# Application of the notion of $\varphi$-object to the study of $p$-class groups and $p$-ramified torsion groups of abelian extensions

Georges Gras

# APPLICATION OF THE NOTION OF $\varphi$-OBJECT TO THE STUDY OF $p$-CLASS GROUPS AND $p$-RAMIFIED TORSION GROUPS OF ABELIAN EXTENSIONS

GEORGES GRAS

ABSTRACT. We revisit, in an elementary way, the statement of the "Main Conjecture for $p$-class groups", in abelian fields $K$, in the non semi-simple case $p \mid [K:\mathbb{Q}]$; for this, we use an "arithmetic" definition of the $p$-adic isotopic components, different from the "algebraic" one used in the literature but not pertinent. The two notions coincide for relative class groups and real $p$-ramified torsion groups, but not for real class groups. Numerical evidence of the gap between the two notions is given (Examples 3.12, 3.13). It would remain to make use of some classical tools (as Kolyvagin Euler systems) for this new non semi-simple real context, still unproved as explained in § 1.4 of the Introduction.

## CONTENTS

Foreword and preliminary remarks 2
1. Introduction and brief historical survey 3
1.1. Main bibliographic reminders 3
1.2. Introduction of Arithmetic $\varphi$-objects 3
1.3. Relation between the modules $\mathscr{H}$ and $\mathscr{T}$ 4
1.4. Main problem today 4
2. Abelian extensions 4
2.1. Characters 5
2.2. Main results of the article 5
3. Definition and study of the $\varphi$-objects 6
3.1. The Algebraic and Arithmetic $\mathscr{G}$-families 6
3.2. Definition of the $\mathscr{G}$-modules $\mathbf{M}_\chi^{\rm alg}$, $\mathbf{M}_\chi^{\rm ar}$, $\mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}_\varphi^{\rm ar}$ 7
3.3. Comparison with classical definitions 10
3.4. Numerical examples 10
3.5. Arithmetic factorization of $\#\mathbf{M}_K$ and $\#\mathscr{M}_K$ 13
4. Semi-simple decomposition of $\mathscr{A}_\chi := \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$ 14
4.1. Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\rm alg}$ 15
4.2. Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\rm ar}$ 17
4.3. Summary of the properties of the $\mathbb{Z}_p[\mathscr{G}]$-families $\mathscr{M}^{\rm alg}$ and $\mathscr{M}^{\rm ar}$ 17
5. Application to relative class groups 18
5.1. Arithmetic definition of relative class groups 18
5.2. Proof of the equality $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$, for all $\chi \in \mathscr{X}^-$ 18
5.3. Computation of $\#\mathbf{H}_\chi^{\rm ar}$ for $\chi \in \mathscr{X}^-$ 21
5.4. Annihilation theorem for $\mathbf{H}_K^-$ 22
6. Application to torsion groups of abelian $p$-ramification 25
6.1. Computation of $\#\mathscr{T}_K$ for $\chi \in \mathscr{X}^+$ 26
6.2. Annihilation theorem for $\mathscr{T}_K$ 26
7. Application to class groups of real abelian extensions 27
7.1. The Leopoldt $\chi$-units 27
7.2. The Leopoldt cyclotomic units 28
7.3. Arithmetic computation of $\#\mathbf{H}_\chi^{\rm ar}$, $\chi \in \mathscr{X}^+$ 28

*Date*: January 30, 2022.
2020 *Mathematics Subject Classification.* Primary 11R18, 11R29, 11R27 ; Secondary 11R37, 12Y05, 08-04.
*Key words and phrases.* abelian fields; $p$-adic characters; class groups and units; $p$-adic L-functions; cyclotomic polynomials; class field theory.

7.4. Class field theory and regulators 29
7.5. Annihilation conjecture for real $p$-class groups 30
8. Invariants (Algebraic, Arithmetic, Analytic) 31
8.1. Algebraic and Arithmetic Invariants $m^{\rm alg}(\mathscr{M})$, $m^{\rm ar}(\mathscr{M})$ 31
8.2. Analytic Invariants $m^{\rm an}(\mathscr{M})$ 32
8.3. Main Conjecture – 1976 original statement 33
8.4. Finite Iwasawa's theory in cyclic $p$-extensions 34
9. Numerical illustrations with cyclic cubic fields 35
9.1. Description of the computations 35
9.2. The general PARI program 36
9.3. Numerical examples 37
10. Conclusion 42
References 42
Original references of the 1976's papers 42
Current References 42

## Foreword and preliminary remarks

This survey provides improvements, new results and numerical illustrations (with PARI programs [Pari2016]), from our original articles in French [Gra1976, Gra1977] and some pioneering articles described in § 1.1.

The "Main Conjecture", about the equality of Arithmetic and Analytic Invariants (giving orders of the $p$-adic isotopic components of class groups) in the theory of abelian fields that we revisit here, were stated in the papers mentioned above (but not in [Gra1977$^b$] as erroneously stated by some authors), 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 [Leo1954, Leo1962] on cyclotomy, written in Germain, in the 1950/1960's.

This conjecture has been proven in the semi-simple case, then in the non semi-simple case for relative class groups and Iwasawa's theory.

The *non semi-simple case of even p-adic characters*, was less understood because of a problematic definition of $p$-adic isotopic components and cyclotomic units; but at the time, we proposed another more natural conjectural context, still unproved to our knowledge, for which the definition of "Arithmetic $\varphi$-objects" may be necessary since the distinction between "algebraic" and "arithmetic" definitions is crucial (see more comments in Remarks 7.11).

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

(i) An algebraic part giving a systematic study of families $(\mathbf{M}_K)_K$ of $\mathbb{Z}[\mathscr{G}]$-modules and of the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_K := \mathbf{M}_K \otimes \mathbb{Z}_p$, including the non semi-simple case $p \mid [K : \mathbb{Q}]$. 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 $\varphi$ of $\mathscr{G}$ (notion of $\varphi$-objects).

The difference between $\mathscr{M}_\varphi^{\rm alg}$ (used in all the literature) and $\mathscr{M}_\varphi^{\rm ar}$ is that the first one relates to algebraic norms $\nu_{k/k'} \in \mathbb{Z}[{\rm Gal}(k/k')]$ for their properties in relative sub-extensions of $K/\mathbb{Q}$, while the second one uses arithmetic norms $\mathbf{N}_{k/k'}$, the gap being given by the relation:

$$\nu_{k/k'} = \mathbf{J}_{k/k'} \circ \mathbf{N}_{k/k'},$$

where the transfer maps $\mathbf{J}_{k/k'}$, of $\mathbb{Z}_p[\mathscr{G}]$-modules, are often non injective in $p$-extensions (see § 3.3 for various contexts and some examples justifying the Definition 3.11 for the statement of the Main Conjecture). Moreover, the "arithmetic" point of view allows more natural analytic formulas (as that given by Theorems 3.15, 4.5, claiming that $\#\mathscr{M}_K = \prod_{\varphi \in \Phi_K} \#\mathscr{M}_\varphi^{\rm ar}$). See § 4.3 for the main properties of these families.

(ii) An arithmetic part where we apply the results on $\varphi$-objects to $p$-class groups $\mathscr{H}_K$, $K$ real or imaginary, then to 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 $\chi$ and any $p$-adic character $\varphi \mid \chi$, 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) then, in § 8.2, we define the corresponding "Analytic Invariants" $m_\varphi^{\rm an}(\mathscr{H})$, $m_\varphi^{\rm an}(\mathscr{T})$ suggested by the classical analytic formulas obtained for the arithmetic $\chi$-components (Theorems 5.10, 6.2, 7.9) and we develop the problem of their comparison (where $m_{\varphi(\mathscr{M})}$ denotes the $p$-valuation of $\#\mathscr{M}_\varphi$). We conjecture a new annihilation theorem for $\mathscr{H}_\varphi^{\rm ar}$, for any even $\varphi$ in the non semi-simple case (Conjecture 7.13).

(iii) An illustration, in the semi-simple case, is given with cyclic cubic fields for $p \equiv 1 \pmod 3$, as well as a PARI program computing the above invariants, which was not possible in the 1970's. It would remain to give non semi-simple computations to verify the conjecture in the real case.

## 1. Introduction and brief historical survey

1.1. **Main bibliographic reminders.** It is difficult to give here the full story of such a subject, from Bernoulli, Kummer, Herbrand classical context, the initiating work of Iwasawa, Leopoldt, Greenberg, on the conjecture, then the deep results obtained by Ribet, Mazur, Wiles, Thaine, Rubin, Kolyvagin, Solomon, Greither, Coates, Sinnott, and others, on cyclotomy and $p$-adic **L**-functions. Several papers also give the Iwasawa formulation of the Main Theorem (see e.g., [Gree1975, Gree1977]); Iwasawa's theory is less general than the expected results for finite extensions, but more conceptual in broader contexts (in fact, describing the similarity with the theory of $p$-adic **L**-functions, a generalizable feature to many fields in number theory). Let's give less known contributions:

We refer, for a very nice story of pioneering works, to Ribet [Rib2008, Rib2008$^b$] for detailed proofs of Iwasawa Main Conjecture, to Washington [Was1997, Chap. 15] following techniques initiated by Thaine then Kolyvagin, Ribet (described by Lang [Lang1990]). A Bourbaki Seminar, by Bernadette Perrin-Riou [PeRi1990], gives a significant lecture (with an impressive bibliography) on the works of Kolyvagin, Rubin and others about the Main Conjectures for number fields and elliptic curves.

Finally, proofs of our conjecture 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 were given (Solomon for $\mathscr{H}^-$ and $p \neq 2$ [Sol1990, Theorem II.1], Greither for $\mathscr{H}^-$, $\mathscr{T}$ with $p \geq 2$ and $\mathscr{H}^+$ in a semi-simple context [Grei1992, Theorems A, B, C, 4.14, Corollary 4.15]). Let us mention the proof by Rubin [Rub1990], from Kolyvagin Euler systems [Kol2007] used in above proofs. Many complementary works about the order or the annihilation of the $\mathscr{H}_\varphi$'s, for irreducible $p$-adic characters $\varphi$, were published before or after the decisive proofs (e.g., [Gra1977$^b$, Gil1977, Gra1979, Or1981, Or1986, GrKu2004, BeNg2005, All2013, BeMa2014, GrKu2014, All2017, Gra2018$^b$, GrKu2021]). Let's mention, for example, the (not very well-known) result of Oriat [Or1986, Theorem, p. 333] using reflection theorem.

In the same way, it is hopeless to outline all generalizations giving "Main Conjectures" in other contexts than the absolute abelian case (e.g., [Dar1995, MaRu2011, CoLi2019, DaKa2020, CoLi2020, BBDS21, BDSS21]); an expository book may be [CoSu2006] for recent works, but excluding the story of the origins of the Main Conjecture as explained in Solomon–Greither papers [Sol1990, Grei1992], Washington's book [Was1997] and Ribet's Lectures [Rib2008, Rib2008$^b$].

In another direction, we refer to enlargements of the algebraic/arithmetic aspects of $p$-adic characters in the area of metabelian Galois groups by Jaulent, with applications to class groups and units (see for instance [Jau1981, Théorème 1 and consequences], [Jau1984, Jau1986] in a class field theory context, then [Lec2018, SchS2019] in a geometric or Galois cohomology context).

Due to the huge number of articles dealing with the concept of "Main Conjecture", many recent (or not) articles may have escaped our notice.

1.2. **Introduction of Arithmetic $\varphi$-objects.** Nevertheless, all these works deal with an *algebraic definition of $\varphi$-class groups* (for irreducible $p$-adic characters $\varphi$); that is to say, when $G := {\rm Gal}(K/\mathbb{Q})$ is cyclic, of order $g$ (i.e., $K$ is the fixed field of a rational character $\chi$ and $\varphi \mid \chi$),

$$\mathscr{H}_\varphi^{\rm alg} := \mathscr{H}_K \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\mu_g],$$

with the $\mathbb{Z}_p[\mu_g]$-action $\sigma \in G \mapsto \psi(\sigma)$ ($\psi \mid \varphi$ of order $g$). We then prove that:

$$\mathscr{H}_\varphi^{\rm alg} = \{x \in \mathscr{H}_K,\ \nu_{K/k}(x) = 1,\ \forall\, k \subsetneqq K\} \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\mu_g] \text{ (Theorem 3.7)}$$

(where $\nu_{K/k}$ is the algebraic norm), contrary to our definition:

$$\mathscr{H}_\varphi^{\rm ar} := \{x \in \mathscr{H}_K,\ \mathbf{N}_{K/k}(x) = 1,\ \forall\, k \subsetneq K\} \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\mu_g],$$

where $\mathbf{N}_{K/k}$ is the arithmetic norm (see § 2.2 for other equivalent definitions of $\mathscr{H}_\varphi^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar}$ using cyclotomic polynomials, then for a summary of the main properties and results of the paper).

In the non semi-simple case $p \mid g$, the distinction between algebraic and arithmetic $\varphi$-components is not done in the literature. This does not matter for relative $p$-class groups $\mathscr{H}_K^-$ and torsion $p$-groups $\mathscr{T}_K$ since we will prove that the two notions coincide (Theorems 5.8, 6.1); so the case of these invariants is definitely solved, contrary to that of $\varphi$-components of $p$-class groups of real fields $K$ in the non semi-simple case deduced from the "$\chi$-formulas" given in Theorem 7.9 and the relation:

$$\#\mathscr{H}_K = \prod_{\varphi \in \Phi_K} \#\mathscr{H}_\varphi^{\rm ar} \ \text{(Theorems 3.15, 4.5)}.$$

We compare the two definitions $\mathscr{H}^{\rm alg}$ and $\mathscr{H}^{\rm ar}$ in § 3.3 with numerical illustration showing the gap between them (§ 3.4, Examples 3.12, 3.13).

1.3. **Relation between the modules $\mathscr{H}$ and $\mathscr{T}$.** If one considers, in the real case, the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{T}_K$, one gets, for them, an easier annihilation theorem from the $p$-adic Mellin transform of Stickelberger elements (see § 6.2). Moreover, the norm maps $\mathbf{N}_{k/k'}$ are surjective and the transfer maps $\mathbf{J}_{k/k'}$ are injective under Leopoldt's conjecture [Gra1982, Théorème I.1], [Jau1986, Ng1986, Jau1998] (collected in [Gra2005, Theorem IV.2.1]); so this family behaves as that of relative class groups, which allows an obvious statement of the Main Conjecture and then its proof with similar techniques, as done for instance in [Grei1992].

For $K$ real, the order of the $p$-group $\mathscr{T}_K$ is closely related to the $p$-adic $\mathbf{L}$-functions "at $s = 1$" [Coa1977] and a particularity of $\mathscr{T}_K$ is its interpretation by means of the three $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{H}_K^{\rm cyc}$, $\mathscr{R}_K$ and $\mathscr{W}_K$; see [Gra2005, Lemma III.4.2.4] leading to the exact sequence (6.1) and the formula $\#\mathscr{T}_K = \#\mathscr{H}_K^{\rm cyc} \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K$, where $\mathscr{W}_K$ is an easy canonical invariant depending on local $p$-roots of unity, $\mathscr{R}_K$ is the normalized $p$-adic regulator [Gra2018, Lemma 3.1] and $\mathscr{H}_K^{\rm cyc}$ a subgroup of $\mathscr{H}_K$ (equal to $\mathscr{H}_K$, except "the part" corresponding to the maximal unramified extension contained in the cyclotomic $\mathbb{Z}_p$-extension of $K$).

The order of the group $\mathscr{R}_K$ is (up to an obvious factor) the classical $p$-adic regulator which intervenes in the $p$-adic analytic formulas due to the pioneering works of Kubota–Leopoldt on $p$-adic $\mathbf{L}$-functions, then that of Amice–Fresnel–Barsky (e.g., [Fre1965]), Coates, Ribet and many other; see a survey in [Gra1978$^b$] and a lecture in [Rib1979] where is used the beginnings of the concept of $p$-adic pseudo-measures of Mazur, developed by Serre [Ser1978]). See in [Gra2016, Gra2019] more complete studies and conjectures about $\mathscr{R}_K$ and $\mathscr{T}_K$.

At this time was stated the Iwasawa formalism of the Main Conjecture by Greenberg [Gree1975, Gree1977] after Iwasawa [Iwa1964].

1.4. **Main problem today.** Let $K/\mathbb{Q}$ be a real cyclic extension with a non trivial maximal $p$-sub-extension (non semi-simple case). Let $\mathbf{E}_K$ (resp. $\mathbf{F}_K$) be the group of units (resp. of Leopoldt's cyclotomic units) then $\mathscr{E}_K = \mathbf{E}_K \otimes \mathbb{Z}_p$ and $\mathscr{F}_K = \mathbf{F}_K \otimes \mathbb{Z}_p$; let $\mathscr{E}_K^0 \subseteq \mathscr{E}_K$ be the subgroup generated by the $\mathscr{E}_k$ for all $k \subsetneq K$.

It would remain to prove our conjecture [Gra1977, § III] for the even $p$-adic characters $\varphi$ of $K$ saying that (see also Remarks 7.11 and 8.2):

$$\#\mathscr{H}_\varphi^{\rm ar} = w_\varphi \cdot \#(\mathscr{E}_K/\mathscr{E}_K^0 \cdot \mathscr{F}_K)_\varphi, \quad w_\varphi \in \{1, p\},$$

where:

$$\mathscr{H}_\varphi^{\rm ar} := \big\{x \in \mathscr{H}_K,\ \ P_\varphi(\sigma) \cdot x = 1 \ \ \&\ \ \mathbf{N}_{K/k}(x) = 1\ \forall\, k \subsetneq K\big\},$$

where $P_\varphi$ is the local cyclotomic polynomial attached to $\varphi$ and $\sigma$ a generator of $\mathrm{Gal}(K/\mathbb{Q})$.

For the $\varphi$-component $(\mathscr{E}_K/\mathscr{E}_K^0 \cdot \mathscr{F}_K)_\varphi$, the two notions (arithmetic and algebraic) obviously coincide, but the $\varphi$-class group must be defined in the arithmetic sense.

## 2. Abelian extensions

The idea of definition of the $\varphi$-objects owes a lot to the work of Leopoldt [Leo1954, Leo1962] and their writing, in french, by Oriat in [Or1975, Or1975$^b$]. Some outdated notations in [Gra1976, Gra1977] are modified, after changing $\ell$ into $p$ (e.g., $\Omega_p \mapsto \overline{\mathbb{Q}}_p$, $\widehat{\Omega}_p \mapsto \mathbb{C}_p$, $\Gamma \mapsto \mathbb{Z}_p$).

2.1. **Characters.** Let $\mathbb{Q}^{\rm ab}$ be the maximal abelian extension of $\mathbb{Q}$ contained in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$; let $\mathbb{Q}_p$ be the $p$-adic field and $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$ containing $\overline{\mathbb{Q}}$. We put $\mathscr{G} := {\rm Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$):

Denote by $\Psi$ the set of irreducible characters of $\mathscr{G}$, of degree 1 and finite order, with values in $\overline{\mathbb{Q}}_p$. We define the sets of irreducible $p$-adic characters $\Phi$, for a prime $p \geq 2$, the set $\mathscr{X}$ of irreducible rational characters and the sets of irreducible characters $\Psi_K$, $\Phi_K$, $\mathscr{X}_K$, 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 $\varphi$ is a term of $\chi$ and $\psi$ a term of $\varphi$.

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

Let $\chi \in \mathscr{X}$; we 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 $K_\chi$, the field of values of the characters, respectively. The set $\mathscr{X}$ has the following obvious property to be considered as a "Main theorem" for rational components (e.g., [Leo1954, Chap. I, § 1, 1]):

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

2.2. **Main results of the article.** 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 finite abelian extensions and provided with the arithmetic norms $\mathbf{N}_{K/k}$ and transfer maps $\mathbf{J}_{K/k}$, for any $k \subseteq K$, where $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} = \nu_{K/k} \in \mathbb{Z}[{\rm Gal}(K/k)]$ (algebraic norm); we will give definitions and well-known details in Section 3.1.

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 $\chi$-components $\mathbf{M}_\chi^{\rm alg}$, $\mathbf{M}_\chi^{\rm ar}$, $\mathscr{M}_\chi^{\rm alg}$, $\mathscr{M}_\chi^{\rm ar}$ (for $\chi \in \mathscr{X}$) and the associated $\varphi$-components $\mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}_\varphi^{\rm ar}$ (for $\varphi \in \Phi$), as follows:

Let $P_\chi$ be the global $g_\chi$th cyclotomic polynomial, let $P_\varphi$ be the local cyclotomic polynomial associated with $\varphi \mid \chi$ (so that $P_\chi = \prod_{\varphi\mid\chi} P_\varphi$ in $\mathbb{Z}_p[X]$). We define (with group algebras actions $x^\Omega$ written $\Omega \cdot x$):

$$\begin{cases} \mathbf{M}_\chi^{\rm alg} := \big\{x \in \mathbf{M}_{K_\chi}, P_\chi(\sigma_\chi)\cdot x = 1\big\}, \quad \mathscr{M}_\chi^{\rm alg} := \mathbf{M}_\chi^{\rm alg} \otimes \mathbb{Z}_p, \\ \mathscr{M}_\varphi^{\rm alg} := \big\{x \in \mathscr{M}_\chi^{\rm alg}, P_\varphi(\sigma_\chi)\cdot x = 1\big\}, \\ \mathbf{M}_\chi^{\rm ar} := \{x \in \mathbf{M}_\chi^{\rm alg}, \mathbf{N}_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneq K_\chi\}, \quad \mathscr{M}_\chi^{\rm ar} := \mathbf{M}_\chi^{\rm ar} \otimes \mathbb{Z}_p, \\ \mathscr{M}_\varphi^{\rm ar} := \{x \in \mathscr{M}_\varphi^{\rm alg},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneq K_\chi\}. \end{cases}$$

Then $\mathscr{M}_\varphi^{\rm ar} := \big\{x \in \mathscr{M}_{K_\chi},\ P_\varphi(\sigma_\chi)\cdot x = 1\ \ \&\ \ \mathbf{N}_{K_\chi/k}(x) = 1\,\forall\, k \subsetneq K_\chi\big\}$.

Being annihilated by $P_\chi(\sigma_\chi)$ (resp. $P_\varphi(\sigma_\chi)$) $\mathbf{M}_\chi^{\rm alg}$ and $\mathscr{M}_\chi^{\rm alg}$ (resp. $\mathbf{M}_\varphi^{\rm alg}$ and $\mathscr{M}_\varphi^{\rm alg}$) are $\mathbb{Z}[\mu_{g_\chi}]$-modules (resp. $\mathbb{Z}_p[\mu_{g_\chi}]$-modules), for the law defined via $\sigma \in \mathscr{G} \mapsto \psi(\sigma) \in \mu_{g_\chi}$, for $\psi \mid \chi$ (resp. $\psi \mid \varphi$).

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

- $\mathbf{M}_\chi^{\rm alg} = \big\{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneq K_\chi\big\}$ (Theorem 3.7),
- $\mathscr{M}_\chi^{\rm alg} = \bigoplus\limits_{\varphi\mid\chi} \mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}_\chi^{\rm ar} = \bigoplus\limits_{\varphi\mid\chi} \mathscr{M}_\varphi^{\rm ar}$ (Theorems 4.1, 4.5).

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

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

- $\#\mathbf{M}_K = \prod\limits_{\chi\in\mathscr{X}_K} \#\mathbf{M}_\chi^{\rm ar}$ (Theorem 3.15),

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

- $\#\mathscr{M}_\chi^{\rm ar} = \prod\limits_{\varphi\mid\chi} \#\mathscr{M}_\varphi^{\rm ar}$ (Theorem 4.5).

(ii‴) The above conditions of surjectivity of the norms are automatically fulfilled for the families $\mathbf{H}$ (class groups), $\mathscr{H} = \mathbf{H} \otimes \mathbb{Z}_p$ ($p$-class groups), $\mathscr{T}$ (torsion groups of abelian $p$-ramification).

(iii) Applying this to $\mathbf{H}$ and $\mathscr{T}$, we obtain:

(iii′) For all characters $\chi \in \mathscr{X}^-$, we have:

- $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg}$, $\forall\, \varphi \mid \chi$ (Theorem 5.8);
- $\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod\limits_{\psi\mid\chi} \big( -\frac{1}{2}\,\mathbf{B}_1(\psi^{-1})\big)$ (Theorem 5.10), in terms of Bernoulli numbers.

(iii″) For all characters $\chi \in \mathscr{X}^+$, we have:

- $\mathbf{H}_\chi^{\rm ar} \subseteq \mathbf{H}_\chi^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar} \subseteq \mathscr{H}_\varphi^{\rm alg}$, $\forall\, \varphi \mid \chi$ (see Examples 3.12, 3.13 for strict inclusions);
- $\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot \big(\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \cdot \mathbf{F}_{K_\chi}\big)$ (Theorem 7.9), in terms of cyclotomic units, where $\mathbf{E}^0_{K_\chi} := \langle\, \mathbf{E}_k \,\rangle_{k \subsetneq K_\chi}$.

(iii‴) For all even characters $\chi$, we have:

- $\mathscr{T}_\chi^{\rm ar} = \mathscr{T}_\chi^{\rm alg}$ and $\mathscr{T}_\varphi^{\rm ar} = \mathscr{T}_\varphi^{\rm alg}$, $\forall\, \varphi \mid \chi$ (Theorem 6.1);
- $\#\mathscr{T}_\chi^{\rm ar} = w_\chi^{\rm cyc} \cdot \prod\limits_{\psi\mid\chi} \frac{1}{2}\,\mathbf{L}_p(1,\psi)$ (Theorem 6.2), in terms of $p$-adic $\mathbf{L}$-functions.

(iv) The Arithmetic Invariants of finite $\mathbb{Z}_p[\mathscr{G}]$ modules $\mathscr{M}_K$ are defined by means of the obvious algebraic writing of $\mathbb{Z}_p[\mu_{g_\chi}]$-modules:

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

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

## 3. Definition and study of the $\varphi$-objects

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

3.1. **The Algebraic and Arithmetic $\mathscr{G}$-families.** Let $\mathscr{K}$ be the family of finite extensions $K$ of $\mathbb{Q}$, contained in $\mathbb{Q}^{\rm ab}$, of Galois group $G_K$. We assume to have a family $\mathbf{M}$ of (multiplicative) $\mathbb{Z}[\mathscr{G}]$-modules, indexed by $\mathscr{K}$ (called a $\mathscr{G}$-family), $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$.

In general there exist two families of $\mathscr{G}$-homomorphisms, indexed by the set of sub-extensions $K/k$, $\mathbf{N}_{K/k} : \mathbf{M}_K \to \mathbf{M}_k$ (arithmetic norms), $\mathbf{J}_{K/k} : \mathbf{M}_k \to \mathbf{M}_K$ (arithmetic transfers). For all sub-extensions $K/k$, we put $\nu_{K/k} := \sum\limits_{\sigma\in{\rm Gal}(K/k)} \sigma \in \mathbb{Z}[{\rm Gal}(K/k)]$ (algebraic norm).

We consider the three following conditions:

(a) For all $K \in \mathscr{K}$, $\mathbf{M}_K^{{\rm Gal}(\mathbb{Q}^{\rm ab}/K)} = \mathbf{M}_K$; so, for $x \in \mathbf{M}_K$ and $\sigma \in \mathscr{G}$, $x^\sigma = x^{\sigma_K}$, where $\sigma_K \in G_K$ is the restriction of $\sigma$ to $K$.

(b) For all sub-extension $K/k$, the arithmetic maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$ are $\mathscr{G}$-module homomorphisms fulfilling the transitivity formulas:

$$\mathbf{N}_{K/k} \circ \mathbf{N}_{L/K} = \mathbf{N}_{L/k} \text{ and } \mathbf{J}_{L/K} \circ \mathbf{J}_{K/k} = \mathbf{J}_{L/k},$$

for all $k, K, L \in \mathscr{K}$, $k \subseteq K \subseteq L$.

(c) For all sub-extension $K/k$, $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} = \nu_{K/k}$ on $\mathbf{M}_K$.

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

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

The following properties are elementary:

**Proposition 3.2.** *(i) For all $K \in \mathscr{K}$, $\nu_{K/K}$, $\mathbf{N}_{K/K}$, $\mathbf{J}_{K/K}$ are the identity,* id, *on $\mathbf{M}_K$.*

*(ii) 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 $[K : k]$.*

*(iii) The previous definitions and properties apply to the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M}_K := \mathbf{M}_K \otimes \mathbb{Z}_p$.*

**Remark 3.3.** Note that cohomology is only of algebraic nature since, for instance in the case of a cyclic extension $K/k$ of Galois group $G =: \langle\sigma\rangle$, using the class group $\mathbf{H}_K$, we have:

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

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

**Examples 3.4.** The most straightforward examples of such arithmetic $\mathscr{G}$-families $\mathbf{M}_K$ are the following ones:

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

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

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

(iv) the group-algebra $A[G_K]$, where $A$ is a commutative ring; then $A[G_K]$ is a $A[\mathscr{G}]$-module if one puts $\sigma\cdot\Omega = \sigma_K\Omega$ (product in $A[G_K]$), for all $\Omega \in A[G_K]$ and $\sigma \in \mathscr{G}$. The maps $\mathbf{N}_{K/k}$ and $\mathbf{J}_{K/k}$ are defined by $A$-linearity by $\mathbf{N}_{K/k}(\sigma_K) := \sigma_k$ and, for $\sigma_k \in G_k$, by:

$$\mathbf{J}_{K/k}(\sigma_k) := \sum_{\tau\in\mathrm{Gal}(K/k)} \tau\cdot\sigma'_k = \nu_{K/k}\cdot\sigma'_k = \nu_{K/k}\sigma'_k,$$

where $\sigma'_k$ is any extension of $\sigma_k$ in $G_K$. So, for $\sigma_K \in G_K$, $\nu_{K/k}(\sigma_K) = \big(\sum_{\tau\in\mathrm{Gal}(K/k)}\tau\big)\cdot\sigma_K = \nu_{K/k}\sigma_K$.

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

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

One defines, following [Ser1998], the $\Gamma_{\kappa_A}$-conjugation on $\Psi$ 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 $\tau$ in $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$. If $\sigma_\chi$ is a generator of $G_\chi := G_{K_\chi}$, then the $\psi^\tau(\sigma_\chi)$ are the conjugates of $\psi(\sigma_\chi)$ in $\kappa_A(\mu_{g_\chi})/\kappa_A$. This defines the irreducible characters over $\kappa_A$ (with values in $A$), $\theta = \sum_{\tau\in\Gamma_{\kappa_A,\chi}}\psi^\tau$.

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

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

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

Thus $P_\chi = \prod_{\theta\mid\chi} P_\theta$; for $A = \mathbb{Z}_p$ we get $P_\chi = \prod_{\varphi\in\Phi,\,\varphi\mid\chi} P_\varphi$, for $A = \mathbb{Z}$, $P_\chi$ is irreducible. So, $A[G_\chi]/(P_\theta(\sigma_\chi)) \simeq A[X]/(X^{g_\chi} - 1, P_\theta(X)) \simeq A[\mu_{g_\chi}]$; then any module annihilated by $P_\theta(\sigma_\chi)$ is a $A[\mu_{g_\chi}]$-module; the law is realized, for $\psi \mid \theta$, via $\sigma \in G_\chi \mapsto \psi(\sigma) \in \mu_{g_\chi}$.

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

**Definition 3.5.** *Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a $\mathscr{G}$-family of $\mathbb{Z}[\mathscr{G}]$-modules and let $\mathscr{M} := \mathbf{M}\otimes\mathbb{Z}_p = (\mathscr{M}_K)_{K\in\mathscr{K}}$ be the corresponding local $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules. Put, for $\chi \in \mathscr{X}$ and for $\varphi \mid \chi$, $\varphi \in \Phi$:*

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

*So, $\mathscr{M}_\varphi^{\mathrm{alg}}$ is a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_{K_\chi}$ (or of $\mathscr{M}_\chi^{\mathrm{alg}}$), for the law $\sigma \in G_{K_\chi} \mapsto \psi(\sigma)$, $\psi \mid \varphi$, and the elements of $\mathscr{M}_\varphi^{\mathrm{alg}}$ are called $\varphi$-objects (in the algebraic sense).*

From relation (3.1), the polynomials $P_\varphi$ depend on the choice of the generator $\sigma_\chi$ of $G_\chi$, but we have the following canonical property:

**Lemma 3.6.** *The Definitions 3.5, of the $\mathbb{Z}[\mu_{g_\chi}]$-modules $\mathbf{M}_\chi^{\rm alg}$ and the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{M}_\varphi^{\rm alg}$, do not depend on the choice of $\sigma_\chi$.*

*Proof.* Let $\varphi \mid \chi$. 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 $G_\chi$ 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:

$$P'_\varphi(\sigma_\chi^a) = \prod_{\psi\mid\varphi}(\sigma_\chi^a - \psi(\sigma_\chi^a)) = \prod_{\psi\mid\varphi}\big[(\sigma_\chi - \psi(\sigma_\chi)) \times (\sigma_\chi^{a-1} + \cdots + \psi^{a-1}(\sigma_\chi))\big],$$

and similarly, writing $1 \equiv a\,a^* \pmod{g_\chi}$, where $a^* > 0$ represents an inverse of $a$ modulo $g_\chi$, we have, from $\sigma_\chi = (\sigma_\chi^a)^{a^*}$:

$$P_\varphi(\sigma_\chi) = \prod_{\psi\mid\varphi}\big[(\sigma_\chi^a - \psi(\sigma_\chi^a)) \times (\sigma_\chi^{a(a^*-1)} + \cdots + \psi^{a(a^*-1)}(\sigma_\chi))\big].$$

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

3.2.4. *Characterization of $\mathbf{M}_\chi^{\rm alg}$, $\mathscr{M}_\chi^{\rm alg}$, with algebraic norms.* For any $\chi \in \mathscr{X}$, we have defined $\mathbf{M}_\chi^{\rm alg}$ and $\mathscr{M}_\chi^{\rm alg}$ (Definition 3.5). We then have the following characterization, only valid for rational characters, but which will allow another definition of $\chi$ and $\varphi$-objects (that of "Arithmetic" objects):

**Theorem 3.7.** *Let $\mathbf{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}[\mathscr{G}]$-modules and let $\mathbf{M}_\chi^{\rm alg} = \big\{x \in \mathbf{M}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\big\}$, for any $\chi \in \mathscr{X}$. Then:*

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

*(one may limit the norm conditions to $\nu_{K_\chi/k_\ell}(x) = 1$ for all prime divisors $\ell$ of $[K_\chi : \mathbb{Q}]$, where $k_\ell \subset K_\chi$ is such that $[K_\chi : k_\ell] = \ell$).*

*Proof. With a contribution of a personal communication from Jacques Martinet (October 1968).* We need three preliminary lemmas:

**Lemma 3.8.** *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 $q \nmid n$.*

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

**Lemma 3.9.** *Let $n = \ell_1 \cdots \ell_t$, $t \geq 2$, the $\ell_i$'s being distinct prime numbers. Then for all pair $(i, j)$, $i \neq j$, there exist $A_i^j$ and $A_j^i$ in $\mathbb{Z}[X]$, such that $A_i^j P_{\frac{n}{\ell_i}} + A_j^i P_{\frac{n}{\ell_j}} = 1$.*

*Proof.* This can be proved by induction on $t \geq 2$.

If $t = 2$, $n = \ell_1\ell_2$ and:

$$P_{\frac{n}{\ell_2}} = P_{\ell_1} = X^{\ell_1-1} + \cdots + X + 1,\ \ P_{\frac{n}{\ell_1}} = P_{\ell_2} = X^{\ell_2-1} + \cdots + X + 1.$$

Let's call "geometric polynomial" any polynomial in $\mathbb{Z}[X]$ 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:

$$\begin{aligned} X^m + \cdots + X + 1 = \\ (X^n + \cdots + X + 1) \times \big[X^{m+1-(n+1)} + X^{m+1-2(n+1)} + \cdots + X^{m+1-q(n+1)}\big] \\ + 1 + X + \cdots + X^{r-1} \end{aligned}$$

(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 $P_{\ell_1}$ and $P_{\ell_2}$.

Suppose $t \geq 3$. Let $\ell_i$, $\ell_j$, $q$, be three distinct primes dividing $n$; put $n' := \frac{n}{q}$; by induction, since $\ell_i$ and $\ell_j$ divide $n'$, there exist polynomials $A_i'^j, A_j'^i$ in $\mathbb{Z}[X]$, such that $A_i'^j(X)P_{\frac{n'}{\ell_i}}(X) + A_j'^i(X)P_{\frac{n'}{\ell_j}}(X) = 1$, thus, $A_i'^j(X^q)P_{\frac{n'}{\ell_i}}(X^q) + A_j'^i(X^q)P_{\frac{n'}{\ell_j}}(X^q) = 1$. But Lemma 3.8 (ii) gives:

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

which yields $A_i'^j(X^q)P_{\frac{n}{\ell_i}}(X)P_{\frac{n'}{\ell_i}}(X) + A_j'^i(X^q)P_{\frac{n}{\ell_j}}(X)P_{\frac{n'}{\ell_j}}(X) = 1$. We have proved the co-maximality, in $\mathbb{Z}[X]$, of any pair of ideals $(P_{\frac{n}{\ell_i}}(X))$, $(P_{\frac{n}{\ell_j}}(X))$, $i \neq j$ (the case $n = \ell$ giving the prime ideal $(P_\ell(X)\mathbb{Z}[X])$). □

**Lemma 3.10.** *Let $n = \prod_{i=1}^{t} \ell_i^{a_i} > 1$, $a_i \geq 1$; put $N_{n,\ell}(X) := \sum_{i=0}^{\ell-1} X^{\frac{n}{\ell}i}$ for any prime $\ell$ 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 $n$ that $P_n(X) = \sum_{\ell|n} A_\ell(X)N_{n,\ell}(X)$ (with $t$ fixed), and let $q \mid n$; we have, from Lemma 3.8 (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, $P_{n_k}(X) = \sum_{1\leq s\leq t,\ s\neq k} A_s^k(X)N_{n_k,\ell_s}(X)$, hence:

$$\begin{aligned} P_{n_k}(X^{\ell_k}) &= P_{n_k\ell_k}(X)\cdot P_{n_k}(X) \\ &= P_n(X)P_{n_k}(X) = \sum_{1\leq s\leq t\ s\neq k} A_s^k(X^{\ell_k})N_{n,\ell_s}(X), \end{aligned}$$

whence $P_n(X)P_{n_k}(X) \in \langle N_{n,\ell}(X),\ \ell \mid n\rangle_{\mathbb{Z}[X]}$, for all $k$; since $t \geq 2$, Lemma 3.9 applies; a Bézout relation in $\mathbb{Z}[X]$ between any two of the $P_{n_k}$ (say $P_{n_i}$ and $P_{n_j}$) yields $P_n(X)\times 1 \in \langle N_{n,\ell}(X),\ \ell \mid n\rangle_{\mathbb{Z}[X]}$, giving the result.

We 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 $\zeta_n$ 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 $P_\chi(\sigma_\chi) = P_{g_\chi}(\sigma_\chi)$ and to $N_{g_\chi,\ell}(\sigma_\chi) = \nu_{K_\chi/k_\ell}$, where $k_\ell$ is, for all $\ell \mid g_\chi$, the unique sub-extension of $K_\chi$ such that $[K_\chi : k_\ell] = \ell$. The theorem immediately follows. □

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

**Definition 3.11.** *By analogy with Theorem 3.7 giving, for $\chi$-objects, the definition $\mathbf{M}_\chi^{\mathrm{alg}} := \{x \in \mathbf{M}_{K_\chi},\ \nu_{K_\chi/k}(x) = 1$, for all $k \subsetneq K_\chi\}$ and $\mathscr{M}_\chi^{\mathrm{alg}} = \mathbf{M}_\chi^{\mathrm{alg}} \otimes \mathbb{Z}_p$, we define the modules of arithmetic $\chi$-objects:*

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

*Then $\mathbf{M}_\chi^{\mathrm{ar}}$ (resp. $\mathscr{M}_\chi^{\mathrm{ar}}$) is a sub-$\mathbb{Z}[\mu_{g_\chi}]$-module of $\mathbf{M}_\chi^{\mathrm{alg}}$ (resp. a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_\chi^{\mathrm{alg}}$).*

We have $\mathbf{M}_\chi^{\rm ar} = \mathbf{M}_\chi^{\rm alg}$ as soon as the $\mathbf{J}_{K_\chi/k}$'s are injective (for all $k \subsetneq K_\chi$ or simply the $k_\ell$'s). One verifies easily that if the norms $\mathbf{N}_{K_\chi/k_\ell}$ are surjective for all $\ell \mid g_\chi$, then $\mathbf{M}_\chi^{\rm alg}/\mathbf{M}_\chi^{\rm ar}$ has exponent a divisor of $\prod_{\ell \mid g_\chi} \ell$, whence $\mathscr{M}_\chi^{\rm alg}/\mathscr{M}_\chi^{\rm ar}$ of exponent 1 or $p$.

3.3. **Comparison with classical definitions.** In all classical papers, the notion of $\theta$-component $\mathbf{M}_\theta$ ($\theta$ rational or $p$-adic, above $\psi \in \Psi$), 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 $A[\theta] := A[\psi]$ is the ring of values of $\theta$ over $A$; the action being defined via $(\sigma, x) \in G \times \mathbf{M}_\theta \mapsto \psi(\sigma) \cdot x \in \mathbf{M}_\theta$. As for the example of cohomology groups, this definition is only algebraic and not arithmetic. We shall compare this definition with Definition 3.11 considering irreducible $p$-adic characters $\varphi$. We have the classical algebraic definition of $\varphi$-objects attached to $\mathscr{M}$, that is to say, the largest quotient such that $G_\chi$ acts by $\psi$ ([Grei1992, Definition, p. 451], [PeRi1990, § 1.3]):

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

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

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

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

Moreover, our forthcoming Definition 4.3 of $\mathscr{M}_\varphi^{\rm ar}$:

$$\mathscr{M}_\varphi^{\rm ar} := \mathscr{M}_\chi^{\rm ar} \cap \mathscr{M}_\varphi^{\rm alg} \quad \text{(with Definition 3.11 of } \mathscr{M}_\chi^{\rm ar}),$$

introduces another kind of computations. Indeed, the Main Theorem on abelian fields in the literature is concerned by algebraic definitions similar to $\widehat{\mathscr{M}_\varphi}$ or $\widehat{\mathscr{M}^\varphi}$, but our conjecture given in the 1970's used $\mathscr{M}_\varphi^{\rm ar}$ and new analytic values giving $\#\mathscr{M}_\chi^{\rm ar}$, justifying the conjectural values of $\#\mathscr{M}_\varphi^{\rm ar}$ for finite $\mathscr{M}$'s.

It is immediate to verify that, in the non semi-simple case $p \mid g_\chi$, $(\mathscr{M}_\varphi^{\rm alg} : \mathscr{M}_\varphi^{\rm ar})$ is equal to the order of the capitulation kernel of $\mathbf{J}_{K_\chi/k_p}$, where $k_p$ is the subfield of $K_\chi$ such that $[K_\chi : k_p] = p$. 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 definitions.

3.4. **Numerical examples.** Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field and let $K$ be the compositum of $k$ with a cyclic extension $L$ of $\mathbb{Q}$ of $p$-power degree; the field $K$ is of the form $K_\chi$ for $\chi \in \mathscr{X}^+$ which is also irreducible $p$-adic. We have given in [Gra2021$^b$] many examples of capitulations of the $p$-class group of $k$ in $K$, giving $\mathscr{H}_\chi^{\rm ar} \subsetneq \mathscr{H}_\chi^{\rm alg}$.

3.4.1. *General PARI program.* For the program, one must precise the prime $p > 2$, the minimal required $p$-rank rpmin of $\mathbf{H}_k$, the length N of the sub-tower considered and the interval for m (the program uses primes $\ell$ (in ell) congruent to 1 modulo $2p^N$; the class group (resp. the $p$-class group) is computed in Ck (resp. Ckp):

```
{p=3;rpmin=1;N=2;bm=2;Bm=10^4;for(m=bm,Bm,if(core(m)!=m,next);P=x^2-m;
k=bnfinit(P,1);Ck=k.clgp;r=matsize(Ck[2])[2];Ckp=List;Ekp=List;rp=0;
for(i=1,r,ei=Ck[2][i];vi=valuation(ei,p);if(vi>0,rp=rp+1;
ai=idealpow(k,Ck[3][i],ei/p^vi);listput(Ckp,ai,rp);
listput(Ekp,p^vi,rp)));if(rp<rpmin,next);L0=List;
for(i=1,rp,listput(L0,0,i));forprime(ell=2,10^4,
if(Mod(ell-1,2*p^N)!=0 || Mod(m,ell)==0,next);
Lq=List;for(i=1,rp,A=Ckp[i];forprime(q=2,10^5,if(q==ell,next);
if(kronecker(m,q)!=1 || Mod((ell-1)/znorder(Mod(q,ell)),p)==0,next);
F=idealfactor(k,q);qi=component(F,1)[1];cij=qi;for(j=1,Ekp[i]-1,
cij=idealmul(k,cij,A);if(Mod(j,p)==0,next);
if(List(bnfisprincipal(k,cij)[1])==L0,listput(Lq,q,i);break(2)))));
print("____");print();print("m=",m," ell=",ell," Lq=",Lq);
for(n=0,N,R=polcompositum(P,polsubcyclo(ell,p^n))[1];K=bnfinit(R,1);
print();print("C",n,"=",K.cyc);for(i=1,rp,Fi=idealfactor(K,Lq[i]);
Qi=component(Fi,1)[1];print(bnfisprincipal(K,Qi)[1])))))}
```

We consider the base field $k = \mathbb{Q}(\sqrt{4409})$.

**Example 3.12.** Let $L$ be the degree 9 subfield of $\mathbb{Q}(\mu_{19})$; for convenience, put $k_0 := k$, $k_1 := L_1k_0$ (resp. $k_2 := L_2k_0$), where $L_1$ (resp. $L_2$) is the degree 3 (resp. 9) subfield of $\mathbb{Q}(\mu_{19})$. The prime 2 splits in $k_0$, is inert in $k_2/k_0$ and such that $\mathfrak{Q}_0 \mid 2$ in $k_0$ generates $\mathscr{H}_{k_0}$ (cyclic of order 9); considering the extensions $\mathfrak{Q}_i = \mathbf{J}_{k_i/k_0}(\mathfrak{Q}_0)$ of $\mathfrak{Q}_0$ in $k_i$, we test its order in $\mathscr{H}_{k_i}$, $i = 1, 2$ (we are going to see that $\mathscr{H}_{k_i} \simeq \mathbb{Z}/9\mathbb{Z}$ for all $i$, which is supported by the fact that $\mathbf{N}_{k_2/k_0}(\mathfrak{Q}_2) = \mathfrak{Q}_0^9$ but $\mathbf{N}_{k_2/k_0}(\mathscr{H}_{k_2}) = \mathscr{H}_{k_0}$ since $k_2/k_0$ is totally ramified at 19):

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

More precisely $\mathsf{C0} = [9]$ denotes the class group of $k_0$ and, using the instruction bnfisprincipal, $[4]^\sim$ means that the class of $\mathfrak{Q}_0 \mid 2$ is $h_0^4$, where $h_0$ is the generator (of order 9) given in kn.cyc by PARI; then $\mathsf{C1} = [9]$, $[6]^\sim$, is the similar data for $k_1$ in which we see a partial capitulation since the class of $\mathfrak{Q}_1 = \mathbf{J}_{k_1/k_0}(\mathfrak{Q}_0)$ becomes of order 3. Finally, $\mathsf{C2} = [9]$, $[0]^\sim$ shows the complete capitulation in $k_2$; the 18 large integers below are the coefficients, over an integral basis, of a generator of $\mathfrak{Q}_2$ 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,-255607858779215282,
-198423813102857420,41058886502087041 4,-110028179006577678,-449600797918214026,-4906665437527948,
10274048566854232,4319852458093887,1325871575594739 4,-6817941144899095,-15448507867705832,2623003974789062,
-3264916449440532,-16606126998680345]~]
```

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

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

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

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

We have $P_{\chi_2}(\sigma_{\chi_2}) = \sigma_{\chi_2}^6 + \sigma_{\chi_2}^3 + 1 = \nu_{k_2/k_1}$ (since $L$ is principal, the norms $\nu_{k_i/L_i}$ does not intervene in the definition of the $\mathscr{H}_{\chi_i}^{\mathrm{alg}}$'s).

Similarly, we have:

$$\nu_{k_1/k_0}(\mathscr{H}_{k_1}) = \mathbf{J}_{k_1/k_0} \circ \mathbf{N}_{k_1/k_0}(\mathscr{H}_{k_1}) = \mathbf{J}_{k_1/k_0}(\mathscr{H}_{k_0}) \simeq \mathbb{Z}/3\mathbb{Z}$$

(partial capitulation of $\mathscr{H}_{k_0} \simeq \mathbb{Z}/9\mathbb{Z}$); whence:

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

Thus, the forthcoming formula of Theorem 3.15 giving:

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

is of the form $\#\mathscr{H}_{k_2} = 9 \times 1 \times 1$, then $\#\mathscr{H}_{k_1} = 9 \times 1$ since $\mathscr{H}_{\chi_0}^{\mathrm{ar}} = \mathscr{H}_{k_0}$.

These formulas are not fulfilled in the algebraic sense, because:

$$\#\mathscr{H}_{\chi_0}^{\mathrm{alg}} \cdot \#\mathscr{H}_{\chi_1}^{\mathrm{alg}} = 9 \times 3 = 3^3 \text{ and } \#\mathscr{H}_{\chi_0}^{\mathrm{alg}} \cdot \#\mathscr{H}_{\chi_1}^{\mathrm{alg}} \cdot \#\mathscr{H}_{\chi_2}^{\mathrm{alg}} = 9 \times 3 \times 3 = 3^4.$$

Now we intend to compute $\#\mathscr{H}_{\chi_1}^{\mathrm{ar}} = \#(\mathscr{E}_{k_1}/\mathscr{E}_{k_1}^0 \cdot \mathscr{F}_{k_1})$ (analytic formula of Theorem 7.9); 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 $|\mathsf{e0}|$ of $k_0$, $|\mathsf{ei}|$ of $L_1$, $|\mathsf{Ej}|$ of $k_1$, and their logarithms; they are, respectively (standard PARI programs):

```
Units                                          Logarithms
e0=664.00150602068057486397714386165380         6.49828441757729630972016
e1=0.28514248182978536439411987353062 74       -1.25476628739511494204754
e2=4.50701864409297629866079992371567 80        1.50563588039686576534798
E1=0.28514248182978536439411987353062 74       -1.25476628739511494204754
E2=0.22187616226319093426666800501850506       -1.50563588039686576534798
E3=664.00150602068057486397714386165380         6.49828441757729630972016
E4=945628377316488.87204143428389231544        34.48287077198255819743 18
E5=0.00257365190752746549299934631279 51       -5.96242941301396593243487
```

```
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(Eta))))}

Eta^s1=945628377316488.87204143428      34.482870771982558197431847l
Eta^s2=2433718277092.6834663091300      28.520441358968592264996969
Eta^s3=0.00257365190752746549299l3      -5.962429413013965932434877
Eta^s4=1.057497875473880465206l E-15   -34.482870771982558197431847l
Eta^s5=4.108939023109111198282 E-13    -28.520441358968592264996969
Eta^s6=388.55293409150677930552135       5.962429413013965932434877
```

One obtains easily the following relations:

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

Then, one gets:

$$(\mathscr{E}_{k_1} : \mathscr{E}^0_{k_1} \cdot \mathscr{F}_{k_1}) = (\mathscr{E}_{k_1} : \mathscr{E}_{k_0} \cdot \mathscr{E}_{L_1} \cdot \mathscr{F}_{k_1}) = 1$$

as expected since $\mathscr{H}^{\rm ar}_{\chi_1} = 1$. Moreover, we see that the conjugates of the cyclotomic units are not independent (due, from Lemma 5.17, to norm relations in $k_i/k_0$ and $k_i/L_i$ since 19 splits in $k_0$ and 4409 splits in the $L_i$'s), but, with our point of view, this does not matter since $\mathscr{E}^0_{k_1}$ is of $\mathbb{Z}_3$-rank 3 and $\mathscr{F}_{k_1}$ is of $\mathbb{Z}_3$-rank 2. Indeed, these relations lead to some difficulties in $\chi$-formulas of the literature *using larger groups of cyclotomic units* like Sinnott's cyclotomic units (see Remark 7.11).

To be complete, compute the 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 $\#\mathscr{H}^{\rm ar}_{\chi_0} = (\mathscr{E}_{k_0} : \mathscr{E}^0_{k_0} \cdot \mathscr{F}_{k_0}) = (\mathscr{E}_{k_0} : \mathscr{F}_{k_0}) = 9$; obviously, 9 is the annihilator of $\mathscr{E}_{k_0}/\mathscr{F}_{k_0}$ and $\mathscr{H}^{\rm ar}_{\chi_0}$ (Conjecture 7.13).

The verification of $(\mathscr{E}_{k_2} : \mathscr{E}^0_{k_2} \cdot \mathscr{F}_{k_2}) = 1$ is analogous since $\mathscr{F}_{k_2}$ is of $\mathbb{Z}_3$-rank 8 ($\mathbf{N}_{k_2/k_1}(\mathscr{F}_{k_2}) = \mathscr{F}_{k_1}$, $\mathbf{N}_{k_2/k_0}(\mathscr{F}_{k_2}) = 1$, $\mathbf{N}_{k_2/L_2}(\mathscr{F}_{k_2}) = 1$).

**Example 3.13.** 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 the ideal $\mathsf{Q}_1 = [2, [-1,0,0,1,0,0]^\sim, 1, 3, [0,0,0,1,0,0]^\sim]$, extending $\mathsf{Q}_0$ in $k_1$, is non-principal and such that its class is $\mathsf{h}_1^6\,\mathsf{h}_2^0\,\mathsf{h}_3^0$ on the PARI basis $\{\mathsf{h}_1, \mathsf{h}_2, \mathsf{h}_3\}$:

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

but its 6-power gives as expected the principality and a 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]~,[821719075630487115396921l,52602828277952742913821l,-687786029075595676594134,
          25130170977215548291757l,-21032376402967976888126,-15609327127430752932511]~]
```

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

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

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

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

**Remark 3.14.** The program gives the following other results, varying only $\mathsf{ell}$, where $\mathsf{q}$ is the prime split in $k_0$ and inert in $k_2$:

```
ell=37  q=2    C0=[9]  [4]~    C1=[18]   [6]~      C2=[18]    [0]~
ell=73  q=2    C0=[9]  [4]~    C1=[9]    [6]~      C2=[171]   [0]~
ell=109 q=5    C0=[9]  [1]~    C1=[9]    [6]~      C2=[9]     [0]~
ell=127 q=23   C0=[9]  [4]~    C1=[9]    [6]~      C2=[9]     [0]~
ell=163 q=2    C0=[9]  [4]~    C1=[54]   [12]~     C2=[54]    [18]~
ell=181 q=2    C0=[9]  [4]~    C1=[27]   [12]~     C2=[81]    [63]~
ell=199 q=2    C0=[9]  [4]~    C1=[9,3]  [6,0]~    C2=[27,3]  [9,0]~
```

The image of $\mathscr{H}_{k_0}$ in $k_1$ is of order 3, except for $\ell \in \{163, 181\}$; then $\mathscr{H}_{k_0}$ capitulates in $k_2$, except for $\ell \in \{163, 181, 199\}$. One verifies that formula of Theorem 3.15 holds with the $\#\mathscr{H}_{k_i}^{\rm ar}$ but not for the $\#\mathscr{H}_{k_i}^{\rm alg}$.

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

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

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

*where $\mathbf{M}_\chi^{\rm ar} := \{x \in \mathbf{M}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneq K_\chi\}$ (Definition 3.11).*

*Assuming only the cyclicity of the $p$-Sylow subgroup of $G_K$, one obtains, $\#\mathscr{M}_K = \prod_{\chi \in \mathscr{X}_K} \#\mathscr{M}_\chi^{\rm ar}$.*

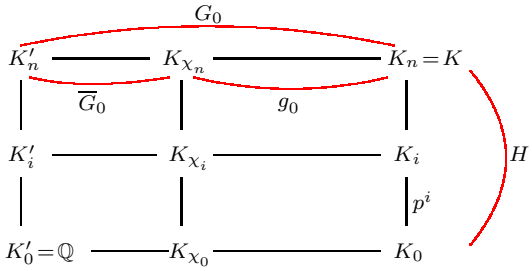
*Proof.* One may replace the $\mathbf{M}_k$, $k \subseteq K$, by the finite $\mathbb{Z}_p[G_K]$-modules $\mathscr{M}_k := \mathbf{M}_k \otimes \mathbb{Z}_p$, for all primes dividing $\#\mathbf{M}_K$, using the previous results, then globalizing at the end. Two classical lemmas are necessary.

**Lemma 3.16.** *Assume that $p \nmid [k : k']$. If $\mathbf{N}_{k/k'} : \mathscr{M}_k \longrightarrow \mathscr{M}_{k'}$ is surjective (resp. if $\mathbf{J}_{k/k'} : \mathscr{M}_{k'} \longrightarrow \mathscr{M}_k$ is injective), then $\mathbf{J}_{k/k'}$ is injective (resp. $\mathbf{N}_{k/k'}$ is surjective).*

*Proof.* From Proposition 3.2, we know that $\mathbf{N}_{k/k'} \circ \mathbf{J}_{k/k'} = [k : k']$; whence the proofs since $[k : k']$ is invertible modulo $p$. □

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

The set of subfields of $K$ is of the form $\{K_{\chi_i},\ \chi_i \in \mathscr{X}_K,\ 0 \le i \le n\}$, where $\chi_i$ is the rational character above $\psi_i := \psi_0\, \psi_p^{p^{n-i}}$, where $\psi_p \in \Psi_{K'_n}$ is of order $p^n$ and $\psi_0 \in \Psi_{K_0}$; thus $K_{\chi_i}$ is the compositum $K_{\chi_0} K'_i$. This leads to the diagram:




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

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

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

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

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

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

*Proof.* For all $i$, we identifie $\mathrm{Gal}(K_i/K_i')$ with $G_0$ acting by restriction and put $\overline{G}_0 := G_0/g_0$, where $g_0 := \mathrm{Gal}(K_n/K_{\chi_n})$. Thus, by abuse of notation, we identify $\nu_{K_i/K_{\chi_i}}$ with $\nu_{K_n/K_{\chi_n}} =: \nu_{g_0}$; moreover, since the degrees of these extensions are prime to $p$, we may identify $\mathbf{N}_{K_i/K_{\chi_i}}$ with $\mathbf{N}_{K_n/K_{\chi_n}} =: \mathbf{N}_{g_0}$ and $\mathbf{J}_{K_i/K_{\chi_i}}$ with $\mathbf{J}_{K_n/K_{\chi_n}} =: \mathbf{J}_{g_0}$. Thus $\mathbf{N}_{g_0}$ is surjective and $\mathbf{J}_{g_0}$ injective. One computes that $e_{\chi_0} = \frac{\nu_{g_0}}{\#g_0}\,\overline{e}_{\chi_0}$, where $\overline{e}_{\chi_0} := \frac{1}{\#\overline{G}_0}\sum_{\overline{\sigma}\in\overline{G}_0}\chi_0(\overline{\sigma}^{-1})\,\sigma \in \mathbb{Z}_p[G_0]$; but we have:

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

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

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

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

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

From the norm definitions of $(\mathscr{M}_{K_{\chi_i}}^{\mathrm{ar}})_{\chi_0}$ and from:

$$\mathscr{M}_{K_{\chi_i}}^* := \{x \in \mathscr{M}_{K_{\chi_i}},\ \ \mathbf{N}_{K_{\chi_i}/K_{\chi_{i-1}}}(x) = 1\},$$

it follows that $\mathscr{M}_{K_{\chi_i}}^{*\,\overline{e}_{\chi_0}} = \mathscr{M}_{\chi_i}^{\mathrm{ar}}$, for all $i \geq 1$. In the finite case, this yields, using the above, the exact sequence (3.2) and $\mathscr{M}_{K_0}^* = \mathscr{M}_{K_0}$:

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

Which ends the proof of the theorem and gives useful relations. □

The assumption on the surjectivity of the norms is fulfilled for class groups $\mathbf{H}$ (resp. $p$-class groups $\mathscr{H}$ and $p$-torsion groups $\mathscr{T}$), as soon as $K/\mathbb{Q}$ (resp. the maximal $p$-sub-extension of $K/\mathbb{Q}$) is cyclic.

## 4. Semi-simple decomposition of $\mathscr{A}_\chi := \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$

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 exist unique $\psi_0$, $\psi_p \in \Psi$ such that $\psi = \psi_0\,\psi_p$, $\psi_0$ of prime-to-$p$ order and $\psi_p$ of $p$-power order. We restrict the study to $K := K_\chi$ for the rational character $\chi$ above $\psi$, so that, from the previous § 3.5, $G_K$ becomes $G_\chi = G_0 \oplus H$ of order $g_\chi = g_{\chi_0}\cdot p^n$.

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

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

where $\varphi_0$ is the $p$-adic character over $\psi_0$. In the semi-simple case $\psi_p = 1$, then $\varphi_0 = \varphi$.

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

**Theorem 4.1.** *Let $\mathscr{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules.*

*(i) For all $\chi \in \mathscr{X}$ we get, by means of the irreducible $p$-adic characters $\varphi \in \Phi$, the decompositions $\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\rm alg}$ (cf. Definition 3.5).*

*More generally, if $\mathscr{M}'_\chi$ is a sub-$\mathscr{A}_\chi$-module of $\mathscr{M}_\chi^{\rm alg}$, then $\mathscr{M}'_\chi = \oplus_{\varphi|\chi} \mathscr{M}'_\varphi$, where $\mathscr{M}'_\varphi = \{x' \in \mathscr{M}'_\chi,\ P_\varphi(\sigma_\chi)\cdot x' = 1\} \subseteq \mathscr{M}_\varphi^{\rm alg}$.*

*(ii) The sub-$\mathscr{A}_\chi$-modules $\mathscr{M}_\varphi^{\rm alg}$, $\varphi \mid \chi$, coincide with the $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}}$'s, where $e^{\varphi_0}$ is the semi-simple idempotent (4.1) associated to $\varphi_0$ above the component $\psi_0$ of prime-to-$p$ order of $\psi \mid \varphi \mid \chi$.*

*(iii) These modules $\mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}'_\varphi$ are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules by means of the choice of $\psi \mid \varphi$ and the action $\sigma \in G_\chi \mapsto \psi(\sigma) \in \mu_{g_\chi}$.*

*Proof.* One may suppose that $g_\chi \equiv 0 \pmod p$, otherwise we are in the semi-simple case and the proof is obvious [Or1975, Part II].

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

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

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

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

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 $D_\chi$ 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 $Q_1$ ($\zeta$ is of order $g_\chi$ and the other roots are the $\zeta^a$ for Artin symbols $\sigma_a \in D_\chi$); we then have:

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

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

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

Recall that $g_\chi = g_{\chi_0}p^n$, $n \geq 1$. Then $1 - \zeta^{ac-1}$ is non invertible in $\mathbb{Z}_p[\mu_{g_\chi}]$ if and only if $ac - 1 \equiv 0 \pmod{g_{\chi_0}}$, which implies $\sigma_a\sigma_c \in D_\chi$ since $\mathrm{Gal}(\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}(\mu_{g_{\chi_0}})) \subseteq D_\chi$ because of the total ramification of $p$ in the $p$-extension, but $\sigma_a \in D_\chi$ implies $\sigma_c \in D_\chi$ (absurd). So $Q_2(\zeta)$ is a $p$-adic unit, whence, from (4.2), $U_2(\zeta) \equiv 0 \pmod{p^k}$, $k \geq 1$.

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

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

where $e = p^{n-1}(p-1)$ (ramification index of $p$ in $\mathbb{Q}(\mu_{g_\chi})/\mathbb{Q}$) and where $\overline{Q}_0$ is irreducible in $\mathbb{F}_p[X]$ (i.e., the irreducible polynomial of $\overline{\zeta}$, in fact that of the image of a generator of $\mu_{g_{\chi_0}}$).

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

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

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

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

Let's show that $\alpha \geq e$; the unique case where, possibly, $p \mid g_\chi$ and $e = 1$ is the case $p = 2$, $n = 1$; this case trivially gives $\alpha \geq e$. Consider the $g_{\chi_0}$th cyclotomic polynomial. Assuming $e > 1$, we have:

$$P_{g_{\chi_0}}(\zeta) = \prod_{a \in (\mathbb{Z}/g_{\chi_0}\mathbb{Z})^*} (\zeta - \zeta^{p^n a}) = \prod_a [\,\zeta(1 - \zeta^{p^n a - 1})\,];$$

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

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

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

hence $U_2 = A'\,(Q_1 - p\,T) + p\,B = A'\,Q_1 + p\,S$, $S \in \mathbb{Z}_p[X]$. Since $A \neq 0$ may be chosen monic by assumption, $A' \neq 0$ is monic, $U_2$ is of degree larger or equal to that of $Q_1$ (absurd). In conclusion, $\overline{U}_2 = 0$, contrary to the assumption $k \geq 1$ in (4.2). □

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

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

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

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

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

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

It remains to verify that:

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

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

In the algebra $\mathscr{A}_\chi = \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$, we obtain two systems of idempotents, that is to say, the images in $\mathscr{A}_\chi$ of the $e_{\varphi_{u,0}} \in \mathbb{Z}_p[G_0]$, where $\varphi_{u,0}$ is above the component $\psi_{u,0}$, of prime-to-$p$ order, of $\psi_u$, and that of the $e_{\varphi_u}(\sigma_\chi)$ corresponding to $\varphi_u$. Fixing the character $\varphi_u =: \varphi$ above $\psi =: \psi_0\, \psi_p$ and its non $p$-part $\varphi_0$ above $\psi_0$, we consider both:

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

and $e_{\varphi_0}(\sigma_\chi)$ defined as follows by means of polynomial relations in $\mathbb{Z}[X]$ deduced from (4.5):

$$\begin{aligned} e_{\varphi_0}(\sigma_\chi) &= \Lambda_\varphi(\sigma_\chi) \cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(\sigma_\chi), \\ \text{such that}\ \ \Lambda_\varphi(X) &\cdot \prod_{\varphi' \neq \varphi} P_{\varphi'}(X) \equiv 1 \pmod{P_\varphi(X)}; \end{aligned} \tag{4.8}$$

we denote $e_{\varphi_0}(\sigma_\chi)$ simply by $e_{\varphi_0}$, which is legitimate by Lemma 3.6.

To verify that $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}} = (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}}$, it suffices to show that $e^{\varphi_0}$ and $e_{\varphi_0}$ correspond to the same simple factor of the algebra $\mathscr{A}_\chi$. For this, we remark that the homomorphism defined, for the fixed character $\varphi$, by $\sigma_\chi \mapsto \psi(\sigma_\chi)$, $\psi \mid \varphi$, induces a surjective homomorphism $\mathscr{A}_\chi \longrightarrow \mathbb{Z}_p[\mu_{g_\chi}]$ whose kernel is equal to $\bigoplus_{\varphi \neq \varphi} \mathscr{A}_\chi\, e_{\varphi_0'}$.

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

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

which is zero for all $\psi_0'$ except $\psi_0' = \psi_0$ where $\psi(e_{\psi_0}) = 1$. Whence $\psi(e^{\varphi_0}) \neq 0$. Let $\mathscr{M}_\chi^{\rm alg}$ as $\mathscr{A}_\chi$-module; on may write (from (4.6)):

$$\mathscr{M}_\chi^{\rm alg} = \bigoplus\nolimits_{\varphi \mid \chi} (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}}$$

and we know that $(\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}}$ coincides with $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}} = \mathscr{M}_\varphi^{\rm alg}$ (Definition (4.7)); then, due to the properties of the $e_{\varphi_0}$ (defined by (4.8)):

$$(\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}} = \{x \in \mathscr{M}_\chi^{\rm alg},\ \ P_\varphi(\sigma_\chi) \cdot x = 1\} = \mathscr{M}_\varphi^{\rm alg}.$$

Denote by $e_{\varphi_0}$ any of these two semi-simple idempotents $e^{\varphi_0}$ or $e_{\varphi_0}$.

If $\mathscr{M}_\chi'$ is a sub-$\mathscr{A}_\chi$-module of $\mathscr{M}_\chi^{\rm alg}$, then:

$$\mathscr{M}_\varphi' := (\mathscr{M}_\chi')^{e_{\varphi_0}} = \{x' \in \mathscr{M}_\chi',\, P_\varphi(\sigma_\chi) \cdot x' = 1\}.$$

Since $\mathscr{A}_\chi\, e_{\varphi_0} \simeq \mathbb{Z}_p[\mu_{g_\chi}]$, $\mathscr{M}_\varphi^{\rm alg}$ and $\mathscr{M}_\varphi'$ are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

This finishes the proof of Theorem 4.1 and we shall apply this to $\mathscr{A}_\chi$-modules. □

4.2. **Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\rm ar}$.** From Definition 3.11, $\mathscr{M}_\chi^{\rm ar} := \{x \in \mathscr{M}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \text{for all } k \subsetneqq K_\chi\}$. This invites to give the following arithmetic definition:

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

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

Note that if $p \mid g_\chi$, then the norm conditions may be limited to $\mathbf{N}_{K_\chi/k_p}(x) = 1$, with $[K_\chi : k_p] = p$.

**Remark 4.4.** Of course $\mathscr{M}_\varphi^{\rm ar} = (\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}}$, $e_{\varphi_0}$ being defined by (4.7) or (4.8), and $\mathscr{M}_\varphi^{\rm ar}$ is a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_\varphi^{\rm alg}$. In the sequel, we shall privilege the notation $\mathscr{M}_\varphi^{\rm ar}$ rather than $(\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}}$ since the definition of $\mathscr{M}_\varphi^{\rm ar} = \{x \in \mathscr{M}_\chi^{\rm ar},\, P_\varphi(\sigma_\chi) \cdot x = 1\}$ is more convenient in any viewpoint.

So, we have the arithmetic version of Theorem 4.1:

**Theorem 4.5.** *Let $\mathscr{M}$ be a $\mathscr{G}$-family of $\mathbb{Z}_p[\mathscr{G}]$-modules. Then we get, for all $\chi \in \mathscr{X}$, the decomposition $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\rm ar}$.*

4.3. **Summary of the properties of the $\mathbb{Z}_p[\mathscr{G}]$-families $\mathscr{M}^{\rm alg}$ and $\mathscr{M}^{\rm ar}$.** From Theorems 3.15, 4.1, 4.5, Definitions 3.5, 3.11, 4.3. Let $\chi \in \mathscr{X}$ and let $\varphi \mid \chi$, $\varphi \in \Phi$.

(i) Let $\sigma_\chi$ be a generator of $G_\chi = {\rm Gal}(K_\chi/\mathbb{Q})$; put $g_\chi := \#G_\chi$. Recall that $P_\chi$ (resp. $P_\varphi \mid P_\chi$) is the $g_\chi$th global cyclotomic polynomial (resp. the local $\varphi$-cyclotomic polynomial); define:

$$\begin{cases} \mathscr{M}_\chi^{\rm alg} := \{x \in \mathscr{M}_{K_\chi},\ P_\chi(\sigma_\chi) \cdot x = 1\}, \\ \mathscr{M}_\varphi^{\rm alg} := \{x \in \mathscr{M}_{K_\chi},\ P_\varphi(\sigma_\chi) \cdot x = 1\}, \\ \mathscr{M}_\chi^{\rm ar} := \{x \in \mathscr{M}_\chi^{\rm alg},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneqq K_\chi\}, \\ \mathscr{M}_\varphi^{\rm ar} := \{x \in \mathscr{M}_\varphi^{\rm alg},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \forall\, k \subsetneqq K_\chi\} = \mathscr{M}_\varphi^{\rm alg} \cap \mathscr{M}_\chi^{\rm ar}. \end{cases}$$

Then $\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\rm alg}$ and $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\rm ar}$. All these components are $\mathbb{Z}_p[\mu_{g_\chi}]$-modules via $\sigma \in G_\chi \mapsto \psi(\sigma)$, for $\psi \mid \chi$, $\psi \mid \varphi$, respectively.

(ii) Assume that the maximal $p$-sub-extension of $K/\mathbb{Q}$ is cyclic and such that for all its sub-extensions $k/k'$, the norms $\mathbf{N}_{k/k'}$ are surjective. Then, if $\mathscr{M}_K$ is finite, $\#\mathscr{M}_K = \prod_{\chi \in \mathscr{X}_K} \#\mathscr{M}_\chi^{\rm ar} = \prod_{\varphi \in \Phi_K} \#\mathscr{M}_\varphi^{\rm ar}$.

## 5. Application to relative class groups

5.1. **Arithmetic definition of relative class groups.** We will apply the previous results using first odd characters $\chi$ giving $\mathbf{H}_\chi^{\rm alg}$ and $\mathbf{H}_\chi^{\rm ar}$. The case of even characters requires some deepening of Leopoldt's results [Leo1954]; it will be considered in the next section.

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

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

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

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

$$1 \to (\mathbf{H}_K^{\rm ar})^- \longrightarrow \mathbf{H}_K \xrightarrow{\mathbf{N}_{K/K^+}} \mathbf{H}_{K^+} = \mathbf{H}_K^+ \to 1$$

and the formula:

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

We denote by $\mathscr{H}_K$ (resp. $(\mathscr{H}_K^{\rm ar})^-$ and $\mathscr{H}_K^+ := \mathscr{H}_{K^+}$), the $p$-Sylow subgroup of $\mathbf{H}_K$ (resp. $(\mathbf{H}_K^{\rm ar})^-$ and $\mathbf{H}_K^+$). For the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{H}_K$, we introduce the $\mathscr{A}_\chi$-modules $\mathscr{H}_\chi^{\rm alg}$ and $\mathscr{H}_\chi^{\rm ar}$ for $\chi \in \mathscr{X}$, then their $\varphi$-components (Definitions 3.5, 3.11, 4.3) which are $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

5.2. **Proof of the equality $\mathbf{H}_\chi^{\rm ar} = \mathbf{H}_\chi^{\rm alg}$, for all $\chi \in \mathscr{X}^-$.** To prove this equality and then 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 to prove the equality of the $\chi$-components $\mathscr{H}_\chi^{\rm alg}$, $\mathscr{H}_\chi^{\rm ar}$, for $\chi \in \mathscr{X}^-$.

**Lemma 5.1.** *Assume that $\mathscr{H}_\chi^{\rm ar} \subsetneq \mathscr{H}_\chi^{\rm alg}$. Then there exists a unique sub-extension $K_{\chi'}$ of $K_\chi$, such that $[K_\chi : K_{\chi'}] = p$ (i.e., if $\psi \mid \chi$ then $\chi'$ 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 $g_\chi$, $\nu_{K_{\chi'}/k'_\ell}(h') = 1$, where $k'_\ell$ is the unique sub-extension of $K_{\chi'}$ such that $[K_{\chi'} : k'_\ell] = \ell$;*

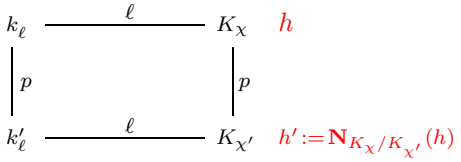
*(ii) $\mathbf{J}_{K_\chi/K_{\chi'}}(h') = 1$;*

*(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 and $\mathscr{H}_\chi^{\rm alg} = \mathscr{H}_\chi^{\rm ar}$. 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 $k_\ell$ is the unique sub-extension of $K_\chi$ such that $[K_\chi : k_\ell] = \ell$ and then $k'_\ell = k_\ell \cap K_{\chi'}$:




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 $K_\chi$, 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 $\mathbf{N}_{K_\chi/k_\ell}(h) = 1$, for all $\ell \neq p$ dividing $g_\chi$; since moreover $h' = \mathbf{N}_{K_\chi/K_{\chi'}}(h) = 1$, this yields by definition $h \in \mathscr{H}_\chi^{\rm ar}$ (absurd). □

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

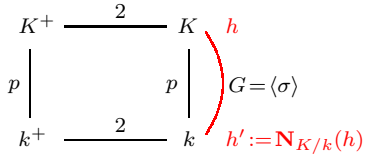
*Proof.* Let $\mathbf{Z}_k$ and $\mathbf{Z}_K$ be the rings of integers of $k$ and $K$, respectively; let $\mathscr{A}_k(\mathfrak{a}) \in \mathscr{H}_k$, with $\mathfrak{a}\mathbf{Z}_K =: (\alpha)\mathbf{Z}_K$, $\alpha \in K^\times$. We then have $\alpha^{1-\sigma} =: \varepsilon \in \mathbf{E}_K^*$.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

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

5.2.1. *Study of the case $p \neq 2$.* We are in the context of Lemma 5.1. Put $K := K_\chi$ and $k := K_{\chi'}$; then $K/k$ is of degree $p$ and the class $h' = \mathbf{N}_{K/k}(h) \in \mathscr{H}_k$ is of order $p$ and capitulates in $K$.

Assume that $K$ is imaginary (i.e., $\chi$ is odd, thus $h \in (\mathscr{H}_K^{\mathrm{ar}})^-$); since $K/k$ is of degree $p \neq 2$, $k$ is also imaginary and $h' \in (\mathscr{H}_k^{\mathrm{ar}})^-$.

We introduce the maximal real subfields, giving the diagram:




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

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

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

**Lemma 5.4.** *The group $q(\mu_K^*)$ (of order 1 or $p$) is of order $p$ if and only if $\mu_K^* = \langle\zeta_1\rangle$ and $\mathbf{E}_K^{1-\sigma} \cap \langle\zeta_1\rangle = 1$, where $\zeta_1$ 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 $\zeta$ be a generator of $\mu_K^*$ (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 that $\zeta^p \in k$ (since $[K : k] = [\mathbb{Q}(\zeta) : k \cap \mathbb{Q}(\zeta)] = p$), thus $K/k$ is a Kummer extension of the form $K = k(\sqrt[p]{\zeta_r})$, $\zeta_r$ of order $p^r$, $r \geq 1$, $\zeta = \zeta_{r+1}$, and $\zeta^{1-\sigma} = \zeta_1$, giving $\mathbf{N}_{K/k}(\zeta) = \zeta^p = 1$, hence $\zeta = \zeta_1 \in k$ (absurd). So we have $\zeta = \zeta_1 \in k$ and $\mathbf{E}_K^{1-\sigma} \cap \mu_K^* \subseteq \langle\zeta_1\rangle$. Thus, $q(\mu_K^*)$ being of order $p$, necessarily $\mathbf{E}_K^{1-\sigma} \cap \mu_K^* = 1$. □

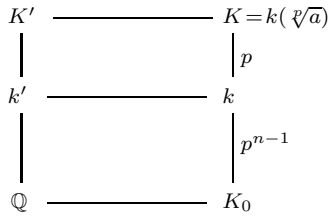
**Lemma 5.5.** *If $(\mathscr{H}_k^{\mathrm{ar}})^- \cap \mathrm{Ker}(\mathbf{J}_{K/k}) \neq 1$, this group is of order $p$ and $K/k$ is a Kummer extension of the form $K = k(\sqrt[p]{a})$, $a \in k^\times$, $a\mathbf{Z}_k = \mathfrak{a}^p$, the ideal $\mathfrak{a}$ of $k$ being non-principal (such a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

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

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

Since $K = k(\sqrt[p]{a})$, with $a\mathbf{Z}_k = \mathfrak{a}^p$, only the prime ideals dividing $p$ can ramify in $K/k$. Consider the following decomposition of the extension $K/\mathbb{Q}$ for $p \neq 2$, with $K/K_0$ and $K'/\mathbb{Q}$ cyclic of $p$-power degree $p^n$, $K/K'$ and $K_0/\mathbb{Q}$ of prime-to-$p$ degree, and let $\ell$ be a prime number totally ramified in $K'/\mathbb{Q}$ (such a

prime does exist since $G_{K'} \simeq \mathbb{Z}/p^n\mathbb{Z}$); this prime is then totally ramified in $K/K_0$, hence in $K/k$, which 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 $p \neq 2$; thus $K'$ is the unique sub-extension of degree $p^n$ of $\mathbb{Q}(\mu_{p^{n+1}})$ and $k'$ is 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). Since $\zeta_1 \in k$, one has $\mu_{p^n} \subset k$, $\mu_{p^{n+1}} \subset K$ and $\mu_{p^{n+1}} \not\subset k$, so $K = k(\zeta) = k(\sqrt[p]{\zeta^p})$, with $\zeta$ 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).

5.2.2. *Case $p = 2$.* The extension $K/\mathbb{Q}$ is still imaginary cyclic, $k$ is necessarily equal to $K^+$ and $\sigma$ is the complex conjugation $s_\infty$.

From [Has1952, Satz 24] the "index of units" $Q_K^-$ is trivial in the cyclic case; thus for all $\varepsilon \in \mathbf{E}_K^*$, $\varepsilon = \varepsilon^+\zeta$, $\varepsilon^+ \in k$, $\zeta$ 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).

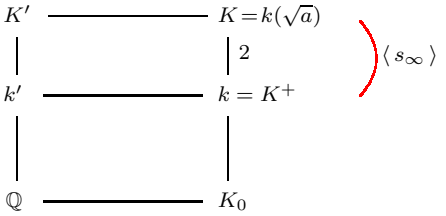
(ii) Case $\varepsilon = \pm i$. Then $\alpha^{1-\sigma} = \pm i$ with $-1 = (\pm i)^{1-\sigma}$; one may assume $\alpha^{1-\sigma} = i$. This yields $\alpha^2 i^{-1} \in k^\times$. Put $\alpha^2 = ic$, $c \in k^\times$; it follows $\mathfrak{a}^2\mathbf{Z}_K = \alpha^2\mathbf{Z}_K = c\mathbf{Z}_K$,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

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

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

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

But $K$ is the direct compositum over $\mathbb{Q}$ of $k = K^+$ and $\mathbb{Q}(i)$ and must be cyclic, so $[k : \mathbb{Q}]$ is necessarily odd and an invariant class in $k/\mathbb{Q}$ is of odd order giving the principality of $\mathfrak{a}$ in $k$ (absurd). So, only 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 $h' = 1$. Whence:

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

Using the order formula (5.2), we get:

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

We have obtained the following result about relative class groups:

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

$$\text{(5.3)} \qquad \begin{cases} (\mathscr{H}_K^{\rm ar})^- := \{h \in \mathscr{H}_K,\ \mathbf{N}_{K/K^+}(h) = 1\} \\ (\mathscr{H}_K^{\rm alg})^- := \{h \in \mathscr{H}_K,\ \nu_{K/K^+}(h) = 1\}. \end{cases}$$

*Then $\mathscr{H}_K^{\rm ar} = \mathscr{H}_K^{\rm alg}$, $\mathscr{H}_\varphi^{\rm ar} = \mathscr{H}_\varphi^{\rm alg}$ for all $\varphi \in \Phi_K^-$, $(\mathbf{H}_K^{\rm ar})^- = (\mathbf{H}_K^{\rm alg})^-$.*

*Proof.* For all subfield $k$ of $K$ with $[K : k] = p$, $\mathbf{J}_{K/k}$ is injective on $(\mathscr{H}_k^{\rm ar})^-$ if $p \neq 2$ and $\mathbf{J}_{K/K^+}$ is injective on $\mathscr{H}_{K^+}$ for $p = 2$; so $\nu_{K/k} = \mathbf{J}_{K/k} \circ \mathbf{N}_{K/k}$ yields $(\mathscr{H}_K^{\rm ar})^- = (\mathscr{H}_K^{\rm alg})^-$ from Definition 3.11, then $(\mathbf{H}_K^{\rm ar})^- = (\mathbf{H}_K^{\rm alg})^-$ by globalization. □

We shall write simply $\mathbf{H}_K^-$ for the two notions "alg" and "ar" in the cyclic case. Using Theorem 4.1 we may write, for all $\chi \in \mathscr{X}^-$, $\#\mathscr{H}_\chi^{\rm alg} = \#\mathscr{H}_\chi^{\rm ar} = \prod_{\varphi|\chi} \#\mathscr{H}_\varphi^{\rm ar}$.

**Corollary 5.9.** *Let $K/\mathbb{Q}$ be an imaginary cyclic extension. Then:*

$$\#\mathbf{H}_K^+ = \textstyle\prod_{\chi \in \mathscr{X}_K^+} \#\mathbf{H}_\chi^{\rm ar} \quad \& \quad \#\mathbf{H}_K^- = \prod_{\chi \in \mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm ar}.$$

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

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

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

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

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

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. Recall that $\mathbf{H}_\chi^{\rm ar} := \{h \in \mathbf{H}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1, \text{ for all } k \subsetneq K_\chi\}$; then we have:

**Theorem 5.10.** *Let $\chi \in \mathscr{X}^-$ and let $g_\chi$ be the order of $\chi$ and $f_\chi$ its conductor; then $\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi|\chi} \big(-\frac{1}{2}\,\mathbf{B}_1(\psi^{-1})\big)$, where $\alpha_\chi = 1$ (resp. $\alpha_\chi = 0$) if $g_\chi$ is a 2-power (resp. if not) and:*

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

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

*(iii) $w_\chi = 1$ if $K_\chi = \mathbb{Q}(\mu_4)$ for $p = 2$.*

*Proof.* We use [Or1975$^b$, Proposition III (g)] or [Leo1954, Chap. I, § 1 (4)] recalled in Theorem 2.1; it is sufficient to prove that for any imaginary cyclic extension $K/\mathbb{Q}$:

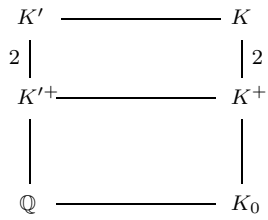
$$\#\mathbf{H}_K^- = \prod_{\chi\in\mathscr{X}_K^-} \big(2^{\alpha_\chi}\cdot w_\chi \cdot \prod_{\psi\mid\chi}\big(-\tfrac{1}{2}\mathbf{B}_1(\psi^{-1})\big)\big),$$

the expected equality will come from Theorem 5.8 and the relation:

$$\#\mathbf{H}_K^- = \prod_{\chi\in\mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm ar}.$$

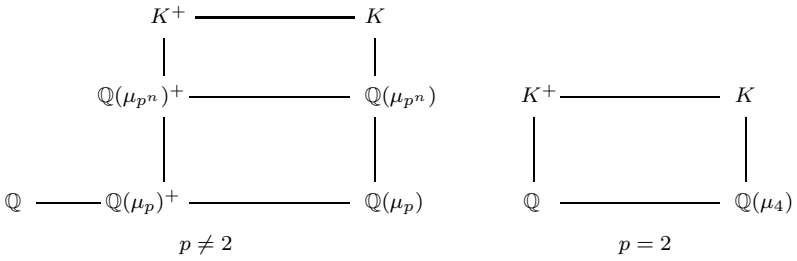
So, it remains to prove that $\prod_{\chi\in\mathscr{X}_K^-}\big(2^{\alpha_\chi}\cdot w_\chi\big) = w_K^-$.

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




As $K^+$ and $K'^+$ are real, then all the $\alpha_\chi$ are zero, except when $g_\chi$ is a 2-power, hence for the unique $\chi_0$ 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 $w_\chi$ 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:




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

**Remark 5.11.** For any imaginary extension $K$, we have:

$$\#\mathbf{H}_K^- = \frac{Q_K^- w_K^-}{2^{n_K^-}} \prod_{\chi\in\mathscr{X}_K^-} \#\mathbf{H}_\chi^{\rm alg},$$

where $n_K^-$ is the number of imaginary cyclic sub-extensions of $K$ of 2-power degree and $w_K^-$ is the 2-part of $w_K$ (resp. $\frac{1}{2}w_K$) if $\mathbb{Q}(\mu_4) \not\subset K$ (resp. $\mathbb{Q}(\mu_4) \subset K$). See [Gra1976, Remarque II 2, p. 32].

5.4. **Annihilation theorem for $\mathbf{H}_K^-$.** Before significant improvements by means of Stickelberger's elements (leading to the construction of $p$-adic measures, to index formulas and annihilators of various invariants), Iwasawa [Iwa1962] 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 $\mathbb{Z}[G_K]^- := \{\Omega \in \mathbb{Z}[G_K], (1+s_\infty)\cdot\Omega = 0\}$, $s_\infty$ 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.

This formula does not generalize for arbitrary imaginary extension $K/\mathbb{Q}$ (see the counterexample given in [Gra1976, p. 33]).

Many contributions have appeared (e.g., [Leo1962, Gil1975, Coa1977, Gra1978, All2013, All2017]; 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 $\varphi$-objects which succeeded to give a correct formula (we shall make the same remark for the index formulas given via cyclotomic units in the real case).

5.4.1. *General definition of Stickelberger's elements.* Let $K \in \mathscr{K} \setminus \{\mathbb{Q}\}$. Let $f_K =: f > 1$ be the conductor of $K$ and let $\mathbb{Q}(\mu_f)$ be the corresponding cyclotomic field. Define the more suitable writing of the Stickelberger element $\mathbf{B}_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f} \left(\frac{a}{f} - \frac{1}{2}\right) \cdot \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ (in the summation, the integers $a$ are prime to $f$ and the Artin symbols are taken over $\mathbb{Q}$). Note that the part $\sum_{a=1}^{f} \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ is the algebraic norm $\nu_{\mathbb{Q}(\mu_f)/\mathbb{Q}}$ which does not modify the image of $\mathbf{B}_{\mathbb{Q}(\mu_f)}$ by $\psi$, 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:

$$\begin{cases} \mathbf{S}_K := \mathbf{B}_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K], \text{ where} \\ \mathbf{B}_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = -\sum_{a=1}^{f} \left(\frac{a}{f} - \frac{1}{2}\right)\left(\frac{K}{a}\right)^{-1}. \end{cases} \tag{5.4}$$

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

*Proof.* We have:

$$\mathbf{B}_K^c = \frac{-1}{f} \sum_a \left[a\left(\frac{K}{a}\right)^{-1} - ac\left(\frac{K}{a}\right)^{-1}\left(\frac{K}{c}\right)^{-1}\right] + \frac{1-c}{2} \sum_a \left(\frac{K}{a}\right)^{-1}.$$

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

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

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

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

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

$$\mathbf{B}_K^c = \mathbf{B}_K'^c \cdot (1 - s_\infty), \quad \mathbf{B}_K'^c \in \mathbb{Z}[G_K], \tag{5.5}$$

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

**Definition 5.13.** *Let $K$ be an imaginary abelian field. Put:*

$$\mathfrak{A}_K := \{\Omega \in \mathbb{Z}[G_K],\ \Omega\, \mathbf{B}_K \in \mathbb{Z}[G_K]\}$$

*($\mathfrak{A}_K$ is an ideal of $\mathbb{Z}[G_K]$ and $\mathbf{S}_K := \mathbf{B}_K \cdot \mathfrak{A}_K$ (cf. (5.4)). Denote by $\Lambda_K \in \mathfrak{A}_K$ the least rational integer such that $\Lambda_K \mathbf{B}_K \in \mathbb{Z}[G_K]$ (thus $\Lambda_K \mid 2f$, where $f$ is the conductor of $K$).*

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

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

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

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

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

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

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

*Proof.* See [Gra1976, p. 35–36]. □

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

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

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

**Lemma 5.16.** *We have $\mathbf{M}_\chi = \prod_{\ell\,|\,g_\chi}(1-\sigma_\chi^{g_\chi/\ell})\,\mathbb{Z}[G_\chi]$, $\mathfrak{a}_\chi := \psi(\mathbf{M}_\chi) = \prod_{\ell\,|\,g_\chi}\left(1-\psi(\sigma_\chi)^{g_\chi/\ell}\right)$; then $\mathbf{S}_\chi$ gives rise to an ideal $\mathfrak{b}_\chi$ multiple of $\mathfrak{a}_\chi$.*

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

The computation of $\mathfrak{b}_\chi$ needs to recall the norm action on Stickelberger's elements; because of the similarity of the result for the norm action on cyclotomic numbers, we recall, without proof, the following well-known formulas (see e.g., [Gra2018$^b$, Section 4]):

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

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

*We have, where $\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)} : \mathbb{Q}[G_{\mathbb{Q}(\mu_f)}] \longrightarrow \mathbb{Q}[G_{\mathbb{Q}(\mu_m)}]$:*

$$\mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = \Omega\cdot\mathbf{B}_{\mathbb{Q}(\mu_m)},\ \mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}(\mathbf{C}_{\mathbb{Q}(\mu_f)}) = \mathbf{C}^{\Omega}_{\mathbb{Q}(\mu_m)},$$

*where* $\Omega := \prod_{p\,|\,f,\ p\nmid m}\left(1-\left(\frac{\mathbb{Q}(\mu_m)}{p}\right)^{-1}\right)$.

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

**Theorem 5.18.** *Let $\chi \in \mathscr{X}^-$ and let $\psi \mid \chi$. Then the $\mathbb{Z}[\mu_{g_\chi}]$-module $\mathbf{H}^{\rm alg}_\chi = \mathbf{H}^{\rm ar}_\chi$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1})\cdot(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}[\mu_{g_\chi}]$, where $\sigma_a := \left(\frac{K}{a}\right)$ is any generator of $G_K$ (cf. Lemma 5.14, Proposition 5.15).*

*The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ is the unit ideal except if $K_\chi \neq \mathbb{Q}(\mu_4)$ is an extension of $\mathbb{Q}(\mu_p)$ of $p$-power degree and if $\Lambda_\chi \equiv 0 \pmod p$, in which case, this ideal is a prime ideal $\mathfrak{p}_\chi \mid p$ in $\mathbb{Q}(\mu_{g_\chi})$. If $K_\chi = \mathbb{Q}(\mu_4)$, this ideal is the ideal $(4)$.*

**Theorem 5.19.** *Let $\varphi \in \Phi^-$ and let $\psi \mid \varphi$. Then the $\mathbb{Z}_p[\mu_{g_\chi}]$-module $\mathscr{H}^{\rm alg}_\varphi = \mathscr{H}^{\rm ar}_\varphi$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1})\cdot(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$, where $\sigma_a$ is any generator of $G_K$.*

*The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$ is the unit ideal except if $K_\chi \neq \mathbb{Q}(\mu_4)$ is an extension of $\mathbb{Q}(\mu_p)$ of $p$-power degree, if $\Lambda_\chi \equiv 0 \pmod p$ and if $\lambda = 1$ in the writing $\psi = \omega^\lambda\cdot\psi_p$ (where $\omega$ is the Teichmüller character and $\psi_p$ of $p$-power order), in which case, this ideal is the prime ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$.*

*If $K_\chi = \mathbb{Q}(\mu_4)$, this ideal is the ideal $(4)$.*

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

$$-\frac{1}{2}\mathbf{B}_1(\psi^{-1}) = -\frac{1}{2}\sum_{a=1}^{46}\big(\frac{a}{47}-\frac{1}{2}\big)\psi^{-1}(\sigma_a) = -\frac{1}{2}\sum_{a=1}^{46}\frac{a}{47}\,\psi^{-1}(\sigma_a).$$

Let's compute $\#\mathbf{H}_\chi = 47\cdot \mathbf{N}_{\mathbb{Q}(\mu_{46})/\mathbb{Q}}\big(-\frac{1}{2}\sum_{a=1}^{46}\frac{a}{47}\,\psi^{-1}(\sigma_a)\big)$:

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

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

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

Whence $\#\mathbf{H}_\chi = 139$ and $\mathbf{H}_\chi \simeq \mathbb{Z}[\mu_{46}]/\mathfrak{p}_{139}$. Since $\Lambda_\chi = 47$, the ideal $\mathfrak{A}_K$ is $\big(\sigma_a - a, 47\big)$, with for instance $a = 5$ (Lemma 5.14), and $\mathfrak{A}_K \cdot \frac{1}{2}\mathbf{B}_K$ annihilates $\mathbf{H}_\chi$; since the image of $\mathfrak{A}_K \cdot \frac{1}{2}\mathbf{B}_K$ is the ideal $\big(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\big) = \mathfrak{p}_{139}$, *the annihilator* of $\mathbf{H}_\chi$ is $\mathfrak{p}_{139}$.

But this ideal is not principal in $\mathbb{Q}(\mu_{46})$ (from [Gra1979$^b$]); PARI checking:

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

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

In [Gra1978, Chap. IV, § 2; Théorème IV1], [Gra1979$^b$, Théorèmes 1, 2, 3], we have given improvements of the annihilation for 2-class groups but it is difficult to say if the case $p = 2$ is optimal or not. By way of example, we cite the following under the above context:

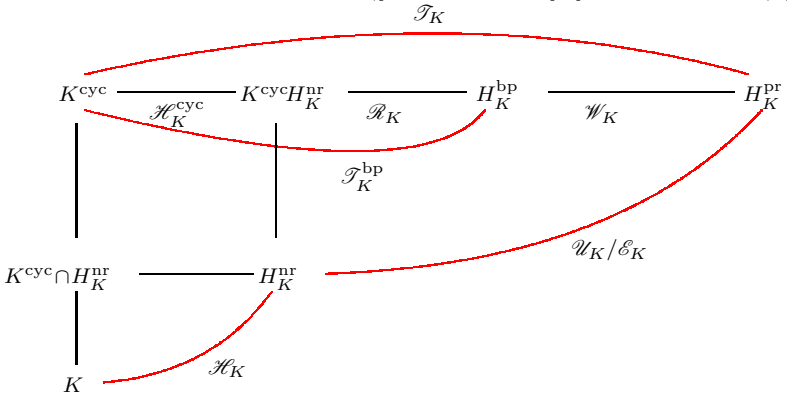
**Theorem 5.21.** *Let $\chi \in \mathscr{X}^-$ and $\psi \mid \varphi \mid \chi$ with $\psi = \psi_0\,\psi_2$, $\psi_0 \neq 1$ of even order, $\psi_2$ of 2-power order. Put $K := K_\chi$.*
*The $\mathbb{Z}_2[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi/\mathbf{J}_{K/K^+}(\mathscr{H}_{\varphi'}^+)$ is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

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

## 6. Application to torsion groups of abelian $p$-ramification

Let $K$ be a totally real number 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 $K$. Under Leopoldt's conjecture, we have $\mathscr{T}_K = {\rm Gal}(H_K^{\rm pr}/K^{\rm cyc})$, where $K^{\rm cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$.

Let $H_K^{\rm nr}$ be the $p$-Hilbert class field and let $H_K^{\rm bp}$ be the Bertrandias–Payan field; the $\mathbb{Z}_p$-module $\mathscr{T}_K^{\rm bp} := {\rm Gal}(H_K^{\rm bp}/K^{\rm cyc})$ is the Bertrandias–Payan module ([Ng1986, Sec. 4], [Jau1990, Sec. 2 (b)]):



Let $K_v$ be the completion of $K$ at the place $v$. The above diagram is related to the exact sequence:

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

where $\mathscr{W}_K := \big(\oplus_{v|p}\,\mu_p(K_v)\big)/\mu_p(K)$, $\mathscr{U}_K$ denotes the group of local units at $p$ and $\mathscr{E}_K = \mathbf{E}_K \otimes \mathbb{Z}_p$ is identified with its diagonal image in $\mathscr{U}_K$ (see [Gra2005, § III.2, (c), Fig. 2.2; Lemma III.4.2.4] and [Gra2018]):

In all the sequel, we assume that $K$ is abelian real.

6.1. **Computation of $\#\mathscr{T}_K$ for $\chi \in \mathscr{X}^+$.** The order of the $\mathbb{Z}_p[G_K]$-module $\mathscr{T}_K$ is well known and given, analytically, by the residue at $s=1$ of the $p$-adic $\zeta$-function of $K$, whence by the values at $s=1$ of $p$-adic $\mathbf{L}$-functions of the non-trivial characters of $K$ (after [Coa1977, Appendix]); see for instance [Gra2019, § 3.4, formula (3.8)] for analytic context. In conclusion we can write:

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

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

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

$$\begin{cases} \mathscr{T}_\chi^{\mathrm{ar}} = \mathscr{T}_\chi^{\mathrm{alg}} = \{x \in \mathscr{T}_{K_\chi},\ P_\chi(\sigma_\chi)\cdot x = 1\} \\ \qquad\qquad = \{x \in \mathscr{T}_{K_\chi},\ \mathbf{N}_{K_\chi/k}(x) = 1,\ \textit{for all } k \subsetneq K_\chi\}, \\ \mathscr{T}_\varphi^{\mathrm{ar}} = \mathscr{T}_\varphi^{\mathrm{alg}} = \{x \in \mathscr{T}_{K_\chi},\ P_\varphi(\sigma_\chi)\cdot x = 1\}. \end{cases}$$

*Moreover, if $K/\mathbb{Q}$ is real cyclic, $\#\mathscr{T}_K = \prod\limits_{\chi \in \mathscr{X}_K} \#\mathscr{T}_\chi^{\mathrm{ar}} = \prod\limits_{\varphi \in \Phi_K} \#\mathscr{T}_\varphi^{\mathrm{ar}}$.*

We denote simply $\mathscr{T}_\chi$ (resp. $\mathscr{T}_\varphi$) these components in the algebraic and arithmetic senses. In the analytic point of view, we have the analogue of Theorems 5.10 and 7.9 (see some $p$-adic formulas about $\mathbf{L}_p$-functions, from classical papers [KuLe1964, AmFr1972, Gra1978$^b$] and a broad presentation in [Was1997, Theorems 5.18, 5.24]):

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

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

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

6.2. **Annihilation theorem for $\mathscr{T}_K$.** An annihilator of $\mathscr{T}_K$ is given by the following statement [Gra2018$^b$, Theorem 5.5] which does not assume any hypothesis on $K$ (real) and $p$ and gives again the known results (e.g., [Gra1979], [Or1981]):

**Theorem 6.3.** *Let $K$ be a real abelian field of conductor $f_K$. 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. Let $c \in \mathbb{Z}$ be prime to $2pf_K$. For all $a \in [1, f_n]$, prime to $f_n$, let $a'_c \in [1, f_n]$ be the unique integer such that $a'_c \cdot c \equiv a \pmod{f_n}$ and put $a'_c \cdot c - a = \lambda_a^n(c)\, f_n$, $\lambda_a^n(c) \in \mathbb{Z}$. Then consider:*

$$\mathbf{A}_{K,n}(c) := \sum_{a=1}^{f_n} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big) =: \mathbf{A}'_{K,n}(c)\cdot(1+s_\infty) \in \mathbb{Z}_p[G_K],$$

*where $s_\infty$ is the complex conjugation and $\mathbf{A}'_{K,n}(c) = \sum\limits_{a=1}^{f_n/2} \lambda_a^n(c)\, a^{-1}\Big(\frac{K}{a}\Big)$.*

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

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

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

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

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

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

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

(ii) Some other annihilation theorems exist for the Jaulent logarithmic class group (see [Jau2021, Jau2022, Jau2022$^b$]); [Jau2022$^b$] is related to Greenberg's conjecture and, when $K$ contains $\mu_p$, [Jau2021] obtains that the Stickelberger ideal annihilates the imaginary component of the logarithmic class group and that its reflection annihilates the real component of the Bertrandias–Payan module. It will be interesting to formulate a "Main Conjecture" about the $\varphi$-components of these modules.

## 7. Application to class groups of real abelian extensions

Denote by $\mathbf{E}$ the $\mathscr{G}$-family for which $\mathbf{E}_K$, $K \in \mathscr{K}$, is the group of absolute value of the global units of $K$, the Galois action being defined by $|\varepsilon|^\sigma = |\varepsilon^\sigma|$ for any unit $\varepsilon$ and any $\sigma \in \mathscr{G}$. The $\mathbf{E}_K$ are free $\mathbb{Z}$-modules of rank $[K : \mathbb{Q}] - 1$ for real fields $K$.

7.1. **The Leopoldt $\chi$-units.** In [Leo1954] Leopoldt defined unit groups, $\mathbf{E}_\chi$, that we shall call (as in [Or1975$^b$]) the group of $\chi$-units for rational characters $\chi \in \mathscr{X}^+ \setminus \{1\}$; from the definition of $\chi$-objects and the results of the previous sections we can write (where $\nu$ may be replaced by $\mathbf{N}$):

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

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

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

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

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

The following computations are also available in [Leo1954, Leo1962, Or1975$^b$].

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

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

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

$$\begin{cases} q_\chi = \prod_{\ell \mid g_\chi} \ell^{\frac{\phi(g_\chi)}{\ell - 1}}, \ \text{if } g_\chi \text{ is not the power of a prime number,} \\ q_\chi = \ell^{\frac{\phi(g_\chi)}{\ell-1} - 1} = \ell^{\ell^{n-1} - 1}, \ \text{if } g_\chi \text{ is a prime power } \ell^n,\ n \geq 1, \\ q_1 = 1 \end{cases}$$

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

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

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

7.2. **The Leopoldt cyclotomic units.** For the main definitions and properties of cyclotomic units, see [Leo1954, § 8 (1)], [Or1975].

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

$$\mathbf{C}_\chi := \prod_{a \in A_\chi} (\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a}), \quad \zeta_{2f_\chi} := \exp\big(\tfrac{i\pi}{f_\chi}\big),$$

*where $A_\chi$ is a half-system of representatives of $(\mathbb{Z}/f_\chi\mathbb{Z})^\times$.*

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

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

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

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

**Proposition 7.8.** *For all $\chi \in \mathscr{X}^+ \setminus \{1\}$, $\#\mathbf{H}_\chi^{\rm ar} = \frac{Q_\chi}{q_\chi} \cdot (\mathbf{E}_\chi : \mathbf{C}_\chi^{\Delta_\chi})$, where $\Delta_\chi = \prod_{\ell \mid g_\chi} \big(1 - \sigma_\chi^{g_\chi/\ell}\big)$. We get the relation $\#\mathbf{H}_\chi^{\rm ar} = \frac{1}{q_\chi}\big(\mathbf{E}_{K_\chi} : \mathbf{E}_{K_\chi}^0 \oplus \mathbf{C}_\chi^{\Delta_\chi}\big)$ interpreting $Q_\chi$* [Gra1976, Corollaire III.1].

To interpret the coefficient $q_\chi$, we have replaced the Leopoldt group $\mathbf{C}_\chi^{\Delta_\chi}$ of cyclotomic units by the larger group $\mathbf{F}_{K_\chi} := \mathbf{C}_{K_\chi} \cap \mathbf{E}_{K_\chi}$ deduced from $\mathbf{C}_{K_\chi}$; see the long proof [Gra1976, Chap. III, § 3] giving the final result interpreting the coefficient $q_\chi$ and giving the analog of Theorem 5.10 for real class groups, where we recall that $\mathbf{E}_{K_\chi}$ is the group of absolute values of units of $K_\chi$, $\mathbf{E}_{K_\chi}^0$ the subgroup of $\mathbf{E}_{K_\chi}$ generated by the $\mathbf{E}_k$ for all the subfields $k \subsetneq K$ (Definition 7.1) and $\mathbf{F}_{K_\chi} = \mathbf{C}_{K_\chi} \cap \mathbf{E}_{K_\chi}$ (Definition 7.7):

**Theorem 7.9.** *Let $\mathbf{H}_\chi^{\rm ar} := \{x \in \mathbf{H}_{K_\chi}, \mathbf{N}_{K_\chi/k}(x) = 1, \text{ for all } k \subsetneq K_\chi\}$. Let $g_\chi$ be the order of $\chi \in \mathscr{X}^+ \setminus \{1\}$ and $f_\chi$ its conductor. Then:*

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

*where $w_\chi$ is defined as follows:*

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

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

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

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

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

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

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

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

**Corollary 7.10.** *If $p \nmid g_\chi$, $\#\mathscr{H}_\chi = \big(\mathscr{E}_\chi : \mathscr{F}_\chi\big)$ and $\#\mathscr{H}_\varphi = \big(\mathscr{E}_\varphi : \mathscr{F}_\varphi\big)$, where $\mathscr{E}_\varphi = \mathscr{E}_{K_\chi}^{e_\varphi}$ and $\mathscr{F}_\varphi$ is generated by $\mathbf{C}_\chi^{e_\varphi}$.*

*Proof.* In the semi-simple case $p \nmid g_\chi$, for any $\mathbb{Z}_p[G_K]$-module $\mathscr{M}_K$, $\mathscr{M}_\chi = \mathscr{M}_K^{e_\chi}$ and $\mathscr{M}_\varphi = \mathscr{M}_K^{e_\varphi}$, with the usual semi-simple idempotents; thus, $\widetilde{\mathscr{E}}_\chi = \widetilde{\mathscr{E}}_\chi^{e_\chi} = \mathscr{E}_{K_\chi}^{e_\chi} / \mathscr{E}_{K_\chi}^{0\, e_\chi} \cdot \mathscr{F}_{K_\chi}^{e_\chi} = \mathscr{E}_\chi / \mathscr{F}_\chi$, since $\mathscr{E}_{K_\chi}^{0\, e_\chi} = 1$. The claim for $\varphi \mid \chi$ is the Main Theorem proved in the semi-simple context. □

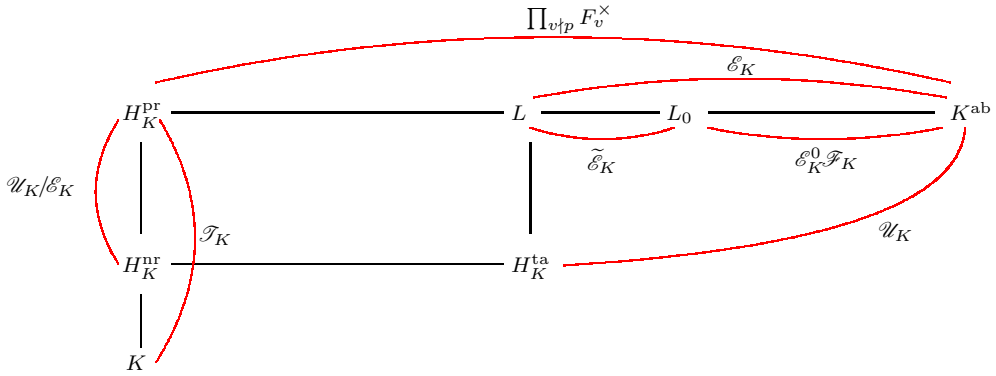
**Remarks 7.11.** (i) The viewpoint given by Theorem 7.9, which appears to have been ignored, seems more convenient than formulas trying to use Sinnott's cyclotomic units. Indeed, compare with [Grei1992, Theorem 4.14] using instead $\mathscr{H}_\chi^{\rm alg}$ (in a partial semi-simple context as explained in Remark 8.2) and Sinnott's group of cyclotomic units, larger than classical Leopoldt's group of Definition 7.7, but which give rise to intricate index formulas. Moreover, as we have mentioned in [Gra1977, Remark III.1], an analytic formula for $\#\mathscr{H}_\chi^{\rm alg}$, $\chi \in \mathscr{X}^+$, does not seem obvious (if any) because of capitulation aspects (see the numerical examples of § 3.3).

We hope that Theorem 7.9 suggests a new statement of the Main Conjecture for the $\mathscr{H}_\varphi$'s, especially in the non semi-simple real case (see § 8.2 for the corresponding analytic values).

(ii) Since $\mathbf{N}_{K_\chi/k}(\mathbf{E}_{K_\chi}) \subseteq \mathbf{E}^0_{K_\chi}$, $\mathbf{N}_{K_\chi/k}(\mathscr{E}_{K_\chi}) \subseteq \mathscr{E}^0_{K_\chi}$, for all $k \subsetneq K_\chi$, the modules $\widetilde{\mathbf{E}}_\chi := \mathbf{E}_{K_\chi}/\mathbf{E}^0_{K_\chi}\cdot \mathbf{F}_{K_\chi}$ and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi}\cdot \mathscr{F}_{K_\chi}$ are $\chi$-objects (algebraic and arithmetic). Then $\widetilde{\mathscr{E}}_\chi = \bigoplus_{\varphi|\chi} \widetilde{\mathscr{E}}_\varphi$, where the $\varphi$-components are $\widetilde{\mathscr{E}}_\varphi = \{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ \ P_\varphi(\sigma_\chi)\cdot \widetilde{x} = 1\}$.

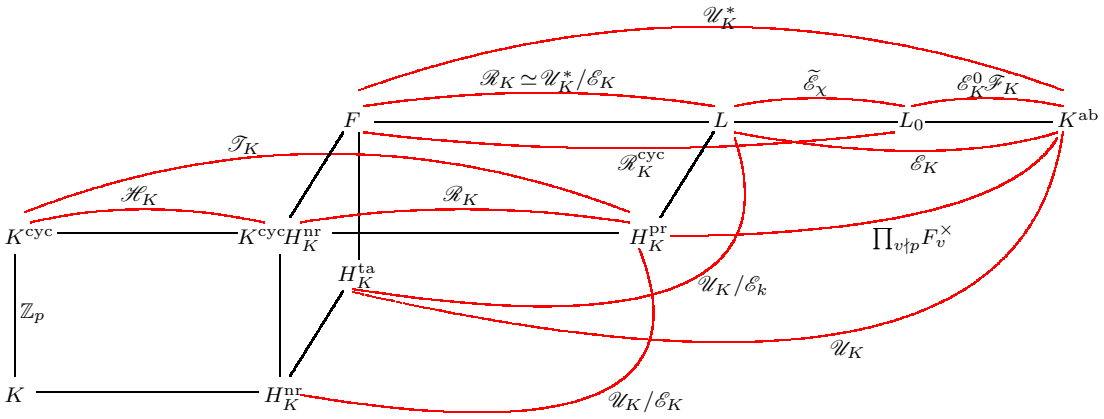
7.4. **Class field theory and regulators.** Let $K \in \mathscr{K}$ (denoting essentially a real field $K_\chi$ in what follows). To simplify the diagrams and the statements, we assume to be in the most common case where $\mathscr{W}_K = 1$ and $K \cap \mathbb{Q}^{\rm cyc} = \mathbb{Q}$, which gives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

The Galois group $\mathscr{T}_K$ may be compared with a "cyclotomic regulator" $\mathscr{R}_K^{\rm cyc}$ as follows. For this purpose, the diagram of the maximal abelian pro-$p$-extension $K^{\rm ab}$ of $K$ is necessary and is the first one below (from [Gra2005, III.4 (d) & Diagram III.4.4.1] with our present notations), where $H_K^{\rm ta}$ is the maximal tamely ramified abelian pro-$p$-extension of $K$ and $F_v^\times$ the $p$-Sylow subgroup of the multiplicative group of the residue field of the tame place $v$; let $L := H_K^{\rm pr}H_K^{\rm ta}$:




In this diagram, class field theory interprets $\mathrm{Gal}(K^{\rm ab}/H_K^{\rm ta})$ as the $\mathbb{Z}_p$-module $\mathscr{U}_K$ and $\mathrm{Gal}(K^{\rm ab}/L)$ as the $\mathbb{Z}_p$-module $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$ (embedded both in $\mathscr{U}_K$ and $\prod_{v\nmid p} F_v^\times$ with suitable Artin maps).

Now, put $\mathscr{U}_K^* := \{u \in \mathscr{U}_K,\ \ \mathbf{N}_{K/\mathbb{Q}}(u) = \pm 1\}$; since $K$ is real, $\mathscr{E}_K$ is of finite index in $\mathscr{U}_K^*$ and $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{U}_K/\mathscr{E}_K) = \mathscr{U}_K^*/\mathscr{E}_K \simeq \mathscr{R}_K$:



Then $F := H_K^{\rm ta}\,K^{\rm cyc}H_K^{\rm nr}$ is fixed by $\mathscr{U}_K^*$ and $F\cap H_K^{\rm pr} = K^{\rm cyc}H_K^{\rm nr}$. Recall the exact sequence $1 \to \mathscr{R}_K^{\rm ram} \to \mathscr{R}_K \to \mathscr{R}_K^{\rm nr} \to 1$, from [Gra2021, § 2 & Figure 3], so that a sub-extension of $L/F$ may be unramified. We assume $K^{\rm cyc}\cap H_K^{\rm nr} = K$ to simplify; we have moreover:

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

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

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

which yields, for $\chi\neq 1$ and $K := K_\chi$, the $\mathbb{Z}_p[G_K]$-modules isomorphism:

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

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

**Remarks 7.12.** Let $\chi\in\mathscr{X}^+\setminus\{1\}$, $K = K_\chi$, and assume to simplify that $\mathscr{W}_K = 1$, $w_\chi = 1$ in Theorem 7.9, $K\cap\mathbb{Q}^{\rm cyc} = \mathbb{Q}$ and $K^{\rm cyc}\cap H_K^{\rm nr} = K$.

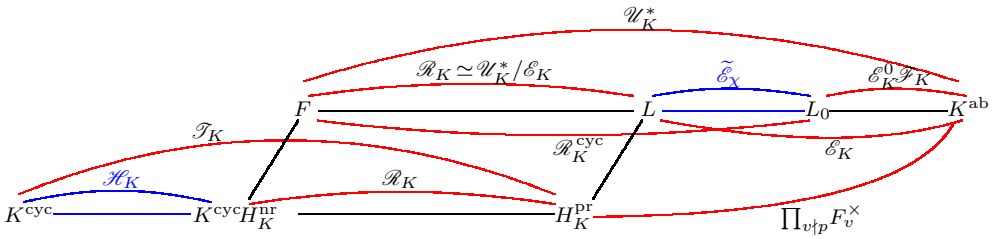
(i) Theorem 7.9 and isomorphism (7.2) give:

$$\#\mathscr{T}_\chi = \#\mathscr{R}_\chi^{\rm cyc} \text{ and } \#\widetilde{\mathscr{E}}_\chi = \#\mathscr{R}_\chi^{\rm cyc}/\#\mathscr{R}_\chi = \#\mathscr{H}_\chi^{\rm ar}.$$

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

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

(ii) The sub-diagram:




given by the extension $K^{\rm ab}/K^{\rm cyc}$, opens perhaps an access way for an interpretation of the Main Conjecture for even characters in the non semi-simple case, or at least an annihilation theorem in the spirit of Thaine's theorem (see Conjecture 7.13).

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

7.5. **Annihilation conjecture for real $p$-class groups.** Before any proof of the conjectural equality $\#\mathscr{H}_\varphi^{\rm ar} = \#\widetilde{\mathscr{E}}_\varphi = \#(\mathscr{E}_{K_\chi}/\mathscr{E}_{K_\chi}^0\cdot\mathscr{F}_{K_\chi})_\varphi$ (giving a Main Theorem for $\varphi\in\Phi_K^+$), it will be interesting to prove that any annihilator of $\widetilde{\mathscr{E}}_\varphi$ annihilates $\mathscr{H}_\varphi^{\rm ar}$, which will be more precise than the annihilators of $\mathscr{T}_\varphi$ (see Theorem 6.2, Remarks 6.4, 7.12).

To our knowledge, the best known annihilation theorem of real $p$-class groups is Thaine's Theorem [Thai1988], [Was1997, Theorem 15.2] saying that any annihilator of $\mathscr{E}_{K_\chi}/\mathscr{F}'_{K_\chi}$ (for a classical definition of the group of cyclotomic units $\mathscr{F}'_{K_\chi}$) is an annihilator of $\mathscr{H}_{K_\chi}$. But Thaine's Theorem only concerns the semi-simple case. Mention also annihilation theorems by Solomon [Sol1992], which are not often optimal because of vanishing of Euler factors; this is discussed in [Gra2018$^b$]. Finally mention the numerous papers of Greither and Kučera (like [GrKu2004, GrKu2014, GrKu2021]) on the annihilation of real class groups, using special units or/and giving information on the Fitting ideals.

**Conjecture 7.13.** *Let $\chi \in \mathscr{X}^+ \setminus \{1\}$ and $\varphi \mid \chi$. Any element of $\mathbb{Z}[\mu_{g_\chi}]$ (resp. $\mathbb{Z}_p[\mu_{g_\chi}]$) annihilating $\mathbf{E}_{K_\chi}/\mathbf{E}^0_{K_\chi}\cdot \mathbf{F}_{K_\chi}$ (resp. $(\mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi}\cdot \mathscr{F}_{K_\chi})_\varphi$), annihilates $\mathbf{H}^{\rm ar}_\chi$ (resp. $\mathscr{H}^{\rm ar}_\varphi$).*

In this direction, we state the following lemma, giving some prerequisites on the subject.

**Lemma 7.14.** *Let $\mathbf{M}_{K_\chi}$ be a torsion-free monogenic $\mathbb{Z}[G_\chi]$-module (i.e., $\mathbb{Z}$-free and $\mathbb{Z}[G_\chi]$-generated by a single element). Let $\mathbf{M}'_{K_\chi}$ be a sub-module of $\mathbf{M}_{K_\chi}$ such that $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$ is annihilated by $P_\chi(\sigma_\chi)\,\mathbb{Z}[G_\chi]$ and finite. Then $(\mathscr{M}_{K_\chi}/\mathscr{M}'_{K_\chi})_\varphi := ((\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi})\otimes\mathbb{Z}_p)_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{\lambda_\varphi}$, $\lambda_\varphi \geq 0$, for all $\varphi \mid \chi$.*

*Proof.* By assumption, $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$ is a finite monogenic $\mathbb{Z}[\mu_{g_\chi}]$-module, of the form $\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A}$, $\mathfrak{A}\neq 0$; so $\mathscr{M}_{K_\chi}/\mathscr{M}'_{K_\chi} \simeq (\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A})\otimes\mathbb{Z}_p$, giving:

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

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

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

Let $\mathbf{M}'_{K_\chi} := \mathbf{E}^0_{K_\chi}\cdot\mathbf{F}_{K_\chi}$. Then, taking into account orders, monogenicity and the fact that $(P_\chi(\sigma_\chi))$ annihilates $\mathbf{M}_{K_\chi}/\mathbf{M}'_{K_\chi}$, Lemma 7.14 is coherent with an annihilation theorem of the $\mathscr{H}^{\rm ar}_\varphi$'s since, from the results of § 7.4, $\mathscr{H}^{\rm ar}_\chi$ is a quotient of $\mathscr{R}^{\rm cyc}_\chi$.

**Example 7.15.** Consider, for $p=7$, the cubic field $K$ of conductor $f=2557$ defined by the polynomial $P = x^3+x^2-852\,x+9281$; then:

$$\mathscr{H}_K \simeq \mathbb{Z}[j]/(1-2j)\mathbb{Z}[j] \quad\text{and}\quad \mathscr{E}_K/\mathscr{F}_K \simeq \mathbb{Z}[j]/(1-2j)\mathbb{Z}[j]$$

where $(1-2j)\mathbb{Z}[j]$ is a prime ideal $\mathfrak{p}$ dividing 7; then we compute:

$$\mathscr{T}_K \simeq \mathbb{Z}/7^2\mathbb{Z}\oplus\mathbb{Z}/7\mathbb{Z}.$$

The following program (only valid for prime conductors $f$) computes the annihilator $\mathbf{A}_K(c)$ of $\mathscr{T}_K$; it defines the classes $\sigma^k\cdot\mathrm{Gal}(\mathbb{Q}(\mu_{fp^N})/K)$, $k=0,1,2$, of Artin symbols, giving $\mathbf{A}_K(c) = A_0 + A_1\sigma + A_2\sigma^2$, then $\beta := A_0 - A_2 + (A_1 - A_2)\,j$, yielding $(\beta) = \mathfrak{p}_1^u\cdot\mathfrak{p}_2^v$ in $\mathbb{Z}[j]$ (up to a prime-to-$p$ ideal):

```
{p=7;f=2557;N=4;pN=p^N;fpN=f*pN;c=lift(znprimroot(f));cm=Mod(c,fpN)^-1;
g=znprimroot(f);lg=lift(Mod((1-lift(g))/f,pN));g=Mod(lift(g)+lg*f,fpN);g3=g^3;
G=znprimroot(pN);lG=lift(Mod((1-lift(G))/pN,f));G=Mod(lift(G)+lG*pN,fpN);
A0=0;A1=0;A2=0;for(k=1,(f-1)/3,for(j=1,p^(N-1)*(p-1),A=g3^k*G^j;gA=g*A;ggA=g^2*A;
a=lift(A);aa=lift(A*cm);la=(aa*c-a)/fpN;A0=A0+la*Mod(a,pN)^-1;
a=lift(gA);aa=lift(gA*cm);la=(aa*c-a)/fpN;A1=A1+la*Mod(a,pN)^-1;
a=lift(ggA);aa=lift(ggA*cm);la=(aa*c-a)/fpN;A2=A2+la*Mod(a,pN)^-1));
print(A0," ",A1," ",A2)}
```

```
Mod(184, 2401) Mod(1526, 2401) Mod(643, 2401)
```

Modulo $7^4$, $A_0 = 184$, $A_1 = 1526$, $A_2 = 643$; since we can compute modulo the norm $1+\sigma+\sigma^2$, this yields the ideal $\mathfrak{p}^3 = (1-2j)^3$. Whence $\mathscr{T}_K \simeq \mathbb{Z}[j]/\mathfrak{p}^2 \oplus \mathbb{Z}[j]/\mathfrak{p} \simeq \mathbb{Z}/7^2\mathbb{Z}\oplus\mathbb{Z}/7\mathbb{Z}$. We note that the annihilator is $\mathfrak{p}^3$ although the structure is not $\mathbb{Z}[j]/\mathfrak{p}^3$.

## 8. Invariants (Algebraic, Arithmetic, Analytic)

We fix an irreducible rational character $\chi\in\mathscr{X} = \mathscr{X}^+\cup\mathscr{X}^-$ and we apply the previous results to the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{H}^{\rm alg}_\varphi$, $\mathscr{H}^{\rm ar}_\varphi$ and $\mathscr{T}^{\rm ar}_\varphi = \mathscr{T}^{\rm alg}_\varphi =: \mathscr{T}_\varphi$, for any $\varphi\mid\chi$, $\varphi\in\Phi^+\cup\Phi^-$ ($\varphi\in\Phi^+$ for $\mathscr{T}_\varphi$).

8.1. **Algebraic and Arithmetic Invariants $m^{\rm alg}(\mathscr{M})$, $m^{\rm ar}(\mathscr{M})$.** Write simply that $\mathscr{H}^{\rm alg}_\varphi$, $\mathscr{H}^{\rm ar}_\varphi$ and $\mathscr{T}_\varphi$ are finite $\mathbb{Z}_p[\mu_{g_\chi}]$-modules whatever $\varphi$; let $\mathfrak{p}_\varphi$ be the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$:

$$\begin{cases} \mathscr{H}^{\rm alg}_\varphi \simeq \displaystyle\prod_{i\geq 1}\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{n^{\rm alg}_{\varphi,i}(\mathscr{H})},\\ \mathscr{H}^{\rm ar}_\varphi \simeq \displaystyle\prod_{i\geq 1}\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{n^{\rm ar}_{\varphi,i}(\mathscr{H})},\\ \mathscr{T}_\varphi \simeq \displaystyle\prod_{i\geq 1}\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{n^{\rm ar}_{\varphi,i}(\mathscr{T})}, \end{cases}$$

where the $n_{\varphi,i}$ are decreasing integers up to 0. Put:

$$\begin{cases} m^{\rm alg}_{\varphi}(\mathscr{H}) := \sum\limits_{i\geq 1} n^{\rm alg}_{\varphi,i}(\mathscr{H}), & m^{\rm alg}_{\chi}(\mathscr{H}) := \sum\limits_{\varphi\vert\chi} m^{\rm alg}_{\varphi}(\mathscr{H}),\\ m^{\rm ar}_{\varphi}(\mathscr{H}) := \sum\limits_{i\geq 1} n^{\rm ar}_{\varphi,i}(\mathscr{H}), & m^{\rm ar}_{\chi}(\mathscr{H}) := \sum\limits_{\varphi\vert\chi} m^{\rm ar}_{\varphi}(\mathscr{H}),\\ m^{\rm ar}_{\varphi}(\mathscr{T}) := \sum\limits_{i\geq 1} n^{\rm ar}_{\varphi,i}(\mathscr{T}), & m^{\rm ar}_{\chi}(\mathscr{T}) := \sum\limits_{\varphi\vert\chi} m^{\rm ar}_{\varphi}(\mathscr{T}). \end{cases}$$

Whence the order formulas:

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

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

$$\sum_{\varphi\vert\chi} m^{\rm ar}_{\varphi}(\mathscr{M}) = \sum_{\varphi\vert\chi} m^{\rm an}_{\varphi}(\mathscr{M}),$$

for any family $\mathscr{M}\in\{\mathscr{H},\mathscr{T}\}$ and $\chi\in\mathscr{X}$ (cf. Theorems 5.10, 7.9, 6.2).

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

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

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

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

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

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

$$m^{\rm an}_{\varphi}(\mathscr{H}^-) := 0, \text{ if } \lambda = 1.$$

(ii) Case $p=2$ (proven by Greither [Grei1992, Theorem B], when $g_\chi$ is not a 2-power and $f_\chi$ is odd).

(ii′) $g_\chi$ is not a 2-power; then:

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

(ii″) $g_\chi$ is a 2-power; then:

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

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

8.2.2. *Case $\varphi\in\Phi^+$, $\varphi\neq 1$, for class groups.* From Definition 7.7 and Theorem 7.9, we consider any real cyclic field $K$, where we recall that:

$\mathbf{E}^0_K := \langle\,\mathbf{E}_k\,\rangle_{k\subsetneq K}$, $\mathbf{F}_K := \mathbf{C}_K\cap\mathbf{E}_K$, $\mathscr{E}_K := \mathbf{E}_K\otimes\mathbb{Z}_p$, $\mathscr{E}^0_K := \mathbf{E}^0_K\otimes\mathbb{Z}_p$, $\mathscr{F}_K := \mathbf{F}_K\otimes\mathbb{Z}_p$, and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi}\cdot\mathscr{F}_{K_\chi}$, for which we have:

$$\widetilde{\mathscr{E}}_\chi = \bigoplus_{\varphi\vert\chi}\widetilde{\mathscr{E}}_\varphi, \quad \widetilde{\mathscr{E}}_\varphi = \{\widetilde{x}\in\widetilde{\mathscr{E}}_\chi,\ P_\varphi(\sigma_\chi)\cdot\widetilde{x}=1\}.$$

Since $\widetilde{\mathscr{E}}_\varphi$ is a monogenic $\mathbb{Z}_p[\mu_{g_\chi}]$-module we can write:

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

Consider the relation $\#\mathscr{H}^{\rm ar}_\chi = w_\chi\cdot\prod\limits_{\varphi\vert\chi}\#\widetilde{\mathscr{E}}_\varphi$ of Theorem 7.9; we remark that $w_\chi=p$ occurs only when $g_\chi$ is a $p$-power, in which case $p$ is totally ramified in $\mathbb{Q}(\mu_{g_\chi})$ and $\varphi=\chi$ (which defines $w_\varphi := w_\chi$).

So, we may define $m^{\rm an}_\varphi(\mathscr{H}^+)$ and $w_\varphi$ as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) Case where $g_\chi$ and $f_\chi$ 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 $f_\chi$ are $p$-powers. Then:

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

8.3. **Main Conjecture – 1976 original statement.** The conjecture we gave in [Gra1976, Gra1977], especially in the non semi-simple case, where simply equality of Arithmetic and Analytic $\varphi$-Invariants. The main justification of such equalities comes from the easy Theorem 2.1 with the arithmetic definitions of § 8.1, the analytic definitions of § 8.2 and the arithmetic expressions of the $\chi$-components that we recall:

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

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

(iii) Theorem 7.9: $\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot (\mathbf{E}_{K_\chi} : \mathbf{E}^0_{K_\chi} \cdot \mathbf{F}_{K_\chi})$, for $\chi \in \mathscr{X}^+$;

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

$$\sum_{\varphi|\chi} m_\varphi^{\rm ar}(\mathscr{M}) = \sum_{\varphi|\chi} m_\varphi^{\rm an}(\mathscr{M}), \text{ for all } \chi \in \mathscr{X},$$

taking into account the decomposition $\mathscr{M}_\chi^{\rm ar} = \oplus_{\varphi|\chi} \mathscr{M}_\varphi^{\rm ar}$ (Theorem 4.5).

Moreover, the annihilation properties of Theorems 5.18, 5.19, 5.21, 6.2, enforce the conjecture 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 $\omega$ is the Teichmüller character. See also [Or1981, Or1986] for similar informations and complements.

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

$$\begin{cases} m_\varphi^{\rm ar}(\mathscr{H}) = m_\varphi^{\rm an}(\mathscr{H}) & (\varphi \in \Phi^+ \cup \Phi^-), \\ m_\varphi^{\rm ar}(\mathscr{T}) = m_\varphi^{\rm an}(\mathscr{T}) & (\varphi \in \Phi^+). \end{cases}$$

**Remark 8.2.** Let $K/\mathbb{Q}$ with a maximal $p$-sub-extension $K/K_0$ cyclic of degree $p^n$, $n \geq 1$, and let $K_i$, $K_0 \subseteq K_i \subset K$, be such that $[K_i : K_0] = p^i$. Let $\psi_0 \in \Psi_{K_0}$ and let $\psi_p \in \Psi_K$ of order $p^n$; we put $\psi_i = \psi_0 \cdot \psi_p^{p^{n-i}} \in \Psi_{K_i}$ and we consider the $p$-adic characters $\varphi_i$ above $\psi_i$, $0 \leq i \leq n$.

The Main Conjecture proven by Greither in [Grei1992, Theorem 4.14, Corollary 4.15], using Sinnott's cyclotomic units, deals with the semi-simple context defined by $\varphi_0$ above $\psi_0$ (it is indeed that of the relations (3.4) which do not give each $\#\mathscr{H}_{\varphi_i}^{\rm ar}$ compared with $\#\widetilde{\mathscr{E}}_{\varphi_i}$).

In other words, in his pioneering work, Greither proves the relation $\sum_{i=0}^{n} m_{\varphi_i}^{\rm ar}(\mathscr{H}^+) = \sum_{i=0}^{n} m_{\varphi_i}^{\rm an}(\mathscr{H}^+)$, for each $\varphi_0 \in \Phi_{K_0}$, instead of our conjecture $m_{\varphi_i}^{\rm ar}(\mathscr{H}^+) = m_{\varphi_i}^{\rm an}(\mathscr{H}^+)$ for all $i \in \{0, 1, \cdots, n\}$. However see many progress by Greither–Kučera in [GrKu2004, GrKu2014] and some of their other papers.

**Remark 8.3.** It remains the problem of the orders, $\#\mathscr{H}_\chi^{\rm alg}$ and $\#\mathscr{H}_\varphi^{\rm alg}$, for which no analytic formula does exist in the non semi-simple real case. For instance, in Example 3.12 with $p=3$, $K$ is the compositum of $k_0=\mathbb{Q}(\sqrt{4409})$ with the degree 9 field of conductor 19, $\chi_i=\varphi_i$ ($i\in\{1,2\}$) is the character of the field $k_i$ of degree $2\cdot 3^i$; then one gets $\mathscr{H}_{\chi_i}^{\rm alg}\simeq\mathbb{Z}/3\mathbb{Z}$ while $\mathscr{H}_{\chi_i}^{\rm ar}=1$, as predicted by the conjecture and checked numerically. In Example 3.13, one finds $\mathscr{H}_{\chi_1}^{\rm alg}\simeq(\mathbb{Z}/3\mathbb{Z})^3$ while $\mathscr{H}_{\chi_1}^{\rm ar}\simeq(\mathbb{Z}/3\mathbb{Z})^2$.

This phenomenon is due to the capitulation of $p$-classes in $p$-extensions and we have given in [Gra2021$^b$, Conjecture 4.1] a general conjecture justified by means of many computations.

8.4. **Finite Iwasawa's theory in cyclic $p$-extensions.** For more details and an application to classical Iwasawa's theory for real abelian fields, in the spirit of Greenberg's conjecture [Gree1976], see [Gra1976, Chap. IV]; nevertheless, *the results hold in arbitrary cyclic $p$-extensions.*

As usual, considering $\chi\in\mathscr{X}^+$ and $\psi\mid\varphi\mid\chi$, we put $\psi=\psi_0\cdot\psi_p$, $\psi_0$ of order $g_0$ prime to $p$, $\psi_p$ of $p$-power order; then $G_\chi=G_0\oplus H$, in an obvious way, and we consider, temporarily, the semi-simple idempotents $e_{\varphi_0}:=\frac{1}{g_0}\sum_{\sigma\in G_0}\varphi_0(\sigma^{-1})\,\sigma$, for $\varphi_0$ above $\psi_0$.

We have $\widetilde{\mathscr{E}}_\chi:=\mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi}\cdot\mathscr{F}_{K_\chi}=\bigoplus_{\varphi\mid\chi}\widetilde{\mathscr{E}}_\varphi$, with $\widetilde{\mathscr{E}}_\varphi=\widetilde{\mathscr{E}}_\chi^{e_{\varphi_0}}$; we note that $\mathscr{E}^{0\,e_{\varphi_0}}_{K_\chi}\simeq\mathscr{E}_{\varphi'}$ and $\widetilde{\mathscr{E}}_\varphi\simeq\mathscr{E}^{e_{\varphi_0}}_{K_\chi}/\mathscr{E}_{\varphi'}\cdot\mathscr{F}^{e_{\varphi_0}}_{K_\chi}$, where $\varphi'$ is above $\psi_0\cdot\psi_p^p$ and $\chi'$ above $\varphi'$. This yields $(\mathscr{E}_{K_\chi}/\mathscr{E}_{K_{\chi'}})_\varphi\simeq\mathbb{Z}_p[\mu_{g_\chi}]$ ([Gra1976, Lemma IV.1]) and the following principle:

**Theorem 8.4.** *Let $\chi\in\mathscr{X}^+$ be such that $g_\chi=g_0\cdot p^n$, $p\nmid g_0$, $n\geq 2$. Let $\chi'$, $\chi''$ be such that $[K_\chi:K_{\chi'}]=[K_{\chi'}:K_{\chi''}]=p$. To simplify, set $K:=K_\chi$, $K':=K_{\chi'}$, $K'':=K_{\chi''}$ and assume that $\mathbf{N}_{K/K'}(\mathscr{F}_K)=\mathscr{F}_{K'}$ (see Lemma 5.17 giving the ramification conditions). Let $\mathfrak{p}_\varphi$ be the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$; put $(\mathscr{F}_K/\mathscr{F}_K\cap\mathscr{E}_{K'})_\varphi\simeq\mathfrak{p}_\varphi^A$, $A\geq 0$ and, in the isomorphism $(\mathscr{E}_{K'}/\mathscr{E}_{K''})_{\varphi'}\simeq\mathbb{Z}_p[\mu_{g_\chi/p}]$, put:*

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

*(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 8.5.** *Let $\chi\in\mathscr{X}^-$ be such that $g_\chi=g_0\cdot p^n$, $p\nmid g_0$, $n\geq 2$. Let $\chi'$ be such that $[K_\chi:K_{\chi'}]=p$. Set $K:=K_\chi$, $K':=K_{\chi'}$ and assume that the Stickelberger elements $\mathbf{B}_K$, $\mathbf{B}_{K'}$ are $p$-integers in $\mathbb{Q}[G_K]$ and that $\mathbf{N}_{K/K'}(\mathbf{B}_K)=\mathbf{B}_{K'}$. Put:*

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

*(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.

Let $k=:k_0$ be real of prime-to-$p$ degree $g$ and let $k^{\rm cyc}=\bigcup_{n\geq 0}k_n$ be its cyclotomic $\mathbb{Z}_p$-extension. The condition $\mu=0$ of Iwasawa's theory is here equivalent to the existence of $n_0\gg 0$ (corresponding to a character $\chi_{n_0}$ of order $g\,p^{n_0}$) such that, for each $\varphi_{n_0}$-component, $a_{n_0-1}<p^{n_0-2}(p-1)$ (case (i) of Theorem 8.4); then the sequence $\#\mathscr{H}_{\chi_n}$ becomes constant giving the $\lambda$-invariant and the relations $\mathscr{E}_{k_{n-1}}=\mathbf{N}_{k_n/k_{n-1}}(\mathscr{E}_{k_n})\cdot\mathscr{E}_{k_{n-2}}$ for all $n\gg 0$; then $p^\lambda=(\mathscr{E}_{k_n}:\mathscr{E}^0_{k_n}\cdot\mathscr{F}_{k_n})$ for $n\gg 0$. More precisely, $p^{\lambda_\varphi}=\#(\mathscr{E}_{k_n}/\mathscr{E}_{k_{n-1}}\cdot\mathscr{F}_{k_n})_\varphi$, for $n\gg 0$.

This methodology does exist in terms of $p$-adic $\mathbf{L}$-functions for abelian fields (see, e.g., [Gra1978$^b$, Chap. V]).

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

**Theorem 8.6.** *Let $k$ be a real abelian field of prime-to-$p$ degree. Greenberg's conjecture is equivalent to $\mathscr{E}_{k_n}=\mathscr{E}^0_{k_n}\cdot\mathscr{F}_{k_n}$, for all $n\gg 0$, where $\mathscr{E}^0_{k_n}$ is the subgroup of $\mathscr{E}_{k_n}$ generated by the units of the strict subfields and $\mathscr{F}_{k_n}$ is the group of Leopoldt cyclotomic units (Definitions 7.1, 7.7).*

## 9. Numerical illustrations with cyclic cubic fields

For $\chi \in \mathscr{X}^+$ and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_{K_\chi}/\mathscr{E}^0_{K_\chi} \cdot \mathscr{F}_{K_\chi}$, we have $\#\mathscr{H}^{\rm ar}_\chi = w_\chi \cdot \#\widetilde{\mathscr{E}}_\chi$ (Theorem 7.9), and for any $\varphi \mid \chi$ we have (conjecturally):

$$\#\mathscr{H}^{\rm ar}_\varphi = w_\varphi \cdot \#\widetilde{\mathscr{E}}_\varphi,\ w_\varphi \in \{1, p\},\ \text{where } \widetilde{\mathscr{E}}_\varphi = \{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ P_\varphi(\sigma_\chi) \cdot \widetilde{x} = 1\}.$$

In another way, we have:

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

and $m^{\rm an}_\varphi(\mathscr{H}) := \sum_{i=1}^{r_\varphi} m^{\rm ar}_{\varphi,i}(\mathscr{H})$ to be compared with $m^{\rm ar}_\varphi(\mathscr{H})$.

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

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

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

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

Thus it is not too difficult to find, from $\mathsf{K.fu}$ giving a $\mathbb{Z}$-basis of $\mathbf{E}_K$, a "Minkowski unit" $\varepsilon$ and its conjugate $\varepsilon^\sigma$ such that $\langle \varepsilon, \varepsilon^\sigma \rangle_{\mathbb{Z}} = \mathbf{E}_K$; indeed, for the 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 $\mathsf{polroot(P)}$. Any change of root gives an inconsequential permutation $(\varepsilon, \varepsilon^\sigma) \mapsto (\varepsilon^\tau, \varepsilon^{\tau\sigma})$, for some $\tau \in G_K$.

For security, we test $\mathsf{Reg_1/Reg} = 1$ where $\mathsf{Reg_1}$ is the regulator of the units $\varepsilon(\rho)$ and $\varepsilon(g(\rho))$, computed with the root $\rho$, and where $\mathsf{Reg} = \mathsf{K.reg}$ is the true regulator given by PARI.

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

If $f$ is prime, $\zeta_{2f} - \zeta_{2f}^{-1}$ generates the prime ideal above $f$; thus:

$$\pi := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\zeta_{2f} - \zeta_{2f}^{-1}) = \pm \mathbf{C}^2$$

with $\pi^3 = f \cdot \eta'$, $\eta' \in \mathbf{E}_K$, whence $\pi^{3\,(1-\sigma)} = \eta'^{1-\sigma} = \eta^6 := (\mathbf{C}^{1-\sigma})^6$ (Proposition 7.8); the program computes $3\log(\mathbf{C}) - \frac{1}{2}\log(f) = \frac{1}{2}\log(\eta')$, so that, to compute $\eta$ from $\eta^3 = \sqrt{\eta'}^{1-\sigma}$, we must divide the regulator $\mathsf{RegC}$ by 3 and multiply $\alpha + j\,\beta$ by $\frac{1-j}{3}$ in that case where $w_\chi = 1$.

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 $w_\chi = 3$, 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 $q$-integer $y$ of $K$, if $q$ is inert in $K/\mathbb{Q}$;

using $x^\sigma = g(x)$, we test the congruence $g(x) - x^q \pmod q$ to decide if $\sigma = \mathrm{Frob}(q)$ or $\mathrm{Frob}(q)^2$, in which case $\zeta_{2f}^\sigma = \zeta_{2f}^q$ or $\zeta_{2f}^{q^2}$, giving easily the conjugate $\eta^\sigma$.

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

Other indications are given in the text of the program (if necessary, the program can be copy and past at (file "Program.tex"):

https://www.dropbox.com/s/t8f4jj5v9sp629j/Program%20Phi-objects.tex?dl=0 ):

```
\p 50
{p=7; \\ Take any prime p congruent to 1 modulo 3
bf=2;Bf=10^6;hmin=p^2;
\\ Arithmetic of Q(j), j^2+j+1=0:
S=y^2+y+1;kappa=bnfinit(S);Y=idealfactor(kappa,p);
 \\ Decomposition (p)=P1*P2 in Z[j]:
P1=component(Y,1)[1];P2=component(Y,1)[2];
\\ Iteration over the conductors f in [bf,Bf]:
for(f=bf,Bf,vf=valuation(f,3);if(vf!=0 & vf!=2,next);
F=f/3^vf;if(core(F)!=F,next);F=factor(F);Div=component(F,1);
d=matsize(F)[1];for(j=1,d,D=Div[j];if(Mod(D,3)!=1,break));
\\ Computation of solutions a and b such that f=(a^2+27*b^2)/4:
\\ Iteration over b, then over a:
for(b=1,sqrt(4*f/27),if(vf==2 & Mod(b,3)==0,next);A=4*f-27*b^2;
if(issquare(A,&a)==1,
\\ computation of the corresponding defining polynomial P:
if(vf==0,if(Mod(a,3)==1,a=-a);P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);
if(vf==2,if(Mod(a,9)==3,a=-a);P=x^3-f/3*x-f*a/27);
K=bnfinit(P,1); \\ PARI definition of the cubic field K
\\ Test on the p-class number #CKp regarding hmin:
if(Mod(K.no,hmin)==0,print();
G=nfgaloisconj(P); \\ Definition of the Galois group G
\\ Frob = Artin symbol defining the PARI generator sigma=G[2]:
forprime(q=2,10^4,if(Mod(f,q)==0,next);
Pq=factor(P+O(q));if(matsize(Pq)[1]==1,Frob=q;break));X=x^Frob-G[2];
if(valuation(norm(Mod(X,P)),Frob)==0,Frob=lift(Mod(Frob^2,f)));
E=K.fu;Reg=K.reg; \\ Group of units, Regulator
\\ We certify that a suitable PARI unit is a Z[G]-generator of E_K:
E1=lift(E[1]);E2=lift(nfgaloisapply(K,G[2],E[1]));
Root=polroots(P);Rho=real(Root[1]); \\  Selecting a root of P
e1= abs(polcoeff(E1,0)+polcoeff(E1,1)*Rho+polcoeff(E1,2)*Rho^2);
e2= abs(polcoeff(E2,0)+polcoeff(E2,1)*Rho+polcoeff(E2,2)*Rho^2);
l1=log(e1);l2=log(e2);Reg1=l1^2+l1*l2+l2^2;quot=Reg1/Reg;
print(quot); \\ This quotient must be equal to 1
\\ Computation of the cyclotomic units C1,C2=sigma(C1):
z=exp(I*Pi/f);C1=1;C2=1;
\\ Case of a prime conductor f using (Z/fZ)^* cyclic):
if(isprime(f)==1,g=znprimroot(f)^3;
\\ Description of a half-system:
for(k=1,(f-1)/6,gk=lift(g^k);sgk=lift(Mod(gk*Frob,f));
C1=C1*(z^gk-z^-gk);C2=C2*(z^sgk-z^-sgk));
 \\ Logarithms of C1,C2:
L1=3*log(abs(C1))-log(f)/2;L2=3*log(abs(C2))-log(f)/2;
\\ 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 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;
 \\ In the prime case one multiply alpha+j.beta by (1-j)/3:
if(isprime(f)==1,
alpha0=(alpha+beta)/3;
beta0=(-alpha+2*beta)/3;alpha=alpha0;beta=beta0);
\\ Writing of alpha and beta as reals for checking:
print("(alpha,beta)=","(",alpha,", ",beta,")");
\\ Computation of alpha and beta as integers:
alpha=sign(alpha)*floor(abs(alpha)+10^-6);
beta=sign(beta)*floor(abs(beta)+10^-6);
\\ Class group (r = global rank;rp = p-rang;expo = exposant of CKp)
\\ vp = valuations of CKp, ve = valuation of the exponent expo of CKp:
CK=K.clgp;r=matsize(CK[2])[2];CKp=List;EKp=List;rp=0;vp=0;ve=0;
for(i=1,r,ei=CK[2][i];vi=valuation(ei,p);
if(vi>0,rp=rp+1;vp=vp+vi;ve=max(ve,vi));expo=p^ve;
\\ The rp following ideals Ai generate the p-class group CKp:
Ai=idealpow(K,CK[3][i],ei/p^vi);listput(CKp,Ai,i);listput(EKp,p^vi,i));
\\ Matrices h and sh of Ai and sAi on the PARI basis of CK
L0=List;for(i=1,r,listput(L0,0,i));LH=List;LsH=List;
for(i=1,rp,Ai=CKp[i];h=bnfisprincipal(K,Ai)[1];
sAi=nfgaloisapply(K,G[2],Ai);sh=bnfisprincipal(K,sAi)[1];
print("h=",h,", ","sigma(h)=",sh);listput(LH,h,i);listput(LsH,sh,i));
\\ Determination of the Pi-valuations of (alpha+j.beta), i=1,2:
Z=Mod(alpha+y*beta,S);w1=idealval(kappa,Z,P1);w2=idealval(kappa,Z,P2);
print(w1,"  ",w2,"  P1 and P2-valuations for alpha+j*beta");
\\ Galois structure of CKp; computation of the phi-components:
if(rp==1,
u=lift(LsH[1][1]*Mod(LH[1][1],expo)^-1);
YY=Mod(y-u,S);v1=idealval(kappa,YY,P1);v2=idealval(kappa,YY,P2);
v1=min(v1,ve);v2=min(v2,ve);
print(v1,"  ",v2,"  P1 and P2-valuations for H"));
if(rp==2,
\\ Computation of ci(mod expo) such that Pi=(ci+j),i=1,2:
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 LH[1],LsH[1],LH[2],LsH[2], on the PARI basis of CK
H1=LH[1];A1=H1[1];B1=H1[2];sH1=LsH[1];C1=sH1[1];D1=sH1[2];
H2=LH[2];A2=H2[1];B2=H2[2];sH2=LsH[2];C2=sH2[1];D2=sH2[2];
\\ Computation of the determinants of the relations:
Delta1=((C1+c1*A1)*(D2+c1*B2)-(D1+c1*B1)*(C2+c1*A2));
Delta1=lift(Mod(Delta1,expo));
Delta2=((C1+c2*A1)*(D2+c2*B2)-(D1+c2*B1)*(C2+c2*A2));
Delta2=lift(Mod(Delta2,expo));
print(Delta1,"  ",Delta2,"   Determinants: Delta1,Delta2");
\\ Computation of the relations defining the phi-components:
r11x=C1+c1*A1;r11y=C2+c1*A2;r12x=D1+c1*B1;r12y=D2+c1*B2;
r11x=lift(Mod(r11x,expo));r11y=lift(Mod(r11y,expo));
r12x=lift(Mod(r12x,expo));r12y=lift(Mod(r12y,expo));
r21x=C1+c2*A1;r21y=C2+c2*A2;r22x=D1+c2*B1;r22y=D2+c2*B2;
r21x=lift(Mod(r21x,expo));r21y=lift(Mod(r21y,expo));
r22x=lift(Mod(r22x,expo));r22y=lift(Mod(r22y,expo));
print("R11=",r11x,"*X+",r11y,"*Y","  R12=",r12x,"*X+",r12y,"*Y");
print("R21=",r21x,"*X+",r21y,"*Y","  R22=",r22x,"*X+",r22y,"*Y"));
\\ Structure of the torsion group Tp of p-ramification:
n=6; \\ Choose any n, large enough, such that p^(n+1) annihilates Tp:
LTp=List;Kpn=bnrinit(K,p^n);Hpn=Kpn.cyc;
dim=component(matsize(Hpn),2);for(k=2,dim,c=component(Hpn,k);
if(Mod(c,p)==0,listput(LTp,p^valuation(c,p),k)));
print("Structure of the ",p,"-torsion group: ",LTp)))))}
```

9.3. **Numerical examples.** Since the approximations are in general very good (with precision \p 50), we have suppressed useless decimals in the numerical results for integers computed and given as real numbers.

But for some conductors, the precision \p 100 may be necessary, because of a fundamental unit close to 0 (e.g., $f = 21193, 30223$). For $f = 42667$, \p 100 does not compute correctly and \p 150 gives a nice result for $\alpha$ and $\beta$; but we see that, for this example,

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

which explains what happens.

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

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

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

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

In all the sequel, from a factorization $p = (r_1 + j\,r'_1)\cdot(r_2 + j\,r'_2)$ giving the ideal product $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[j]$, we associate, for the exponent $p^e$, the two annihilators $c_i + \sigma$ such that $(c_i + j) = \mathfrak{p}_i^e$ (up to a prime-to-$p$ ideal); this preserves the definition of the $\varphi_1$ and $\varphi_2$-components.

For instance, for $p = 7$, $\mathfrak{p}_1 := (-2 + j)\mathbb{Z}[j]$ and $\mathfrak{p}_2 := (3 + j)\mathbb{Z}[j]$; writing $(\alpha + j\,\beta) =: \mathfrak{p}_1^u \cdot \mathfrak{p}_2^v \cdot \mathfrak{a}$, $\mathfrak{a}$ prime to 7, we get immediately the two $\varphi$-components of $\widetilde{\mathscr{E}}_K = \mathscr{E}_K/\mathscr{F}_K$ (e.g., if $e = 2$, the two annihilators are $19 + j$ and $-18 + j$, respectively; for $p = 13$, we get $23 + j$ and $-22 + j$).

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

We first replace the generators of $\mathbf{H}_K$ by generators Ai of $\mathscr{H}_K$ (where $r_p \le r$ is the $p$-rank). The Galois action on the Ai is computed using the instructions (where G[2] gives the $\sigma$-conjugate, G[1] being the identity):

```
h=bnfisprincipal(K,Ai)[1];sAi=nfgaloisapply(K,G[2],Ai);
sh=bnfisprincipal(K,sAi)[1]};
```

so the Galois structure of $\mathscr{H}_K$ becomes linear algebra from the matrices given by the program, via the relations:

$$h = \textstyle\prod_{i=1}^{r_p} h_i^{a_i} \text{ (in h)} \quad \& \quad h^\sigma = \prod_{i=1}^{r_p} h_i^{b_i} \text{ (in sh)}.$$

(a) **Case of 7-rank** $r_7 = 1$. This case is obvious, writing $h = h_1^a$, $h^\sigma = h_1^b$; we put $P_{\varphi_1} \equiv c_1 + y \pmod{7^e}$ 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 one computes $-a^* b + j$, where $a^*$ is inverse of $a$ modulo $7^e$, and write $(-a^* b + j) = \mathfrak{p}_i^u$ for the suitable $i \in \{1, 2\}$.

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

v 0 P1 and P2 − valuations for alpha + j ∗ beta

v 0 P1 and P2 − valuations for H

give the structures $\mathbb{Z}[j]/\mathfrak{p}_1^v \cdot \mathfrak{p}_2^0$ for "$\mathscr{M} = \widetilde{\mathscr{E}} = \mathscr{E}/\mathscr{F}$ and $\mathscr{H}$", respectively, whence $\mathscr{M}_{\varphi_1} \simeq \mathbb{Z}[j]/\mathfrak{p}_1^v$, $\mathscr{M}_{\varphi_2} = 1$, and so on. First examples:

```
P=x^3+x^2-104*x+371  f=313=Mat([313,1])  (a,b)=(35,1)
Class group=[7]  sigma=4
(alpha,beta)=(-3.000000000,-2.000000000)  Index [E_K:C_K]=7.000000000
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 $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathscr{H}_{\varphi_1} \simeq (\mathbb{Z}[j]/\mathfrak{p}_1) \otimes \mathbb{Z}_7 \simeq \mathbb{Z}/7\mathbb{Z}$ and the conjugation $h^\sigma = h^2$, giving the annihilator $(-2+j) = \mathfrak{p}_1$ as expected; whence the two columns given by the program. We deduce that $\mathscr{T}_K = \mathscr{H}_K \oplus \mathscr{R}_K$.

```
P=x^3+x^2-2450*x-1089  f=7351=Mat([7351,1])  (a,b)=(-1,33)
Class group=[49]  sigma=4
(alpha,beta)=(5.000000000,8.000000000)  Index [E_K:C_K]=49.000000000
h=[1]~,  sigma(h)=[30]~
2  0   P1 and P2-valuations for alpha+j*beta
2  0   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([2401])
```

We have $(\alpha + j\,\beta) = (5 + 8j)$, thus the annihilator $(19 + j) = \mathfrak{p}_1^2$; then $h^\sigma = h^{30}$ gives (modulo $7^2$) the same annihilator. The two $\varphi_2$-components are of course trivial. Since $\mathscr{T}_K \simeq \mathbb{Z}/7^4\mathbb{Z}$, $\mathscr{R}_K = \mathscr{T}_K^{7^2}$ and $\mathscr{H}_K \simeq \mathscr{T}_K/\mathscr{R}_K \simeq \mathbb{Z}/7^2\mathbb{Z}$.

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

```
P=x^3+x^2-77006*x-34225  f=231019=Mat([231019,1])  (a,b)=(-1,185)
Class group=[343]  sigma=4
(alpha,beta)=(19.000000000,18.000000000)  Index [E_K:C_K]=343.000000000
h=[1]~,  sigma(h)=[18]~
0  3   P1 and P2-valuations for alpha+j*beta
0  3   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([343,7])
```

The annihilator of $\mathscr{H}_K$ is $(-18 + j) = \mathfrak{p}_2^3$. The structures are similar with the $\varphi_2$-components since $(19 + 18j) = \mathfrak{p}_2^3$. In that case, $\mathscr{T}_K = \mathscr{H}_K \oplus \mathscr{R}_K$ 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:

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

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

```
P=x^3+x^2-3422*x-1521  f=10267=Mat([10267,1])  (a,b)=(-1,39)
Class group=[7,7]  sigma=2
(alpha,beta)=(-7.000000000,-7.000000000)  Index [E_K:C_K]=49.000000000
h=[1,0]~,  sigma(h)=[0,1]~
h'=[0,1]~, sigma(h')=[6,6]~
1  1   P1 and P2-valuations for alpha+j*beta
R11=3*X+6*Y  R12=1*X+2*Y
R21=5*X+6*Y  R22=1*X+4*Y
Structure of the 7-torsion group: List([49,7])
```

This case means that $\widetilde{\mathscr{E}}_K \simeq \mathbb{Z}[j]/(7)$, giving the two non trivial $\varphi$-components of order 7. The relations, for $\mathscr{H}_K$, reduce to:

$$\mathsf{R11} = 3 * \mathsf{X} + 6 * \mathsf{Y},\ \ \mathsf{R21} = 5 * \mathsf{X} + 6 * \mathsf{Y}.$$

Thus $\mathscr{H}_K = \mathscr{H}_{\varphi_1} \oplus \mathscr{H}_{\varphi_2} \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$, $\mathscr{R}_K = \mathscr{T}_K^7 \simeq \mathbb{Z}/7\mathbb{Z}$.

```
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)=(-32.000000000,-20.000000000) Index [E_K:C_K]=784.000000000
h=[6,0,0,0]~, sigma(h)=[108,1,0,0]~
0  2   P1 and P2-valuations for alpha+j*beta
0  2   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([49])
```

Here $\mathscr{R}_K = 1$ and $\mathscr{T}_K = \mathscr{H}_K \simeq (\mathbb{Z}[j]/\mathfrak{p}_2^2) \otimes \mathbb{Z}_7 \simeq \mathbb{Z}_7/7^2\mathbb{Z}_7$.

```
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)=(42.000000000,28.000000000)  Index [E_K:C_K]=1372.000000000
h=[1,0]~,  sigma(h)=[44,11]~
h'=[0,1]~, sigma(h')=[7,11]~
2  1   P1 and P2-valuations for alpha+j*beta
R11=14*X+7*Y  R12=11*X+30*Y
```

```
R21=26*X+7*Y  R22=11*X+42*Y
Structure of the 7-torsion group: List([49,7,7])
```

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

```
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)=(-112.00000000,-70.00000000)  Index [E_K:C_K]=9604.00000000
h=[2,0]~,  sigma(h)=[36,2]~
h'=[0,2]~, sigma(h')=[0,4]~
1   3   P1 and P2-valuations for alpha+j*beta
R11=74*X+0*Y  R12=2*X+42*Y
R21=0*X+0*Y  R22=2*X+311*Y
Structure of the 7-torsion group: List([343,49])
```

In that case, $\mathscr{T}_K\simeq Z/7^3\mathbb{Z}\oplus\mathbb{Z}/7^2\mathbb{Z}$ and $\mathscr{R}_K\simeq(\mathbb{Z}/7^3\mathbb{Z})^0\oplus(7\,\mathbb{Z}/7^2\mathbb{Z})$ 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 cubic field with 7-rank 3 is the following:

```
P=x^3-4792107*x+4022175142 f=14376321=[3,2;1597369,1] (a,b)=(-7554,128)
Class group=[21,7,7] sigma=5
(alpha,beta)=(-7.000000000,-21.000000000) Index [E_K:C_K]=343.000000000
h =[3,0,0]~, sigma(h) =[15, 4, 0]~
h'=[0,1,0]~, sigma(h')=[3, 1, 0]~
h"=[0,0,1]~, sigma(h")=[6, 5, 2]~
2   1   P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([7,7,7])
```

Using the information on $\alpha$ and $\beta$, we obtain, for $\widetilde{\mathscr{E}}_K=\mathscr{E}_K/\mathscr{F}_K$:

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

where $\mathfrak{p}_1=(-2+j)$ and $\mathfrak{p}_2=(3+j)$. We get the $\varphi$-components $\widetilde{\mathscr{E}}_{\varphi_1}\simeq(\mathbb{Z}[j]/\mathfrak{p}_1^2)\otimes\mathbb{Z}_7\simeq\mathbb{Z}/7^2\mathbb{Z}$ and $\widetilde{\mathscr{E}}_{\varphi_2}\simeq(\mathbb{Z}[j]/\mathfrak{p}_2)\otimes\mathbb{Z}_7\simeq\mathbb{Z}/7\mathbb{Z}$.

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

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

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

$$2x+3y+6z=0\ (H^{-2+\sigma}=1)\quad\&\quad\big[x+y=0\ \ \&\ \ z=0\big]\ (H^{3+\sigma}=1).$$

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

$$\mathscr{H}_{\varphi_1}\simeq\big[(\mathbb{Z}[j]/\mathfrak{p}_1)\otimes\mathbb{Z}_7\big]\oplus\big[(\mathbb{Z}[j]/\mathfrak{p}_1)\otimes\mathbb{Z}_7\big]\quad\&\quad\mathscr{H}_{\varphi_2}\simeq(\mathbb{Z}[j]/\mathfrak{p}_2)\otimes\mathbb{Z}_7.$$

We have indeed equalities for the orders of the $\varphi$-components relative to $\widetilde{\mathscr{E}}_K$ and $\mathscr{H}_K$, respectively, but of course with different structures of $\mathbb{Z}_7[j]$-modules since $\widetilde{\mathscr{E}}_{\varphi_1}\simeq\mathbb{Z}/7^2\mathbb{Z}$ and $\mathscr{H}_{\varphi_1}\simeq\big[\mathbb{Z}/7\mathbb{Z}\big]^2$.

The two other examples are similar:

```
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)=(28.000000000,-7.000000000) Index [E_K:C_K]=1029.000000000
h =[3,0,0]~,  sigma(h) =[3,9,0]~
h'=[0,3,0]~,  sigma(h')=[18,15,0]~
h"=[0,0,1]~,  sigma(h")=[15,6,4]~
```

```
1   2  P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([7,7,7])

P=x^3+x^2-14455754*x-16977480367
f=43367263=[43,1;1008541,1] (a,b)=(-10567,1513)
class group=[273,7,7] sigma=2
(alpha,beta)=(42.000000000,77.000000000) Index [E_K:C_K]=4459.000000000
h =[39,0,0]~,  sigma(h) =[0,5,1]~
h'=[0,1,0]~,   sigma(h')=[156,6,5]~
h"=[0,0,1]~,   sigma(h")=[0,0,2]~
2   1  P1 and P2-valuations for alpha+j*beta
Structure of the 7-torsion group: List([49,7,7])
```

(d) **Larger primes** $p$. Let's give, without comments, some examples:

```
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)=(15.000000000,8.000000000) Index [E_K:C_K]=169.000000000
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=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)=(7.000000000,-8.000000000) Index [E_K:C_K]=169.000000000
h =[1,0]~, sigma(h) =[9,0]~
h'=[0,1]~, sigma(h')=[0,9]~
0  2   P1 and P2-valuations for alpha+j*beta
R11=0*X+0*Y  R12=0*X+0*Y
R21=6*X+0*Y  R22=0*X+6*Y
Structure of the 13-torsion group: List([13,13])

p=19 P=x^3-137271*x+45757 f=411813=[3,2;45757,1] (a,b)=(-3,247)
Class group=[1083] sigma=2
(alpha,beta)=(-21.000000000,-5.000000000) Index [E_K:C_K]=361.000000000
h=[3]~, sigma(h)=[204]~
0  2   P1 and P2-valuations for alpha+j*beta
0  2   P1 and P2-valuations for H
Structure of the 19-torsion group: List([361])

p=19 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)=(19.00000000,4.19514516 E-69) Index [E_K:C_K]=361.00000000
h =[3,0]~,  sigma(h) =[51,16]~
h'=[0,1]~,  sigma(h')=[3,1]~
1  1   P1 and P2-valuations for alpha+j*beta
R11=18*X+3*Y  R12=16*X+9*Y
R21=11*X+3*Y  R22=16*X+13*Y
Structure of the 19-torsion group: List([19,19])

p=31 P=x^3+x^2-63804*x+6181931 f=191413=Mat([191413,1]) (a,b)=(875,1)
class group=[31,31] sigma=4
(alpha,beta)=(31.00000000,-4.10842850 E-69) Index [E_K:C_K]=961.00000000
h=[1,0]~,  sigma(h) =[30,30]~
h'=[0,1]~, sigma(h')=[1,0]~
1  1  P1 and P2-valuations for alpha+j*beta
R11=5*X+1*Y  R12=30*X+6*Y
R21=25*X+1*Y  R22=30*X+26*Y
Structure of the 31-torsion group: List([31,31])

p=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)=(-11.000000000,-35.000000000) Index [E_K:C_K]=961.000000000
h=[1]~, sigma(h)=[439]~
2  0  P1 and P2-valuations for alpha+j*beta
2  0  P1 and P2-valuations for H
Structure of the 31-torsion group: List([961])
```

## 10. Conclusion

Some standard probabilistic approaches, may confirm (or not) the classical Cohen–Lenstra–Malle–Martinet heuristics on $p$-class groups; indeed, heuristics on the $\mathscr{H}_\varphi^{\rm ar}$'s (which yield information on the whole $p$-class group) must be compatible with that obtained with the $\widetilde{\mathscr{E}}_\varphi$'s.

Then, the main problem remains *a proof of the Main Conjecture in the non semi-simple real case* using the statement with Arithmetic $\varphi$-objects, especially a proof that for all abelian real field $K$, with a cyclic maximal $p$-sub-extension, we have, for all $\varphi \in \Phi_K$ (cf. § 8.2.2):

$$\#\mathscr{H}_\varphi^{\rm ar} = w_\varphi \cdot \#(\mathscr{E}_K/\mathscr{E}_K^0 \cdot \mathscr{F}_K)_\varphi, \quad w_\varphi \in \{1, p\}.$$

## References


[Gra1976] G. Gras, Application de la notion de $\varphi$-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 pp. https://doi.org/10.5802/pmb.a-10 2, 4, 22, 23, 24, 27, 28, 32, 33, 34

[Gra1977] G. Gras, Étude d'invariants relatifs aux groupes des classes des corps abéliens, *Journées Arithmétiques de Caen (1976), Astérisque* **41–42** (1977), 19 pp. http://www.numdam.org/item/?id=AST_1977__41-42__35_0 2, 4, 29, 32, 33


## Original references of the 1976's papers


[Coa1977] J. Coates, $p$-adic $L$-functions and Iwasawa's theory, In: *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975).* Academic Press, London 1977, pp. 269–353. https://lib.ugent.be/catalog/rug01:000005363 4, 22, 26

[Gil1975] R. Gillard, Relations de Stickelberger, *Séminaire de théorie des nombres de Grenoble* **4** (1974–1975), Exposé no. 1, 10 pp. http://www.numdam.org/item/?id=STNG_1974-1975__4__A1_0 22

[Has1952] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin (1952). 19, 20, 21, 22, 28

[Iwa1962] K. Iwasawa, A class number formula for cyclotomic fields, *Ann. of Math., Second Series* **76**(1) (1962), 171–179. https://doi.org/10.2307/1970270 22

[Leo1954] H.W. Leopoldt, Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, *Abh. Deutsche Akad. Wiss. Berlin, Math.* **2** (1954), 47 pp. 2, 4, 5, 13, 14, 18, 22, 27, 28

[Leo1962] H.W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, *Jour, für die reine und ang. Math.* **209** (1962), 54–71. 2, 4, 13, 22, 27

[KuLe1964] 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. http://eudml.org/doc/150624 26

[Or1975] B. Oriat, Quelques caractères utiles en arithmétique, *Publications Mathématiques de Besançon* **4** (1975), 27 pp. https://doi.org/10.5802/pmb.a-4 4, 15, 28

[Or1975$^b$] B. Oriat, Sur l'article de Leopoldt "Über Einheintengruppe und Klassenzahl reeller abelscher Zahlkörper", *Publications Mathématiques de Besançon* **5** (1975), 35 pp. https://doi.org/10.5802/pmb.a-5 4, 22, 27

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


## Current References


[AmFr1972] Y. Amice et 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 26

[All2013] T. All, On p-adic annihilators of real ideal classes, *J. Number Theory* **133**(7) (2013), 2324–2338. https://doi.org/10.1016/j.jnt.2012.12.013 3, 22

[All2017] T. All, Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups, *Acta Arithmetica* **178** (2017), 273–299. https://doi.org/10.4064/aa8537-2-2017 3, 22

[BBDS21] D. Bullach, D. Burns, A. Daoud and S. Seo, Dirichlet $L$-series at $s = 0$ and the scarcity of Euler systems (2021). https://arxiv.org/abs/2111.14689 3

[BDSS21] D. Burns, A. Daoud, T. Sano and S. Seo, On Euler systems for the multiplicative group over general number fields; to appear in *Publicacions Matemàtiques*. 3

[BeMa2014] J-R. Belliard and A. Martin, Annihilation of real classes (2014), 10 pp. http://jrbelliard.perso.math.cnrs.fr/BM1.pdf 3

[BeNg2005] J-R. Belliard and T. Nguyen Quang Do, On modified circular units and annihilation of real classes, *Nagoya Math. J.* **177** (2005), 77–115. https://doi.org/10.1017/S0027763000009065 3

[BePa1972] F. Bertrandias et J-J. Payan, $\Gamma$-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 and Y. Li, Non-vanishing theorems for central $L$-values of some elliptic curves with complex multiplication II (2019). https://arxiv.org/pdf/1904.05756 3

[CoLi2020] J. Coates and 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. https://doi.org/10.1112/plms.12379 3

[CoSu2006] J. Coates and R. Sujatha, *Cyclotomic Fields and Zeta Values*, Springer 2006. https://doi.org/10.1007/978-3-540-33069-1_6 3

[DaKa2020] S. Dasgupta and M. Kakde, On the Brumer-Stark Conjecture (2020). https://arxiv.org/abs/2010.00657 3

[Dar1995] H. Darmon, Thaine's method for circular units and a conjecture of Gross, Canad. J. Math. **47**(2) (1995), 302–317. https://doi.org/10.4153/CJM-1995-016-6 3

[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. http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A3_0 4

[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. http://eudml.org/doc/275207 3

[Gra1977$^b$] G. Gras, Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, *Ann. Inst. Fourier* **27**(1) (1977), 1–66. https://doi.org/10.5802/aif.641 2, 3

[Gra1978] G. Gras, Sommes de Gauss sur les corps finis, *Publications Mathématiques de Besançon (Algèbre et théorie des nombres)* **1**(2) (1978), 72 pp. https://doi.org/10.5802/pmb.a-16 22, 25

[Gra1978$^b$] 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. http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A1_0 4, 26, 34

[Gra1979] G. Gras, Annulation du groupe des $\ell$-classes généralisées d'une extension abélienne réelle de degré premier à $\ell$, *Ann. Inst. Fourier* **29**(1) (1979), 15–32. http://www.numdam.org/item?id=AIF_1979__29_1_15_0 3, 26

[Gra1979$^b$] 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. https://mr.math.ca/article/sur-lannulation-en-2/ 25

[Gra1982] G. Gras, Groupe de Galois de la p-extension abélienne $p$-ramifiée maximale d'un corps de nombres, *J. reine angew. Math.* **333** (1982), 86–132. https://eudml.org/doc/152440 https://eudml.org/doc/152547 4

[Gra1998] G. Gras, Théorèmes de réflexion, *J. Théorie Nombres Bordeaux* **10**(2) (1998), 399–499. http://www.numdam.org/item/JTNB_1998__10_2_399_0/ 33

[Gra2005] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). 4, 26, 29, 30, 33

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

[Gra2018] G. Gras, The $p$-adic Kummer–Leopoldt Constant: Normalized $p$-adic Regulator, *Int. J. Number Theory* **14**(2) (2018), 329–337. https://doi.org/10.1142/S1793042118500203 4, 26

[Gra2018$^b$] 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. https://dergipark.org.tr/tr/download/article-file/543993 3, 24, 26, 30

[Gra2019] G. Gras, Heuristics and conjectures in direction of a $p$-adic Brauer–Siegel theorem, *Math. Comp.* **88**(318) (2019), 1929–1965. https://doi.org/10.1090/mcom/3395 4, 26, 34, 35

[Gra2021] G. Gras, Algorithmic complexity of Greenberg's conjecture, *Arch. Math.* **117** (2021), 277–289. https://doi.org/10.1007/s00013-021-01618-9 30

[Gra2021$^b$] G. Gras, On the $\lambda$-stability of $p$-class groups along cyclic $p$-towers of a number field (preprint 2021). https://arxiv.org/abs/2103.01565 10, 34

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

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

[Gree1976] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98**(1) (1976), 263–284. https://doi.org/10.2307/2373625 34

[Grei1992] C. Greither, Class groups of abelian fields, and the main conjecture, *Ann. Inst. Fourier* **42**(3) (1992), 449–499. https://doi.org/10.5802/aif.1299 3, 4, 10, 29, 32, 33

[GrKu2004] C. Greither and R. Kučera, Annihilators for the class group of a cyclic field of prime power degree III, *Publicationes Mathematicae Debrecen* (2015). https://doi.org/10.5486/PMD.2015.7029 3, 30, 33

[GrKu2014] C. Greither and R. Kučera, Eigenspaces of the ideal class group, *Ann. Inst. Fourier* **64**(5) (2014), 2165–2203. https://doi.org/10.5802/aif.2908 3, 30, 33

[GrKu2021] C. Greither and R. Kučera, Washington units, semispecial units, and annihilation of class groups, *Manuscr. Math.* **166**(1–2) (2021), 277–286. https://doi.org/10.1007/s00229-020-01241-y 3, 30

[Iwa1964] K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16**(1) (1964), 42–82. https://doi.org/10.2969/jmsj/01610042 4

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

[Jau1984] J-F. Jaulent, Représentations $\ell$-adiques et invariants cyclotomiques, *Publications Mathématiques de Besançon (Algèbre et théorie des nombres)* **3** (1984), 41 pp. https://doi.org/10.5802/pmb.a-39 3

[Jau1986] J-F. Jaulent, L'arithmétique des $\ell$-extensions (Thèse d'état), *Publications Mathématiques de Besançon* **1**(1) (1986), 1–357. https://doi.org/10.5802/pmb.a-42 3, 4

[Jau1990] J-F. Jaulent, La théorie de Kummer et le $\mathrm{K}_2$ 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 25

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

[Jau2021] J-F. Jaulent, Annulateurs de Stickelberger des groupes de classes logarithmiques, *Acta Arithmetica* **201** (2021), 241–253. https://doi.org/10.4064/aa201127-22-6 27

[Jau2022] J-F. Jaulent, Annulateurs circulaires des groupes de classes logarithmiques (preprint 2022) https://arxiv.org/pdf/2003.05768.pdf 27

[Jau2022$^b$] J-F. Jaulent, Annulateurs circulaires et conjecture de Greenberg https://hal.archives-ouvertes.fr/hal-02519397 27

[Kol2007] V.A. Kolyvagin, *Euler Systems*. In: Cartier P., Katz N.M., Manin Y.I., Illusie L., Laumon G., Ribet K.A. (eds), The Grothendieck Festschrift (2007). Modern Birkhäuser Classics. Birkhäuser, Boston, MA. https://doi.org/10.1007/978-0-8176-4575-5_11 3

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

[Lang1990] S. Lang, *Cyclotomic fields I and II*, Graduate Texts in Mathematics **121**, With an appendix by Karl Rubin (Combined 2nd ed.), Berlin, New York, Springer–Verlag 1990. https://link.springer.com/content/pdf/bbm%3A978-1-4612-0987-4%2F1 3

[MaRu2011] B. Mazur and 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. https://doi.org/10.5802/aif.1045 4, 25

[NgLeB06] T. Nguyen Quang Do and M. Lescop (with an appendix by J.-R. Belliard), Iwasawa Descent and Co-descent for Units modulo Circular Units (Special Issue: In honor of John H. Coates), *Pure and Applied Mathematics Quarterly* **2**(2) (2006), 465–496. https://doi.org/10.4310/PAMQ.2006.V2.N2.A4

[Or1981] B. Oriat, Annulation de groupes de classes réelles, *Nagoya Math. J.* **81** (1981), 45–56. https://projecteuclid.org/download/pdf_1/euclid.nmj/1118786304 3, 26, 33

[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. https://doi.org/10.4064/aa-46-4-331-354 3, 33

[Pari2016] The PARI Group, *PARI/GP, version 2.9.0*, Université de Bordeaux (2016). 2

[PeRi1990] B. Perrin-Riou, Travaux de Kolyvagin et Rubin, *Séminaire Bourbaki : volume 1989/90, exposés 715–729, Astérisque* **189–190** (1990), Exposé no. 717, 38 pp. http://www.numdam.org/item/SB_1989-1990__32__69_0/ 3, 10

[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. https://www.imo.universite-paris-saclay.fr/~biblio/cours-m2/Fonctions_L_p-adiques_et_theorie_Iwasawa.pdf 4

[Rib2008] K.A. Ribet, Bernoulli numbers and ideal classes, *SMF, Gazette* **118** (2008). https://www.dropbox.com/s/1uir9crhidorejy/smf.Ribet.pdf?dl=0 3

[Rib2008$^b$] 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. https://math.berkeley.edu/~ribet/herbrand.pdf 3

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

[SchS2019] K. Schaefer and 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, Série I* **287** (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. https://doi.org/10.1007/BF01389158 22

[Sol1990] D. Solomon, On the class groups of imaginary abelian fields, *Ann. Inst. Fourier* **40**(3) (1990), 467–492. https://doi.org/10.5802/aif.1221 3, 10, 32

[Sol1992] D. Solomon, On a construction of $p$-units in abelian fields, *Invent. Math.* **109**(2) (1992), 329–350. http://eudml.org/doc/144024 30

[Thai1988] F. Thaine, On the ideal class groups of real abelian number fields, *Ann. of Math. second series* **128**(1) (1988), 1–18. http://www.jstor.org/stable/1971460 30

[Was1997] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997. 3, 21, 22, 26, 30

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