\mathscr{H}^+)$ as follows (the corresponding conjecture is proven by Greither [Grei1992, Theorem 4.14, Corollary 4.15], essentially in the tame case $p \nmid g_\chi$ and using Sinnott's definition of cyclotomic units):

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

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

(ii″) Case f_χ non prime power. Then $w_\chi = p$ 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 $w_\chi = 1$ and:

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

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

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

7.2.3. *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:

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

7.3. **Motivations for the Main Conjecture.** The conjectures we have given in [Gra1976, Gra1976/77, Gra1977] where simply equality of Arithmetic and Analytic Invariants, due to numerical observations, the specific property of the p-adic characters given by Theorem 2.23, 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 4.7, 4.8, 4.10, 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 7.1. *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 7.2 and the arithmetic expressions that we recall:

(i) Theorem 3.10 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 5.10 giving $\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot (\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \oplus \mathbf{F}_{K_\chi})$, for $\chi \in \mathscr{X}^+$,

(iii) Theorem 6.2 giving $\#\mathscr{T}_\chi = w_\chi^{\rm c} \cdot \prod_{\psi|\chi} \frac{1}{2}\,\mathbf{L}_p(1, \psi)$, 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 7.2. Before any proof of the above conjecture $\#\mathscr{H}_\varphi^{\rm ar} = (\mathscr{E}_{K_\varphi} : \mathscr{E}^0_{K_\varphi} \oplus \mathscr{F}_{K_\varphi})$ for even characters φ (g_χ non p-power, otherwise $\varphi = \chi$ makes the result obvious), about the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{H}_\varphi^{\rm ar}$ and $\widetilde{\mathscr{E}}_\varphi = \mathscr{E}_\varphi/\mathscr{E}_\varphi^0 \oplus \mathscr{F}_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\chi^{m_\varphi^{\rm an}(\mathscr{H}^+)}$, it will be interesting to prove first that $\mathfrak{p}_\chi^{m_\varphi^{\rm an}(\mathscr{H}^+)}$ annihilates $\mathscr{H}_\varphi^{\rm ar}$, which is not given by the well-known annihilation of $\mathscr{T}_\varphi$ (Theorem 6.3 and Remark 6.4).

8. Finite Iwasawa's principle

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*:

Theorem 8.1. *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 $\mathfrak{p}_\chi$ be the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$; in the isomorphism $\mathscr{E}_K^{e_\varphi}/\mathscr{E}_{K'}^{e_\varphi} \simeq \mathbb{Z}_p[\mu_{g_\chi}]$, where the e_φ's are the tame idempotents attached to $\mathbb{Z}_p[G_\chi]$, put:*

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

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

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

(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 8.2. *Let $\chi \in \mathscr{X}^-$ be such that $g_\chi = g_0 \cdot p^n$, $p \nmid g_0$, $n \geq 2$. Denote by χ' the rational character such that $[K_\chi : K_{\chi'}] = p$ and put $K := K_\chi$, $K' := K_{\chi'}$. Assume that the Stickelberger elements $\mathbf{B}_K$ and $\mathbf{B}_{K'}$ are p-integers in the group algebra and that $\mathbf{N}_{K/K'}(\mathbf{B}_K) = \mathbf{B}_{K'}$ (see Lemma 4.6 giving the ramification conditions). Put, for $\psi \mid \varphi \mid \chi$:*

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

(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 $G_0 := \mathrm{Gal}(k/\mathbb{Q})$ is of prime-to-p order, and let $k^{\mathrm{c}} = \bigcup_{n \geq 0} k_n$ be its cyclotomic $\mathbb{Z}_p$-extension. The condition $\mu = 0$ of Iwasawa's theory is here equivalent to the existence (for all the tame 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 8.1); 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 $p^\lambda = (\mathscr{E}_{k_n} : \mathscr{E}{k_n}^0\, \mathscr{F}k_n)$ for $n \gg 0$. Finally, Greenberg's conjecture [Gree1976] becomes $\mathscr{E}_{k_n} = \mathscr{E}_{k_n}^0 \cdot \mathscr{F}_{k_n}$ from some layer.

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

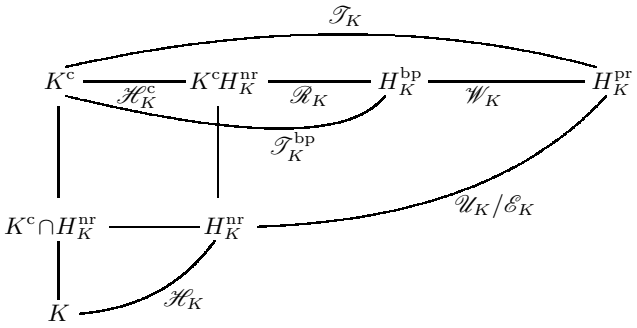
9. Class field interpretation of the regulators

We still consider a real abelian field K and we recall the classical diagram dealing with the p-adic invariants $\mathscr{H}_K$, $\mathscr{R}_K$, $\mathscr{U}_K/\mathscr{E}_K$, $\mathscr{W}_K := \big(\oplus_{v|p}\mu_p(K_v)\big)/\mu_p(K)$ (with obvious notations), and related to the exact sequence [Gra2005, Lemma III.4.2.4]:

$$1 \to \mathscr{W}_K \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}\big(\mathscr{U}_K/\mathscr{E}_K\big) \xrightarrow{\log_p} \mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}\big(\log_p\big(\mathscr{U}_K\big)/\log_p(\mathscr{E}_K)\big) \to 0, \tag{9.1}$$

[2] See Lemma 4.6 giving the ramification conditions for this. 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 K, at least from a suitable layer.

where $\mathscr{U}_K$ denotes the group of local units at p and where $\mathscr{E}_K = \mathbf{E}_K \otimes \mathbb{Z}_p$ is identified with its diagonal image in $\mathscr{U}_K$ (see [Gra2005, § III.2, (c), Fig. 2.2]):



Let's recall that $K^{\rm c}$ is the cyclotomic $\mathbb{Z}_p$-extension, $H_K^{\rm nr}$ the p-Hilbert class field, $H_K^{\rm pr}$ the maximal abelian p-ramified pro-p-extension, $H_K^{\rm bp}$ the Bertrandias–Payan field and $\mathscr{T}_K^{\rm bp} := {\rm Gal}(H_K^{\rm bp}/K^{\rm c})$, called the Bertrandias–Payan module (see [Ng1986, Section 4], [Jau1990, Section 2 (b)]). This Galois group may be compared with the "cyclotomic regulator" $\mathscr{R}_K^{\rm c}$ as follows.

Let's consider some p-adic formulas about $\mathbf{L}_p$-functions (from classical papers, as for instance [KL1964, AF1972, Gra1978/79a] and a very broad presentation in [Was1997, Theorems 5.18, 5.24, Thaine's Theorem 15.2 on annihilation of real p-class groups]):

$$\begin{aligned}\mathbf{L}_p(1,\psi) &= -\Big(1-\frac{\psi(p)}{p}\Big)\cdot\frac{\tau(\psi)}{f_\chi}\cdot\sum_{a=1}^{f_\chi}\psi^{-1}(a)\,\log_p(1-\zeta_{f_\chi}^a),\\ \#\mathscr{T}_\chi &\sim w_\chi^{\rm c}\cdot\prod_{\psi\mid\chi}\tfrac{1}{2}\,\mathbf{L}_p(1,\psi),\quad w_\chi^{\rm c}\in\{1,p\}\ \text{(Theorem 6.2)},\end{aligned}\tag{9.2}$$

where $\tau(\psi)$ is the usual Gauss sum.

To simplify the comments, we shall assume to be in the general case $w_\chi^{\rm c}=1$ and $\mathscr{W}_K=1$ which gives $\mathscr{T}_K=\mathscr{T}_K^{\rm bp}$, $\#\mathscr{T}_\chi\sim\prod_{\psi\mid\chi}\frac{1}{2}\,\mathbf{L}_p(1,\psi)$, and the following result using the Main Theorem:

Theorem 9.1. *Let $K=K_\chi$, $\chi\in\mathscr{X}^+$, $\chi\neq1$, be such that $\big(\bigoplus_{v\mid p}\mu_p(K_v)\big)/\mu_p(K)=1$, $K\cap\mathbb{Q}^{\rm c}=\mathbb{Q}$ and $K^{\rm c}\cap H_K^{\rm pr}=K$. We have the exact sequence $1\to\mathscr{R}_\chi\to\mathscr{T}_\chi\to\mathscr{H}_\chi\to1$ and $\#\mathscr{T}_\chi=\#\mathscr{R}_\chi^{\rm c}$ where:*

$$\mathscr{R}_\chi^{\rm c}:={\rm tor}_{\mathbb{Z}_p}(\mathscr{U}_\chi/\mathscr{E}_\chi^0\oplus\mathscr{F}_\chi)={\rm tor}_{\mathbb{Z}_p}(\log(\mathscr{U}_\chi)/\log(\mathscr{E}_\chi^0\oplus\mathscr{F}_\chi)).$$

In the semi-simple case, we get the exact sequence $1\to\mathscr{R}_\varphi\to\mathscr{T}_\varphi\to\mathscr{H}_\varphi\to1$, for all $\varphi\mid\chi$, and $\#\mathscr{T}_\varphi=\#\mathscr{R}_\varphi^{\rm c}$. Defining $m_\varphi(\mathscr{R}^{\rm c})$, for all $\varphi\neq1$, by means of the isomorphism:

$$\mathscr{R}_\varphi^{\rm c}=\big(\log(\mathscr{U}_\chi)/\log(\mathscr{E}_\chi^0\oplus\mathscr{F}_\chi)\big)^{e_\varphi}\simeq\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\chi^{m_\varphi(\mathscr{R}^{\rm c})},$$

we get $m_\varphi(\mathscr{R}^{\rm c})=m_\varphi(\mathscr{R})+m_\varphi(\mathscr{H})$.

10. Numerical illustrations with cyclic cubic fields

As we have seen, in the semi-simple case, for any irreducible even rational character χ and any p-adic character $\varphi\mid\chi$ we have $\#\mathscr{H}_\varphi=(\mathscr{E}_\varphi:\mathscr{E}_\varphi^0\oplus\mathscr{F}_\varphi)$ and:

$$\mathscr{E}_\varphi/\mathscr{E}_\varphi^0\oplus\mathscr{F}_\varphi\simeq\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\chi^{m_\varphi^{\rm an}(\mathscr{H})},\ m_\varphi^{\rm an}(\mathscr{H})\geq0,\qquad\mathscr{H}_\varphi\simeq\bigoplus_{i=1}^{r_p}\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\chi^{m_{\varphi,i}^{\rm ar}(\mathscr{H})},\ m_{\varphi,i}^{\rm ar}(\mathscr{H})\geq0,$$

for a decreasing sequence $(m_{\varphi,i}^{\rm ar}(\mathscr{H}))_i$ giving $m_\varphi^{\rm an}(\mathscr{H})=\sum_{i=1}^{r_p}m_{\varphi,i}^{\rm ar}(\mathscr{H})$.

We intend to see more precisely what happens for these analytic and arithmetic invariants since the above equality can be fulfilled in various ways. We will examine the case of the cyclic cubic fields K for primes $p\equiv1\pmod3$ giving two p-adic characters; in that case, $\mathscr{E}_\varphi^0=1$ and $\#\mathscr{H}_\varphi=(\mathscr{E}_\varphi:\mathscr{F}_\varphi)$.

For $p=7$, the two possible kind of representations, for $\mathscr{E}_\varphi/\mathscr{F}_\varphi$, are $\mathbb{Z}_7[j]/(-2+j)^m$ and $\mathbb{Z}_7[j]/(3+j)^m$, $m\geq0$ ($j^2+j+1=0$).

10.1. **Description of the method.** 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 modules $\mathscr{E}_K/\mathscr{F}_K$ and $\mathscr{H}_K$ could be misleading, is the definition of a generator σ of $\mathrm{Gal}(K/\mathbb{Q})$ 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 clear conjugation does exist for the invariants given by $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P})$ from the explicit instruction $\mathsf{G} = \mathsf{nfgaloisconj}(\mathsf{P})$ giving x^σ under the form $g(x)$, $g \in \mathbb{Q}[X]$, for a root x of the defining polynomial P.

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 σ-conjugate ε^σ such that $\langle \varepsilon, \varepsilon^\sigma \rangle = E_K$. 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 a permutation $(\varepsilon, \varepsilon^\sigma) \mapsto (\varepsilon^\tau, \varepsilon^{\tau\sigma})$, $\tau \in \mathrm{Gal}(K/\mathbb{Q})$.

For security, we test $\mathsf{reg_1}/\mathsf{Reg} = 1$ where $\mathsf{reg_1}$ is computed with a root ρ and where $\mathsf{Reg} = \mathsf{K.reg}$ is the true regulator given by PARI.

Then we must write the cyclotomic unit η of K 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 $|\mathbf{C}| = \prod_{a \in [1, f/2[, \sigma_a \in A_\chi} |\zeta_{2f}^a - \zeta_{2f}^{-a}|$ (f is the conductor of K), as product of the $|\zeta_{2f}^a - \zeta_{2f}^{-a}|$ for the integers $a < f/2$ such that the Artin symbol $\left(\frac{Q(\mu_f)/\mathbb{Q}}{a}\right)$ is in $\mathrm{Gal}(K/\mathbb{Q})$ (which is tested using prime numbers congruent to a modulo f).

If f is prime, $\zeta_{2f} - \zeta_{2f}^{-1}$ generates the prime ideal above p; thus, $\pi := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\zeta_{2f} - \zeta_{2f}^{-1})$ is such that $\pi^3 = f \cdot \eta'$, $\eta' \in \mathbf{E}_K$, whence $\pi^{3\,(1-\sigma)} = \eta'^{1-\sigma} = \eta^6$ (Proposition 5.9); the program computes $3\log(\mathbf{C}) - \frac{1}{2}\log(f)$ so that we must divide the regulator RegC by 3 and $\alpha + j\,\beta$ by $1 - j^2$ 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 5.10), 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 $y^{\mathrm{Frob}(q)} \equiv y^q \pmod q$ for any integer y of K and any prime q inert in $K/\mathbb{Q}$; using $x^\sigma = g(x)$, we test the congruence $g(x) - x^q \pmod q$ to decide if $\sigma = \mathrm{Frob}(q)$ or $\mathrm{Frob}(q)^2$, in wich case $\zeta_{2f}^\sigma = \zeta_{2f}^q$ or $\zeta_{2f}^{q^2}$, giving easily the conjugate η^σ.

Then, to compute $\mathfrak{q}^\sigma$ for a prime ideal $\mathfrak{q} \mid q$ of degree 1 given trough PARI instructions, we use the instruction $\mathsf{nfgaloisapply}(\mathsf{K}, \mathsf{G}[2], \mathsf{Q})$, where Q is an ideal dividing q and where $\mathsf{G}[2]$ gives the conjugate by σ.

10.2. **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 on abelian fields); $\mathsf{hmin} = \mathsf{p^{vp}}$ means that the program only computes fields with p-class groups CKp of order at least $\mathsf{p^{vp}}$, 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/2o6rqpy815qcru2/Program.pdf?dl=0):

```
\p 50
{p=7; \\ Take any 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,hf=valuation(f,3);if(hf!=0 & hf!=2,next);
F=f/3^hf;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(hf==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(hf==0,if(Mod(a,3)==1,a=-a);P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);
if(hf==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=2,2*10^5,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]); \\ Roots 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);reg=l1^2+l1*l2+l2^2;quot=reg/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;
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);
\\ Writting 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 = valuation of CKp, ve = valuation of the exponent 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 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));
```

```
\\ We replace ai by an equivalent split prime ideal above qi (List Lq):
L0=List;for(i=1,r,listput(L0,0,i));Lq=List;LH=List;LsH=List;
for(i=1,rp,
forprime(q=5,2*10^5,fac=idealfactor(K,q);if(matsize(fac)[1]!=3,next);
\\ We test the non-principality of the prime ideal Q:
Q=component(fac,1)[1];if(List(bnfisprincipal(K,Q)[1])==L0,next);
cij=Q;for(j=1,EKp[i],cij=idealmul(K,cij,CKp[i]);if(Mod(j,p)==0 & j!=EKp[i],next);
if(List(bnfisprincipal(K,cij)[1])==L0,listput(Lq,q,i);
Qi=Q;sQi=nfgaloisapply(K,G[2],Qi); \\ Qi=prime ideal dividing qi, sQi=sigma(Qi)
\\ Computation of the matrices h and sh of Qi and sQi on the PARI basis of CK
h=bnfisprincipal(K,Qi)[1];sh=bnfisprincipal(K,sQi)[1];
print("h=",h,", ","sigma(h)=",sh);listput(LH,h,i);listput(LsH,sh,i);break(2)));
print("auxiliary primes qi: ",Lq);
\\ 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=(j+ci),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)))))}
```

10.3. **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 for this example that:

$$\mathsf{e}_1 = 3062171948818717694.348000505806 \quad \text{and} \quad \mathsf{e}_2 = 1.221295564694\ \mathsf{E}-69,$$

which explains what happens.

10.3.1. *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 cyclotomic units; thus we have $\eta = \varepsilon^{\alpha+\beta\,\sigma}$ and obtain the isomorphism:

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

where j is root of $\mathsf{S} := \mathsf{y}^2 + \mathsf{y} + 1$. For instance, for $p = 7$, we put $\mathfrak{p}_1 := (-2 + j)\mathbb{Z}[j]$ and $\mathfrak{p}_1 := (3 + j)\mathbb{Z}[j]$; 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 $\mathscr{E}_K/\mathscr{F}_K$.

In all the sequel, from a factorization $p = (r_1 + j) \cdot (r_2 + j)$ in $\mathbb{Z}[j]$, we associate $\mathfrak{p}_1$ (resp. $\mathfrak{p}_2$) with any annihilator $c_1 + \sigma \equiv r_1 + \sigma \pmod{p^e}$ (resp. $c_2 + \sigma \equiv r_2 + \sigma \pmod{p^e}$) in $\mathbb{Z}_p[G]$, such that $(c_i + j) = \mathfrak{p}_i^e$, $i = 1, 2$; this preserves the definition of the φ_1 and φ_2-components.

10.3.2. *Galois structure of $\mathscr{H}_K$.* Concerning the structure of $\mathscr{H}_K$, recall that the instruction bnfisprincipal(K, Ideal)[1] gives the matrix of components, of the class of the ideal, on the basis $\{h_1, h_2, \ldots, h_r\}$ given by K.clgp (in CK) and the fact that 0 means that the corresponding component of cl(Ideal), on h_i, is trivial.

Since the Galois action on the h_i is not given by PARI, we have replaced this classes by that of a prime ideal $\mathfrak{Q}_i \mid q_i$, for auxiliary primes q_i ($1 \leq i \leq r_p$), for which the Galois action is computed; so the Galois structure of $\mathscr{H}_K$ becomes linear algebra from the matrices given by the program, via the relations $h = \prod_{i=1}^{r} h_i^{a_i}$ and $h^\sigma = \prod_{i=1}^{r} h_i^{b_i}$.

(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 identical in all our computations (to be read in columns). 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
auxiliary primes qi: List([5])
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 $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathscr{H}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_1$; whence the two columns given by the program; the valuations

v 0

in a line mean that $\mathscr{M}_K \simeq \mathbb{Z}[j]/\mathfrak{p}_1^v \cdot \mathfrak{p}_2^0$ and so on. We deduce that $\mathscr{T}_K = \mathscr{H}_K \bigoplus \mathscr{R}_K$.

```
P=x^3+x^2-2450*x-108 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
auxiliary primes qi: List([11])
h=[48]~,  sigma(h)=[19]~
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 $(\alpha + j\,\beta) = \mathfrak{p}_1^2\,\mathfrak{p}_2^0$; for an exponent 7^2, $c_1 = 19$, $c_2 = 31$. With $c_2 = 31$, we get $(31 + \sigma)(\alpha + \sigma\beta) = 343 - 49\sigma \equiv 0 \pmod{7^2}$, whence a trivial φ_2-component (or compute directly $\widetilde{\mathscr{E}}_{\varphi_2}$ with the definition).

Then $h^{(31+\sigma)(a+b\sigma)} = h^{31a-b+\sigma(a+30b)} = 1$ if and only if $b \equiv 31a \pmod{7^2}$ and $a \equiv -30b \pmod{7^2}$, equivalent to the first relation, whence a non trivial φ_1-component since $1 + 31j \equiv 19 + j \equiv 0 \pmod{\mathfrak{p}_1^2}$. 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 $\mathscr{H}_K \simeq \mathscr{T}_K/\mathscr{R}_K$.

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
auxiliary primes qi: List([5])
h=[260]~,  sigma(h)=[221]~
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 structures are similar with the φ_2-components. 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 PARI 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.

```
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
auxiliary primes qi: List([13,43])
h=[6,0]~, sigma(h)=[0,6]~
h=[0,5]~, sigma(h)=[2,2]~
1  1   P1 and P2-valuations for alpha+j*beta
0  0   Determinants Delta1, Delta2
R11=4*X+2*Y  R12=6*X+3*Y
R21=2*X+2*Y  R22=6*X+6*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 $\mathsf{R11} = 2 * \mathsf{X} + 1 * \mathsf{Y}$ and $\mathsf{R21} = 4 * \mathsf{X} + 4 * \mathsf{Y}$. Thus $\mathscr{H}_K = \mathscr{H}_{\varphi_1} \oplus \mathscr{H}_{\varphi_2} \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$. 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
auxiliary primes qi: List([521])
h=[6,0,0,0]~, sigma(h)=[108,0,0,0]~
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
auxiliary primes qi: List([[373,14197]])
h=[26,0]~, sigma(h)=[66,6]~
h=[0,6]~, sigma(h)=[42,10]~
2  1   P1 and P2-valuations for alpha+j*beta
0  0   Determinants Delta1,Delta2
R11=21*X+42*Y  R12=6*X+26*Y
R21=39*X+42*Y  R22=6*X+0*Y
Structure of the 7-torsion group: List([49,7,7])
```

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
auxiliary primes qi: List([103,3121])
h=[172,0]~, sigma(h)=[352,4]~
h=[0,8]~,  sigma(h)=[0,2]~
1    3   P1 and P2-valuations for alpha+j*beta
105  0   Determinants Delta1,Delta2
R11=190*X+0*Y  R12=4*X+154*Y
R21=0*X+0*Y  R22=4*X+201*Y
Structure of the 7-torsion group: List([343,49])
```

In that case, $\mathscr{T}_K \simeq Z/7^3\mathbb{Z} \oplus \mathbb{Z}/7^2\mathbb{Z}$ and $\mathscr{R}_K = (\mathbb{Z}/7^3\mathbb{Z})^0 \times (7\,\mathbb{Z}/7^2\mathbb{Z})$ 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)=(21.000000000000,14.000000000000), Index [E_K:C_K]=343.000000000000
auxiliary primes qi: List([467,773,1871])
h =[9,0,0]~, sigma(h) =[3,5,0]~
h'=[0,6,0]~, sigma(h')=[18,6,0]~
h"=[0,0,5]~, sigma(h")=[9,4,3]~
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:

```
[1029,[21,7,7],[[2,1,0;0,1,0;0,0,1],[4,2,3;0,2,1;0,0,1],[53,28,15;0,1,0;0,0,1]]]
```

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

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

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:

$$\widetilde{\mathscr{E}}_{\varphi_1} = \{x \in \mathbb{Z}_7[j]/\mathfrak{p}_1^2\,\mathfrak{p}_2,\ \ (19+\sigma)\cdot x = 1\} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_1^2,$$
$$\widetilde{\mathscr{E}}_{\varphi_2} = \{x \in \mathbb{Z}_7[j]/\mathfrak{p}_1^2\,\mathfrak{p}_2,\ \ (31+\sigma)\cdot x = 1\} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_2.$$

To obtain the two φ-components of $\mathscr{H}_K = \mathscr{T}_K$, we put $H = h^x h'^y h''^z$ 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):

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

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

$$x - 4y - 2z = 0 \ \text{ (for } H^{-2+\sigma} = 1) \ \text{ and } \ x + 2y = 0 \ \&\ z = 0 \ \text{ (for } H^{3+\sigma} = 1).$$

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

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

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; nevertheless the structures of $\mathbb{F}_7$-vector spaces are the same since $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_1^2 \simeq \mathbb{F}_7^2$.

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
auxiliary primes qi: List([6091,34537,1723])
h =[15,0,0]~, sigma(h) =[15,3,0]~
h'=[0,6,0]~,  sigma(h')=[15,9,0]~
h"=[0,0,3]~,  sigma(h")=[3,18,5]~
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
auxiliary primes qi: List([29327,78577,2797])
h =[156,0,0]~, sigma(h) =[0,6,4]~
h'=[0,5,0]~,   sigma(h')=[234,2,4]~
h"=[0,0,3]~,   sigma(h")=[0,0,6]~
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
auxiliary primes qi: List([7])
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
auxiliary primes qi: List([47])
h=[93]~, sigma(h)=[18]~
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
auxiliary primes qi: List([71,13])
h=[3,0]~, sigma(h)=[9,0]~
h=[0,6]~, sigma(h)=[9,2]~
1  1   P1 and P2-valuations for alpha+j*beta
0  0   Determinants Delta1,Delta2
R11=8*X+9*Y  R12=0*X+0*Y
R21=0*X+9*Y  R22=0*X+10*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
auxiliary primes qi: List([17,43])
h=[12,0]~, sigma(h)=[4,0]~
h=[0,3]~,  sigma(h)=[0,1]~
0  2   P1 and P2-valuations for alpha+j*beta
0  9   Determinants Delta1,Delta2
R11=0*X+0*Y  R12=0*X+0*Y
R21=7*X+0*Y  R22=0*X+5*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
auxiliary primes qi: List([19])
h=[501]~, sigma(h)=[495]~
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
auxiliary primes qi: List([977,337])
h=[42,0]~, sigma(h)=[30,15]~
h=[0,4]~,  sigma(h)=[12,4]~
1  1   P1 and P2-valuations for alpha+j*beta
0  0   Determinants: Delta1,Delta2
R11=5*X+12*Y  R12=15*X+17*Y
R21=2*X+12*Y  R22=15*X+14*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'=[0,23]~, sigma(h')=[23,0]~
auxiliary primes qi: List([5,983])
1  1  P1 and P2-valuations for alpha+j*beta
0  0   Determinants: Delta1,Delta2
R11=5*X+23*Y   R12=30*X+14*Y
R21=25*X+23*Y  R22=30*X+9*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]~
auxiliary primes qi: List([5])
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 may be used to make statistics about the repartition of the various structures of class groups $\mathscr{H}_\varphi$ and quotients $\widetilde{\mathscr{E}}_\varphi = \mathscr{E}_\varphi/\mathscr{E}_\varphi^0\mathscr{F}_\varphi$. Some probabilistic approaches, taking into account the relations between these invariants, due to the Main Theorem, may confirm (or not) the classical 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 to another project, as well as a new proof of the Main Theorem in the real non semi-simple case using the statement with arithmetic φ-objects.

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, 5, 23, 25, 27, 28, 30, 31, 32
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, 5, 28, 30, 31
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. 3, 23, 28
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. 23
http://www.numdam.org/item/?id=STNG_1974-1975__4__A1_0

[Has1952] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin (1952). 20, 21, 22, 23, 27

[Iwa1962a] K. Iwasawa, A class number formula for cyclotomic fields, Ann. of Math., Second Series **76**(1) (1962), 171–179. 23
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, 18, 22, 26, 27

[Leo1962] H.W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, Jour, für die reine und ang. Math. **209** (1962), 54–71. 4, 14, 23, 26

[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. 33
http://eudml.org/doc/150624

[Or1975a] B. Oriat, Quelques caractères utiles en arithmétique, Publications Mathématiques de Besançon (1975), no. 4, 27 pp. 4, 15, 27
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, 22, 26
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)

[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 33

[All2013] T. All, On p-adic annihilators of real ideal classes, J. Number Theory **133**(7) (2013), 2324–2338. 3, 23
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, 23
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. 3
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. 23
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, 5, 30, 31
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. 23, 26
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. 3, 32, 33
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
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. 31
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). 3, 31, 32, 33

[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. 3, 28
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, 29
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, 28, 34
https://doi.org/10.1090/mcom/3395

[Gra2021] 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. 2, 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. 2, 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. 32
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, 10, 28, 30, 31
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
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 33

[Jau1998] J-F. Jaulent, Théorie ℓ-adique globale du corps de classes, J. Théorie Nombres Bordeaux **10**(2) (1998), 355–397. 3
https://doi.org/10.5802/jtnb.233

[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

[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. 3, 33
https://doi.org/10.5802/aif.1045

[Or1981] B. Oriat, Annulation de groupes de classes réelles, Nagoya Math. J. **81** (1981), 45–56. 3, 29, 31
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, 31
https://doi.org/10.4064/aa-46-4-331-354

[Pari2016] The PARI Group, *PARI/GP, version* `2.9.0`, Université de Bordeaux (2016). 34

[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). 2, 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. 2, 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

[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. 23
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, 10, 30
https://doi.org/10.5802/aif.1221

[Was1997] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997. 2, 12, 22, 23, 33

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