North-Western European Journal of Mathematics

Notion of abelian arithmetic φ-objects for the study of p-class groups and p-ramified torsion groups

Georges Gras[1]

Received: February 8, 2022/Accepted: October 27, 2023/Online: December 15, 2023

Abstract

We revisit, in an elementary way, the *classical statement* of various "Main Conjectures" for p-class groups $\mathscr{H}_K$ and p-ramified torsion groups $\mathscr{T}_K$ of abelian fields K, in the non semi-simple case $p \mid [K:\mathbb{Q}]$. The classical "algebraic" definition of the p-adic isotypic components, $\mathscr{H}_{K,\varphi}^{\rm alg}$, used in the literature, is inappropriate with respect to analytical formulas. For that reason we have introduced, in the 1970's, an "arithmetic" definition, $\mathscr{H}_{K,\varphi}^{\rm ar}$, in perfect correspondence with all analytical formulas and giving a natural "Main Conjecture", still unproved for real fields in the non semi-simple case. The two notions coincide for relative class groups $\mathscr{H}_K^-$ and groups $\mathscr{T}_K$ since transfer maps are injective, in p-extensions for these groups, but not necessarily for real class groups. Numerical evidence of the gap between the two notions is given (Examples Appendix A.2 on p. 175, Appendix A.2 on p. 178) and PARI calculations corroborate that the true Real Abelian Main Conjecture writes $\#\mathscr{H}_{K,\varphi}^{\rm ar} = \#(\mathscr{E}_K/\widehat{\mathscr{E}}_K\,\mathscr{F}_K)^{e_{\varphi_0}}$ ($\varphi = \varphi_0\varphi_p$, φ_0 of prime-to-p order, φ_p of p-power order, e_{φ_0} being the corresponding idempotent), in terms of units $\mathscr{E}_K$, $\widehat{\mathscr{E}}_K$ (units of the strict subfields) and $\mathscr{F}_K$ (Leopoldt's cyclotomic units). A recent approach, conjecturing the capitulation of $\mathscr{H}_K$ in some auxiliary cyclotomic extensions $K(\mu_\ell)$, $\ell \equiv 1 \pmod{2p^N}$ prime, proves the difficult non semi-simple real case.

Keywords: abelian fields, p-adic characters, class groups and units, p-adic L-functions, cyclotomic polynomials, class field theory.

MSC: Primary 11R18, 11R29, 11R27 ; Secondary 11R37, 12Y05, 08-04.

[1] In retirement from Besançon University,
Villa la Gardette, 4, chemin Château Gagnière, 38520, Le Bourg d'Oisans (France),
e-mail: g.mn.gras@wanadoo.fr

Foreword and preliminary remarks

This survey provides improvements, new results, numerical illustrations (with programs using PARI[2]) and some history, regarding our original articles[3]. These two papers were written, in French, with illegible fonts due to the use of "typits" on typewriters and hand written characters, for mathematical symbols ! So they were hardly accessible and only Gras (1977a) is cited in replacement of them. This survey also mentions, in Subsection 1.1, pioneering references, as well as some significant Leopoldt's papers on cyclotomy[4], written in german in the 1950/1960's.

In this presentation, the definitions of various p-adic isotypic components deal with irreducible p-adic characters $\varphi = \varphi_0\varphi_p$ (φ_0 of prime-to-p order, φ_p of p-power order and e_{φ_0} being the semi-simple idempotent associated to φ_0).

As the Referee pointed out, one must avoid any confusion with the *Iwasawa Main Conjecture*, dealing for instance with cyclotomic $\mathbb{Z}_p$-extensions of abelian fields.

So, the conjectures for the case of finite abelian extensions are supposed to give, in the real case, the most precise analytic information $\#\mathcal{H}_{K,\varphi}^{\rm ar} = \#(\mathscr{E}_K/\widehat{\mathscr{E}_K}\,\mathscr{F}_K)_{\varphi_0}$, in terms of units $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$, $\widehat{\mathscr{E}_K} := \widehat{\mathbf{E}}_K \otimes \mathbb{Z}_p$ (units of the strict subfields) and $\mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p$ (cyclotomic units), which will be specified later; this conjecture will be called "Finite Abelian Main Conjectures" in this paper (FAMC for short). This may be legitimate since beyond the Iwasawa Main Conjecture, after the Mazur–Wiles Main Theorem and generalizations, our purposes and conjectures deal always with **finite abelian extensions $K/\mathbb{Q}$, without any hypothesis on the degree**, a context which, of course, must apply to the finite layers of the cyclotomic $\mathbb{Z}_p$-extension.

Moreover, Thaine's technique and our new philosophy, using capitulation of classes in auxiliary cyclotomic extensions $K(\mu_\ell)$, strengthen the interest of the finite cases.

The FAMC, giving analytic expressions of annihilators and orders of p-adic isotypic components of class groups, that we revisit here, were first stated (*especially in the non semi-simple case*) in our papers mentioned above (but not in Gras (1977a), as erroneously stated by some authors), and that we have given at the meeting "Journées arithmétiques de Caen" Gras (1977b) as it is correctly recalled for instance in Solomon[5] and Ribet[6].

This gives the occasion to mention that Gras (1977a), only recalling the statements of the conjectues in the semi-simple case, is especially devoted to a method

[2] Group, 2016, *PARI/GP, version 2.9.0*.

[3] Gras, 1976, "Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes";
Gras, 1977b, "Étude d'invariants relatifs aux groupes des classes des corps abéliens".

[4] Leopoldt, 1954, "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper";
Leopoldt, 1962, "Zur Arithmetik in abelschen Zahlkörpern".

[5] Solomon, 1990, "On the class groups of imaginary abelian fields".

[6] Ribet, 2008a, "Bernoulli numbers and ideal classes".

using formal series, giving non-trivial congruences when p-adic $\mathbf{L}$-functions have a trivial zero; for instance we proved the following complement of Ankeny–Artin–Chowla–Kudo congruences[7] or Washington (1997, Theorem 5.37)):

Proposition 1 – *Let $f \equiv 0 \pmod 3$ be the conductor of a real quadratic field K; we consider the case $f/3 \equiv -1 \pmod 3$ ("special case" when 3 splits in the mirror field $K' := \mathbb{Q}(\sqrt{-f/3})$). Let $\varepsilon = t + u\sqrt{f}$, $t, u > 0$, be the fundamental unit of K and let h and h' be the class numbers of K and K', respectively. Then $h \cdot t \cdot u + h' \equiv 0 \pmod 3$.*

A program, in Appendix A.1, only checks this congruence. But this analytic result, which seems unknown, is perhaps off topic for our purpose, even if the tricky case, given by the mirror character ψ^* of $\psi = \psi_0\psi_p$, always intervenes in such context (see, e.g., Gras (1987, Théorème (0.2) (iii)), after the general case[8], then Theorems 8, 9 when $\psi_0 = \omega$ yielding $\psi^* = \omega\psi^{-1} = \psi_p^{-1}$).

The conjecture has been proven in the semi-simple case, then in the non semi-simple one for *imaginary relative class groups* and mainly in the framework of Iwasawa's theory (a large overview on the precise proofs and classical references are given in Washington (1997, Chapters 6, 8, 13, 15)).

The *non semi-simple real case* was less understood because of a problematic definition of p-adic isotypic components for p-adic characters φ and of cyclotomic units; but at the time, we proposed another more natural conjectural context, still unproved, for which the definition of "Arithmetic φ-objects" has become essential since the distinction between "Algebraic" definitions (classical framework) and "Arithmetic" definitions is crucial regarding analytic formulas (we shall give more comments in Remarks 3).

Let $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be the Galois group of the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ and denote by K a subfield of finite degree of $\mathbb{Q}^{\mathrm{ab}}$. In fact, since abelian arithmetic deals with invariants defined in cyclic fields "$K = K_\chi$", indexed by rational characters χ, for which K_χ is the subfield of $\mathbb{Q}^{\mathrm{ab}}$ fixed by χ, there is no restriction to take cyclic K's in any result or comment; conversely, K define an unique rational character χ.

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 approaches giving, under some assumptions, proofs of a "Main Theorem":

(i) An algebraic part giving a systematic study of families $(\mathbf{M}_K)_K$ of $\mathbb{Z}[\mathcal{G}]$-modules and of the $\mathbb{Z}_p[\mathcal{G}]$-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 $\mathscr{M}_\varphi^{\mathrm{alg}}$ (algebraic) and $\mathscr{M}_\varphi^{\mathrm{ar}}$ (arithmetic), indexed by the set of irreducible p-adic characters φ of $\mathcal{G}$.

[7] Ankeny, Artin, and Chowla, 1952, "The class number of real quadratic fields"; Kudo, 1975, "On a class number relation of imaginary abelian fields".

[8] Gras, 1986, "Théorie des genres analytique des fonctions L p-adiques des corps totalement réels".

The difference between $\mathscr{M}_\varphi^{\rm alg}$ (used in all the literature) and $\mathscr{M}_\varphi^{\rm ar}$ is that the first one relates to algebraic norms $\mathcal{V}_{k/k'} := \sum_{\sigma\in{\rm Gal}(k/k')}\sigma \in \mathbb{Z}[{\rm Gal}(k/k')]$ 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:

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

where the transfer maps $\mathbf{J}_{k/k'}$ are often non injective in p-extensions (see § 3.3 for examples justifying Definition 2 for the statement of the FAMC and § 4.3 for the main properties). Moreover, the "arithmetic" point of view is naturally related to the formula:

$$\#\mathscr{M}_K = \prod_{\varphi\in\Phi_K} \#\mathscr{M}_\varphi^{\rm ar} \text{ (Theorems 3 and 5)},$$

where the $\#\mathscr{M}_\varphi^{\rm ar}$'s have (conjecturally) analytic expressions, contrary to the $\#\mathscr{M}_\varphi^{\rm alg}$'s which do not always fulfill this formula.

(ii) An arithmetic part where we apply the above results 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 (i.e., unramified outside p and non-complexified) abelian pro-p-extension of K real. For a survey about abelian p-ramification, see Gras (2019c, Appendix).

For rational characters χ and p-adic characters $\varphi \mid \chi$, we define the "Class Invariants" $m_\varphi^{\rm alg}(\mathscr{H})$ (algebraic), $m_\varphi^{\rm ar}(\mathscr{H})$, $m_\varphi^{\rm ar}(\mathscr{T})$ (arithmetic) then, in § 8.2, the corresponding "Analytic Invariants" $m_\varphi^{\rm an}(\mathscr{H})$, $m_\varphi^{\rm an}(\mathscr{T})$ suggested by the analytic formulas of the arithmetic χ-components deduced from Leopoldt's Theorem 1 (cf. Theorems 7, 12, 14) and we develop the problem of their comparison. We conjecture a new annihilation theorem for $\mathscr{H}_\varphi^{\rm ar}$ in the real non semi-simple case (Conjecture 1).

In § 7.6, we shed new light on the proof of the FAMC in the real semi-simple case for K, in the spirit of Thaine's theorem described in Washington's book, and we give numerical illustrations. It becomes clear that *the knowledge of the sole cyclotomic unit η_K of K* contains, by means of very elementary arithmetic, all the information on annihilation and orders of the φ-components of its p-class group. A new observation is that Thaine's method[9] uses auxiliary cyclotomic extensions $K(\mu_\ell)$ with *ℓ prime totally split in K*, while our approach[10]

[9] Thaine, 1988, "On the ideal class groups of real abelian number fields".

[10] Gras, 2023a, "Algebraic norm and capitulation of p-class groups in ramified cyclic p-extensions";
Gras, 2023b, "The Chevalley–Herbrand formula and the real abelian Main Conjecture (New criterion using capitulation of the class group)";
Gras, 2024b, "The real abelian main conjecture in the non semi-simple case".

uses same auxiliary extensions, but with ℓ *totally inert in* K, *which assumes* $K \cap \mathbb{Q}(\mu_{p^\infty}) = \mathbb{Q}$, the case $K \cap \mathbb{Q}(\mu_{p^\infty}) \neq \mathbb{Q}$ being considered separately.

(iii) An illustration, of 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. After a first writing of this paper, more computations have been done and confirm the theoretical claims.

Since numerical experiments have some importance and take much place, we report in the Appendix, PARI programs, tables and explanations for their use; the programs may be copied and pasted from any pdf-file.

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, among others, on cyclotomy and p-adic $\mathbf{L}$-functions. Several papers also give the Iwasawa formulation of the Main Theorem (see, e.g., Greenberg[11]), in terms of p-adic $\mathbf{L}$-functions, a generalizable feature to many fields. The fundamental difference, regarding finite p-extensions, is that, in Iwasawa's theory, capitulation kernels are hidden in statements using pseudo-isomorphisms, whence only giving results for the projective limit of the p-class groups in the $\mathbb{Z}_p$-extensions and, in general, no precise information is available in the finite layers. It's quite clear in a numerical setting that any possible structure occurs in the first layers, up to the algebraic regularity predicted by Iwasawa's theory; see for instance the numerical computations given in Kraft–Schoof–Pagani[12]. An enlightening result about capitulation kernels is given in Grandet–Jaulent[13].

Let's give less known contributions of the beginnings:

We refer, for a very nice story of pioneering works, to Ribet[14], for detailed proofs of Iwasawa Main Conjecture to Washington[15] following techniques initiated by

[11] Greenberg, 1975, "On p-adic L-functions and cyclotomic fields";
Greenberg, 1977, "On p-adic L-functions and cyclotomic fields. II".

[12] Kraft and Schoof, 1995, "Computing Iwasawa modules of real quadratic number fields";
Pagani, 2022, "Greenberg's conjecture for real quadratic fields and the cyclotomic $\mathbb{Z}_2$-extension".

[13] Grandet and Jaulent, 1985, "Sur la capitulation dans une $\mathbb{Z}_\ell$-extension", Théorème, p. 214.

[14] Ribet, 2008a, "Bernoulli numbers and ideal classes";
Ribet, 2008b, *Modular constructions of unramified extensions and their relation with a theorem of Herbrand (Class groups and Galois representations)*.

[15] Washington, 1997, *Introduction to Cyclotomic Fields*, Chap. 15.

Thaine then Kolyvagin, Ribet (exposed by Lang[16]). A Bourbaki Seminar, by Perrin-Riou[17], gives a significant lecture, with an impressive bibliography, on the works of Kolyvagin, also Perrin-Riou[18], the survey of Rubin[19], and others about the Main Conjectures for number fields and elliptic curves.

The story is also given in the famous Mazur–Wiles paper[20], where the attribution of the various statements of the conjecture, in the semi-simple case, is accurately discussed (see Mazur and Wiles (1984, § 1 and § 10 (i, ii)) for more comments on the works of Iwasawa, Leopoldt, Greenberg and us), even if some references are missing.

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 in Solomon (1990, Theorem II.1) for $\mathscr{H}^-$ and $p \neq 2$, then in Greither (1992, Theorems A, B, C, 4.14, Corollary 4.15) for $\mathscr{H}^-$, $\mathscr{T}$ with $p \geq 2$ and $\mathscr{H}^+$, but in a semi-simple context.

Let's mention the proof by Rubin[21], from the Kolyvagin Euler systems[22] used in above proofs.

Many complementary works about the order or the annihilation of the $\mathscr{H}_\varphi$'s, for irreducible p-adic characters φ, were published before or after the decisive proofs[23]. Mention a result of Oriat using reflection theorem[24].

---

[16] Lang, 1990, *Cyclotomic fields. I and II. With an appendix by Karl Rubin: The main conjecture*.

[17] Perrin-Riou, 1990, *Travaux de Kolyvagin et Rubin*.

[18] Perrin-Riou, 1998, "Systèmes d'Euler p-adiques et théorie d'Iwasawa".

[19] Rubin, 2000, *Euler Systems (Hermann–Weyl lectures)*.

[20] Mazur and Wiles, 1984, "Class fields of abelian extensions of $\mathbb{Q}$".

[21] Rubin, 1990, *The main conjecture, Appendix to Cyclotomic fields I, II, by Lang, S.*.

[22] Kolyvagin, 2007, *Euler Systems*.

[23] All, 2013, "On p-adic annihilators of real ideal classes";
All, 2017, "Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups";
Belliard and Martin, 2014, "Annihilation of real classes";
Belliard and Nguyen Quang Do, 2005, "On modified circular units and annihilation of real classes";
Gillard, 1976, *Sur le groupe des classes des extensions abéliennes réelles*;
Gras, 1977a, "Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés";
Gras, 1979a, "Annulation du groupe des ℓ-classes généralisées d'une extension abélienne réelle de degré premier à ℓ";
Gras, 2018a, "Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{C}\ell^{\mathrm{ab}}_{K,S})$ for real abelian extensions $K/\mathbb{Q}$";
Greither and Kučera, 2014, "Eigenspaces of the ideal class group";
Greither and Kučera, 2015, "Annihilators for the class group of a cyclic field of prime power degree III";
Greither and Kučera, 2021, "Washington units, semispecial units, and annihilation of class groups";
Jaulent, 2021, "Annulateurs de Stickelberger des groupes de classes logarithmiques";
Jaulent, 2023, "Annulateurs circulaires des groupes de classes logarithmiques";
Oriat, 1981, "Annulation de groupes de classes réelles";
Oriat, 1986, "Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens".

[24] Oriat, 1986, "Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens", Théorème, p. 333.

In the same way, it is hopeless to outline all generalizations giving "Main Conjectures" in other contexts than the absolute abelian case[25], using essentially the technique of Kolyvagin's Euler systems, if any; an expository book may be Coates and Sujatha (2006) for recent works, but excluding the story of the origins of the Main Conjecture as explained in Solomon–Greither papers, Washington's book and Ribet's Lectures.

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 Jaulent (1981, Théorème 1 and consequences), Jaulent (1984, 1986) in a class field theory context, then Lecouturier (2018) and Schaefer and E. Stubley (2019) 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. We hope that the following new presentation of the "elementary" abelian case, with a properly stated FAMC, will serve as a model for generalizations.

1.2 Introduction of Arithmetic φ-objects

Nevertheless, all these works deal with an *algebraic definition of the isotypic components* $\widehat{\mathscr{H}_\varphi^{\rm alg}}$ (for irreducible p-adic characters φ) or $\widehat{\mathscr{H}_\chi^{\rm alg}}$ (for rational characters χ); that is to say, when $G_K := {\rm Gal}(K/\mathbb{Q}) =: \langle \sigma_\chi \rangle$ is cyclic, of order g_χ (i.e., $K = K_\chi$ is the fixed field by the kernel of a rational character χ):

$$\begin{cases} \widehat{\mathscr{H}_\chi^{\rm alg}} := \mathscr{H}_K / \mathscr{H}_K^{P_\chi(\sigma_\chi)}, \\ \widehat{\mathscr{H}_\varphi^{\rm alg}} := \mathscr{H}_K \otimes_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[\mu_{g_\chi}] \simeq \mathscr{H}_K / \mathscr{H}_K^{P_\varphi(\sigma_\chi)}, \text{ for all } \varphi \mid \chi, \end{cases}$$

with the $\mathbb{Z}_p[G_K]$-action $\sigma \in G_K \mapsto \psi(\sigma)$ ($\psi \mid \varphi$ of order g_χ), where P_φ is the corresponding local cyclotomic polynomial dividing the global cyclotomic polynomial P_χ of g_χ-th roots of unity. We shall use instead similar definitions giving modules of same order:

$$\mathscr{H}_\chi^{\rm alg} := {\rm Ker}(P_\chi(\sigma_\chi)) \ \ \& \ \ \mathscr{H}_\varphi^{\rm alg} := {\rm Ker}(P_\varphi(\sigma_\chi)).$$

[25] Bullach et al., 2021, "Dirichlet L-series at $s = 0$ and the scarcity of Euler systems";
Burns et al., 2023, "On Euler systems for the multiplicative group over general number fields";
Coates and Li, 2020, "Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication";
Darmon, 1995, "Thaine's method for circular units and a conjecture of Gross";
Dasgupta and Kakde, 2023, "On the Brumer-Stark Conjecture";
Dasgupta, Kakde, et al., 2023, "The residually indistinguishable case of Ribet's method for GL_2";
Kezuka and Li, 2023, "Non-vanishing of central L-values of the Gross family of elliptic curves";
Mazur and Rubin, 2011, "Refined class number formulas and Kolyvagin systems";
Viguié, 2011, "Contribution à l'étude de la conjecture de Gras et de la conjecture principale d'Iwasawa, par les systèmes d'Euler (Thèse: Université de Franche–Comté)".

The corresponding norm characterization of $\mathscr{H}_\chi^{\rm alg}$ being (Theorem 2):

$$\mathscr{H}_\chi^{\rm alg} := \{x \in \mathscr{H}_K,\ \mathcal{V}_{K/k}(x) = 1,\ \forall\, k \subsetneq K\},$$

where $\mathcal{V}_{K/k} = \mathbf{J}_{K/k} \circ \mathbf{N}_{K/k}$ is the algebraic norm with the disadvantage of possible non injective maps $\mathbf{J}_{K/k}$ when $p \mid [K : k]$.

Put $K = K'K_0$, where $g_0 := [K_0 : \mathbb{Q}]$ is prime to p and $[K' : \mathbb{Q}] = p^n$, $n \geq 0$. We prove (Theorem 4 (ii)) that from the above expression one gets:

$$\mathscr{H}_\varphi^{\rm alg} = \left(\mathscr{H}_\chi^{\rm alg}\right)_{\varphi_0} = (\{x \in \mathscr{H}_K,\ \mathcal{V}_{K/k}(x) = 1, \forall\, k \subsetneq K\})_{\varphi_0},$$

(where φ_0 is above the prime-to-p part ψ_0 of $\psi =: \psi_0\psi_p$, where ψ_p is of order p^n, and where $(\ )_{\varphi_0}$ denotes a φ_0-component obtained with the corresponding semi-simple idempotent e_{φ_0} of $G_0 := {\rm Gal}(K_0/\mathbb{Q})$), contrary to our definitions that will be the crucial ones in the sequel:

$$\begin{cases} \mathscr{H}_\chi^{\rm ar} := \{x \in \mathscr{H}_K,\ \mathbf{N}_{K/k}(x) = 1, \forall\, k \subsetneq K\}, \\ \mathscr{H}_\varphi^{\rm ar} := \left(\mathscr{H}_\chi^{\rm ar}\right)_{\varphi_0} = (\{x \in \mathscr{H}_K,\ \mathbf{N}_{K/k}(x) = 1, \forall\, k \subsetneq K\})_{\varphi_0}. \end{cases}$$

where $\mathbf{N}_{K/k}$ is the arithmetic norm. See § 2.2 about this characterizations of $\mathscr{H}_\varphi^{\rm alg}$ and $\mathscr{H}_\varphi^{\rm ar}$ using local cyclotomic polynomials P_φ, whence giving structures of modules over cyclotomic rings, then for a summary of the main properties and results of the paper.

In the non semi-simple case $p \mid [K : \mathbb{Q}]$, the distinction between algebraic and arithmetic φ-components is not done in the literature. This does not matter for relative p-class groups $\mathscr{H}_K^-$ and torsion p-groups $\mathscr{T}_K$ of abelian p-ramification since we will prove that the two notions coincide (Theorems 6, 11); so the case of these invariants is definitely solved, contrary to that of φ-components of p-class groups of real fields K in the non semi-simple case deduced from the "χ-formulas" given in Theorem 14 and the important relation that we talked about:

$$\#\mathscr{H}_K = \prod_{\varphi \in \Phi_K} \#\mathscr{H}_\varphi^{\rm ar} \text{ (Theorems 3, 5).}$$

We compare the two definitions $\mathscr{H}^{\rm alg}$, $\mathscr{H}^{\rm ar}$ in § 3.3 and Appendix A.2, with numerical illustrations showing the gap between them and involving capitulation phenomenon of p-classes in p-extensions (the detailed examples Appendix A.2 on p. 175, Appendix A.2 on p. 178 may be read right now).

1.3 Relation between the modules $\mathscr{H}_K$ and $\mathscr{T}_K$

If one considers, in the abelian real case, the $\mathbb{Z}_p[\mathcal{G}]$-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, for $K_0 \subseteq k' \subseteq k \subseteq K$, the norm maps $\mathbf{N}_{k/k'}$ are surjective and the transfer maps $\mathbf{J}_{k/k'}$ are injective under Leopoldt's conjecture[26][27][28] (collected in Gras (2005, Theorem IV.2.1)); so this family behaves as that of relative class groups, which allows an obvious statement of the FAMC and then its proof with similar techniques, as done for instance in Greither (1992).

The order of the p-group $\mathscr{T}_K$ is closely related to Coates's approach[29] of the p-adic $\mathbf{L}$-functions "at $s = 1$" and a particularity of $\mathscr{T}_K$ is its interpretation by means of the three $\mathbb{Z}_p[\mathcal{G}]$-modules $\mathscr{H}_K^{\mathrm{cyc}}$, $\mathcal{R}_K$ and $\mathcal{W}_K$; see Gras (2005, Lemma III.4.2.4) leading to the exact sequence (17) and the formula $\#\mathscr{T}_K = \#\mathscr{H}_K^{\mathrm{cyc}} \times \#\mathcal{R}_K \times \#\mathcal{W}_K$, where $\mathcal{W}_K$ is an easy canonical invariant depending on local p-roots of unity, $\mathcal{R}_K$ is the normalized p-adic regulator[30] and $\mathscr{H}_K^{\mathrm{cyc}}$ 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, which simply depends on ramification of p in K.

The order of the group $\mathcal{R}_K$ 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 and Fresnel[31], then Coates, Ribet and many other; see a survey in Gras[32] and a lecture in Ribet[33] where is used the beginnings of the concept of p-adic pseudo-measures of Mazur, developed by Serre[34] and that we have used for a genus theory[35]). See in Gras (2016, 2019a) 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 (1975, 1977) after Iwasawa[36].

1.4 Unsolved non semi-simple abelian conjecture

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

[26] Gras, 1982, "Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres", Théorème I.1.

[27] Gras, 1983, "Logarithme p-adique et groupes de Galois".

[28] Jaulent, 1986, "L'arithmétique des ℓ-extensions (Thèse d'état)";
Jaulent, 1998, "Théorie ℓ-adique globale du corps de classes";
Nguyen Quang Do, 1986, "Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens".

[29] Coates, 1977, *p-adic L-functions and Iwasawa's theory*.

[30] Gras, 2018b, "The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator", Lemma 3.1.

[31] Fresnel, 1967, *Nombres de Bernoulli et fonctions L p-adiques*.

[32] Gras, 1980, *Sur la construction des fonctions L p-adiques abéliennes*.

[33] Ribet, 1979, "Fonctions L p-adiques et théorie d'Iwasawa (par P. Satgé, d'après un cours de K. Ribet 1977/78)".

[34] Serre, 1978, "Sur le résidu de la fonction zêta p-adique d'un corps de nombres".

[35] Gras, 1986, "Théorie des genres analytique des fonctions L p-adiques des corps totalement réels";
Gras, 1987, "Pseudo-mesures associées aux fonctions L de $\mathbb{Q}$".

[36] Iwasawa, 1964, "On some modules in the theory of cyclotomic fields".

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 $\widehat{\mathscr{E}}_K$ be the subgroup of $\mathscr{E}_K$ generated by the $\mathscr{E}_k$'s for all $k \subsetneq K$.

It would remain to prove our conjecture Gras (1977b, § III) for the p-adic characters $\varphi \mid \chi$ of $K =: K_\chi$ saying that (see Remarks 3, 8):

$$\#\mathscr{H}_\varphi^{\rm ar} = w_\varphi \cdot \#(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}, \quad w_\varphi \in \{1, p\},$$

where:

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

and:

$$(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0} = (\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)^{e_{\varphi_0}} := \left\{\widetilde{\varepsilon} \in \mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K, \ \widetilde{\varepsilon}^{P_\varphi(\sigma_\chi)} = 1\right\},$$

where P_φ is the local cyclotomic polynomial attached to φ and σ_χ a generator of $\mathrm{Gal}(K/\mathbb{Q})$ ($\varphi = \varphi_0\varphi_p$, φ_0 of prime-to-p order, φ_p of p-power order, from Remark 1). The module $\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K$ is called an algebraic χ-object since it is annihilated by all the relative algebraic norms $\mathcal{V}_{K/k}$, which explains that its φ-component is given by its φ_0-component; indeed, one proves, Theorem 4 (ii), that $(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_\varphi = (\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$. Thus, the φ-components $(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$ are *algebraic* φ-objects, but the φ-class groups $\mathscr{H}_\varphi^{\rm ar}$ must be defined in the *arithmetic* sense, which should be subject to a philosophical interpretation that we ignore since transfer maps of the form $\mathscr{E}_k/\widehat{\mathscr{E}}_k\mathscr{F}_k \to \mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K$ are trivial.

2 Abelian extensions

The idea of definition of the φ-objects owes a lot to the work of Leopoldt[37] and their writing, in french, by Oriat[38]. Some outdated notations in these papers and ours are modified, after changing ℓ into p (e.g., $\Omega_p \mapsto \overline{\mathbb{Q}}_p$, $\widehat{\Omega}_p \mapsto \mathbb{C}_p$, $\Gamma \mapsto \mathbb{Z}_p$).

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 $\mathscr{G} := \mathrm{Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$):

[37] Leopoldt, 1954, "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper"; Leopoldt, 1962, "Zur Arithmetik in abelschen Zahlkörpern".

[38] Oriat, 1975a, "Quelques caractères utiles en arithmétique"; Oriat, 1975b, "Sur l'article de Leopoldt "Über Einheintengruppe und Klassenzahl reeller abelscher Zahlkörper"".

Notations 1 – Let Ψ be the set of irreducible characters of $\mathcal{G}$, of degree 1 and finite order, with values in $\overline{\mathbb{Q}}_p$. We define the sets of irreducible p-adic characters Φ, for a prime $p \geq 2$, the set $\mathcal{X}$ of irreducible rational characters and the sets of irreducible characters Ψ_K, Φ_K, $\mathcal{X}_K$, of $K \subset \mathbb{Q}^{\rm ab}$.

The notation $\psi \mid \varphi \mid \chi$, for $\psi \in \Psi$, $\varphi \in \Phi$, $\chi \in \mathcal{X}$, means that φ is a term of χ and ψ a term of φ.

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

Let $\chi \in \mathcal{X}$; we denote by g_χ, K_χ, $G_\chi =: \langle \sigma_\chi \rangle$, f_χ, $\mathbb{Q}(\mu_{g_\chi})$, the order of any $\psi \mid \chi$, the subfield of $\mathbb{Q}^{\rm ab}$ fixed by $\mathrm{Ker}(\chi) := \mathrm{Ker}(\psi)$, $\mathrm{Gal}(K_\chi/\mathbb{Q})$, the conductor of K_χ, the field of values of the characters, respectively.

In most developments, we suppress the indices χ, it being understood that K and χ correspond to each other and that the p-adic characters φ divide χ.

Remark 1 – In the non semi-simple case, let χ be the rational character defining K. Recall that $K = K'K_0$, where $g_0 := [K_0 : \mathbb{Q}]$ is prime to p and $[K' : \mathbb{Q}] = p^n$, $n \geq 1$. The field of values of $\psi \mid \chi$ is $\mathbb{Q}(\mu_{g_0 p^n})$, direct compositum of the form $\mathbb{Q}(\mu_{g_0})\mathbb{Q}(\mu_{p^n})$; thus $\psi = \psi_0 \psi_p$, ψ_0 of order g_0, ψ_p of order p^n and $\chi = \chi_0 \chi_p$, $\chi_0 \in \mathcal{X}_{K_0}$ above ψ_0, $\chi_p \in \mathcal{X}_{K'}$ above ψ_p.

Similarly, in $\mathbb{Q}_p(\mu_{g_0})\mathbb{Q}_p(\mu_{p^n})$, irreducible p-adic characters $\varphi \mid \chi$ are of the form $\varphi_0 \varphi_p$, $\varphi_p = \chi_p$ since $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$.

The set $\mathcal{X}$ has the following easy property considered as the "Main theorem" for rational components (e.g., Leopoldt (1954, Chap. I, § 1, 1)):

Theorem 1 – *Let $K/\mathbb{Q}$ be a finite abelian extension and let $(A_\rho)_{\rho \in \mathcal{X}_K}$, $(A'_\rho)_{\rho \in \mathcal{X}_K}$ be two families of positive numbers, indexed by the set $\mathcal{X}_K$ of irreducible rational characters of K. If for all subfields k of K, one has $\prod_{\rho \in \mathcal{X}_k} A'_\rho = \prod_{\rho \in \mathcal{X}_k} A_\rho$, then $A'_\rho = A_\rho$ for all $\rho \in \mathcal{X}_K$.*

The interest of this property is that analytic formulas (giving for instance orders A_K of some finite p-adic invariants $\mathcal{A}_K$ of abelian fields K) may be *canonically* decomposed under identities $A_K = \prod_{\rho \in \mathcal{X}_K} A_\rho$, to be compared with algebraic relations $\#\mathcal{A}_K = \prod_{\rho \in \mathcal{X}_K} \#\mathcal{A}_\rho$ for suitable $\mathbb{Z}_p[\mathcal{G}]$-modules $\mathcal{A}_\rho$, so that $\#\mathcal{A}_\rho = A_\rho$ for all ρ; the corresponding FAMC being the same statement, replacing rational characters ρ by p-adic ones φ, under the existence of natural relations $\#\mathcal{A}_\rho = \prod_{\varphi \mid \rho} \#\mathcal{A}_\varphi$ and $A_\rho = \prod_{\varphi \mid \rho} A_\varphi$ for suitable $\mathbb{Z}_p[\mathcal{G}]$-modules $\mathcal{A}_\varphi$ (e.g., in the case where $\mathcal{A}_\rho = \oplus_{\varphi \mid \rho} \mathcal{A}_\varphi$); the main problem being precisely what definition for the isotypic components $\mathcal{A}_\rho$ and $\mathcal{A}_\varphi$.

2.2 Main results of the article

Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a family of $\mathbb{Z}[\mathscr{G}]$-modules, indexed with the set $\mathscr{K}$ of finite abelian extensions K and provided with the arithmetic norms $\mathbf{N}_{K/k}$ and transfer maps $\mathbf{J}_{K/k}$, for any $k \subseteq K$, where $\mathbf{J}_{K/k} \circ \mathbf{N}_{K/k} = \mathcal{V}_{K/k} \in \mathbb{Z}[\mathrm{Gal}(K/k)]$ (algebraic norm). We associate with $\mathbf{M}$ the family of $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{M} := \mathbf{M} \otimes \mathbb{Z}_p$.

We will give more definitions and details in Section 3.1 with the study of the notion of $\mathscr{G}$-families, but we take note of the fact that, in the class field theory framework about p-class groups and generalizations, the following remarks are of great specific significance:

Remarks 1 – (i) Let H_k^{nr} and H_K^{nr} be the p-Hilbert class fields of k and K, respectively; then the map $\mathrm{Gal}(H_K^{\mathrm{nr}}/K) \to \mathrm{Gal}(H_k^{\mathrm{nr}}/k)$, given by the restriction of the Artin automorphisms, corresponds, by class field theory, to the map $\mathbf{N}_{K/k} : \mathscr{H}_K \to \mathscr{H}_k$ (from norms of ideals) which is surjective as soon as the p-sub-extension of K/k is totally ramified, which is almost always the case in the present abelian theory; more precisely, *this is always the case* when $K = K_\chi$, since then K is the compositum of K_0, of prime-to-p degree, with K' cyclic of p-power degree over $\mathbb{Q}$, thus totally ramified.

(ii) On the contrary, the transfer map $\mathbf{J}_{K/k}$, corresponding to extension of classes (from that of ideals), is not necessarily injective in p-extensions; if this fact is well known precisely in H_k^{nr}/k (but H_k^{nr} is not abelian over $\mathbb{Q}$), it is very frequent in totally ramified abelian p-extensions as K/K_0, described above; a fact less known which has interesting consequences (see, e.g., in Gras[39] for an extensive study of capitulation phenomena, where numerical experiments show that capitulation is a common occurrence contrary to what one might think).

We will define (see Definition 1, 2, 3 and Remark 3) various χ-components $\mathbf{M}_\chi^{\mathrm{alg}}$, $\mathbf{M}_\chi^{\mathrm{ar}}$, $\mathscr{M}_\chi^{\mathrm{alg}}$, $\mathscr{M}_\chi^{\mathrm{ar}}$, $\chi \in \mathscr{X}$, and the associated φ-components $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi^{\mathrm{ar}}$, $\varphi \in \Phi$, as follows:

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

[39] Gras, 2023a, "Algebraic norm and capitulation of p-class groups in ramified cyclic p-extensions";
Gras, 2023b, "The Chevalley–Herbrand formula and the real abelian Main Conjecture (New criterion using capitulation of the class group)";
Gras, 2024b, "The real abelian main conjecture in the non semi-simple case".

with $G_\chi =: \langle \sigma_\chi \rangle$; then:

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

So, $\mathscr{M}_\varphi^{\rm ar} = \left\{ x \in \mathscr{M}_K,\ x^{P_\varphi(\sigma_\chi)} = 1\ \&\ \mathbf{N}_{K/k}(x) = 1, \forall\, k \subsetneq K \right\}$, that we can restrict to $\mathbf{N}_{K/k_p}(x) = 1$ with $[K : k_p] = p$, also equal to the φ_0-component of $\mathscr{M}_\chi^{\rm ar}$ (notations of Remark 1).

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. $\psi \mid \varphi$).

We have proved the following results, justifying the above arithmetic norm definitions $\mathbf{M}^{\rm ar}$ and $\mathscr{M}^{\rm ar}$:

(i) Let's denote by $\mathcal{V}$ the algebraic norms; then:

- $\mathbf{M}_\chi^{\rm alg} = \{ x \in \mathbf{M}_K,\ \mathcal{V}_{K/k}(x) = 1,\ \forall\, k \subsetneq K \}$ (Theorem 2),
- $\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\rm alg}$, $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi \mid \chi} \mathscr{M}_\varphi^{\rm ar}$ (Theorems 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:

- $\#\mathbf{M}_K = \prod_{\rho \in \mathscr{X}_K} \#\mathbf{M}_\rho^{\rm ar}$ (Theorem 3),

(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:

- $\#\mathscr{M}_\chi^{\rm ar} = \prod_{\varphi \mid \chi} \#\mathscr{M}_\varphi^{\rm ar}$ (Theorem 5).

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) and $\mathscr{T}$ (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 6);

- $\#\mathbf{H}_\chi^{\rm ar} = \#\mathbf{H}_\chi^{\rm alg} = 2^{\alpha_\chi}\cdot w_\chi\cdot\prod_{\psi|\chi}\left(-\frac{1}{2}\,\mathbf{B}_1(\psi^{-1})\right)$ (Theorem 7), in terms of generalized 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 Appendix A.2 on p. 175, Appendix A.2 on p. 178 for strict inclusions);
- $\#\mathbf{H}_\chi^{\rm ar} = w_\chi\cdot\left(\mathbf{E}_K:\widehat{\mathbf{E}}_K\mathbf{F}_K\right)$ (Theorem 14), in terms of cyclotomic units, where $\widehat{\mathbf{E}}_K := \langle\,\mathbf{E}_k\,\rangle_{k\subsetneq K}$.

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

- $\mathscr{T}_\chi^{\rm ar} = \mathscr{T}_\chi^{\rm alg}$ and $\mathscr{T}_\varphi^{\rm ar} = \mathscr{T}_\varphi^{\rm alg}$, $\forall\,\varphi\mid\chi$ (Theorem 11);
- $\#\mathscr{T}_\chi^{\rm ar} = w_\chi^{\rm cyc}\cdot\prod_{\psi|\chi}\frac{1}{2}\,\mathbf{L}_p(1,\psi)$ (Theorem 12), in terms of p-adic $\mathbf{L}$-functions.

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

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

where $\mathfrak{p}_\varphi$ is the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$; the definition of the Analytic Invariants $m_\varphi^{\rm an}(\mathscr{M})$ comes directly from the formulas of $\#\mathscr{M}_\chi^{\rm ar}$ given above in (iii), taking into account the decompositions $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi|\chi}\mathscr{M}_\varphi^{\rm ar}$, whence the statement of the FAMC:

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

for all $\varphi\in\Phi$ (Section 8, Conjecture 3).

3 Definition and study of the φ-objects

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

3.1 The Algebraic and Arithmetic $\mathcal{G}$-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 $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ of (multiplicative) $\mathbb{Z}[\mathcal{G}]$-modules, indexed by $\mathscr{K}$ (fulfilling some natural conditions and called a $\mathcal{G}$-family).

In general there exist two families of $\mathcal{G}$-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

$$\mathcal{V}_{K/k} := \sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma \in \mathbb{Z}[\mathrm{Gal}(K/k)] \quad \text{(algebraic norm)}.$$

We consider the three following conditions:

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

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

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

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

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

Definitions 1 – (i) If $\mathbf{M} = (\mathbf{M}_K)_{K \in \mathscr{K}}$ only fulfills condition (**a**), we shall say that the family $(\mathbf{M}, \mathcal{V})$ is an algebraic $\mathcal{G}$-family; one may only use Galois theory in K/k and the algebraic norms $\mathcal{V}_{K/k} \in \mathbb{Z}[\mathrm{Gal}(K/k)]$.

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

The following properties of $\mathbf{M}_K$ and $\mathscr{M}_K := \mathbf{M}_K \otimes \mathbb{Z}_p$ are elementary:

Proposition 2 – *(i) For all $K \in \mathscr{K}$, $\mathcal{V}_{K/K}$, $\mathbf{N}_{K/K}$, $\mathbf{J}_{K/K}$ 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 $\mathbf{N}_{K/k} \circ \mathbf{J}_{K/k} = [K : k]$.

Remark 2 – Note that cohomology is only of algebraic nature (case (i) of the above definitions) since, using the $\mathcal{G}$-family $(\mathbf{H}, \mathcal{V})$ for class groups $\mathbf{H}_K$, we have, for instance in the case of a cyclic extension K/k of Galois group $G =: \langle \sigma \rangle$:

$$\mathrm{H}^1(G, \mathbf{H}_K) \simeq \mathrm{Ker}(\mathcal{V}_{K/k}) \Big/ \mathbf{H}_K^{1-\sigma}, \quad \mathrm{H}^2(G, \mathbf{H}_K) \simeq \mathbf{H}_K^G \Big/ \mathcal{V}_{K/k}(\mathbf{H}_K);$$

in general $\mathcal{V}_{K/k}(\mathbf{H}_K)$ is not isomorphic to $\mathbf{N}_{K/k}(\mathbf{H}_K) \subseteq \mathbf{H}_k$, even if $\mathbf{N}_{K/k}$ is surjective. The fact that $\mathbf{J}_{K/k}$ may be non-injective will be the main phenomenon in this survey.

Examples 1 – The most straightforward examples of such arithmetic $\mathcal{G}$-families $\mathbf{M}_K$ are the following ones:

(i) the group $\mathbf{E}_K$ of units of K,for which 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 $\mathcal{T}_K$ of the Galois group of the maximal p-ramified abelian pro-p-extension of K;

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

3.2 Definition of the $\mathcal{G}$-modules $\mathbf{M}_\chi^{\mathrm{alg}}$, $\mathbf{M}_\chi^{\mathrm{ar}}$, $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}_\varphi^{\mathrm{ar}}$

We shall use for instance $\mathbb{A}\in\{\mathbb{Z},\,\mathbb{Z}_p\}$ and we recall, in the two Subsections 3.2, 3.2, some well-known facts that may be omitted by the reader.

The $\Gamma_{\mathcal{K}_\mathbb{A}}$-conjugation

Let $\chi\in\mathscr{X}$. Let $P_\chi(X)\in\mathbb{Z}[X]$ be the g_χth global cyclotomic polynomial. Let $\mathcal{K}_\mathbb{A}$ be the field of quotients of $\mathbb{A}$; so, $\Gamma_{\mathcal{K}_\mathbb{A},\chi}:=\mathrm{Gal}(\mathcal{K}_\mathbb{A}(\mu_{g_\chi})/\mathcal{K}_\mathbb{A})$ is isomorphic to a subgroup of $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$.

One defines, following Serre[40], the $\Gamma_{\mathcal{K}_\mathbb{A}}$-conjugation on Ψ by putting, for all $\tau\in\Gamma_{\mathcal{K}_\mathbb{A},\chi}$ and $\psi\in\Psi$, $\psi\mid\chi$, $\psi^\tau:=\psi^a$, where $a\in\mathbb{Z}$ is a representative of τ in $(\mathbb{Z}/g_\chi\mathbb{Z})^\times$. Then the $\psi^\tau(\sigma_\chi)$ are the conjugates of $\psi(\sigma_\chi)$ in $\mathcal{K}_\mathbb{A}(\mu_{g_\chi})/\mathcal{K}_\mathbb{A}$. This defines the irreducible characters over $\mathcal{K}_\mathbb{A}$ (with values in $\mathbb{A}$), $\theta=\sum_{\tau\in\Gamma_{\mathcal{K}_{\mathbb{A},\chi}}}\psi^\tau$.

Correspondence between characters and cyclotomic polynomials

Let $\chi\in\mathscr{X}$. In $\mathcal{K}_\mathbb{A}[X]$, P_χ splits into a product of irreducible distinct polynomials $P_{\chi,i}$; each $P_{\chi,i}$ splits into degree 1 polynomials over $\mathcal{K}_\mathbb{A}(\mu_{g_\chi})$ and is of degree $[\mathcal{K}_\mathbb{A}(\mu_{g_\chi}):\mathcal{K}_\mathbb{A}]$.

If $\zeta_i\in\mu_{g_\chi}$ is a root of $P_{\chi,i}$, the other roots are the ζ_i^τ for $\tau\in\Gamma_{\mathcal{K}_{\mathbb{A},\chi}}$; thus, these sets of roots are in one by one correspondence with the sets of the form $(\psi^\tau(\sigma_\chi))_{\tau\in\Gamma_{\mathcal{K}_{\mathbb{A},\chi}}}$, $\psi^\tau\mid\chi$, $\psi^\tau\in\Psi$ of order g_χ, describing a representative set of characters for the $\Gamma_{\mathcal{K}_\mathbb{A}}$-conjugation. One may index, *non-canonically*, the irreducible divisors of P_χ in

[40] Serre, 1998, *Représentations linéaires des groupes finis, 5ième éd., corr. et augm. de nouveaux exercices.*

$\mathcal{K}_{\mathbb{A}}[X]$ by means of the characters θ obtained from the characters $\psi \in \Psi$ of orders g_χ and by choosing a generator σ_χ of G_χ. Put:

$$P_\theta := \prod_{\psi|\theta} (X - \psi(\sigma_\chi)) \in \mathbb{A}[X]. \tag{1}$$

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

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 Φ of irreducible p-adic characters of $\mathcal{G}$.

Definition 1 – Let $\mathbf{M} = (\mathbf{M}_K)_{K\in\mathscr{K}}$ be a $\mathcal{G}$-family of $\mathbb{Z}[\mathcal{G}]$-modules (cf. Subsection 3.1) and let $\mathscr{M} := \mathbf{M} \otimes \mathbb{Z}_p = (\mathscr{M}_K)_{K\in\mathscr{K}}$. Put, for $\chi \in \mathscr{X}$, $K = K_\chi$ and let $\varphi \mid \chi$, $\varphi \in \Phi$:

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

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

From relation (1), the polynomials P_φ depend on the choice of the generator σ_χ of G_χ, but we have the following property:

Lemma 1 – *The Definitions 1, of the $\mathbb{Z}[\mu_{g_\chi}]$-modules $\mathbf{M}_\chi^{\mathrm{alg}}$ and the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{M}_\varphi^{\mathrm{alg}}$, do not depend on the choice of σ_χ.*

Proof. Let $\varphi \mid \chi$. We have $P_\varphi(\sigma_\chi) = \prod_{\psi|\varphi}(\sigma_\chi - \psi(\sigma_\chi))$ and, for $a > 0$ with $\gcd(a, g_\chi) = 1$, let $\sigma'_\chi =: \sigma_\chi^a$ another generator of G_χ giving the relation $P'_\varphi(\sigma'_\chi) = \prod_{\psi|\varphi}(\sigma'_\chi - \psi(\sigma'_\chi))$; one must compare $P_\varphi(\sigma_\chi)$ and $P'_\varphi(\sigma'_\chi)$. Then:

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

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

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

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

Now we introduce a property of algebraic norms, only related to that of the group algebra $\mathbb{Z}[\mathcal{G}]$.

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 $\mathscr{M}_\chi^{\rm alg}$. We then have the following characterization, only valid for rational characters, but which will allow another definition of χ-objects (that of "Arithmetic" χ-objects), *even in the global case of $\mathcal{G}$-families* $\mathbf{M}$ *of* $\mathbb{Z}[\mathcal{G}]$*-modules* (as $\mathbf{M} \in \{\mathbf{E}, \mathbf{H}, \ldots\}$), the corresponding definition for $\mathscr{M} = \mathbf{M} \otimes \mathbb{Z}_p$ being trivial:

Theorem 2 – *Let* $\mathbf{M}$ *be a* $\mathcal{G}$*-family of* $\mathbb{Z}[\mathcal{G}]$*-modules and for* $K = K_\chi$, $\chi \in \mathscr{X}$, *let* $\mathbf{M}_\chi^{\rm alg} := \left\{x \in \mathbf{M}_K,\ x^{P_\chi(\sigma_\chi)} = 1\right\}$. *Then:*

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

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

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

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

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

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

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

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:

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

(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_{ℓ_1} and P_{ℓ_2}.

Suppose $t \geq 3$. Let ℓ_i, ℓ_j, q, be three distinct primes dividing n; put $n' := \frac{n}{q}$; by induction, since ℓ_i and ℓ_j divide n', there exist polynomials $A_i'^j, A_j'^i$ in $\mathbb{Z}[X]$, such that $A_i'^j(X)P_{\frac{n'}{\ell_i}}(X) + A_j'^i(X)P_{\frac{n'}{\ell_j}}(X) = 1$, thus, $A_i'^j(X^q)P_{\frac{n'}{\ell_i}}(X^q) + A_j'^i(X^q)P_{\frac{n'}{\ell_j}}(X^q) = 1$. But Lemma 2 (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 4 – *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 ℓ dividing n. Then there exist polynomials $A_\ell(X) \in \mathbb{Z}[X]$ such that $P_n(X) = \sum_{\ell|n} A_\ell(X)N_{n,\ell}(X)$ and $\left\langle N_{n,\ell}(X),\ \ell \mid n \right\rangle_{\mathbb{Z}[X]} = P_n(X)\mathbb{Z}[X]$.*

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 2 (i):

$$P_{nq}(X) = P_n(X^q) = \sum_{\ell|n} A_\ell(X^q)N_{n,\ell}(X^q).$$

Since we have $N_{n,\ell}(X^q) = \sum_{i=0}^{\ell-1} X^{\frac{n}{\ell} q i} = N_{nq,\ell}(X)$, we obtain that if the lemma is true for n, it is true for nq for all $q \mid n$. It follows that if the property is true for all square-free integers n, it is true for all $n > 1$. So we may assume n square-free to prove the lemma by induction on t.

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

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

whence $P_n(X)P_{n_k}(X)\in\left\langle N_{n,\ell}(X),\ \ell\mid n\right\rangle_{\mathbb{Z}[X]}$, for all k; since $t\geq 2$, Lemma 3 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 ζ_n of order n (i.e., root of $P_n(X)$), is a root of $N_{n,\ell}(X)$ since $\zeta_n^{\frac{n}{\ell}}=\zeta_\ell\neq 1$ and $\sum_{i=0}^{\ell-1}\zeta_\ell^i=0$; then $P_n(X)\mid N_{n,\ell}(X)$ in $\mathbb{Z}[X]$ (monic polynomials). □

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

Application to the definition of $\mathbf{M}_\chi^{\rm ar}$

Let $\mathbf{M}$ be an arithmetic $\mathcal{G}$-family, provided with norms $\mathbf{N}$ and transfer maps $\mathbf{J}$ with $\mathbf{J}\circ\mathbf{N}=\mathcal{V}$.

Definition 2 – By analogy with Theorem 2 giving, for χ-objects, the characterization $\mathbf{M}_\chi^{\rm alg}:=\{x\in\mathbf{M}_K,\ \mathcal{V}_{K/k}(x)=1,\text{ for all } k\subsetneq K\}$ and $\mathscr{M}_\chi^{\rm alg}=\mathbf{M}_\chi^{\rm alg}\otimes\mathbb{Z}_p$, we define the modules of arithmetic χ-objects:

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

Then $\mathbf{M}_\chi^{\rm ar}$ is a sub-$\mathbb{Z}[\mu_{g_\chi}]$-module of $\mathbf{M}_\chi^{\rm alg}$ and $\mathscr{M}_\chi^{\rm ar}$ is a sub-$\mathbb{Z}_p[\mu_{g_\chi}]$-module of $\mathscr{M}_\chi^{\rm alg}$, with laws defined via the choice of $\psi\mid\chi$ (resp. $\psi\mid\varphi$).

We have $\mathbf{M}_\chi^{\rm ar}=\mathbf{M}_\chi^{\rm alg}$ as soon as the $\mathbf{J}_{K/k}$'s are injective, for all $k\subsetneq K$ or simply for the k_ℓ's. One verifies easily that if the norms $\mathbf{N}_{K/k_\ell}$ are surjective for all prime $\ell\mid g_\chi$, 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 θ-components $\mathbf{M}_\theta$ (θ rational or p-adic, above $\psi \in \Psi$) is defined, in an abelian field K of Galois group G_K, by:

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

where $\mathbb{A}[\theta] := \mathbb{A}[\psi]$ is the ring of values of θ over $\mathbb{A}$; the action being defined via $(\sigma, x) \in G_K \times \mathbf{M}_\theta \mapsto x^{\psi(\sigma)} \in \mathbf{M}_\theta$. We shall compare this definition with Definition 2 considering irreducible p-adic characters φ. We have the classical algebraic definition of φ-objects attached to $\mathscr{M}$, that is to say, the largest quotient such that G_χ acts by ψ (Greither (1992, Definition, p. 451), Perrin-Riou (1990, § 1.3), Mazigh (2017)):

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

Another viewpoint[41], is to define $\widehat{\mathscr{M}^\varphi}$ as the largest sub-$\mathbb{Z}_p[G_\chi]$-module of $\mathscr{M}$, such that G_χ acts by ψ. Whence, one obtains our basic definition:

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

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

Moreover, our forthcoming Definition 3 of $\mathscr{M}_\varphi^{\mathrm{ar}}$:

$$\mathscr{M}_\varphi^{\mathrm{ar}} := \mathscr{M}_\varphi^{\mathrm{alg}} \cap \mathscr{M}_\chi^{\mathrm{ar}} \quad \text{(with Definition 2 of } \mathscr{M}_\chi^{\mathrm{ar}}),$$

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 $\mathscr{M}_\varphi^{\mathrm{ar}}$ and new analytic expressions giving $\#\mathscr{M}_\chi^{\mathrm{ar}}$, justifying the conjectural values of $\#\mathscr{M}_\varphi^{\mathrm{ar}}$ for finite $\mathscr{M}_K$'s.

It is immediate to verify that, in the non semi-simple case $p \mid g_\chi$, $(\mathscr{M}_\varphi^{\mathrm{alg}} : \mathscr{M}_\varphi^{\mathrm{ar}})$ is equal to the order of the capitulation kernel of $\mathbf{J}_{K/k_p}$, where k_p is the subfield of $K = K_\chi$ such that $[K : k_p] = p$. In the semi-simple case $p \nmid \#G_\chi$, $\mathscr{M} \simeq \mathscr{M}_\varphi \bigoplus \left[\mathscr{M}^{P_\varphi(\sigma_\chi)}\right]$ whatever the definitions (see again Examples of Appendix A.2).

3.4 Arithmetic factorization of $\#\mathbf{M}_K$ and $\#\mathscr{M}_K$

Let $\mathbf{M}$ be an arithmetic $\mathcal{G}$-family where all the $\mathbb{Z}[\mathcal{G}]$-modules $\mathbf{M}_K$, $K \in \mathscr{K}$, are finite; then we can state:

[41] Solomon, 1990, "On the class groups of imaginary abelian fields", § II.1, pp. 469–471.

Theorem 3 – *(i) Let $K/\mathbb{Q}$, $K = K_\chi$, be a cyclic extension and assume that, for all sub-extension k/k' of $K/\mathbb{Q}$, $\mathbf{N}_{k/k'}$ is surjective. Then:*

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

where $\mathbf{M}_\rho^{\rm ar} := \{x \in \mathbf{M}_{K_\rho},\ \mathbf{N}_{K_\rho/k}(x) = 1,\ \forall\, k \subsetneq K_\rho\}$ (Definition 2).

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

Proof. One may replace the $\mathbf{M}_k$, $k \subseteq K$, by the finite $\mathbb{Z}_\ell[G_K]$-modules $\mathscr{M}_k := \mathbf{M}_k \otimes \mathbb{Z}_\ell$, for all primes ℓ dividing $\#\mathbf{M}_K$, using the previous results, then globalizing at the end. Two classical elementary lemmas are necessary; to obtain both (i) and (ii), we work with the prime p.

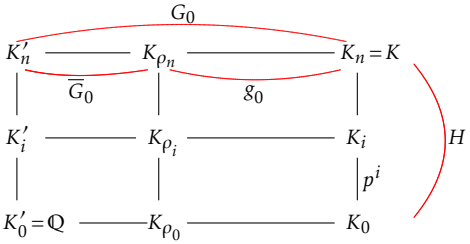
Lemma 5 – *Assume that $p \nmid [k : k']$. If $\mathbf{N}_{k/k'} : \mathscr{M}_k \longrightarrow \mathscr{M}_{k'}$ is surjective (resp. if $\mathbf{J}_{k/k'} : \mathscr{M}_{k'} \longrightarrow \mathscr{M}_k$ is injective), then $\mathbf{J}_{k/k'}$ is injective (resp. $\mathbf{N}_{k/k'}$ is surjective).*

Proof. From Proposition 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 $\{K_{\rho_i},\ \rho_i \in \mathscr{X}_K,\ 0 \le i \le n\}$, where ρ_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_{ρ_i} is the compositum $K_{\rho_0} K'_i$:

Schema I



Let $\mathscr{M}^*_{K_{\rho_i}} := \mathrm{Ker}(\mathbf{N}_{K_{\rho_i}/K_{\rho_{i-1}}})$, $1 \le i \le n$, then put $\mathscr{M}^*_{K_{\rho_0}} := \mathscr{M}_{K_{\rho_0}}$. By assumption, we have the exact sequences of $\mathbb{Z}_p[G_K]$-modules:

$$1 \longrightarrow \mathscr{M}^*_{K_{\rho_i}} \longrightarrow \mathscr{M}_{K_{\rho_i}} \xrightarrow{\mathbf{N}_{K_{\rho_i}/K_{\rho_{i-1}}}} \mathscr{M}_{K_{\rho_{i-1}}} \longrightarrow 1,\ 1 \le i \le n. \tag{2}$$

One considers them as exact sequences of $\mathbb{Z}_p[G_0]$-modules. The idempotents of this algebra are, for all $\rho_0 \in \mathscr{X}_{K_0}$, of the form:

$$e_{\rho_0} = \frac{1}{\#G_0} \sum_{\sigma \in G_0} \rho_0(\sigma^{-1})\, \sigma \in \mathbb{Z}_p[G_0].$$

From Leopoldt (1954) and Leopoldt (1962, 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 6 – *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 $\mathscr{M}_{K_i}^{e_{\rho_0}} \simeq \mathscr{M}_{K_{\rho_i}}^{e_{\rho_0}}$ and $(\mathscr{M}_{K_i}^*)^{e_{\rho_0}} \simeq (\mathscr{M}_{K_{\rho_i}}^*)^{e_{\rho_0}}$.*

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 $g_0 := \mathrm{Gal}(K_n/K_{\rho_n})$. Thus, by abuse of notation, we identify $\mathcal{V}_{K_i/K_{\rho_i}}$ with $\mathcal{V}_{K_n/K_{\rho_n}} =: \mathcal{V}_{g_0}$; moreover, since the degrees of these extensions are prime to p, we may identify $\mathbf{N}_{K_i/K_{\rho_i}}$ with $\mathbf{N}_{K_n/K_{\rho_n}} =: \mathbf{N}_{g_0}$ and $\mathbf{J}_{K_i/K_{\rho_i}}$ with $\mathbf{J}_{K_n/K_{\rho_n}} =: \mathbf{J}_{g_0}$. Thus $\mathbf{N}_{g_0}$ is surjective and $\mathbf{J}_{g_0}$ injective. One computes that $e_{\rho_0} = \dfrac{\nu_{g_0}}{\#g_0}\, \overline{e}_{\rho_0}$, where $\overline{e}_{\rho_0} := \dfrac{1}{\#\overline{G}_0} \displaystyle\sum_{\overline{\sigma} \in \overline{G}_0} \rho_0(\overline{\sigma}^{-1})\, \sigma \in \mathbb{Z}_p[G_0]$; but we have:

$$\mathcal{V}_{g_0}(\mathscr{M}_{K_i}) = \mathbf{J}_{g_0} \circ \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathbf{N}_{g_0}(\mathscr{M}_{K_i}) \simeq \mathscr{M}_{K_{\rho_i}}; \tag{3}$$

whence $\mathscr{M}_{K_i}^{e_{\rho_0}} \simeq \mathscr{M}_{K_{\rho_i}}^{\overline{e}_{\rho_0}}$. To get $(\mathscr{M}_{K_i}^*)^{e_{\rho_0}} \simeq \mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*)^{\overline{e}_{\rho_0}} \simeq (\mathscr{M}_{K_{\rho_i}}^*)^{\overline{e}_{\rho_0}}$, it suffices to verify that, for all $i \geq 1$, $\mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*) = \mathscr{M}_{K_{\rho_i}}^*$. The inclusion $\mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*) \subseteq \mathscr{M}_{K_{\rho_i}}^*$ being obvious, let $x \in \mathscr{M}_{K_{\rho_i}}^*$; we have $x = \mathbf{N}_{g_0}(y)$, $y \in \mathscr{M}_{K_i}$, then $1 = \mathbf{N}_{K_{\rho_i}/K_{\rho_{i-1}}} \circ \mathbf{N}_{g_0}(y) = \mathbf{N}_{g_0} \circ \mathbf{N}_{K_i/K_{i-1}}(y)$. Let $z := \mathbf{N}_{K_i/K_{i-1}}(y)$, we have $\mathbf{N}_{g_0}(z) = 1$; applying $\mathbf{J}_{K_{i-1}/K_{\rho_{i-1}}}$, one gets $\mathcal{V}_{g_0}(z) = 1$; but we have, as for (3), $\mathcal{V}_{g_0}(\mathscr{M}_{K_{i-1}}) \simeq \mathscr{M}_{K_{\rho_{i-1}}}$; whence $z = 1$, $y \in \mathscr{M}_{K_i}^*$ and $x \in \mathbf{N}_{g_0}(\mathscr{M}_{K_i}^*)$. □

From Leopoldt (1954, Chap. I, § 1, 2, formula (6), p. 21) or our previous norm computations since $p \nmid \#G_0$, we have the relations, from the surjectivity of the norms and Lemma 5:

$$\begin{cases} \mathscr{M}_{K_{\rho_i}}^{\overline{e}_{\rho_0}} = \{x \in \mathscr{M}_{K_{\rho_i}},\ \mathbf{N}_{K_{\rho_i}/k}(x) = 1 \text{ for all } k,\ \ K_i' \subseteq k \subsetneq K_{\rho_i}\}, \\ \mathscr{M}_{K_{\rho_i}}^{*\,\overline{e}_{\rho_0}} = \{x \in \mathscr{M}_{K_{\rho_i}}^*,\ \mathbf{N}_{K_{\rho_i}/k}(x) = 1 \text{ for all } k,\ \ K_i' \subseteq k \subsetneq K_{\rho_i}\}. \end{cases}$$

From the norm definitions of $(\mathscr{M}^{\rm ar}_{K_{\rho_i}})_{\rho_0}$ and from:

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

it follows that $\mathscr{M}^{*\overline{e}_{\rho_0}}_{K_{\rho_i}} = \mathscr{M}^{\rm ar}_{\rho_i}$, for all $i \geq 1$. In the finite case, this yields, using the above, the exact sequence (2) and $\mathscr{M}^{*}_{K_0} := \mathscr{M}_{K_0}$:

$$\begin{cases} \displaystyle\prod_{i=0}^{n} \#\mathscr{M}^{*\overline{e}_{\rho_0}}_{K_{\rho_i}} = \#\mathscr{M}^{*\overline{e}_{\rho_0}}_{K_0} \prod_{i=1}^{n} \frac{\#\mathscr{M}^{\overline{e}_{\rho_0}}_{K_i}}{\#\mathscr{M}^{\overline{e}_{\rho_0}}_{K_{i-1}}} = \#\mathscr{M}^{\overline{e}_{\rho_0}}_{K}, \\ \displaystyle\prod_{\rho \in \mathscr{Y}_K} \#\mathscr{M}^{\rm ar}_{\rho} = \prod_{\rho_0} \#\mathscr{M}^{\overline{e}_{\rho_0}}_{K} = \#\mathscr{M}_K. \end{cases} \tag{4}$$

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, whence totally ramified, class field theory implying the claim (see Remark 1 (i)).

The p-cyclicity is necessary as shown by $K = \mathbb{Q}(\sqrt{6}, \sqrt{130})$, where $p = 2$ is totally ramified (so, arithmetic norms are surjective) with class group $\mathscr{H}_K$ of order 4, while class groups of the three strict subfields of K, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{130})$, $\mathbb{Q}(\sqrt{195})$ are $1, 4, 4$, respectively.

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 ψ_0, $\psi_p \in \Psi$ such that $\psi = \psi_0\,\psi_p$, ψ_0 of prime-to-p order and ψ_p of p-power order. We restrict the study to $K := K_\chi$ for χ above ψ, so that, from the previous § 3.4, G_K becomes $G_\chi =: G_0 \oplus H$ of order $g_\chi = g_{\chi_0} p^n$.

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

$$e_{\varphi_0} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\,\sigma \in \mathbb{Z}_p[G_0], \tag{5}$$

where φ_0 is the p-adic character over ψ_0 and put $(\ )_{\varphi_0} := (\ )^{e_{\varphi_0}}$.

4.1 Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\mathrm{alg}}$

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

Theorem 4 – *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 $\mathscr{M}_\chi^{\mathrm{alg}} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\mathrm{alg}}$ (cf. Definition 1). Moreover, if $\mathscr{M}'_\chi$ is a sub-$\mathscr{A}_\chi$-module of $\mathscr{M}_\chi^{\mathrm{alg}}$, then $\mathscr{M}'_\chi = \bigoplus_{\varphi|\chi} \mathscr{M}'_\varphi$, where $\mathscr{M}'_\varphi = \{x' \in \mathscr{M}'_\chi,\ x'^{P_\varphi(\sigma_\chi)} = 1\} \subseteq \mathscr{M}_\varphi^{\mathrm{alg}}$.

(ii) The sub-$\mathscr{A}_\chi$-modules $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\varphi \mid \chi$, coincide with the $(\mathscr{M}_\chi^{\mathrm{alg}})^{e_{\varphi_0}}$'s, where e_{φ_0} is the semi-simple idempotent (5) associated to φ_0 above the component ψ_0 of prime-to-p order of $\psi \mid \varphi \mid \chi$. Idem for the $\mathscr{M}'_\varphi$'s.

(iii) These modules $\mathscr{M}_\varphi^{\mathrm{alg}}$, $\mathscr{M}'_\varphi$, are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules by means of the choice of $\psi \mid \varphi$ 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[42].

Let φ_1 and φ_2 be two distinct p-adic characters dividing χ (if $\chi = \varphi$ is p-adic irreducible, the result is trivial). Put $P_{\varphi_1} =: Q_1$, $P_{\varphi_2} =: Q_2$ in $\mathbb{Z}_p[X]$ (cf. § 3.2 for the definition of P_φ). The following fundamental lemma is perhaps clear for cyclotomic polynomials, but it is not general (e.g., for $p = 5$, take $P = x^4 - 2x^3 + 55x^2 - 54x + 379$, irreducible in $\mathbb{Z}[X]$, giving, in $\mathbb{Z}_5[X]$, $P \equiv (x^2 + 24x + 12) \cdot (x^2 + 24x + 17) \pmod{5^2}$ and the PARI relation bezout($x^2 + 24*x + 12$, $x^2 + 24*x + 17$) = [−1/5, 1/5, 1]).

Lemma 7 – *There exist $U_1, U_2 \in \mathbb{Z}_p[X]$ such that $U_1 Q_1 + U_2 Q_2 = 1$.*

Proof. We assume that such a relation does not exist and we shall find a contradiction. 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 (with U_1, U_2 not both in $p\mathbb{Z}_p[X]$):

$$U_1 Q_1 + U_2 Q_2 = p^k,\ k \geq 1,$$

choosing U_1 (resp. U_2) of degree less than the degree of Q_2 (resp. of Q_1); moreover, since Q_1 and Q_2 are monic, one may suppose that (for instance):

$$U_2 \notin p\mathbb{Z}_p[X],$$

otherwise, since $k \geq 1$, necessarily $U_1 \in p\mathbb{Z}_p[X]$, which is excluded.

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

$$U_2(\zeta)\, Q_2(\zeta) = p^k \text{ in } \mathbb{Z}_p[\mu_{g_\chi}]; \tag{6}$$

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

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

$$\overline{Q}_1 = (\overline{Q}_0)^e, \tag{7}$$

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:

$$Q_0^\alpha(\zeta) \equiv 0 \pmod{p}. \tag{8}$$

Let's show that $\alpha \geq e$; the unique case where, possibly, $p \mid g_\chi$ and $e = 1$ is the case $p = 2$, $n = 1$; this case trivially gives $\alpha \geq e$. Consider the g_{χ_0}th cyclotomic polynomial. Assuming $e > 1$, we have:

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

$\zeta^{p^n a-1}$ 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 (8), 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 (7):

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

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), whence $A' = 0$ and $\overline{U}_2 = 0$, contrary to the assumption $U_2 \notin p\mathbb{Z}_p[X]$. □

Give now some elementary properties of the system of idempotents of the algebra $\mathscr{A}_\chi = \mathbb{Z}_p[G_\chi]/(P_\chi(\sigma_\chi))$, which may be useful for PARI computations.

Let $\{\varphi_1, \ldots, \varphi_{g_p}\}$ be the set of distinct p-adic characters dividing χ (thus, $g_p \mid \phi(g_{\chi_0})$ is the number of prime ideals dividing p in $\mathbb{Q}(\mu_{g_{\chi_0}})/\mathbb{Q}$, so that, only the case $g_p = 1$ is trivial for the FAMC); from the property of co-maximality, given by Lemma 7, one may write:

$$\mathbb{Z}_p[X]\Big/(P_\chi(X)) \simeq \prod_{u=1}^{g_p} \mathbb{Z}_p[X]/(Q_u(X)) \simeq (\mathbb{Z}_p[\mu_{g_\chi}])^{g_p}. \tag{9}$$

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

$$\mathscr{M}_\chi^{\mathrm{alg}} = \bigoplus_{u=1}^{g_p} \left(\mathscr{M}_\chi^{\mathrm{alg}}\right)^{e^{\varphi_u}(\sigma_\chi)}. \tag{10}$$

It remains to verify that:

$$\left(\mathscr{M}_\chi^{\mathrm{alg}}\right)^{e^{\varphi_u}(\sigma_\chi)} = \mathscr{M}_{\varphi_u}^{\mathrm{alg}} = \left\{x \in \mathscr{M}_\chi^{\mathrm{alg}},\ x^{P_{\varphi_u}(\sigma_\chi)} = 1\right\}.$$

If $x \in \left(\mathscr{M}_\chi^{\mathrm{alg}}\right)^{e^{\varphi_u}(\sigma_\chi)}$, $x = y^{e^{\varphi_u}(\sigma_\chi)}$ with $y \in \mathscr{M}_\chi^{\mathrm{alg}}$; then $x^{P_{\varphi_u}(\sigma_\chi)}$ is $y^{e^{\varphi_u}(\sigma_\chi)P_{\varphi_u}(\sigma_\chi)}$, 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 $y \in \mathscr{M}_\chi^{\mathrm{alg}}$ and $x \in \mathscr{M}_{\varphi_u}^{\mathrm{alg}}$.

If $x \in \mathscr{M}_{\varphi_u}^{\rm alg}$, then $x^{P_{\varphi_u}(\sigma_\chi)} = 1$; writing $x = \prod_v x^{e^{\varphi_v}(\sigma_\chi)}$, 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 ψ_u, and that of the $e^{\varphi_u}(\sigma_\chi)$ corresponding to φ_u. Fixing the character $\varphi_u =: \varphi$ above $\psi =: \psi_0\,\psi_p$ and its non p-part φ_0 above ψ_0, we consider both:

$$e_{\varphi_0} := \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \varphi_0(\sigma^{-1})\,\sigma \tag{11}$$

and $e^{\varphi_0}(\sigma_\chi)$ defined as follows by means of polynomial relations in $\mathbb{Z}[X]$ deduced from (9):

$$e^{\varphi_0}(\sigma_\chi) = \Lambda_\varphi(\sigma_\chi) \prod_{\varphi' \neq \varphi} P_{\varphi'}(\sigma_\chi), \text{ such that: } \Lambda_\varphi(X) \prod_{\varphi' \neq \varphi} P_{\varphi'}(X) \equiv 1 \pmod{P_\varphi(X)}; \tag{12}$$

we will denote $e^{\varphi_0}(\sigma_\chi)$ simply by e^{φ_0}, which is legitimate by Lemma 1.

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^{φ_0} and e_{φ_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 φ, by $\sigma_\chi \mapsto \psi(\sigma_\chi)$, $\psi \mid \varphi$, induces a surjective homomorphism $\mathscr{A}_\chi \longrightarrow \mathbb{Z}_p[\mu_{g_\chi}]$ whose kernel is equal to $\bigoplus_{\varphi' \neq \varphi} \mathscr{A}_\chi\, e^{\varphi'_0}$. 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 (11), e_{φ_0} is a sum of the idempotents $e_{\psi'_0} = \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \psi'_0(\sigma^{-1})\sigma$ where $\psi'_0 \mid \varphi_0$. It follows, since $\psi = \psi_0\,\psi_p$, that $\psi(\sigma) = \psi_0(\sigma)$ and then:

$$\psi(e_{\psi'_0}) = \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \psi'_0(\sigma^{-1})\psi(\sigma) = \frac{1}{g_{\chi_0}} \sum_{\sigma \in G_0} \psi'_0(\sigma^{-1})\psi_0(\sigma),$$

which is zero for all ψ'_0 except $\psi'_0 = \psi_0$ where $\psi(e_{\psi_0}) = 1$. Whence $\psi(e_{\varphi_0}) \neq 0$. Let $\mathscr{M}_\chi^{\rm alg}$ as $\mathscr{A}_\chi$-module; on may write $\mathscr{M}_\chi^{\rm alg} = \bigoplus_{\varphi \mid \chi} (\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}}$ (from (10)) but $(\mathscr{M}_\chi^{\rm alg})^{e^{\varphi_0}}$ coincides with $(\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}} = \mathscr{M}_\varphi^{\rm alg}$ (Definition (11)); then, due to the properties of the e^{φ_0} (defined by (12)):

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

Denote simply by e_{φ_0} any of these two semi-simple idempotents and by $(\ )_{\varphi_0}$ any components, not to be confused with $(\ )_\varphi$.

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

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

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

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. □

4.2 Semi-simple decomposition of the $\mathscr{A}_\chi$-modules $\mathscr{M}_\chi^{\rm ar}$

From Definition 2, $\mathscr{M}_\chi^{\rm ar} := \{x \in \mathscr{M}_K,\ \mathbf{N}_{K/k}(x) = 1,\ \text{for all } k \subsetneq K\}$. This invites to give the following arithmetic definition:

Definition 3 – Let $\mathscr{M}$ be an arithmetic family of $\mathbb{Z}_p[\mathcal{G}]$-modules. Assume to be in the non semi-simple case $p \mid g_\chi$ (otherwise, $\mathscr{M}_\varphi^{\rm ar} = \mathscr{M}_\varphi^{\rm alg}$). For $\varphi \mid \chi$, $\chi \in \mathscr{X}$, $\varphi \in \Phi$, we define the arithmetic $\mathbb{Z}_p[\mu_{g_\chi}]$-module:

$$\mathscr{M}_\varphi^{\rm ar} := \mathscr{M}_\varphi^{\rm alg} \cap \mathscr{M}_\chi^{\rm ar} = \{x \in \mathscr{M}_\varphi^{\rm alg},\ \mathbf{N}_{K/k_p}(x) = 1,\ \text{with } [K : k_p] = p.\}.$$

Remark 3 – So, $\mathscr{M}_\varphi^{\rm ar} = (\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}}$, e_{φ_0} being defined by (11) or (12), 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 use both the notations $\mathscr{M}_\varphi^{\rm ar} = \{x \in \mathscr{M}_\chi^{\rm ar},\ x^{P_\varphi(\sigma_\chi)} = 1\}$ and $(\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}}$. We also have $\mathscr{M}_\varphi^{\rm ar} = \{x \in \mathscr{M}_K^{e_{\varphi_0}},\ \mathbf{N}_{K/k_p}(x) = 1\} = (\mathscr{M}_K^*)_{\varphi_0}$, in the meaning of exact sequence (2) for K/k_p, since the other relative norm conditions are trivially fulfilled for any e_{φ_0}-components. In recent papers, we privilege the notations $\mathscr{M}_\varphi^{\rm ar} = (\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}} =: (\mathscr{M}_\chi^{\rm ar})_{\varphi_0}$, giving, for instance, the φ-component $(\mathscr{E}_K/\widetilde{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$ of $\mathscr{E}_K/\widetilde{\mathscr{E}}_K\mathscr{F}_K$ since this module is, as we have yet explained, trivially an algebraic χ-object.

So, we have the arithmetic version of Theorem 4:

Theorem 5 – *Let $\mathscr{M}$ be an arithmetic $\mathcal{G}$-family of $\mathbb{Z}_p[\mathcal{G}]$-modules. Then we get, for all $\chi \in \mathscr{X}$, the decomposition $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\rm ar}$. The $\mathscr{M}_\varphi^{\rm ar}$'s are canonically $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.*

4.3 Summary of the properties of the $\mathcal{G}$-families $\mathscr{M}^{\rm alg}$, $\mathscr{M}^{\rm ar}$

From Notations 1, Definitions 1, 2, 3, Theorems 3, 4, 5:

[42] Oriat, 1975a, "Quelques caractères utiles en arithmétique", Part II.

(i) Recall that P_χ (resp. $P_\varphi \mid P_\chi$) is the g_χth global cyclotomic polynomial (resp. the local φ-cyclotomic polynomial for $\varphi \mid \chi$) and that:

$$\begin{cases} \mathscr{M}_\chi^{\rm alg} := \left\{x \in \mathscr{M}_K,\ x^{P_\chi(\sigma_\chi)} = 1\right\}, \\ \mathscr{M}_\varphi^{\rm alg} := \left\{x \in \mathscr{M}_K,\ x^{P_\varphi(\sigma_\chi)} = 1\right\} = (\mathscr{M}_\chi^{\rm alg})^{e_{\varphi_0}}, \\ \mathscr{M}_\chi^{\rm ar} := \left\{x \in \mathscr{M}_\chi^{\rm alg},\ \mathbf{N}_{K/k_p}(x) = 1\right\}, \\ \mathscr{M}_\varphi^{\rm ar} := \left\{x \in \mathscr{M}_\varphi^{\rm alg},\ \mathbf{N}_{K/k_p}(x) = 1\right\} = (\mathscr{M}_\chi^{\rm ar})^{e_{\varphi_0}}, \end{cases}$$

where $K = K_\chi$, $\varphi = \varphi_0\varphi_p$, φ_0 of prime to p order, φ_p of p-power order.

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 $\sigma \in G_K \mapsto \psi(\sigma)$, for $\psi \mid \chi$, $\psi \mid \varphi$, respectively.

(ii) Assume that the maximal p-sub-extension of an abelian extension $K/\mathbb{Q}$ 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, $\#\mathscr{M}_K = \prod_{\rho\in\mathscr{X}_K} \#\mathscr{M}_\rho^{\rm ar} = \prod_{\varphi\in\Phi_K} \#\mathscr{M}_\varphi^{\rm ar}$.

5 Application to relative imaginary class groups

5.1 Arithmetic definition of relative class groups

We will apply the previous results using first odd characters χ giving $\mathbf{H}_\chi^{\rm alg}$ and $\mathbf{H}_\chi^{\rm ar}$. The case of even characters requires some deepening of Leopoldt's results[43]; 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:

$$\mathbf{H}_K^{{\rm ar}-} := \{h \in \mathbf{H}_K,\ \mathbf{N}_{K/K^+}(h) = 1\} \tag{13}$$

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

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:

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

and the formula:

$$\#\mathbf{H}_K = \#\mathbf{H}_K^{{\rm ar}-} \times \#\mathbf{H}_K^+. \tag{14}$$

[43] Leopoldt, 1954, "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper".

We denote by $\mathscr{H}_K$ (resp. $\mathscr{H}_K^{\mathrm{ar}-}$ and $\mathscr{H}_K^{+} := \mathscr{H}_{K^+}$), the p-Sylow subgroup of $\mathbf{H}_K$ (resp. $\mathbf{H}_K^{\mathrm{ar}-}$ and $\mathbf{H}_K^{+}$). For the $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{H}_K$, we introduce the $\mathscr{A}_\chi$-modules $\mathscr{H}_\chi^{\mathrm{alg}}$ and $\mathscr{H}_\chi^{\mathrm{ar}}$ for $\chi \in \mathscr{X}$, then their φ-components (Definitions 1, 2, 3) which are $\mathbb{Z}_p[\mu_{g_\chi}]$-modules.

5.2 Proof of the equality $\mathbf{H}_\chi^{\mathrm{ar}} = \mathbf{H}_\chi^{\mathrm{alg}}$, for $\chi \in \mathscr{X}^-$

To prove this equality and then the equalities $\mathscr{H}_\varphi^{\mathrm{ar}} = \mathscr{H}_\varphi^{\mathrm{alg}}$, $\varphi \mid \chi$, it is sufficient to consider, for any $p \geq 2$ dividing $[K : \mathbb{Q}]$, the p-Sylow subgroups $\mathscr{H}_K$, $K = K_\chi$, and to prove the equality of the χ-components $\mathscr{H}_\chi^{\mathrm{alg}}$, $\mathscr{H}_\chi^{\mathrm{ar}}$.

Lemma 8 – *Assume that $\mathscr{H}_\chi^{\mathrm{ar}} \subsetneq \mathscr{H}_\chi^{\mathrm{alg}}$. Then there exists a unique sub-extension $K_{\chi'}$ of K, such that $[K : K_{\chi'}] = p$ (i.e., if $\psi \mid \chi$ then χ' is above $\psi' = \psi^p$; $K_{\chi'}$ is also denoted k_p), and a class $h \in \mathscr{H}_\chi^{\mathrm{alg}}$ such that $h' := \mathbf{N}_{K/K_{\chi'}}(h)$ fulfills the following properties:*

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

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

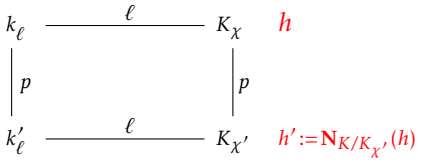
(iii) h' is of order p in $\mathscr{H}_{K_{\chi'}}$.

Proof. Indeed, if $[K : \mathbb{Q}]$ is prime to p, we are in the semi-simple case and $\mathscr{H}_\chi^{\mathrm{alg}} = \mathscr{H}_\chi^{\mathrm{ar}}$. So we assume that $p \mid [K : \mathbb{Q}]$, whence the existence and unicity of $K_{\chi'}$.

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

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

Schema II



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

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

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

Lemma 9 – *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 $\mathbf{E}_K^*=\mathrm{Ker}(\mathcal{V}_{K/k})$). 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 $\mathscr{C}\ell_k(\mathfrak{a})\in\mathscr{H}_k$, 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 $\mathscr{C}\ell_k(\mathfrak{a})\in\mathrm{Ker}(\mathbf{J}_{K/k})$ the class of ε modulo $\mathbf{E}_K^{1-\sigma}$, is obviously injective.

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

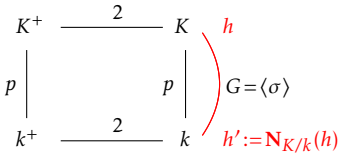
Study of the case $p\neq 2$

We are in the context of Lemma 8. Put $K:=K_\chi$ and $k:=K_{\chi'}$; then K/k is of degree p and the class $h'=\mathbf{N}_{K/k}(h)\in\mathscr{H}_k$ is of order p and capitulates in K.

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

We introduce the maximal real subfields, giving the diagram:

Schema III



Lemma 10 – *Let μ_K^* be the p-torsion sub-group of $\mathbf{E}_K^*$, that is to say the set of p-roots of unity ζ of K such that $\mathbf{N}_{K/k}(\zeta)=1$. Then the image of $\mathscr{H}_k^{\rm ar-}\cap\mathrm{Ker}(\mathbf{J}_{K/k})$, by the map $\mathrm{Ker}(\mathbf{J}_{K/k})\to\mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$ of Lemma 9, is contained in the image of μ_K^* modulo $\mathbf{E}_K^{1-\sigma}$.*

Proof. Let q be the map $\mathbf{E}_K^*\to\mathbf{E}_K^*/\mathbf{E}_K^{1-\sigma}$. Denote by $x\mapsto\overline{x}$ the complex conjugation in K. If $h'\in\mathscr{H}_k^{\rm ar-}\cap\mathrm{Ker}(\mathbf{J}_{K/k})$, then $\mathbf{N}_{k/k^+}(h')=1$ and $\mathcal{V}_{k/k^+}(h')=h'\overline{h'}=1$; if $h'=\mathscr{C}\ell_k(\mathfrak{a})$ 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 Hasse (1985, 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:

$$q(\varepsilon) = q(\zeta) \in q(\mu_K^*) = \mu_K^*/(\mathbf{E}_K^{1-\sigma} \cap \mu_K^*),$$

and the lemma. □

Lemma 11 – *The group $q(\mu_K^*)$, of order 1 or p, is of order p if and only if $\mu_K^* = \langle\zeta_1\rangle$ and $\mathbf{E}_K^{1-\sigma} \cap \langle\zeta_1\rangle = 1$, where ζ_1 is of order p.*

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

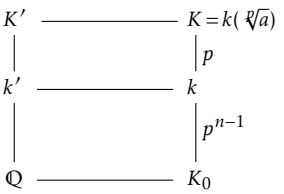
If $\zeta \notin k$, $K = k(\zeta)$; it follows that $\zeta_1 \in k$ and that $\zeta^p \in k$, since $[K : k] = [\mathbb{Q}(\zeta) : k \cap \mathbb{Q}(\zeta)] = p$; thus K/k is a Kummer extension of the form $K = k(\sqrt[p]{\zeta_r})$, ζ_r of order p^r, $r \geq 1$, $\zeta = \zeta_{r+1}$, and $\zeta^{1-\sigma}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

Lemma 12 – *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 $h' \in \mathscr{H}_k^{\mathrm{ar}-} \cap \mathrm{Ker}(\mathbf{J}_{K/k})$, $h' := c\ell_k(\mathfrak{a}) \neq 1$, this means that $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$, $\alpha \in K^\times$; so $\alpha^{1-\sigma} = \varepsilon$, $\varepsilon \in \mathbf{E}_K^*$; from Lemma 11, $q(\varepsilon) = q(\zeta_1)^\lambda$, hence $\varepsilon = \zeta_1^\lambda \eta^{1-\sigma}$, $\eta \in \mathbf{E}_K$, whence $\alpha^{1-\sigma} = \zeta_1^\lambda \eta^{1-\sigma}$ and in the equality $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$ one may suppose α chosen modulo $\mathbf{E}_K$ such that $\alpha^{1-\sigma} = \zeta_1^\lambda$; moreover we have $\lambda \not\equiv 0 \pmod{p}$, otherwise α should be in k and $\mathfrak{a}$ should be principal. Thus $\alpha^{1-\sigma} = \zeta_1'$ of order p and $\alpha^p = a \in k^\times$, whence $K = k(\alpha)$ is the Kummer extension $k(\sqrt[p]{a})$; we have $a\mathbf{Z}_K = \mathfrak{a}^p\mathbf{Z}_K$, hence $a\mathbf{Z}_k = \mathfrak{a}^p$, since extension of ideals is injective. □

We shall show now that the context of Lemma 12 is not possible for a cyclic extension $K/\mathbb{Q}$, which will apply to $K = K_\chi$:

Schema IV



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 above 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 ℓ be a prime number totally ramified in $K'/\mathbb{Q}$ (such a prime does exist since $G_{K'} \simeq \mathbb{Z}/p^n\mathbb{Z}$); this prime is then totally ramified in K/K_0, hence in K/k, 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 ζ of order p^{n+1}.

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

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

Case $p = 2$

The extension $K/\mathbb{Q}$ is still imaginary cyclic, k is necessarily equal to K^+ and σ is the complex conjugation s_∞.

From Hasse (1985, Satz 24) the "index of units" Q_K^- is trivial in the cyclic case; thus for all $\varepsilon \in \mathbf{E}_K^*$, $\varepsilon = \varepsilon^+\zeta$, $\varepsilon^+ \in k$, ζ root of unity of 2-power order; then $\mathbf{N}_{K/k}(\varepsilon) = 1$ yields $\varepsilon^{+2} = 1$, thus $\varepsilon^+ = \pm 1$ and $\varepsilon = \zeta' = \pm\zeta$; since $K/\mathbb{Q}$ is cyclic, whence $\mathbb{Q}(\zeta)/\mathbb{Q}$ cyclic, we shall have $\varepsilon \in \{1, -1, i, -i\}$. Recall that $h' = \mathbf{N}_{K/k}(h) \in \mathrm{Ker}(\mathbf{J}_{K/k})$, $h' = cl_k(\mathfrak{a}) \neq 1$, with $\mathfrak{a}\mathbf{Z}_K = \alpha\mathbf{Z}_K$ and $\alpha^{1-\sigma} = \varepsilon \in \mathbf{E}_K^*$. One may assume $\varepsilon \in \{-1, i, -i\}$ ($\varepsilon \neq 1$ since $\alpha \notin k^\times$):

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

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

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

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

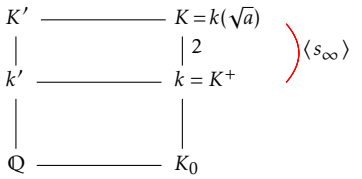
If $d \notin k^{\times 2}$, the relation $\alpha^{2\tau} = \alpha^2 d$ shows that $d = (\alpha^{\tau-1})^2 \in K^{\times 2}$; from Kummer theory, since $K = k(\sqrt{d}) = k(i)$, one obtains $d = -\delta^2$, $\delta \in k^\times$, and $\mathfrak{a}^{2\tau} = \mathfrak{a}^2\delta^2\mathbf{Z}_K$, still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

Schema V



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 3 – *For an imaginary cyclic extension $K/\mathbb{Q}$ and a sub-extension K/k of degree p (i.e., $k = k_p$), $\mathcal{H}_k^{\mathrm{ar}-} \cap \mathrm{Ker}(\mathbf{J}_{K/k}) = 1$ 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 (14) yields:

Corollary 1 – *We get*

$$\mathbf{J}_{K/K^+}(\mathcal{H}_{K^+}) \simeq \mathcal{H}_K^+ = \mathcal{H}_{K^+} = \mathbf{N}_{K/K^+}(\mathcal{H}_K)$$

and the direct sum

$$\mathcal{H}_K = \mathcal{H}_K^{\mathrm{ar}-} \bigoplus \mathbf{J}_{K/K^+}(\mathcal{H}_{K^+}) \simeq \mathcal{H}_K^{\mathrm{ar}-} \bigoplus \mathcal{H}_K^+.$$

We have obtained the following result about relative class groups:

Theorem 6 – *Let $K = K_\chi$ be an imaginary cyclic field of maximal real subfield K^+. Let p be any prime number and set $\mathcal{H} = \mathbf{H} \otimes \mathbb{Z}_p$. Define:*

$$\mathcal{H}_K^{\mathrm{ar}-} := \{h \in \mathcal{H}_K, \mathbf{N}_{K/K^+}(h) = 1\}, \quad \mathcal{H}_K^{\mathrm{alg}-} := \{h \in \mathcal{H}_K, \mathcal{V}_{K/K^+}(h) = 1\}.$$

Then $\mathcal{H}_K^{\mathrm{ar}-} = \mathcal{H}_K^{\mathrm{alg}-}$, $\mathcal{H}_\varphi^{\mathrm{ar}} = \mathcal{H}_\varphi^{\mathrm{alg}}$ for all $\varphi \in \Phi_K^-$.

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

We shall write simply $\mathbf{H}_K^-$ for the two notions "alg" and "ar" in the cyclic case. Using Theorem 4 we may write, for all $\chi\in\mathscr{X}^-$, $\#\mathscr{H}_\chi^{\mathrm{alg}}=\#\mathscr{H}_\chi^{\mathrm{ar}}=\prod_{\varphi|\chi}\#\mathscr{H}_\varphi^{\mathrm{ar}}$.

Corollary 2 – *Let $K/\mathbb{Q}$ be an imaginary cyclic extension. Then:*

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

Proof. To apply Theorem 3, 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. This comes from Remark 1 about cyclic extensions. So Theorem 3 implies $\#\mathbf{H}_K=\prod_{\rho\in\mathscr{X}_K}\#\mathbf{H}_\rho^{\mathrm{ar}}$.

From (14), $\#\mathbf{H}_K=\#\mathbf{H}_K^-\times\#\mathbf{H}_K^+$ and we can also apply Theorem 3 to the maximal real subfield K^+ of K, giving $\#\mathbf{H}_K^+=\prod_{\rho\in\mathscr{X}_K^+}\#\mathbf{H}_\rho^{\mathrm{ar}}$, whence the formulas taking into account the relation $\mathbf{H}_\rho^{\mathrm{ar}}=\mathbf{H}_\rho^{\mathrm{alg}}$ for odd characters (Theorem 6). □

5.3 Computation of $\#\mathbf{H}_\chi^{\mathrm{ar}}$ for $\chi\in\mathscr{X}^-$

For an arbitrary imaginary extension $K/\mathbb{Q}$, we have (e.g., from[44] or[45]), in terms of generalized Bernoulli numbers, the formula:

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

where w_K^- is the order of the group of roots of unity of K and Q_K^- the index of units; from[46], $Q_K^-=1$ when $K=K_\chi$. Recall that $\mathbf{H}_\chi^{\mathrm{ar}}:=\{h\in\mathbf{H}_K,\ \mathbf{N}_{K/k}(x)=1,\text{ for all }k\subsetneq K\}$; then:

Theorem 7 – *Let $\chi\in\mathscr{X}^-$, let g_χ be the order of χ, f_χ its conductor; then*

$$\#\mathbf{H}_\chi^{\mathrm{ar}}=\#\mathbf{H}_\chi^{\mathrm{alg}}=2^{\alpha_\chi}\cdot w_\chi\cdot\prod_{\psi|\chi}\left(-\tfrac{1}{2}\,\mathbf{B}_1(\psi^{-1})\right),$$

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

[44] Hasse, 1985, *Über die Klassenzahl abelscher Zahlkörper. Mit einer Einleitung zur Reprintausgabe von Jacques Martinet.* p. 12.

[45] Washington, 1997, *Introduction to Cyclotomic Fields*, Theorem 4.17.

[46] Hasse, 1985, *Über die Klassenzahl abelscher Zahlkörper. Mit einer Einleitung zur Reprintausgabe von Jacques Martinet.* Satz 24.

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

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

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

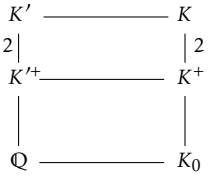
Proof. We use Oriat (1975b, Proposition III (g)) or Leopoldt (1954, Chap. I, § 1 (4)) recalled in Theorem 1; it is sufficient to prove that for any imaginary cyclic extension $K/\mathbb{Q}$, $\#\mathbf{H}_K^- = \prod_{\rho\in\mathscr{X}_K^-}\left(2^{\alpha_\rho}\cdot w_\rho\cdot\prod_{\psi|\rho}\left(-\frac{1}{2}\,\mathbf{B}_1(\psi^{-1})\right)\right)$, the expected equality will come from Theorem 6 and the relation:

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

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

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:

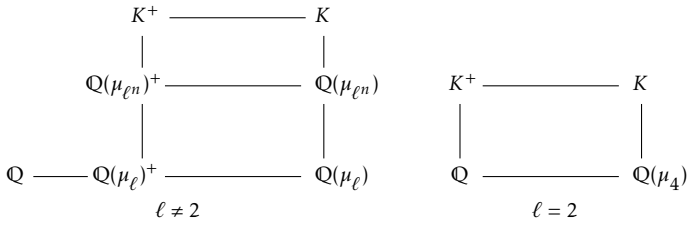
Schema VI



As K^+ and K'^+ are real, $\alpha_\rho = 0$, except when g_ρ is a 2-power, hence for the unique ρ_0 defining K' for which $\alpha_\rho = 1$; whence $\prod_{\rho\in\mathscr{X}_K^-} 2^{\alpha_\rho} = 2$.

If K does not contain any cyclotomic field different from $\mathbb{Q}$, then $w_K^- = 2$, moreover, all the w_ρ are trivial and the required equality holds in that case. So, let $\mathbb{Q}(\mu_{\ell^n})$, $n \geq 1$, be the largest cyclotomic field contained in K; this yields two possibilities:

Schema VII



If $\ell \neq 2$, $\prod_{\rho\in\mathscr{X}_K^-} w_\rho = \ell^n$ (due to the n odd characters defined by the $\mathbb{Q}(\mu_{p^i})$, $1 \leq i \leq n$) and, for $\ell = 2$, this gives $\prod_{\rho\in\mathscr{X}_K^-} w_\rho = 2$; whence the result (cf. Hasse (1985, Chap. III, § 33, Theorem 34 and others)). □

Remark 4 – We have $\#\mathbf{H}_K^- = \frac{Q_K^- w_K^-}{2^{n_K^-}} \prod_{\rho \in \mathscr{X}_K^-} \#\mathbf{H}_\rho^{\mathrm{alg}}$, for any imaginary extension K, 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 Gras (1976, Remarque II 2, p. 32).

5.4 Annihilation theorem for $\mathscr{H}_K^-$

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[47] 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:

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

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

This formula does not generalize for arbitrary imaginary extension $K/\mathbb{Q}$ (see the counterexample given in Gras (1976, p. 33)). Many contributions have appeared[48]; for more precise formulas, see Sinnott (1980) or Washington (1997, § 6.2, § 15.1), among many others. Nevertheless, we gave in Gras (1976) another definition in the spirit of the φ-objects which succeeded to give a correct formula.

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 defined in Gras (1978, Chap.IV, § 1) or Gras (1980, Chap.I, § 1), from the study of partial zêta-functions in Coates (1977, §§ 2.1, 3.2), and that leads to a new normalized definition of Gauss sums; in the summation, integers a are prime to f and Artin symbols are taken over $\mathbb{Q}$:

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

Note that the part $\sum_{a=1}^{f} \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ is the algebraic norm $\mathcal{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}}$ which does not modify the image of $\mathbf{B}_{\mathbb{Q}(\mu_f)}$ by ψ, for $\psi \in \Psi$, $\psi \neq 1$.

[47] Iwasawa, 1962, "A class number formula for cyclotomic fields".

[48] All, 2013, "On p-adic annihilators of real ideal classes";
All, 2017, "Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups";
Coates, 1977, *p-adic L-functions and Iwasawa's theory*;
Gillard, 1974, *Relations de Stickelberger*;
Gras, 1978, "Sommes de Gauss sur les corps finis";
Leopoldt, 1962, "Zur Arithmetik in abelschen Zahlkörpern".

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

$$\begin{cases} \mathbf{S}_K := \mathbf{B}_K\mathbb{Z}[G_K] \cap \mathbb{Z}[G_K], \text{ where} \\ \mathbf{B}_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\mathbf{B}_{\mathbb{Q}(\mu_f)}) = -\sum_{a=1}^{f}\left(\frac{a}{f}-\frac{1}{2}\right)\left(\frac{K}{a}\right)^{-1}. \end{cases} \tag{15}$$

Lemma 13 – *For any c, prime to $2f$, let $\mathbf{B}_K^c := \left(1 - c\left(\frac{K}{c}\right)^{-1}\right)\mathbf{B}_K$; 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 $a'_c c \equiv a \pmod f$; put:

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

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

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

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

$$\mathbf{B}_K^c = \mathbf{B}_K'^c(1 - s_\infty), \ \ \mathbf{B}_K'^c \in \mathbb{Z}[G_K], \tag{16}$$

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

Definition 4 – 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 $\mathbf{S}_K := \mathbf{B}_K\mathfrak{A}_K$ (cf. (15)). 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:

$$\left(1-c\left(\frac{K}{c}\right)^{-1}\right)\sum_{a=1}^{f}\frac{1}{2}\left(\frac{K}{a}\right)^{-1} \in \mathbb{Z}[G_K],$$

and that such considerations only concerns the case $p=2$ when f is an odd prime power with $[\mathbb{Q}(\mu_f) : K]$ odd (see Example A.3 with $K=\mathbb{Q}(\mu_{47})$).

Lemma 14 – *Let α_σ be the coefficient of $\sigma \in G_K$ in the writing of $\sum_{a=1}^{f} a\left(\frac{K}{a}\right)^{-1}$ on the canonical basis G_K of $\mathbb{Z}[G_K]$; in particular, we have $\alpha_1 = \sum_{a,\ \sigma_a|_K=1} a$. Then $\alpha_\sigma \equiv c\,\alpha_1 \pmod f$, where c is a representative modulo f such that $\sigma_c = \sigma^{-1}$. Thus, we have $\Lambda_K = \frac{f}{\gcd(f,\alpha_1)}$.*

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

Proposition 4 – *(i) The ideal $\mathfrak{A}_K$ of $\mathbb{Z}[G_K]$ is a free $\mathbb{Z}$-module; a $\mathbb{Z}$-basis is given by the set $\left\{\cdots, \left(\frac{K}{a}\right)-a, \cdots;\ \Lambda_K\right\}$, 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 Λ_K, where $\left(\frac{K}{c}\right)$ is any generator of G_K.

Proof. See Gras (1976, p. 35–36). □

Study of the algebraic $\mathcal{G}$-families $\mathbf{M}_K := \mathbb{Z}[G_K]$, $\mathbf{S}_K := \mathbf{B}_K\mathfrak{A}_K$

We then have (where $\mathbf{M}_\chi$ and $\mathbf{S}_\chi$ are ideals of $\mathbf{M}_K$):

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

Lemma 15 – *We have*

$$\mathbf{M}_\chi = \prod_{\ell \mid g_\chi,\ \ell\ prime} (1-\sigma_\chi^{g_\chi/\ell})\,\mathbb{Z}[G_K], \quad \mathfrak{a}_\chi := \psi(\mathbf{M}_\chi) = \prod_{\ell \mid g_\chi}\left(1-\psi(\sigma_\chi)^{g_\chi/\ell}\right).$$

Then $\mathbf{S}_\chi$ gives rise to an ideal $\mathfrak{b}_\chi$ multiple of $\mathfrak{a}_\chi$.

Proof. See Gras (1976, 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 classical formulas (see, e.g., Gras (2018a, Section 4)):

Lemma 16 – *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:*

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

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

$$\begin{cases} \mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}\left(\mathbf{B}_{\mathbb{Q}(\mu_f)}\right) = \Omega\cdot\mathbf{B}_{\mathbb{Q}(\mu_m)}, \\ \mathbf{N}_{\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_m)}\left(\eta_{\mathbb{Q}(\mu_f)}\right) = \eta_{\mathbb{Q}(\mu_m)}^{\Omega}, \end{cases}$$

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

We can conclude by the following[49]:

Theorem 8 – *Let $\chi \in \mathscr{X}^-$ and let $\psi \mid \chi$, $\psi \in \Psi$. The $\mathbb{Z}[\mu_{g_\chi}]$-module $\mathbf{H}_\chi^{\mathrm{alg}} = \mathbf{H}_\chi^{\mathrm{ar}}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1})(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}[\mu_{g_\chi}]$, where $\sigma_a := \left(\frac{K}{a}\right)$ is any generator of G_K (Lemma 14, Proposition 4). The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ is the unit ideal except if $K \neq \mathbb{Q}(\mu_4)$ 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 $K = \mathbb{Q}(\mu_4)$, this ideal is the ideal* (4).

Theorem 9 – *Let $\varphi \in \Phi^-$ and let $\psi \mid \varphi$, $\psi \in \Psi$. Then the $\mathbb{Z}_p[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi^{\mathrm{alg}} = \mathscr{H}_\varphi^{\mathrm{ar}}$ is annihilated by the ideal $\mathbf{B}_1(\psi^{-1})(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$, where σ_a is any generator of G_K. The ideal $(\psi(\sigma_a)-a, \Lambda_\chi)$ of $\mathbb{Z}_p[\mu_{g_\chi}]$ is the unit ideal except if $K \neq \mathbb{Q}(\mu_4)$ is extension of $\mathbb{Q}(\mu_p)$ of p-power degree, if $\Lambda_\chi \equiv 0 \pmod p$ and if $\lambda = 1$ in the writing $\psi = \omega^\lambda\psi_p$ (where ω is the Teichmüller character and ψ_p of p-power order), in which case, this ideal is the prime ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$. If $K = \mathbb{Q}(\mu_4)$, this ideal is the ideal* (4).

[49] Gras, 1976, "Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes", Théorèmes II.5, II.6.

We have detailed, in Appendix A.3, the case of $K := K_\chi = \mathbb{Q}(\mu_{47})$ by computing $\#\mathbf{H}_\chi$ by means of the Bernoulli number with some annihilation properties.

In Gras (1978, Chap. IV, § 2 & Théorème IV1) and Gras (1979b, 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:

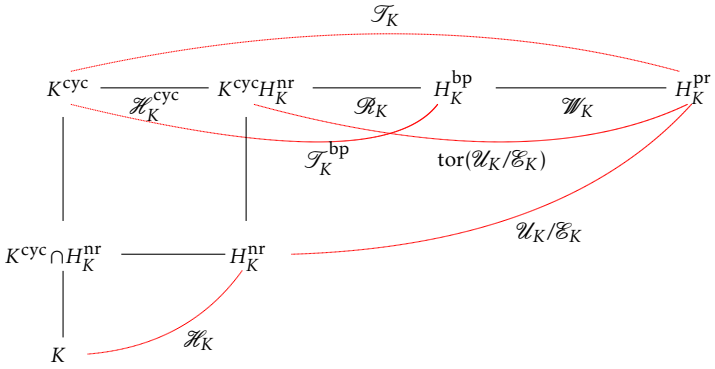
Theorem 10 – *Let $\chi \in \mathscr{X}^-$ and let $\psi \mid \varphi \mid \chi$ with $\psi = \psi_0\,\psi_2$, $\psi_0 \neq 1$ of even order, ψ_2 of 2-power order. The $\mathbb{Z}_2[\mu_{g_\chi}]$-module $\mathscr{H}_\varphi \big/ \mathbf{J}_{K/K^+}(\mathscr{H}^+_{\varphi'})$ is annihilated by $\left(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)$, where $\mathscr{H}^+_{\varphi'} := \{h \in \mathscr{H}_{K^+},\ x^{P_{\varphi'}(\sigma_\chi)} = 1\}$, with $\varphi' \in \Phi^+$ above $\psi' := \psi_0\,\psi_2^2$.*

6 Application to torsion groups of abelian p-ramification

Let K be a totally real number field, non necessarily abelian, 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[50]; the $\mathbb{Z}_p$-module $\mathscr{T}_K^{\rm bp} := {\rm Gal}(H_K^{\rm bp}/K^{\rm cyc})$ is the Bertrandias–Payan module (Nguyen Quang Do (1986, Sec. 4), Jaulent (1990, Sec. 2 (b))).

Schema VIII



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

$$1 \to \mathscr{W}_K \longrightarrow {\rm tor}_{\mathbb{Z}_p}\left(\mathscr{U}_K \big/ \mathscr{E}_K\right) \xrightarrow{\log_p} \mathscr{R}_K := {\rm tor}_{\mathbb{Z}_p}\left(\log_p(\mathscr{U}_K) \big/ \log_p(\mathscr{E}_K)\right) \longrightarrow 0 \quad (17)$$

[50] Bertrandias and Payan, 1972, "Γ-extensions et invariants cyclotomiques".

where $\mathscr{U}_K$ denotes the group of local units at p, $\mathscr{E}_K = \mathbf{E}_K \otimes \mathbb{Z}_p$ is identified with its diagonal image in $\mathscr{U}_K$, $\mathscr{W}_K := \left(\bigoplus_{v|p} \mu_p(K_v)\right)/\mu_p(K)$ (see Gras (2005, § III.2, (c), Fig. 2.2, Lemma III.4.2.4) and Gras (2018b)).

Since $[\mathbb{Q}_p(\mu_{p^e}) : \mathbb{Q}_p] = (p-1)p^{e-1}$, for K fixed there are only finite number of primes p such that $\mathscr{W}_K \neq 1$; for K totally real $\mu_p(K) = 1$ for all $p > 2$. For instance, if $K = \mathbb{Q}(\sqrt{m})$ is a real quadratic field, then for $p = 2$, $\mathscr{W}_K \simeq \mu_2 \times \mu_2/\mu_2$ (2 split in K) or μ_4/μ_2 ($m \equiv -1 \pmod 8$); for $p = 3$, $\mathscr{W}_K \simeq \mu_3$ if and only if $m \equiv -3 \pmod 9$.

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

6.1 Computation of $\#\mathscr{T}_K$

The order of the $\mathbb{Z}_p[G_K]$-module $\mathscr{T}_K$ is given, analytically, by the residue at $s = 1$ of the p-adic ζ-function of K, whence by the values at $s = 1$ of p-adic $\mathbf{L}$-functions of the non-trivial characters of K (after[51]); see for instance[52] for analytic context.

In conclusion we can write, up to p-adic units:

$$\#\mathscr{T}_K = \#\mathscr{H}_K^{\mathrm{cyc}} \times \#\mathcal{R}_K \times \#\mathcal{W}_K \sim [K \cap \mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}] \prod_{\psi \neq 1} \tfrac{1}{2}\, \mathbf{L}_p(1, \psi). \tag{18}$$

Since the arithmetic family of these $\mathbb{Z}_p[\mathscr{G}]$-modules $\mathscr{T}_K$, for real K's, follows the most favorable properties (i.e. surjectivity of the norms, injectivity of the transfer maps in relative sub-extensions), we can state, in a similar context as for Theorems 6:

Theorem 11 – *For all $\chi \in \mathscr{X}^+$ (resp. $\varphi =: \varphi_0\varphi_p \mid \chi$), $K = K_\chi$, then:*

$$\begin{cases} \mathscr{T}_\chi^{\mathrm{ar}} = \mathscr{T}_\chi^{\mathrm{alg}} = \{x \in \mathscr{T}_K,\ x^{P_\chi(\sigma_\chi)} = 1\} \\ \qquad\qquad\quad = \{x \in \mathscr{T}_K,\ \mathbf{N}_{K/k}(x) = 1,\ \textit{for all } k \subsetneq K\}, \\ \mathscr{T}_\varphi^{\mathrm{ar}} = \mathscr{T}_\varphi^{\mathrm{alg}} = \{x \in \mathscr{T}_K,\ x^{P_\varphi(\sigma_\chi)} = 1\} = (\mathscr{T}_\chi^{\mathrm{ar}})_{\varphi_0}. \end{cases}$$

Moreover, if $K/\mathbb{Q}$ is real, $\#\mathscr{T}_K = \prod_{\rho \in \mathscr{X}_K} \#\mathscr{T}_\rho^{\mathrm{ar}} = \prod_{\varphi \in \Phi_K} \#\mathscr{T}_\varphi^{\mathrm{ar}}$.

We denote simply $\mathscr{T}_\chi^{\mathrm{ar}}$ (resp. $\mathscr{T}_\varphi^{\mathrm{ar}}$) these components in the algebraic or arithmetic senses. In the analytic point of view, we have the analogue of Theorems 7 and 14 (see some p-adic formulas about $\mathbf{L}_p$-functions, from classical papers[53] and a broad presentation in Washington (1997, Theorems 5.18, 5.24)):

[51] Coates, 1977, *p-adic L-functions and Iwasawa's theory*, Appendix.

[52] Gras, 2019a, "Heuristics and conjectures in direction of a p-adic Brauer-Siegel theorem", § 3.4, formula (3.8).

[53] Amice and Fresnel, 1972, "Fonctions zêta p-adiques des corps de nombres abéliens réels";
Gras, 1980, *Sur la construction des fonctions L p-adiques abéliennes*;
Kubota and Leopoldt, 1964, "Eine p-adische Theorie der Zetawerte. I: Einführung der p-adischen Dirichletschen L-Funktionen".

Theorem 12 – *Let $\chi \in \mathscr{X}^+ \setminus \{1\}$. Then $\#\mathscr{T}_\chi^{\rm ar} \sim w_\chi^{\rm cyc} \prod_{\psi|\chi} \frac{1}{2}\mathbf{L}_p(1,\psi)$, where $w_\chi^{\rm cyc}$ is as follows, from analytic formula* (18)*:*

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

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

6.2 Annihilation theorem for $\mathscr{T}_K$

An annihilator of $\mathscr{T}_K$ is given by the following statement[54] which does not assume any hypothesis on K (real) and p and gives again the following results (recall for instance Gras (1979a), Oriat (1981)):

Theorem 13 – *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 $a'_c c \equiv a \pmod{f_n}$ and put $a'_c c - a = \lambda_a^n(c)\, f_n$, $\lambda_a^n(c) \in \mathbb{Z}$. Then consider:*

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

where s_∞ is the complex conjugation and $\mathbf{A}'_{K,n}(c) = \sum_{a=1}^{f_n/2} \lambda_a^n(c)\, a^{-1} \left(\frac{K}{a}\right)$.

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

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

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

It is immediate, using these formulas modulo a suitable power of p, to compute annihilators; examples are given in Appendix A.4.

Remarks 2 – (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 $\mathbf{A}_K(c)$ is related to p-adic $\mathbf{L}$-functions via the formula:

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

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

This theorem is the analog of Theorem 9, using Bernoulli's numbers, linked to $\mathbf{L}_p(0, \omega\psi^{-1})$, instead of $\mathbf{L}_p(1,\psi)$.

[54] Gras, 2018a, "Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{G}_{K,S}^{\rm ab})$ for real abelian extensions $K/\mathbb{Q}$", Theorem 5.5.

(ii) Some other annihilation theorems exist for the Jaulent logarithmic class group[55]; then Jaulent (2023) is related to Greenberg's conjecture and, when K contains μ_p, Jaulent (2021) 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 "FAMC" about the φ-components of these modules.

(iii) Using Gras (1986, Théorème (0.3)) and Gras (1987, Théorème (0.2)), we know that the normalized valuation of p-adic $\mathbf{L}$-functions fulfills the condition $v_p(\frac{1}{2}\mathbf{L}_p(s,\psi)) \geq \mathbf{C}$ for all $s \in \mathbb{Z}_p$, for some explicit constant $\mathbf{C}$ and that either there is equality for all $s \in \mathbb{Z}_p$ or strict inequality for all $s \in \mathbb{Z}_p$. Thus, when equality holds, one obtains other orders and annihilation theorems (e.g., that of Hilbert's kernels of $\mathbf{K}$-theory for $p \in \{2,3\}$ in Gras (2024a)).

7 Application to class groups of real abelian fields

Denote by $\mathbf{E}$ the $\mathcal{G}$-family for which $\mathbf{E}_K$, $K \in \mathscr{K}$, is the group of absolute value of the global units of K, the Galois action being defined by $|\varepsilon|^\sigma = |\varepsilon^\sigma|$ for any unit ε and any $\sigma \in \mathcal{G}$. As we explain in the beginning of the Appendix for explicit computations, conjugates of algebraic numbers are managed by PARI in a coherent manner corresponding to an (unknown) embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$; thus $|\ |$ is, for us, the real absolute value, taken after a fixed embedding $K \to \mathbb{R}$, or after PARI numerical results.

The $\mathbf{E}_K$'s are free $\mathbb{Z}$-modules of rank $[K:\mathbb{Q}]-1$ for real fields K.

7.1 The Leopoldt χ-units

In Leopoldt (1954, 1962) are defined unit groups, $\mathbf{E}_\chi$, that we shall call, as in Oriat (1975b), the group of χ-units for rational characters $\chi \in \mathscr{X}^+ \setminus \{1\}$; from the definition of χ-objects in $K = K_\chi$ and the results of the previous sections we can write, where $\mathcal{V}$ may be replaced by $\mathbf{N}$:

$$\mathbf{E}_\chi = \left\{|\varepsilon| \in \mathbf{E}_K,\ |\varepsilon|^{P_\chi(\sigma_\chi)} = 1\right\} = \left\{|\varepsilon| \in \mathbf{E}_K,\ \mathcal{V}_{K/k}(|\varepsilon|) = 1, \text{ for all } k \subsetneq K\right\}. \tag{19}$$

What follows is also available in Leopoldt (1954, 1962) and Oriat (1975b).

Definitions 2 – (i) For any cyclic real field $K = K_\chi$, denote by $\widehat{\mathbf{E}}_K$ the subgroup of $\mathbf{E}_K$ generated by the $\mathbf{E}_k$'s for all the subfields $k \subsetneq K$ (or simply by each of the k_ℓ such that $[K:k_\ell] = \ell \mid [K:\mathbb{Q}]$, ℓ prime).

[55] Jaulent, 2021, "Annulateurs de Stickelberger des groupes de classes logarithmiques"; Jaulent, 2023, "Annulateurs circulaires des groupes de classes logarithmiques".

(ii) Let $Q_K = \left(\mathbf{E}_K : \bigoplus_{\rho\in\mathscr{X}_K} \mathbf{E}_\rho\right)$ where $\mathbf{E}_\rho$ is the group of ρ-units (Definition (19)) and, for all $\rho \in \mathscr{X}^+$, let $Q_\rho = \left(\mathbf{E}_{K_\rho} : \widehat{\mathbf{E}}_{K_\rho} \bigoplus \mathbf{E}_\rho\right)$.

(iii) Let ϕ be the Euler totient function and put, for $\rho \in \mathscr{X}^+$:

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

Set $q_K = \left(\frac{g^{g-2}}{\prod_{\rho\in\mathscr{X}_K} d_\rho}\right)^{\frac{1}{2}}$, where $g := [K : \mathbb{Q}]$ and d_ρ is the discriminant of $\mathbb{Q}(\mu_{g_\rho})$.

Lemma 17 – *(i) We have $\widehat{\mathbf{E}}_{K_\rho}\mathbf{E}_\rho = \widehat{\mathbf{E}}_{K_\rho} \bigoplus \mathbf{E}_\rho$, for all $\rho \in \mathscr{X}^+$.*

(ii) For all cyclic real field K, $Q_K = \prod_{\rho\in\mathscr{X}_K} Q_\rho$, Gras (1976, pp. 72–75).

(iii) For all cyclic real field K, $q_K = \prod_{\rho\in\mathscr{X}_K} q_\rho$, Gras (1976, pp. 76–77).

Proof. (i) One may find various equivalent definitions of the χ-units and their properties in Leopoldt (1954, Chap. 5, § 4) or Oriat (1975b); but knowing the norm characterization (19) of $\mathbf{E}_\chi$, the proof of (i) is obvious.

(ii) This may be proved locally; for this, we use the $\mathcal{G}$-family $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$, for any prime p and $\mathscr{E}_\chi \simeq \mathbf{E}_\chi \otimes \mathbb{Z}_p$ defined as above. Then one uses, inductively, Lemma 17 (i) with characters $\psi \mid \varphi \mid \chi$, written as $\psi = \psi_0\,\psi_p$ (ψ_0 of prime-to-p order, ψ_p of non-trivial p-power order). Let k_p be the subfield of K of relative degree p. We implicitly consider the χ_0-components for the rational (semi-simple) character above ψ_0, which allows to write for instance $(\widehat{\mathscr{E}_K})_{\chi_0} = (\mathscr{E}_{k_p})_{\chi_0}$ and any integer A replaced by its p-part (A_p); in what follows, we omit the indices χ_0 and p.

Assume to have proved $Q_{k_p} := \left(\mathscr{E}_{k_p} : \bigoplus_{\widetilde{\rho}\in\mathscr{X}_{k_p}} \mathscr{E}_{\widetilde{\rho}}\right) = \prod_{\widetilde{\rho}\in\mathscr{X}_{k_p}} Q_{\widetilde{\rho}}$; then:

$$\begin{aligned} Q_{k_p} \times Q_\chi &= \left(\mathscr{E}_{k_p} : \oplus_{\widetilde{\rho}\in\mathscr{X}_{k_p}} \mathscr{E}_{\widetilde{\rho}}\right) \times (\mathscr{E}_K : \widehat{\mathscr{E}_K} \oplus \mathscr{E}_\chi) \\ &= \left(\mathscr{E}_{k_p} \oplus \mathscr{E}_\chi : \oplus_{\widetilde{\rho}\in\mathscr{X}_{k_p}} \mathscr{E}_{\widetilde{\rho}} \oplus \mathscr{E}_\chi\right) \times (\mathscr{E}_K : \mathscr{E}_{k_p} \oplus \mathscr{E}_\chi) \\ &= (\mathscr{E}_K : \oplus_{\rho\in\mathscr{X}_K} \mathscr{E}_\rho) = Q_K. \end{aligned}$$

(iii) From Hasse (1985, § 15, p. 34, (2), p. 35). □

7.2 The Leopoldt cyclotomic units

For the main definitions and properties of cyclotomic units, see Leopoldt (1954, § 8 (1)) or Oriat (1975a).

Definitions 3 – (i) Let $\chi \in \mathscr{X}^+$ of conductor f_χ; we define the "cyclotomic numbers" $\mathbf{C}_\chi := \prod_{a \in A_\chi} (\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a})$, with $\zeta_{2f_\chi} := \exp\left(\frac{i\pi}{f_\chi}\right)$, where A_χ is a half-system of representatives, in $(\mathbb{Z}/f_\chi\mathbb{Z})^\times$, of $\mathrm{Gal}(\mathbb{Q}(\mu_{f_\chi})/K_\chi)$.

(ii) Let K be a real abelian field and let $\mathbf{C}_K$ be the multiplicative group generated by the conjugates of $|\mathbf{C}_\rho|$, for all $\rho \in \mathscr{Z}_K$. Then we define the group of cyclotomic units $\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K$ and $\mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p$.

Recall that $\mathbf{C}_\rho^2 \in K_\rho^\times$ and that any conjugate $\mathbf{C}'_\rho$ of $\mathbf{C}_\rho$ is such that $\frac{\mathbf{C}'_\rho}{\mathbf{C}_\rho} \in \mathbf{E}_{K_\rho}$. If f_ρ is not a prime power, then $\mathbf{C}_\rho$ is a unit and $\mathbf{F}_{K_\rho} = \mathbf{C}_{K_\rho}$. The following formula links the definitions of $\mathbf{C}_\rho$ and $\eta_\rho := 1 - \zeta_{f_\rho}$:

$$\mathbf{C}_\rho^2 = (-1)^{\#A_\rho} \mathbf{N}_{\mathbb{Q}(\zeta_{f_\rho})/K_\rho}(1 - \zeta_{f_\rho}) =: (-1)^{\#A_\rho} \eta_{K_\rho} \in K_\rho^\times, \tag{20}$$

where $\eta_{K_\rho} = \mathbf{N}_{\mathbb{Q}(\zeta_{f_\rho})/K_\rho}(1 - \zeta_{f_\rho})$ (e.g., Oriat (1975b, IV, § 1)).

7.3 Arithmetic computation of $\#\mathbf{H}_\chi^{\mathrm{ar}}$, for $\chi \in \mathscr{X}^+$

Using the Leopoldt formula[56] and Lemma 17 (ii), (iii), we obtain (see Gras (1976, Théorème III.1)):

Proposition 5 – *For $\chi \in \mathscr{X}^+ \setminus \{1\}$, let $\Delta_\chi = \prod_{\ell \mid g_\chi, \ell\, prime} \left(1 - \sigma_\chi^{g_\chi/\ell}\right)$; then*

$$\#\mathbf{H}_\chi^{\mathrm{ar}} = \frac{Q_\chi}{q_\chi}(\mathbf{E}_\chi : \mathbf{C}_\chi^{\Delta_\chi}) \quad \textit{and} \quad \#\mathbf{H}_\chi^{\mathrm{ar}} = \frac{1}{q_\chi}\left(\mathbf{E}_K : \widehat{\mathbf{E}}_K \bigoplus \mathbf{C}_\chi^{\Delta_\chi}\right) \quad \textit{for } K = K_\chi,$$

interpreting Q_χ[57].

To interpret the coefficient q_χ, we have replaced the Leopoldt group $\mathbf{C}_\chi^{\Delta_\chi}$ of cyclotomic units by the larger group $\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K$ (Definition 3); whence the main final result interpreting the coefficient q_χ and giving the analog of Theorem 7 for real class groups:

[56] Leopoldt, 1954, "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper", Satz 21, § 8 (4).

[57] Gras, 1976, "Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes", Corollaire III.1.

Theorem 14 – *For $K = K_\chi$, $\chi \in \mathscr{X}^+ \setminus \{1\}$, of order g_χ and conductor f_χ, let*

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

Then:

$$\#\mathbf{H}_\chi^{\rm ar} = w_\chi \left(\mathbf{E}_K : \widehat{\mathbf{E}}_K \mathbf{F}_K\right),$$

where w_χ is defined as follows:

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

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

(ii') Case f_χ prime-power. Then $w_\chi = 1$;

(ii") Case f_χ non prime-power. Then $w_\chi = \ell$;

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

(iii') Case f_χ prime-power. Then $w_\chi = 1$;

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

Proof. For the original proof see Gras (1976, Théorème III.2, pp. 78–85), done by localization in the spirit of the proof of Lemma 17 using χ_0-components. In other words, let $\mathscr{C}_\chi := \mathbf{C}_\chi \otimes \mathbb{Z}_p$; then the claim is equivalent to prove that $(\mathscr{E}_{k_p}\mathscr{F}_{k_p} : \mathscr{E}_{k_p} \oplus \mathscr{C}_\chi^{\Delta_\chi}) = q_\chi$. For $\chi_0 \neq 1$, this equality becomes $(\mathscr{E}_{k_p}\mathscr{C}_{k_p} : \mathscr{E}_{k_p} \oplus \mathscr{C}_\chi^{\Delta_\chi}) = q_\chi$ which simply relies on Δ_χ and gives point (i); the case of a character of p-power order depends on the Galois action on cyclotomic units, hence of the conductor of χ and gives rise to the coefficient $w_\chi \in \{1, \ell\}$. □

Corollary 3 – *If $p \nmid g_\chi$, $\#\mathscr{H}_\chi = \left(\mathscr{E}_\chi : \mathscr{F}_\chi\right) = \prod_{\varphi|\chi} \left(\mathscr{E}_\varphi : \mathscr{F}_\varphi\right)$, where $\mathscr{E}_\varphi = \mathscr{E}_K^{e_\varphi}$ and $\mathscr{F}_\varphi = \left(\langle \mathbf{C}_\chi \rangle \otimes \mathbb{Z}_p\right)^{e_\varphi}$ now giving the semi-simple Main Theorem of the literature $\#\mathscr{H}_\varphi = \left(\mathscr{E}_\varphi : \mathscr{F}_\varphi\right)$.*

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, $\widetilde{\mathscr{E}}_\chi = \widetilde{\mathscr{E}}_\chi^{e_\chi} = \mathscr{E}_K^{e_\chi}/\widetilde{\mathscr{E}}_K^{e_\chi}\mathscr{F}_K^{e_\chi} = \mathscr{E}_\chi/\mathscr{F}_\chi$, since $\widetilde{\mathscr{E}}_K^{e_\chi} = 1$. The claim for $\varphi \mid \chi$ is the Main Theorem known in the semi-simple context. □

Remarks 3 – The viewpoint given by Theorem 14, which appears to have been ignored, seems more convenient than formulas trying to use Sinnott's cyclotomic units. Indeed, compare with Greither (1992, Theorem 4.14) using instead $\mathscr{H}_\chi^{\rm alg}$ (in a partial semi-simple context as explained in Remark 8) and Sinnott's group of

cyclotomic units, larger than classical Leopoldt's group of Definition 3, but which gives rise to intricate index formulas. For the Iwasawa context, see for instance Nguyen Quang Do and Lescop (2006).

Moreover, as we have mentioned in Gras (1977b, Remark III.1), an analytic formula for $\#\mathscr{H}_\chi^{\mathrm{alg}}$, $\chi \in \mathscr{X}^+$, does not seem obvious (if any) because of capitulation aspects (see the examples of Appendix A.2).

Theorem 14 suggests a new and simpler statement of the FAMC for the $\mathscr{H}_\varphi$'s, especially in the non semi-simple real case (see § 8.2 for the corresponding analytic values).

Recent publications[58] greatly strengthen the definition of the FAMC, using the algebraic χ-objects $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_K/\widetilde{\mathscr{E}}_K\mathscr{T}_K$ with the semi-simple decompositions:

$$\widetilde{\mathscr{E}}_\chi = \bigoplus_{\varphi|\chi} \widetilde{\mathscr{E}}_\varphi = \bigoplus_{\varphi|\chi} \left\{\widetilde{x} \in \widetilde{\mathscr{E}}_\chi,\ \widetilde{x}^{P_\varphi(\sigma_\chi)} = 1\right\} = \bigoplus_{\varphi|\chi} (\widetilde{\mathscr{E}}_\chi)_{\varphi_0}.$$

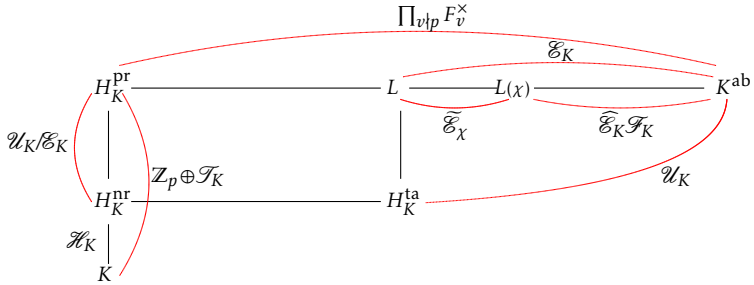
7.4 Interpretations from class field theory and regulators

Let $K \in \mathscr{K}$ be a real cyclic field defining $\chi \in \mathscr{X}^+$ in what follows. To simplify some diagrams in this subsection, we assume to be in the case where $\mathscr{W}_K = 1$ and $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, which gives $\mathscr{T}_K = \mathscr{T}_K^{\mathrm{bp}}$ (cf. Diagram of Section 6) and $\#\mathscr{T}_K \sim \prod_{\psi|\chi,\,\psi\neq 1} \frac{1}{2}\mathbf{L}_p(1,\psi)$ (Formula (18)). Otherwise, formulas are modified by means of standard coefficients or indices which do not modify the philosophy of the results/conjectures; moreover the character of $\mathscr{W}_K$, related to local cyclotomic Teichmüller ones, gives trivial information for conjectural aspects.

The Galois group $\mathscr{R}_K \subseteq \mathscr{T}_K$ may be compared with a larger "cyclotomic regulator" $\mathscr{R}_K^{\mathrm{cyc}}$ interpreted as a Galois group only depending of χ. For this purpose, the following diagram of the maximal abelian pro-p-extension K^{ab} of K is necessary (from Gras (2005, III.4 (d) & Diagram III.4.4.1) with our present notations), where H_K^{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 $L := H_K^{\mathrm{pr}} H_K^{\mathrm{ta}}$:

[58] Gras, 2023a, "Algebraic norm and capitulation of p-class groups in ramified cyclic p-extensions";
Gras, 2023b, "The Chevalley–Herbrand formula and the real abelian Main Conjecture (New criterion using capitulation of the class group)";
Gras, 2024b, "The real abelian main conjecture in the non semi-simple case".

Schema IX



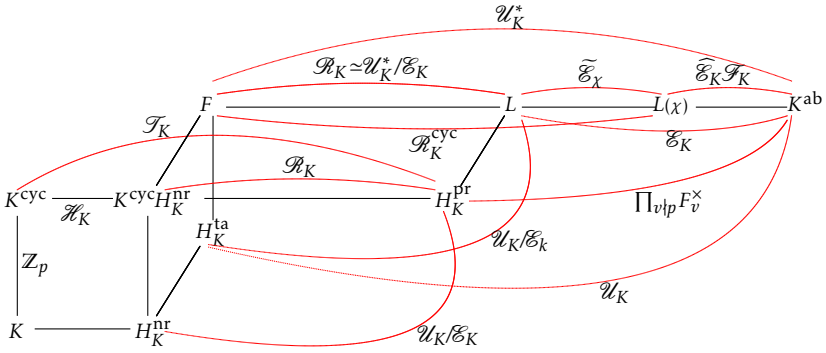
In this diagram, class field theory interprets $\mathrm{Gal}(K^{\rm ab}/H_K^{\rm ta})$ as the $\mathbb{Z}_p$-module $\mathscr{U}_K$ of principal local units at p (isomorphic to the direct product of the inertia groups of the p-places) and $\mathrm{Gal}(K^{\rm ab}/L)$ as the $\mathbb{Z}_p$-module $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$ (embedded both in $\mathscr{U}_K$ and the product $\prod_{v\mid p} F_v^\times$ of the inertia groups of the tame places, with suitable Artin maps described in Gras (2005, § III.4.4.5.1)).

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 $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{U}_K/\mathscr{E}_K) = \mathscr{U}_K^*/\mathscr{E}_K \simeq \mathscr{R}_K$.

Assume $K^{\rm cyc} \cap H_K^{\rm nr} = K$ to simplify; so $H_K^{\rm ta} \cap K^{\rm cyc} = H_K^{\rm nr}$ 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 $1 \to \mathscr{R}_K^{\rm ram} \to \mathscr{R}_K \to \mathscr{R}_K^{\rm nr} \to 1$[59], due to genus theory; so, a sub-extension of L/F may be unramified.

We have moreover $\mathrm{Gal}(F/K^{\rm cyc}H_K^{\rm nr}) \simeq \mathrm{Gal}(L/H_K^{\rm pr}) \simeq \left(\prod_{v\mid p} F_v^\times\right)/\mathscr{E}_K$:

Schema X



Define, under the previous assumptions, $\mathscr{R}_K^{\rm cyc} := \mathscr{U}_K^*/\widehat{\mathscr{E}}_K\mathscr{F}_K$, which yields, for $\chi \neq 1$ and $K = K_\chi$, the $\mathbb{Z}_p[G_K]$-modules isomorphism:

$$\mathscr{R}_K \simeq \mathscr{R}_K^{\rm cyc}/\widetilde{\mathscr{E}}_\chi. \tag{21}$$

[59] Gras, 2021, "Algorithmic complexity of Greenberg's conjecture", § 2 & Figure 3.

We then have $\mathscr{R}_K^{\rm cyc} \simeq {\rm Gal}(L(\chi)/F)$, where $L(\chi)$ is the subfield of $K^{\rm ab}$ fixed by the image of $\widehat{\mathscr{E}}_K\mathscr{F}_K$.

Remark 5 – Let $\chi \in \mathscr{X}^+ \setminus \{1\}$, $K = K_\chi$; assume to simplify that $\mathscr{W}_K = 1$, $w_\chi = 1$ in Theorem 14, $K \cap \mathbb{Q}^{\rm cyc} = \mathbb{Q}$ and $K^{\rm cyc} \cap H_K^{\rm nr} = K$:

(i) Theorem 14 and isomorphism (21) give the χ-components:

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

The $\mathscr{A}_\chi$-modules $\mathscr{T}_\chi^{\rm ar}$ and $\mathscr{R}_\chi^{\rm cyc}$ (resp. $\widetilde{\mathscr{E}}_\chi$ and $\mathscr{H}_\chi^{\rm ar}$) are not necessarily isomorphic as shown by the following excerpt giving cyclic cubic fields K such that $\mathscr{R}_\chi$ is of 7-rank 2 and $\mathscr{T}_\chi^{\rm ar}$ of 7-rank ≥ 3 implying $\mathscr{H}_\chi \neq 1$ with $\mathscr{H}_\chi \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ for the followings (no example of 7-rank ≥ 4 exists in the interval considered):

```
x^3+x^2-39666*x-2582719        7-torsion group: [7,7,7]
x^3+x^2-43300*x-3411104        7-torsion group: [7^2,7,7]
x^3+x^2-13226*x-508479         7-torsion group: [7^3,7,7]
x^3+x^2-427660*x-31551829      7-torsion group: [7^4,7,7]
x^3+x^2-2033484*x-966131001    7-torsion group: [7^2,7^2,7]
```

(ii) The sub-diagram given by the extension $K^{\rm ab}/K^{\rm cyc}$, opens an access way for an interpretation of the FAMC for even characters or at least for an annihilation theorem of $\mathscr{H}_\varphi^{\rm ar}$ by $\widetilde{\mathscr{E}}_\varphi$, in the spirit of Thaine's theorem (see § 7.6, Conjectures 1, 2). Indeed, $\widetilde{\mathscr{E}}_\chi$ has same order as $\mathscr{H}_\chi^{\rm ar}$ and the units may be seen diagonally embedded in the (infinite) product of the places of K. Remark that $\widetilde{\mathscr{E}}_\varphi$ is a sub-module of $\mathscr{R}_\varphi^{\rm cyc}$ (quotient $\mathscr{R}_\varphi$) but $\mathscr{H}_\varphi^{\rm ar}$ is the quotient of $\mathscr{T}_\varphi^{\rm ar}$, by $\mathscr{R}_\varphi$.

7.5 Annihilation conjecture for real p-class groups

Before any proof of the conjectural equality $\#\mathscr{H}_\varphi^{\rm ar} = \#\widetilde{\mathscr{E}}_{\varphi_0} = \#(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$ (giving a Main Theorem for $\varphi \in \Phi_K^+$), it will be interesting to prove that any annihilator of $\widetilde{\mathscr{E}}_{\varphi_0}$ annihilates $\mathscr{H}_\varphi^{\rm ar}$, which will be more precise than the annihilators of $\mathscr{T}_\varphi^{\rm ar}$ (see Theorem 6.2, Remarks 2, 5).

To our knowledge, the best known annihilation theorem of real p-class groups is Thaine's Theorem[60], Washington (1997, Theorem 15.2) saying that any annihilator of $\mathscr{E}_K/\mathscr{F}_K'$ (for a suitable definition of the group of cyclotomic units $\mathscr{F}_K'$) is an annihilator of $\mathscr{H}_K$. But Thaine's Theorem only concerns the semi-simple case.

Mention also annihilation theorems by Solomon[61], which are not often optimal because of vanishing of Euler factors; we have discussed this in Gras (2018a). Finally

[60] Thaine, 1988, "On the ideal class groups of real abelian number fields".

[61] Solomon, 1992, "On a construction of p-units in abelian fields".

mention the numerous papers of Greither and Kučera, like Greither and Kučera (2014, 2015, 2021), on the annihilation of real class groups, using special units or/and giving information on the Fitting ideals.

Conjecture 1 – *Let $\chi \in \mathscr{X}^+$ be distinct from* 1, *let $K = K_\chi$, and let $\varphi \mid \chi$. Any element of $\mathbb{Z}[\mu_{g_\chi}]$ (resp. $\mathbb{Z}_p[\mu_{g_\chi}]$) annihilating $\mathbf{E}_K/\widehat{\mathbf{E}}_K\mathbf{F}_K$ (resp. $(\mathscr{E}_K/\widehat{\mathscr{E}_K\mathscr{F}_K})_{\varphi_0}$), annihilates $\mathbf{H}^{\rm ar}_\chi$ (resp. $\mathscr{H}^{\rm ar}_\varphi$).*

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

Lemma 18 – *Let $\mathbf{M}_K$, $K = K_\chi$, be a torsion-free $\mathbb{Z}[G_K]$-module such that $\mathbf{M}_K \otimes \mathbb{Q}_p$ is $\mathbb{Q}_p[G_K]$-monogenic and $\mathbf{M}'_K$ a sub-module of finite index of $\mathbf{M}_K$ such that $P_\chi(\sigma_\chi)\mathbb{Z}[G_K]$ annihilates $\mathbf{M}_K/\mathbf{M}'_K$. Then $(\mathscr{M}_K/\mathscr{M}'_K)_\varphi := ((\mathbf{M}_K/\mathbf{M}'_K)\otimes\mathbb{Z}_p)_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{\lambda_\varphi}$, $\lambda_\varphi \geq 0$, for all $\varphi \mid \chi$.*

Proof. By assumption, $\mathbf{M}_K/\mathbf{M}'_K$ is a finite $\mathbb{Z}[\mu_{g_\chi}]$-module, of the form $\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A}$, $\mathfrak{A} \neq 0$; so $\mathscr{M}_K/\mathscr{M}'_K \simeq (\mathbb{Z}[\mu_{g_\chi}]/\mathfrak{A})\otimes\mathbb{Z}_p$, giving $\mathscr{M}_K/\mathscr{M}'_K \simeq \bigoplus_{\varphi\mid\chi}\left[\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^{\lambda_\varphi}\right]$, with the usual correspondence between primes $\mathfrak{p} \mid p$ and p-adic characters $\varphi \mid \chi$; whence the claim. □

Let $\mathscr{M}_K := \mathscr{E}_K$ and $\mathscr{M}'_K := \widehat{\mathscr{E}_K\mathscr{F}_K}$. Taking into account orders and the fact that $(P_\chi(\sigma_\chi))$ annihilates $\mathscr{E}_K/\widehat{\mathscr{E}_K\mathscr{F}_K}$, the lemma is coherent with an annihilation theorem of the $\mathscr{H}^{\rm ar}_\varphi$'s from the results of § 7.4.

Remark 6 – As the Referee pointed out about a possible confusion, the Galois-module $\mathscr{E}_K$ is not necessarily monogenic, as Galois module, in the non semi-simple case. The reader may consider one of the two degree-9 cyclic fields K of conductor $19\cdot 229$ (class groups $\mathbb{Z}/3\mathbb{Z}$ from PARI), with principal cubic subfield k of conductor 19; application of the Chevalley–Herbrand fixed-points formula[62] in cyclic p-extensions K/k,

$$\#\mathscr{H}_K^g = \#\mathscr{H}_k \times \frac{\prod_{\mathfrak{q}} e_{\mathfrak{q}}}{[K:k](\mathscr{E}_k : \mathscr{E}_k \cap \mathbf{N}_{K/k}(K^\times))},$$

and the classicl exact sequence defining $\mathscr{H}_K^g$ (obtained from the invariant class of $\mathfrak{A}_K$, $\mathfrak{A}_K^{1-\sigma} =: (\alpha_K) \mapsto \mathbf{N}_{K/k}(\alpha_K) =: \varepsilon_k$),

$$1 \to \mathbf{J}_{K/k}\mathscr{H}_k \cdot \mathscr{H}_K^{\rm ram} \longrightarrow \mathscr{H}_K^g \longrightarrow \mathscr{E}_k \cap \mathbf{N}_{K/k}(K^\times)/\mathbf{N}_{K/k}(\mathscr{E}_K) \to 1$$

($g = {\rm Gal}(K/k) = \langle\sigma\rangle$, $e_{\mathfrak{q}}$ is the ramification index, $\mathscr{H}_K^{\rm ram}$ is the subgroup of $\mathscr{H}_K$ generated by the ramified primes), lead, here, to $\#\mathscr{H}_K^g = \#\mathscr{H}_K = 3$, then $(\mathscr{E}_k : \mathscr{E}_k \cap \mathbf{N}_{K/k}(K^\times)) = 9$ whence $\mathbf{N}_{K/k}(\mathscr{E}_K) = \mathscr{E}_k^3$, an obstruction for monogenicity of $\mathscr{E}_K$. Theorem 14(ii ′′) gives $\mathscr{E}_K = \mathscr{F}_K$ but $w_\chi = 3$.

Only $\mathscr{E}_K/\widehat{\mathscr{E}}_K$ and its quotients $\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K$ are monogenic in the non semi-simple case, which is the only property that we need in all the paper.

7.6 Mysterious link between cyclotomic units and classes

The brief overview, that we give now, must be completed by technical elements that the reader can find especially in Washington (1997, § 15.2, 15.3) (all of them borrow from classical arithmetic) and in the references that we talked about, giving systematic generalizations of "Euler systems".

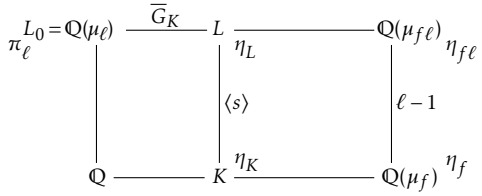
To simplify, consider the real semi-simple case for $p > 2$ with $K = K_\chi$ of conductor f; for $\varphi \mid \chi$, we need to establish *arithmetic links* between $\widetilde{\mathscr{E}}_\varphi = \mathscr{E}_\varphi/\mathscr{F}_\varphi$ and $\mathscr{H}_\varphi$, where $\mathscr{E}_\varphi =: \langle \varepsilon_\varphi \rangle_{\mathbb{Z}_p[\mu_{g_\chi}]}$ and $\mathscr{F}_\varphi =: \langle \eta_\varphi \rangle_{\mathbb{Z}_p[\mu_{g_\chi}]}$ is built from Leopoldt's cyclotomic units (Definitions 3). But $\widetilde{\mathscr{E}}_\varphi$ has, a priori, no obvious connection with class groups, except the analytic equality $\prod_{\varphi|\chi} \#\mathscr{H}_\varphi = \prod_{\varphi|\chi} \#\widetilde{\mathscr{E}}_\varphi$ (Corollary 3).

The trick, for the proof of the FAMC, consists in using a context of "analytic genus theory", by means of auxiliary cyclic ℓ-ramified extensions $K(\mu_\ell)$ of degree multiple of the exponent λp^e, $e \geq 1$, of $\mathbf{H}_K$.

Let $\ell \nmid f$, $\ell \equiv 1 \pmod{2\lambda p^N}$, $N \gg e$, totally split in K; put $L_0 = \mathbb{Q}(\mu_\ell)$ and $L := L_0 K$:

Let $\eta_{f\ell} = 1 - \zeta_{f\ell}$, $\eta_f = 1 - \zeta_f$, $\eta_\ell = 1 - \zeta_\ell$ and consider the cyclotomic numbers $\eta_L := \mathbf{N}_{\mathbb{Q}(\mu_{f\ell})/L}\left(\eta_{f\ell}\right)$, $\eta_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}(\eta_f)$; by assumption on the total splitting of ℓ in $K/\mathbb{Q}$, $\mathbf{N}_{L/K}(\eta_L) = 1$ (cf. Lemma 16). We remark that $\eta_{f\ell} \equiv \eta_f \pmod{\pi_\ell}$ where $\pi_\ell := \eta_\ell$ is an uniformizing parameter at the place above ℓ in L_0, so that $\eta_L \equiv \eta_K \pmod{\pi_\ell}$, giving a ℓ-adic link between η_K and η_L which will be fundamental for the congruences (25):

Schema XI



A main step is to apply Hilbert's Theorem 90 (Kummer's Theorem[63]), saying that $\eta_L = \alpha_L^{s-1}$, where s is a generator of $\mathrm{Gal}(L/K)$ and $\alpha_L \in L^\times$ is such that $(\alpha_L) \in \mathbf{I}_L^{\langle s \rangle}$,

[62] Chevalley, 1933, "Sur la théorie du corps de classes dans les corps finis et les corps locaux", pp. 402-406.

[63] Kummer, 1855, "Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke", p. II.

where $\mathbf{I}$ denotes ideal groups; since α_L is defined modulo $K^\times$, we can take α_L integer in L, or at least ℓ-integer, whence:

$$(\alpha_L) = \mathbf{J}_{L/K}(\mathfrak{a}_K)\mathfrak{L}_0^{\Omega_\ell}, \tag{22}$$

where $\mathfrak{a}_K \in \mathbf{I}_K$ may be taken prime to ℓ, where $\mathfrak{L}_0$ is a fixed prime ideal dividing ℓ in L and:

$$\Omega_\ell = \textstyle\sum_{\tau \in \overline{G}_K} r_\tau\, \tau^{-1},\ r_\tau \geq 0; \tag{23}$$

thus, since $\mathbf{N}_{L/K}(\mathfrak{L}_0) = \mathfrak{l}_0$, $\mathfrak{L}_0 \mid \mathfrak{l}_0 \mid \ell$ in L/K:

$$(\alpha_K) := (\mathbf{N}_{L/K}(\alpha_L)) = \mathfrak{a}_K^{\ell-1}\, \mathfrak{l}_0^{\Omega_\ell}. \tag{24}$$

But $\mathfrak{a}_K^{\ell-1}$ is principal, whence $\mathfrak{l}_0^{\Omega_\ell}$ principal, Ω_ℓ seen in $\mathbb{Z}[G_K]$.

The following property elucidates the "mysterious link" giving an information that we can "project" on each φ-component of $\mathscr{H}_K$ and obtain the annihilation of the φ-class of $\mathfrak{l}_0$ by the φ-component of Ω_ℓ:

Lemma 19 – *Except a finite number of primes ℓ, the ideal $\mathfrak{L}_0^{\Omega_\ell}$ of* (22) *gives a non-trivial relation, in the meaning that Ω_ℓ in* (23) *is not of the form $\lambda\, \mathcal{V}_{L/L_0}$, $\lambda \geq 0$, giving $\mathfrak{l}_0^{\Omega_\ell} = (\ell)^\lambda$ in* (24).

Proof. Assume that $\Omega_\ell = \lambda\, \mathcal{V}_{L/L_0}$; the character of $\mathfrak{L}_0^{\Omega_\ell} = (\pi_\ell^\lambda)$ is the unit one and any non-trivial φ-component $\alpha_{L,\varphi}$ of α_L is prime to ℓ, thus congruent, modulo any $\mathfrak{L} \mid \ell$, to $\rho_\mathfrak{l} \in \mathbb{Z}$, $\rho_\mathfrak{l} \not\equiv 0 \pmod{\ell}$ (residue degrees 1 in $L/\mathbb{Q}$). Since $\mathfrak{L}^s = \mathfrak{L}$, we obtain $\eta_{L,\varphi} = \alpha_{L,\varphi}^{s-1} \equiv 1 \pmod{\mathfrak{L}}$; but $\eta_{K,\varphi} \equiv \eta_{L,\varphi} \pmod{\pi_\ell}$ leads to $\eta_{K,\varphi} \equiv 1 \pmod{\mathfrak{l}}$, for all $\mathfrak{l} \mid \ell$, giving $\eta_{K,\varphi} \equiv 1 \pmod{\ell}$ (absurd for almost all ℓ). □

Reducing modulo $\mathcal{V}_{L/L_0}$, one may get $\Omega_\ell \neq 0$, "minimal" in an obvious sense, with $r_\tau \geq 0$ but not all zero. Consider $\dfrac{\alpha_L^\sigma}{\pi_\ell^{r_\sigma}}$ (prime to $\mathfrak{L}_0$) modulo $\mathfrak{L}_0$ for $\sigma \in G_K$, and the conjugations $\alpha_L^s = \alpha_L \eta_L$ and $\dfrac{\pi_\ell^s}{\pi_\ell} = \dfrac{1-\zeta_\ell^{\mathbf{g}_\ell}}{1-\zeta_\ell} \equiv \mathbf{g}_\ell \pmod{\pi_\ell}$, where $\mathbf{g}_\ell$ is a primitive root modulo ℓ such that $\zeta_\ell^s =: \zeta_\ell^{\mathbf{g}_\ell}$; one gets:

$$\left[\frac{\alpha_L^\sigma}{\pi_\ell^{r_\sigma}}\right]^s = \frac{\alpha_L^{s\sigma}}{\pi_\ell^{sr_\sigma}} \equiv \frac{\eta_L^\sigma \alpha_L^\sigma}{(\mathbf{g}_\ell \pi_\ell)^{r_\sigma}} \equiv \frac{\eta_L^\sigma}{\mathbf{g}_\ell^{r_\sigma}} \left[\frac{\alpha_L^\sigma}{\pi_\ell^{r_\sigma}}\right] \pmod{\mathfrak{L}_0},$$

whence $\dfrac{\eta_L^\sigma}{\mathbf{g}_\ell^{r_\sigma}} \equiv 1 \pmod{\mathfrak{L}_0}$ since $\dfrac{\alpha_L^\sigma}{\pi_\ell^{r_\sigma}}$ is congruent to a prime-to-ℓ rational number:

$$\mathbf{g}_\ell^{r_\sigma} \equiv \eta_L^\sigma \equiv \eta_K^\sigma \pmod{\mathfrak{l}_0}, \text{ for all } \sigma \in G_K. \tag{25}$$

So we have obtained a non-trivial relation between the classes of the conjugates of $\mathfrak{l}_0$, computable from η_K and its conjugates; indeed, put $\eta_K^{\sigma} \equiv a_\sigma \equiv \mathbf{g}_\ell^{\rho_\sigma} \pmod{\mathfrak{l}_0}$ gives $r_\sigma \equiv \rho_\sigma \pmod{(\ell-1)}$ and an annihilation of $\mathscr{H}_K$ by $\sum_{\sigma\in G_K} \rho_\sigma \sigma^{-1}$. Recall that α_L is also given by an explicit Hilbert resolvent allowing explicit computations.

Remarks 4 – (i) The properties of the α_L's give rise to an homomorphism of $\mathbb{Z}_p[G_K]$-modules, $\mathbf{F}_K/\mathbf{F}_K^{p^N} \to \mathbb{Z}/p^N\mathbb{Z}[G_K]$, allowing reasoning for the φ-components. To get more information, one varies ℓ, using Chebotarev's Theorem and Nakayama's Lemma. Then the problem of the $\#\mathscr{H}_\varphi$'s needs the knowledge of the whole analytic formula of Theorem 14 (see the details in Washington (1997, § 15.2, 15.3), from Thaine's Theorem).

(ii) We will return elsewhere to the links with genus theory given by the following fixed-points exact sequence, obtained from the invariant class of $\mathfrak{A}_L$, $\mathfrak{A}_L^{1-s} =: (\alpha_L) \mapsto \mathbf{N}_{L/K}(\alpha_L) =: \varepsilon_K$:

$$1 \to cl_L(\mathbf{I}_L^{\langle s\rangle}) \otimes \mathbb{Z}_p \longrightarrow \mathscr{H}_L^{\langle s\rangle} \longrightarrow \mathscr{E}_K \cap \mathbf{N}_{L/K}(L^\times)/\mathbf{N}_{L/K}(\mathscr{E}_L) \to 1$$

and (in the present context totally ramified) the Chevalley–Herbrand formula, $\#\mathscr{H}_L^{\langle s\rangle} = \#\mathscr{H}_K \times \frac{p^{n([K:\mathbb{Q}]-1)}}{(\mathscr{E}_K:\mathscr{E}_K\cap \mathbf{N}_{L/K}(L^\times))}$ and similar formulas in the sub-extensions of L/K (noting that the exact sequence and Chevalley–Herbrand's formula may be written in terms of φ-objects without too difficulties; cf. Gras (2023b, 2024b) and Jaulent (1986)). The reason of such a link with genus theory is the fact that, assuming $\mathscr{F}_M = \mathscr{E}_M$ for the subfield M of L of degree p over K we know that $\mathbf{N}_{L/M}(\mathscr{F}_L) = \mathscr{F}_M = \mathscr{E}_M$, so that the above exact sequence reduces to $\mathscr{H}_L^{\langle s^p\rangle} = cl_L(\mathbf{I}_L^{\langle s^p\rangle}) \otimes \mathbb{Z}_p$ in L/M and $\#\mathscr{H}_L^{\langle s^p\rangle} = \#\mathscr{H}_M \times p^{n([K:\mathbb{Q}]-1)}$.

(iii) Any "$\mathscr{G}$-family of numbers η" satisfying, in cyclic extensions L/K, relations of the form $\mathbf{N}_{L/K}(\eta_L) = \eta_K^{1-\mathrm{Frob}_{L/K}(\ell)}$ and $\eta_L \equiv \eta_K \pmod{\prod_{\mathfrak{l}|\ell}\mathfrak{l}}$, for suitable primes ℓ, is called an "Euler system"[64] and gives rise to similar reasonings in many domains.

(iv) Equations of the general form $\mathbf{N}_{L/K}(y) = \mathbf{N}_{L/K}(\mathfrak{B})$, giving $(y) = \mathfrak{B}\mathfrak{A}^{s-1}$, are fundamental in various questions, as Greenberg's conjecture, in a genus theory framework (see Gras (2018b, § 3, Algorithm)). Such equations are due to some $x \in K^\times$, local norm in L/K at the ℓ-places, such that $(x) = \mathbf{N}_{L/K}(\mathfrak{B})$, giving the relation $x = \mathbf{N}_{L/K}(y)$, for some unknown y (Hasse's norm theorem in L/K). In various papers, as in Gras (2019b, § 7.1), we have discussed these random aspects by computing some ideals $\mathfrak{A}$, so that we may conjecture the following more precise property (see Schemas 7.4, 7.4, Lemma 19, Relations (22)–(25)).

Conjecture 2 – *Let K be a real abelian field of conductor f, of p-class group such that $\mathscr{H}_K^{p^e} = 1$ and let $\eta_K := \mathbf{N}_{\mathbb{Q}(\mu_f)/K}\left(1-\zeta_f\right)$. Consider primes $\ell \equiv 1 \pmod{2p^N}$, totally split in K, $N \gg e$; let $\mathfrak{l}_0 \mid \ell$ in K and let $\mathbf{g}_\ell$ be a primitive root modulo ℓ. When ℓ varies, η_K provides infinitely many elements $\Omega_\ell = \sum_{\sigma\in G_K} r_\sigma \sigma^{-1}$, with $\eta_K^\sigma \equiv \mathbf{g}_\ell^{r_\sigma} \pmod{\mathfrak{l}_0}$, such that the ideal generated by these relations yields annihilators of the φ-components $\mathscr{H}_\varphi^{\rm ar}$ as $\mathbb{Z}_p[G_K]$-modules and structure informations.*

The program in Appendix A.5, for cyclic cubic fields, computes the invariants $\psi(\Omega_\ell) \in \mathbb{Z}[j]$, $j := \exp(2i\pi/3)$, from the explicit expression $\sum_{\sigma\in G_K} \rho_\sigma \sigma^{-1}$ as we have explained, only knowing η_K, and gives tables of results.

These numerical experiments are particularly remarkable and confirm that the Ω_ℓ's define an universal Ω_K which replaces, in the real case, the Stickelberger element of the imaginary case. For this, we notice that the embeddings (injectivity from Gras (2005, Theorem III.4.4)) of $\mathscr{F}_K$ and $\mathscr{E}_K$ in the direct product $\prod_{v\nmid p}(F_v^\times \otimes \mathbb{Z}_p)$ (see Schemas 7.4, 7.4) govern the congruences (25) giving the relations Ω_ℓ involving only $\mathbf{F}_K$, without any memory of the arithmetic of the auxiliary fields $\mathbb{Q}(\mu_\ell)$. Then, the Schmidt–Chevalley theorem (or local–global principle for powers, e.g., Gras (2005, § 6.3, Theorem II.6.3.3)) claims that there are infinitely many primes ℓ, totally split in K, giving the "good" Ω_K.

From Lemma 18 giving standard structure of $\mathscr{E}_\varphi$ and $\mathscr{F}_\varphi$, it is then obvious that one obtains equalities of the φ-invariants $m_\varphi^{\rm ar}$ of $\mathscr{E}_\varphi/\mathscr{F}_\varphi$ and $\mathscr{H}_\varphi$ in the semi-simple case.

Are there improvements of these techniques being able to distinguish, for instance, the structures $\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi \times \mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi$ and $\mathbb{Z}_p[\mu_{g_\chi}]/\mathfrak{p}_\varphi^2$?

Remark 7 – After the writing of this paper, we have considered the phenomenon of capitulation of p-classes in auxiliary p-extensions L/K, $L/\mathbb{Q}$ abelian, to give another approach of the FAMC in any real case (semi-simple or not). We develop, in Gras (2023b, 2024b), new promising links between:

(i) the Chevalley–Herbrand formula giving the number of "ambiguous classes" in p-extensions L/K, $L \subset K(\mu_\ell)$, for auxiliary primes $\ell \equiv 1 \pmod{2p^N}$ totally inert in K (of course, if $K \cap \mathbb{Q}(\mu_{p^\infty}) = \mathbb{Q}$);

(ii) the phenomenon of capitulation of $\mathscr{H}_K$ in L;

(iii) the real FAMC $\#\mathscr{H}_\varphi^{\rm ar} = (\mathscr{E}_K : \widehat{\mathscr{E}_K\mathscr{F}_K})_{\varphi_0}$ for all $\varphi \mid \chi$.

We prove that the real FAMC is trivially fulfilled as soon as $\mathscr{H}_K$ capitulates in L and conjecture that there exist infinitely many such primes ℓ leading to capitulation.

[64] Kolyvagin, 2007, *Euler Systems*;
Perrin-Riou, 1990, *Travaux de Kolyvagin et Rubin*;
Perrin-Riou, 1998, "Systèmes d'Euler p-adiques et théorie d'Iwasawa".

Computations with PARI programs support this new philosophy of the FAMC and justifies, once again, the relevance of the analytic definitions given in the 1970's, especially in the non semi-simple case.

8 Invariants (Algebraic, Arithmetic, Analytic)

We fix an irreducible rational character $\chi \in \mathscr{X} = \mathscr{X}^+ \cup \mathscr{X}^-$, of order $g_\chi \neq 1$, and we apply the previous results to the $\mathbb{Z}_p[\mu_{g_\chi}]$-modules $\mathscr{H}_\varphi^{\rm alg}$, $\mathscr{H}_\varphi^{\rm ar}$ and $\mathscr{T}_\varphi^{\rm ar}$, for any $\varphi \mid \chi$ ($\varphi \in \Phi^+$ for $\mathscr{T}_\varphi^{\rm ar}$).

8.1 Algebraic and Arithmetic Invariants $m^{\rm alg}(\mathscr{M})$, $m^{\rm ar}(\mathscr{M})$

Write simply that $\mathscr{H}_\varphi^{\rm alg}$, $\mathscr{H}_\varphi^{\rm ar}$ and $\mathscr{T}_\varphi^{\rm ar}$ are finite $\mathbb{Z}_p[\mu_{g_\chi}]$-modules whatever φ; let $\mathfrak{p}_\varphi$ be the maximal ideal of $\mathbb{Z}_p[\mu_{g_\chi}]$:

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

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

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

Whence the order formulas:

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

8.2 Analytic Invariants $m^{\rm an}(\mathscr{M})$

We define, in view of the statement of the FAMC, the following Analytic Invariants $m_\varphi^{\rm an}$, from the expressions given with rational characters, where $\mathrm{val}_p(\bullet)$ denotes the usual p-adic valuation; the purpose is to satisfy the necessary relations implied by Theorems 3, 4 about arithmetic components:

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

for any family $\mathscr{M} \in \{\mathscr{H}, \mathscr{T}\}$ and $\chi \in \mathscr{X}$ (cf. Theorems 7, 14, 12).

Case $\varphi \in \Phi^-$, $\varphi \mid \chi$, for imaginary class groups

Then, Algebraic and Arithmetic Invariants coincide. The definitions given in Gras (1976, 1977b) for $K = K_\chi$, $\chi \neq 1$, were:

(i) Case $p \neq 2$ (proven in Solomon (1990, Theorem II.1)):

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

- $m_\varphi^{\mathrm{an}}(\mathscr{H}^-) := \mathrm{val}_p\left(\prod_{\psi|\varphi}\left(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)\right)$.

(i'') $K = \mathbb{Q}(\mu_{p^n})$, $n \geq 1$; let $\psi = \omega^\lambda \psi_p$, ψ_p of order p^{n-1} (where ω is the Teichmüller character and λ is prime to $p-1$); then:

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

(ii) Case $p = 2$ (proven by Greither[65], in the case g_χ non 2-power and f_χ odd):

(ii') g_χ is not a 2-power; then:

- $m_\varphi^{\mathrm{an}}(\mathscr{H}^-) := \mathrm{val}_2\left(\prod_{\psi|\varphi}\left(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)\right)$.

(ii'') g_χ is a 2-power; then:

- $m_\varphi^{\mathrm{an}}(\mathscr{H}^-) := \mathrm{val}_2\left(\prod_{\psi|\varphi}\left(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)\right) + 1$, if $K \neq \mathbb{Q}(\mu_4)$,
- $m_\varphi^{\mathrm{an}}(\mathscr{H}^-) := 0$, if $K = \mathbb{Q}(\mu_4)$.

Case $\varphi \in \Phi^+$, $\varphi \mid \chi \neq 1$, for real class groups

From Definition 3 and Theorem 14, we consider any real cyclic field $K = K_\chi$, where we recall that:

$\widehat{\mathbf{E}}_K := \langle \mathbf{E}_k \rangle_{k \subsetneq K}$, $\mathbf{F}_K := \mathbf{C}_K \cap \mathbf{E}_K$, $\mathscr{E}_K := \mathbf{E}_K \otimes \mathbb{Z}_p$, $\widehat{\mathscr{E}}_K := \widehat{\mathbf{E}}_K \otimes \mathbb{Z}_p$, $\mathscr{F}_K := \mathbf{F}_K \otimes \mathbb{Z}_p$, and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_K / \widehat{\mathscr{E}}_K \mathscr{F}_K$, for which $\widetilde{\mathscr{E}}_\chi = \oplus_{\varphi|\chi}(\widetilde{\mathscr{E}}_\chi)_{\varphi_0}$.

Consider the relation $\#\mathscr{H}_\chi^{\mathrm{ar}} = w_\chi \prod_{\varphi|\chi} \#\widetilde{\mathscr{E}}_\varphi = w_\chi \prod_{\varphi|\chi} \#(\widetilde{\mathscr{E}}_\chi)_{\varphi_0}$ of Theorem 14; we remark that $w_\chi = p$ occurs only when g_χ is a p-power, in which case p is totally ramified in $\mathbb{Q}(\mu_{g_\chi})$ and $\varphi = \chi$, i.e., $\varphi_0 = 1$ (which defines $w_\varphi := w_\chi$).

So, we may define $m_\varphi^{\mathrm{an}}(\mathscr{H}^+)$ and w_φ from $\widetilde{\mathscr{E}}_\varphi \simeq \mathbb{Z}_p[\mu_{g_\chi}] \big/ \mathfrak{p}_\varphi^{m_\varphi^{\mathrm{an}}(\mathscr{H}^+)}$, $m_\varphi^{\mathrm{an}}(\mathscr{H}^+) \geq 0$, as follows (where ℓ denotes any prime):

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

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

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

[65] Greither, 1992, "Class groups of abelian fields, and the main conjecture", Theorem B.

(ii') Case where f_χ is a ℓ-power. Then $w_\varphi = 1$ and:

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

(ii'') Case where f_χ is not a ℓ-power. Then $w_\varphi = p$ and:

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

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

(iii') Case where f_χ is a ℓ-power. Then $w_\varphi = 1$ and:

- $m_\varphi^{\mathrm{an}}(\mathscr{K}^+) := \mathrm{val}_2(\#\widetilde{\mathscr{E}_\varphi})$,

(iii'') Case where f_χ is not a ℓ-power. Then $w_\varphi \in \{1, 2\}$ and:

- $m_\varphi^{\mathrm{an}}(\mathscr{K}^+) \in \{\mathrm{val}_2(\#\widetilde{\mathscr{E}_\varphi}), \mathrm{val}_2(\#\widetilde{\mathscr{E}_\varphi}) + 1\}$.

Case $\varphi \in \Phi^+$ for real p-torsion groups

From Theorem 12, we define $m_\varphi^{\mathrm{an}}(\mathscr{T})$ as follows (proven in Greither (1992, Theorem C), when g_χ is not a 2-power):

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

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

(ii) Case where g_χ and f_χ are p-powers. Then:

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

Note that for $K \subset \mathbb{Q}^{\mathrm{cyc}}$ (case (ii)), $\mathscr{T}_K = 1$ for trivial reasons, in particular since $\mathscr{T}_K^{G_K} = 1$[66].

8.3 Finite Abelian Main Conjecture

The conjecture we gave in Gras (1976, 1977b), especially in the non semi-simple case, where simply equality of Arithmetic and Analytic φ-Invariants. The main justification of such equalities comes from the easy Theorem 1 with the arithmetic definitions of § 8.1, the analytic definitions of § 8.2 and the arithmetic expressions of the χ-components that we recall:

(i) Theorem 7: $\mathbf{H}_\chi^{\mathrm{ar}} = 2^{a_\chi} \cdot w_\chi \cdot \prod_{\psi|\chi}\left(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)$, for $\chi \in \mathscr{X}^-$,

(ii) Theorem 12: $\#\mathscr{T}_\chi^{\mathrm{ar}} = w_\chi^{\mathrm{cyc}} \cdot \prod_{\psi|\chi} \frac{1}{2}\mathbf{L}_p(1, \psi)$, for $\chi \in \mathscr{X}^+$,

[66] Gras, 2005, *Class Field Theory: from theory to practice, corr. 2nd ed.* Theorem IV.3.3.

(iii) Theorem 14: $\#\mathbf{H}_\chi^{\rm ar} = w_\chi \cdot (\mathbf{E}_K : \widehat{\mathbf{E}}_K \mathbf{F}_K)$, for $\chi \in \mathscr{X}^+$.

Taking into account the decomposition $\mathscr{M}_\chi^{\rm ar} = \bigoplus_{\varphi|\chi} \mathscr{M}_\varphi^{\rm ar}$ (Theorem 5), they satisfy, for families $\mathscr{M} \in \{\mathscr{H}^-, \mathscr{H}^+, \mathscr{T}\}$, the equalities:

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

Moreover, the annihilation properties of Theorems 8, 9, 10, 6.2, enforce the conjecture as well as reflection theorems that were given, after the Leopoldt's Spiegelungsatz, in Gras (1998) or Gras (2005, Theorem II.5.4.5) giving a more suitable comparison, for instance between $\mathscr{H}_\varphi^{\rm ar}$ and $\mathscr{T}_{\omega\varphi^{-1}}^{\rm ar}$, $\varphi \in \Phi^-$, where ω is the Teichmüller character. See also Oriat[67] for similar informations and complements.

Conjecture 3 – *For any p-adic irreducible character $\varphi \in \Phi$, we have:*

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

Remark 8 – 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 $\psi_i = \psi_0 \psi_p^{p^{n-i}} \in \Psi_{K_i}$ and we consider the p-adic characters φ_i above ψ_i, $0 \leq i \leq n$.

The Main Conjecture proven in Greither (1992, Theorem 4.14, Corollary 4.15), using Sinnott's cyclotomic units, deals with the semi-simple context defined by φ_0 above ψ_0 (it is indeed that of the relations (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, for each $\varphi_0 \in \Phi_{K_0}$, the relation $\sum_{i=0}^n m_{\varphi_i}^{\rm ar}(\mathscr{H}^+) = \sum_{i=0}^n m_{\varphi_i}^{\rm an}(\mathscr{H}^+)$, 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 improvements by Greither–Kučera[68] and some of their other papers.

Remark 9 – It remains the problem of $\#\mathscr{H}_\chi^{\rm alg}$ and $\#\mathscr{H}_\varphi^{\rm alg}$, for which no obvious analytic formula does exist in the non semi-simple real case. For instance, in Example 1Appendix A.2 on p. 175 with $p = 3$, K is the compositum of $k_0 = \mathbb{Q}(\sqrt{4409})$ with the degree 9 field of conductor 19, $\chi_i = \varphi_i$ ($i \in \{0, 1, 2\}$) 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

[67] Oriat, 1981, "Annulation de groupes de classes réelles";
Oriat, 1986, "Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens".

[68] Greither and Kučera, 2014, "Eigenspaces of the ideal class group";
Greither and Kučera, 2015, "Annihilators for the class group of a cyclic field of prime power degree III".

the conjecture and checked numerically. In Example 2 Appendix A.2 on p. 178, one finds $\mathscr{H}_{\chi_1}^{\rm alg} \simeq (\mathbb{Z}/3\mathbb{Z})^3$ while $\mathscr{H}_{\chi_1}^{\rm ar} \simeq (\mathbb{Z}/3\mathbb{Z})^2$.

Of course, formulas $\#\mathscr{H}_{\chi_0}^{\rm alg} \times \#\mathscr{H}_{\chi_1}^{\rm alg} \times \#\mathscr{H}_{\chi_2}^{\rm alg} = \#\mathscr{H}_K^{\rm alg}$ do not hold in general for algebraic definition of class groups. See Remark 3.

This phenomenon is due to the capitulation of p-classes in p-extensions K/K_0 and we have given in Gras (2022, Conjecture 4.1) a general conjecture justified by means of many computations.

8.4 "Iwasawa's theory" in cyclic p-extensions

For more details and an application to classical Iwasawa's theory for the cyclotomic $\mathbb{Z}_p$-extensions, see Gras (1976, Chap. IV), the real case being in the spirit of Greenberg's conjecture; nevertheless, *the results hold in arbitrary totally ramified cyclic p-extensions* of an abelian field, as follows depending of a base field real or imaginary:

Real case

Let $\psi \mid \varphi \mid \chi \in \mathscr{X}^+$ and set $\psi = \psi_0\psi_p$, where ψ_0 is of prime-to-p order g_0 and ψ_p of p-power order; then, for $K = K_\chi$, $G_K = G_0 \oplus H$ in an obvious meaning. We consider the semi-simple idempotents $e_{\varphi_0} := \frac{1}{g_0}\sum_{\sigma\in G_0} \varphi_0(\sigma^{-1})\,\sigma$, for φ_0 above ψ_0. We have:

$$\widetilde{\mathscr{E}}_\chi := \mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K = \bigoplus_{\varphi\mid\chi} \widetilde{\mathscr{E}}_\varphi = \bigoplus_{\varphi\mid\chi} (\widetilde{\mathscr{E}}_\chi)_{\varphi_0};$$

we note that $(\widetilde{\mathscr{E}}_K)_{\varphi_0} \simeq \mathscr{E}_{\varphi'}$ and $\widetilde{\mathscr{E}}_\varphi \simeq \mathscr{E}_K^{e_{\varphi_0}}/\mathscr{E}_{\varphi'}\mathscr{F}_K^{e_{\varphi_0}}$, where φ' is above $\psi_0\psi_p^p$ and χ' above φ'. This yields $(\mathscr{E}_K/\mathscr{E}_{K_{\chi'}})_\varphi = (\mathscr{E}_K/\mathscr{E}_{K_{\chi'}})_{\varphi_0} \simeq \mathbb{Z}_p[\mu_{g_\chi}]$ (Gras (1976, Lemma IV.1)) and the following principle taking place in the layers K_n of p-tower K/K_0, of degree p^N over an abelian field K_0, and totally ramified (Gras (1976, Proposition IV.1)):

Theorem 15 – *Let $\chi \in \mathscr{X}^+$ be such that $g_\chi = g_0 p^n$, $p \nmid g_0$, $n \geq 2$. Let χ', χ'' 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 16 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, for $a, b \geq 0$:*

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

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

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

This allows to prove again Iwasawa's formula in the case $\mu = 0$, see Gras (1976, Theorems IV.1, IV.2, Remark IV.4), and gives an analytic algorithm to study the p-class groups in the first layers, as follows:

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 χ_{n_0} of order $g\,p^{n_0}$) such that, for each φ_{n_0}-component, $a_{n_0-1} < p^{n_0-2}(p-1)$ (case (i) of Theorem 15); then the sequence $\#\mathscr{H}_{\chi_n}$ becomes constant giving the λ-invariant and the relations $\mathscr{E}_{k_{n-1}} = \mathbf{N}_{k_n/k_{n-1}}(\mathscr{E}_{k_n})\mathscr{E}_{k_{n-2}}$, for all $n \gg 0$; then $p^\lambda = (\mathscr{E}_{k_n} : \widehat{\mathscr{E}}_{k_n}\mathscr{F}_{k_n})$ for $n \gg 0$. More precisely:

$$p^{\lambda_\varphi} = \#(\mathscr{E}_{k_n}/\mathscr{E}_{k_{n-1}}\mathscr{F}_{k_n})_{\varphi_0},\ n \gg 0.$$

This methodology does exist in terms of p-adic $\mathbf{L}$-functions for abelian fields (see, e.g., Gras (1980, Chapitre V)).

Recall that Greenberg's conjecture for a totally real base field k (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 Gras (2019a, Corollary 3.4)). Whence the result:

Theorem 16 – *Let k be a real abelian field of prime-to-p degree. Then, Greenberg's conjecture is equivalent to $(\mathscr{E}_{k_n} : \widehat{\mathscr{E}}_{k_n}\mathscr{F}_{k_n}) = $ constant, for all $n \gg 0$, where $\widehat{\mathscr{E}}_{k_n}$ is the subgroup of $\mathscr{E}_{k_n}$ generated by the units of the strict subfields of k_n and $\mathscr{F}_{k_n}$ is the group of Leopoldt cyclotomic units (Definitions 2 (i), 3).*

Imaginary case

This part Gras (1976, Proposition IV.2, Théorème IV.2) is related to relative p-class groups for $p \neq 2$:

Theorem 17 – *Let $\chi \in \mathscr{X}^-$ be such that $g_\chi = g_0 p^n$, $p \nmid g_0$, $n \geq 2$. Let χ' 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 $\mathbf{N}_{K/K'}(\mathbf{B}_K) = \mathbf{B}_{K'}$ (see Lemma 16). Put:*

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

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

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

Remark 10 – The integers A and a are the Analytic Invariants $m_\varphi^{\rm an}(\mathscr{H}^-)$ and $m_{\varphi'}^{\rm an}(\mathscr{H}^-)$, respectively, defined § 8.2. From Gras (1976, Remark IV.4), the Iwasawa μ-invariant is zero as soon as there exists $n_0 \gg 0$ such that the case (i) of the theorem is satisfied for all φ of K_{n_0}. In a $\mathbb{Z}_p$-extension $\widetilde{k}/k$, this condition implies that the p-rank of the $\mathscr{H}_{k_n}^{\rm ar}$'s is bounded, a well-known result of Iwasawa's theory given in Washington (1997, Proposition 13.23)).

9 Illustrations of the real FAMC with cubic fields

9.1 Specific aspects of the cubic case

For $\chi \in \mathscr{X}^+$, $\chi \neq 1$, and $\widetilde{\mathscr{E}}_\chi := \mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K$, we have $\#\mathscr{H}_\chi^{\rm ar} = w_\chi\,\#\widetilde{\mathscr{E}}_\chi$ (Theorem 14), and for $\varphi \mid \chi$ we have, conjecturally:

$$\#\mathscr{H}_\varphi^{\rm ar} = w_\varphi\,\#\widetilde{\mathscr{E}}_\varphi = w_\varphi\,\#(\widetilde{\mathscr{E}}_\chi)_{\varphi_0},\ w_\varphi \in \{1,p\}.$$

In another way, we have:

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

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

We intend to see more precisely what happens for these analytic and arithmetic invariants since the above equality defining $m_\varphi^{\rm an}(\mathscr{H})$ can be fulfilled in various ways; indeed, $\widetilde{\mathscr{E}}_\varphi$ is monogenic and $\mathscr{H}_\varphi^{\rm ar}$ may have arbitrary structure.

We will examine the case of the cyclic cubic fields K for primes $p \equiv 1 \pmod 3$ giving two p-adic characters $\varphi \mid \chi$; in that case, $\widehat{\mathscr{E}}_K = 1$ and $\#\mathscr{H}_\varphi^{\rm ar} = \#(\mathscr{E}_K/\mathscr{F}_K)_\varphi$; here, $\varphi = \varphi_0$ (semi-simple case).

For example, for $p = 7$, the possible structures, for the $\mathbb{Z}[j]$-module $\mathbf{E}_K/\mathbf{F}_K$, are of the form (with $m_1, m_2 \geq 0$ and $\mathfrak{a}$ prime to 7):

$$\mathbb{Z}[j]\Big/[(-2+j)^{m_1}\cdot(3+j)^{m_2}\cdot\mathfrak{a}],$$

giving the two φ_i-components $\mathbb{Z}_7/7^{m_1}\mathbb{Z}_7$ and $\mathbb{Z}_7/7^{m_2}\mathbb{Z}_7$ (from $[\mathbb{Z}[j]/(-2+j)^{m_1}]\otimes\mathbb{Z}_7$ and $[\mathbb{Z}[j]/(3+j)^{m_2}\otimes\mathbb{Z}_7]$), for the $\widetilde{\mathscr{E}}_\varphi$'s.

9.2 Theoretical aspects of the computations

The PARI program computing the cyclic cubic fields K is that given in Gras (2019a, § 6.1).

The main PARI instructions are K = bnfinit(P,1), where $P(x)$ is the cubic polynomial defining K, G = nfgaloisconj(P) = {x, g$_1$(x), g$_2$(x)} for the Galois group $\{1,\sigma,\sigma^2\}$, K.fu = {ε_1(x), ε_2(x)} for the set of two independent units, K.clgp giving the structure of the class group.

A crucial fact, without which the checking of the φ-components of the $\mathbb{Z}[j]$-modules $\mathscr{E}_K/\mathscr{F}_K$ and $\mathscr{H}_K$ could be misleading, is the definition of a generator σ of G_K giving the correct conjugation g(x), both for the fundamental units, the

cyclotomic ones and the elements of the class group (see more similar comments at the beginning of Appendix A).

It is not too difficult to find, from K.fu, a "Minkowski unit" ε and its conjugate ε^σ such that $\langle \varepsilon, \varepsilon^\sigma \rangle_{\mathbb{Z}} = \mathbf{E}_K$, up to a prime-to-$p$ index, with σ given by $g(x)$; 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 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 $\mathsf{Reg}_1 = \mathsf{Reg}$ where Reg_1 is the regulator of the units $\varepsilon(\rho)$ and $\varepsilon(g(\rho))$, computed with the root ρ, and where Reg = K.reg is the true regulator given by PARI.

Then we must write the Leopoldt cyclotomic unit η of K of conductor f (Definition 3, formula (20)) under the form $\eta = \varepsilon^{\alpha+\beta\sigma}$, $\alpha, \beta \in \mathbb{Z}$, which is easy as soon as we have η and η^σ. But η is computed by means of the analytic expression of:

$$|\mathbf{C}| = \prod_{a \in [1, f/2[, \sigma_{a|_K} = 1} |\zeta_{2f}^a - \zeta_{2f}^{-a}|,$$

as product of the $|\zeta_{2f}^a - \zeta_{2f}^{-a}|$ for the prime-to-f integers $a < f/2$ such that $\sigma_a = \left(\frac{\mathbb{Q}(\mu_f)/\mathbb{Q}}{a}\right) \in \mathrm{Gal}(\mathbb{Q}(\mu_f)/K)$ (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).

(i) 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 $\pi^3 = f\,\eta'$, $\eta' \in \mathbf{E}_K$, whence $\pi^{3(1-\sigma)} = \eta'^{1-\sigma} = \eta^6 := (\mathbf{C}^{1-\sigma})^6$ (Proposition 5); the program computes $3\ln(\mathbf{C}) - \frac{1}{2}\ln(f) = \frac{1}{2}\ln(\eta')$, so that, to compute η from $\eta^3 = (\sqrt{\eta'})^{1-\sigma}$, we must divide the regulator RegC, built over the conjugates of $\mathbf{C}$, by 3, and multiply $\alpha + j\beta$ by $\frac{1-j}{3}$ in that case where $w_\chi = 1$.

(ii) 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. Indeed, for the first example $f = 13 \cdot 97$, $P = x^3 + x^2 - 420x - 1728$, $\mathbf{H}_K = \mathbb{Z}/21\mathbb{Z}$, $[\mathbf{E}_K : \mathbf{C}_K] = 7$, but $\alpha + j\beta = -3 - 2j$ of norm 7; for $f = 3^2 \cdot 307$, $P = x^3 - 921x - 10745$, $\mathbf{H}_K = \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $[\mathbf{E}_K : \mathbf{C}_K] = 21$, but $\alpha + j\beta = -5 - j$ of norm 21; but in these two cases one must multiply by $w_\chi = 3$.

(iii) 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 η^σ.

The program and the numerical results are given in Appendix A.6. For all the experiments, the real FAMC holds.

Conclusion

Standard probabilistic approaches may confirm (or not) the classical Cohen-Lenstra-Malle-Martinet heuristics on p-class groups, especially in the non semi-simple case. Indeed, heuristics on the order of the whole p-class group of $K = K_\chi$ are given by that of the components $\mathscr{H}_\varphi^{\rm ar}$ which must be compatible with that obtained for the $(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$'s (where $\varphi = \varphi_0\varphi_p \mid \chi = \chi_0\chi_p$ and where e_{φ_0} is the semi-simple idempotent associated to φ_0; see Remark 1); a remarkable fact being that the structures are independent, but with $(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0}$ monogenic and $\mathscr{H}_\varphi^{\rm ar}$ arbitrary as $\mathbb{Z}_p[\mu_{g_\chi}]$-module, which means that heuristics on the *structure* of $\mathscr{H}_\varphi^{\rm ar}$ is another probabilistic problem which clearly depends on that of the filtration that we have studied in Gras (2017) and accessible to probabilities in the spirit of Koymans–Pagano[69] and Smith[70] techniques.

Then, the main problem remains *a proof of the FAMC in the non semi-simple real case* using Arithmetic φ-objects, especially a proof that for all abelian real field K, with a cyclic maximal p-sub-extension, we have, for all $\varphi \in \Phi_K$, $\varphi_0 \neq 1$ (cf. § 8.2 when $[K : \mathbb{Q}]$ a p-power):

$$\#\mathscr{H}_\varphi^{\rm ar} = \#(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0} := (\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)^{e_{\varphi_0}},$$

and:

$$(\mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K)_{\varphi_0} = \left\{\widetilde{\varepsilon} \in \mathscr{E}_K/\widehat{\mathscr{E}}_K\mathscr{F}_K,\ \widetilde{\varepsilon}^{P_\varphi(\sigma_\chi)} = 1\right\};$$

this definition, using $P_\varphi(\sigma_\chi)$ (but not $P_{\varphi_0}(\sigma_\chi)$!) instead of idempotents, may be more convenient in practice.

As we have explained in Remark 7, new tools using auxiliary cyclotomic extensions $K(\mu_\ell)$, $\ell \equiv 1 \pmod{p^N}$, and capitulation of $\mathscr{H}_K$ in these extensions *proves unconditionally* the Finite Real Abelian Main Conjecture; unfortunately, this capitulation conjecture (existence of infinitely many such ℓ's) is not yet proved, but is very attractive since it governs several other arithmetic properties and we believe in this a lot.

A Numerical examples – PARI programs

As the referee pointed out to us, explicit computations in Galois fields K need to define an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, especially with PARI; so, let's recall that PARI

[69] Koymans and Pagano, 2022, "On the distribution of $Cl(K)[\ell^\infty]$ for degree ℓ cyclic fields".
[70] Smith, 2022, "The distribution of ℓ^∞-Selmer groups in degree ℓ twist families".

works in $\mathbb{Q}[x]/(P)$ for an irreducible monic polynomial P defining K and gives a list G = nfgaloisconj(P), of the form $\{s_1(x) = x, s_2(x), \ldots, s_g(x)\}$, $g := \#G_K$, an automorphism $\sigma \in G_K$ being defined by means of $x \mapsto s(x)$, where $s(x) \in \mathbb{Q}[x]$ defines a conjugate, but nfgaloisapply(K, G[i], G[j]) (where s_i = G[i], s_j = G[j]) computes $s_i s_j$, and so on.

Similarly, nfgaloisapply(K, G[i], E[j]) computes the corresponding conjugate of the unit E[j].

For instance, for $P = x^3 - x^2 - 30*x - 27$ (K of conductor $7*13$), PARI gives $G = [x, -1/3*x^2 + 1/3*x + 7, 1/3*x^2 - 4/3*x - 6]$.

In other words, if one chooses a root ρ of P, in the list polroots(P), this defines an embedding and the evaluations $x \mapsto \rho$ in G allow suitable computations which, of course, depend numerically of ρ.

But usual cyclotomic definitions work in $\mathbb{Q}(\zeta_f) \subset \mathbb{C}$ by means of the choice of $\zeta_f := \exp\left(\frac{2i\pi}{f}\right)$, generating the subfield K. This is problematic when one also defines K via PARI since it is ugly to express x, formal root of P, in terms of roots of unity; so, in the programs, conjugates of cyclotomic units are computed from the ζ_f's, and conjugates ζ_f^a, $a \in (\mathbb{Z}/f\mathbb{Z})^\times$, while the units of K are computed via the instruction K.fu, and we must find the correspondence of the two systems, which may be rough as we have explained § 9.2, but always possible. It is what we do in the forthcoming explicit examples when we say, for instance, that for s1 ∈ G the s1-conjugate of a cyclotomic unit Eta is Eta^s1 = 945628377316488.87204143, and so on. This explains that running the programs may give, for the user, results different from ours, without any worries.

A.1 Exceptional congruences

The program verifies the exceptional congruence described in Proposition 1, for the conductors f up to 10^4:

```
{for(m=5,10^4,if(core(m)!=m,next);if(Mod(m,9)!=-3,next);
f=quaddisc(m);PP=x^2-f;PM=x^2+f/3;KP=bnfinit(PP,1);
KM=bnfinit(PM,1);hP=KP.no;hM=KM.no;E=lift(KP.fu[1]);
t=abs(polcoeff(E,0));u=abs(polcoeff(E,1));X=lift(Mod(hP*t*u+hM,3));
print("f=",f," t=",t," u=",u," h=",hP," h'=",hM," htu+h'=",X))}
f=24    t=5     u=1     h=1   h'=1   htu+h'=0
f=60    t=4     u=1/2   h=2   h'=2   htu+h'=0
f=33    t=23    u=4     h=1   h'=1   htu+h'=0
f=168   t=13    u=1     h=2   h'=4   htu+h'=0
f=204   t=50    u=7/2   h=2   h'=4   htu+h'=0
f=69    t=25/2  u=3/2   h=1   h'=3   htu+h'=0
(...)
```

A.2 Numerical examples about the gap $\mathscr{H}_\chi^{\mathrm{ar}}$ v.s. $\mathscr{H}_\chi^{\mathrm{alg}}$

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, of prime conductor ℓ; the field K is of the form K_χ for $\chi\in\mathscr{X}^+$ which is also irreducible p-adic. We have given in Gras (2022) many examples of capitulations of $\mathscr{H}_k$ in K, giving $\mathscr{H}_\chi^{\mathrm{ar}}\subsetneq\mathscr{H}_\chi^{\mathrm{alg}}$.

General PARI program

One must precise the prime $p>2$, the minimal required p-rank rpmin of $\mathscr{H}_k$, the length N of the sub-tower of $k(\mu_\ell)/k$ considered and the interval for m; the program uses primes ℓ (in ell) congruent to 1 modulo $2p^N$, up to Bell; the class group (resp. the p-class group) is computed in Ck (resp. Ckp). To compute $\mathbf{J}_{K/k}(\mathscr{H}_k)$, we represent the p-classes of k by prime ideals $\mathfrak{q}\mid q$ inert in K/k.

```
{p=3;rpmin=1;N=2;bm=2;Bm=10^4;Bell=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,Bell,
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 shall consider the base field $k=\mathbb{Q}(\sqrt{4409})$ (i.e., $m=4409$ in the program) with $\ell=19$, then $\ell=1747$.

Example 1

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 $\mathscr{H}_{k_0}\simeq\mathbb{Z}/9\mathbb{Z}$; 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]
```

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

```
[[0],[-270476874595642910,323533824277028894,-236208800298303000,
      119737461690335806,-255607858779215282,-198423813102857420,
      41058886502087041 4,-110028179006577678,-449600797918214026,
      -4906665437527948,10274048566854232,4319852458093887,
      13258715755947394,-6817941144899095,-15448507867705832,
      2623003974789062,-3264916449440532,-166061269986803 45]]
```

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:

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

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:

$$\mathscr{H}_{\chi_2}^{\mathrm{ar}} = \{x \in \mathscr{H}_{k_2},\ \mathbf{N}_{k_2/k_1}(x) = 1\} = 1, \quad \mathscr{H}_{\chi_2}^{\mathrm{alg}} = \{x \in \mathscr{H}_{k_2},\ \mathcal{V}_{k_2/k_1}(x) = 1\} = \mathscr{H}_{k_2}^3 \simeq \mathbb{Z}/3\mathbb{Z}.$$

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

Similarly, we have:

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

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

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

Thus, the formula of Theorem 3 giving:

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

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:

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

Now we intend to check $\#\mathscr{H}_{\chi_1}^{\mathrm{ar}} = \#(\mathscr{E}_{k_1}/\widehat{\mathscr{E}}_{k_1}\mathscr{F}_{k_1})$ (analytic formula of Theorem 14); in the general definition, $\mathscr{F}_K$ denotes the Leopoldt group of cyclotomic units of K, $\widehat{\mathscr{E}}_K$ the group of units generated by the units of the strict subfields of K.

We give numerical values of the non independent units |e0| of k_0, |ei| of L_1, |Ej| of k_1, and their logarithms; they are, respectively, using 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=0.22187616226319093426668005018505 06     -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      34.48287077198255819743184 71
Eta^s2=2433718277092.6834663091300      28.52044135896859226499696 95
Eta^s3=0.00257365190752746549299 93      -5.96242941301396593243487 762
Eta^s4=1.05749787547388046520 63 E-15   -34.48287077198255819743184 71
Eta^s5=4.10893902310911119828 24 E-13   -28.52044135896859226499696 95
Eta^s6=388.55293409150677930552135       5.96242941301396593243487 762
```

One obtains easily the following relations:

```
E1=e1,   E2=e2^-1,   E3=e0,   E4^2=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 $(\mathscr{E}_{k_1} : \widehat{\mathscr{E}}_{k_1}\mathscr{F}_{k_1}) = (\mathscr{E}_{k_1} : \mathscr{E}_{k_0}\mathscr{E}_{L_1}\mathscr{F}_{k_1}) = 1$ 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 16, 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 $\widehat{\mathscr{E}}_{k_1}$ is of $\mathbb{Z}_3$-rank 3 and $\mathscr{F}_{k_1}$ is of $\mathbb{Z}_3$-rank 2. Indeed, these relations lead to some difficulties in χ-formulas of the literature *using larger groups of cyclotomic units* like Sinnott's cyclotomic units (see Remark 3).

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 log(Eta0) = –9 * log(e0) from the above computation of log(e0); whence $\#\mathscr{H}^{\rm ar}_{\chi_0} = (\mathscr{E}_{k_0} : \widehat{\mathscr{E}}_{k_0}\mathscr{F}_{k_0}) = (\mathscr{E}_{k_0} : \mathscr{F}_{k_0}) = 9$; obviously, 9 is the annihilator of $\mathscr{E}_{k_0}/\mathscr{F}_{k_0}$ and $\mathscr{H}^{\rm ar}_{\chi_0}$ (Conjecture 1).

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

Example 2

Consider the same framework, replacing 19 by the prime 1747; one obtains 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 $\mathfrak{Q}_1$, extending $\mathfrak{Q}_0$ in k_1, is non-principal and such that its class is $\mathfrak{h}_1^6\mathfrak{h}_2^0\mathfrak{h}_3^0$ on the PARI basis $\{\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3\}$:

```
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],[821719075630487115396921 3,52602828277952742913821 8,
           -687786029075595676594134,25130170977215548291757 7,
           -210323764029679768881 26,-15609327127430752932511]]
```

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

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

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

Formula of Theorem 3 is of the form $\#\mathscr{H}_{k_1} = \#\mathscr{H}_{\chi_0}^{\rm ar} \times \#\mathscr{H}_{\chi_1}^{\rm ar} = 9 \times 9$, since we have $\mathscr{H}_{\chi_0}^{\rm ar} = \mathscr{H}_{k_0}$ of order 9; of course a same formula with the $\mathscr{H}^{\rm alg}$'s does not exist since $\#\mathscr{H}_{\chi_0}^{\rm alg} \times \#\mathscr{H}_{\chi_1}^{\rm alg} = 9 \times 27$.

Varying $\ell \equiv 1 \pmod 9$

The program gives the following other results, for $k = \mathbb{Q}(\sqrt{4409})$, varying only ell, where q is the prime split in $k_0 = k$ 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 holds with the $\#\mathscr{H}_{k_i}^{\rm ar}$'s but not for the $\#\mathscr{H}_{k_i}^{\rm alg}$'s.

A.3 Computation of $\#\mathbf{H}_\chi$ for $K = \mathbb{Q}(\mu_{47})$

Let $K := K_\chi$ be the field $\mathbb{Q}(\mu_{47})$, of degree $g_\chi = 46$. From Theorem 7, we have $\#\mathbf{H}_\chi = 2^{\alpha_\chi} \cdot w_\chi \cdot \prod_{\psi|\chi} \left(-\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right)$ with in that case $\alpha_\chi = 0$, $w_\chi = 47$ where $-\frac{1}{2}\mathbf{B}_1(\psi^{-1}) = -\frac{1}{2}\sum_{a=1}^{46}\left(\frac{a}{47} - \frac{1}{2}\right)\psi^{-1}(\sigma_a) = -\frac{1}{2}\sum_{a=1}^{46}\frac{a}{47}\,\psi^{-1}(\sigma_a)$.

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

```
{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)=",47*norm(B))}
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 $(\sigma_a - a, 47)$, with for instance $a = 5$ (Lemma 14), and then $\mathfrak{A}_K \times \frac{1}{2}\mathbf{B}_K$ annihilates $\mathbf{H}_\chi$; since the image of $\mathfrak{A}_K \times \frac{1}{2}\mathbf{B}_K$ is the ideal $\left(\frac{1}{2}\mathbf{B}_1(\psi^{-1})\right) = \mathfrak{p}_{139}$, *the annihilator* of $\mathbf{H}_\chi$ is $\mathfrak{p}_{139}$. But this ideal is not principal in $\mathbb{Q}(\mu_{46})$:

```
{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.

A.4 Computation of annihilators of torsion groups $\mathscr{T}_K$

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, using the main program of Appendix A.6, one obtains:

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

where $(1-2j)\mathbb{Z}[j]$ is a prime $\mathfrak{p}$ dividing 7, and $\mathscr{T}_K \simeq \mathbb{Z}/7^2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

The following program, only valid for prime conductors f, computes the annihilator $\mathbf{A}_K(c)$ of $\mathscr{T}_K$; it defines the classes $\sigma^k\mathrm{Gal}(\mathbb{Q}(\mu_{f\,p^N})/K)$, $k = 0, 1, 2$, 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 $(\beta) = \mathfrak{p}_1^u\mathfrak{p}_2^v$ 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, $A_0 = 184$, $A_1 = 1526$ and $A_2 = 643$; this yields the ideal $(1-2j)^3 = \mathfrak{p}^3$. Necessarily, $\mathscr{T}_K \simeq \mathbb{Z}[j]/\mathfrak{p}^2 \times \mathbb{Z}[j]/\mathfrak{p}$. We note that the annihilator is $\mathfrak{p}^3$ (and not $\mathfrak{p}^2$) although the structure is not $\mathbb{Z}[j]/\mathfrak{p}^3$.

A.5 Computation of the invariants of $\psi(\Omega_\ell)$

The program computes, for cyclic cubic fields, the $\psi(\Omega_\ell) = r_1 - r_2 - (r_1 + 2r_2)\,j$ only with the knowledge of η_K; here, the PARI notations become $\Omega_\ell =: r_1 + r_2\sigma^{-1} + r_3\sigma^{-2}$, with $r_1 + r_2 + r_3 \equiv 0 \pmod{(\ell-1)}$ because of relation (25) with $\mathbf{N}_{K/\mathbb{Q}}(\eta_K) = 1$), whence $\psi(\Omega_\ell)$ with $\psi(\sigma) = j$; taking a primitive root $\mathbf{g}_\ell$ modulo ℓ, the r_σ's come from the PARI instructions r = znlog(L[j],g), where the L[j]'s are the rationals a_σ such that $\eta_K^\sigma \equiv a_\sigma \pmod{\mathfrak{l}_0}$ in K (we use the results of Appendix A.6 to compute $\eta_K = \varepsilon_K^{\alpha+\beta\sigma}$ and $\mathbf{H}_K$).

The line Orders of components of cl(Lell) of the form $(p^u, p^v, \cdot\cdot)$ means that the components of the p-class of $\mathfrak{l}_0$, on the PARI system of generators of $\mathscr{H}_K$, are of orders p^u, p^v, $\cdots$; one sees that the annihilator Ω_ℓ is independent on these orders, but it is clear that, using Chebotarev's theorem, any set of components may be obtained.

```
{p=7;n=3;P=x^3+x^2-884540*x-393129;alpha=-112;beta=-70;
Q=y^2+y+1;k=bnfinit(Q);J=Mod(y,Q);pi=idealfactor(k,p);
pi1=component(pi,1)[1];pi2=component(pi,1)[2];
K=bnfinit(P,1);G=nfgaloisconj(P);CK=K.cyc;d=matsize(CK)[2];
CKp=List;for(i=1,d,h=p^valuation(CK[i],p);listput(CKp,h,i));
print("P=",P," p-class group=",CKp);
E=K.fu;E1=E[1];E2=nfgaloisapply(K,G[2],E[1]);
F1=E1^alpha*E2^beta;F2=nfgaloisapply(K,G[2],F1);
F1=lift(F1);F2=lift(F2);forprime(ell=1,5*10^5,
if(Mod(ell,p^n)!=1 || matsize(factor(P+O(ell)))[1]!=3,next);
g=znprimroot(ell);Lell=component(idealfactor(K,ell),1)[1];
F10=Mod(polcoeff(F1,0),ell);F11=Mod(polcoeff(F1,1),ell);
F12=Mod(polcoeff(F1,2),ell);Eta1=lift(F12*x^2+F11*x+F10);
F20=Mod(polcoeff(F2,0),ell);F21=Mod(polcoeff(F2,1),ell);
F22=Mod(polcoeff(F2,2),ell);Eta2=lift(F22*x^2+F21*x+F20);
Leta=List;listput(Leta,Eta1,1);listput(Leta,Eta2,2);L=List;
for(i=1,2,A=Mod(Leta[i],P);for(a=1,ell-1,v=idealval(K,A-a,Lell);
if(v>0,listput(L,a,i))));Lr=List;for(i=1,2,r=znlog(L[i],g);
listput(Lr,r));print();print("ell=",ell," Omega=",Lr);
X=Lr[1]-Lr[2]+(-Lr[1]-2*Lr[2])*J;
w1=idealval(k,X,pi1);w2=idealval(k,X,pi2);
Y=alpha+beta*J;W1=idealval(k,Y,pi1);W2=idealval(k,Y,pi2);print
("Cyclotomic invariants=",W1,",",W2," Omega invariants=",w1,",",w2);
```

```
Exp=List;Order=bnfisprincipal(K,Lell)[1];for(i=1,d,
tp=valuation(CK[i],p);if(Order[i]==0,Or=1);if(Order[i]!=0,
t=valuation(Order[i],p);Or=p^(tp-t));listput(Exp,Or));
print("Orders of components of cl(Lell)=",Exp))}
```

For $P = x^3 + x^2 - 884540x - 393129$ (conductor $f = 2653621$, $\alpha = -112$, $\beta = -70$), the φ-components of $\mathscr{H}_K$ for $p = 7$ are $\mathscr{H}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_1}$, $\mathscr{H}_{\varphi_2} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_2}^3$; we have $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_1}$, $\widetilde{\mathscr{E}}_{\varphi_2} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_2}^3$.

```
P=x^3+x^2-884540*x-393129 p-class group=List([343,7])
conductor f=2653621

ell=1373 Omega=List([1162, 1246])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=7547 Omega=List([6888, 1526])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=8233 Omega=List([6496, 742])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([49, 7])

ell=18523 Omega=List([11830, 12586])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 1])

ell=22639 Omega=List([4004, 13104])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=30871 Omega=List([27734, 5390])
Cyclotomic invariants=1,3 Omega invariants=2,3
Orders of components of cl(Lell)=List([343, 1])

ell=39103 Omega=List([32018, 35812])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([49, 7])

ell=42533 Omega=List([1330, 17262])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=54881 Omega=List([44366, 18662])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([49, 7])

ell=58997 Omega=List([5236, 21938])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=72031 Omega=List([24276, 51884])
```

```
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=76147 Omega=List([17066, 25606])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=80263 Omega=List([22036, 79352])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])

ell=93983 Omega=List([69174, 5558])
Cyclotomic invariants=1,3 Omega invariants=1,3
Orders of components of cl(Lell)=List([343, 7])
```

For $P = x^3 - 4792107\,x + 4022175142$ ($f = 3^2 \cdot 1597369$, $\alpha = -7$, $\beta = -21$), the φ-components of $\mathscr{H}_K$ are $\mathscr{H}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_1} \times \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_1}$ and $\mathscr{H}_{\varphi_2} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_2}$; nevertheless, we have $\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_1}^2$ (non-isomorphic to $\mathscr{H}_{\varphi_1}$) and $\widetilde{\mathscr{E}}_{\varphi_2} \simeq \mathbb{Z}_7[j]/\mathfrak{p}_{\varphi_2}$.

But almost all Ω_ℓ give the expected response $(2,1)$ whatever the order of the p-class of $\mathfrak{l}_0 \mid \ell$:

```
P=x^3 - 4792107*x + 4022175142 p-class group=List([7,7,7])
conductor f=9*1597369

ell=1373 Omega=List([917, 1267])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=8233 Omega=List([1141, 3535])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 1, 7])

ell=49393 Omega=List([41069, 39277])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([1, 7, 1])

ell=54881 Omega=List([14357, 31311])
Cyclotomic invariants=2,1 Omega invariants=2,2
Orders of components of cl(Lell)=List([7, 7, 7])

ell=63799 Omega=List([53977, 53767])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=76147 Omega=List([44912, 73514])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([1, 7, 7])

ell=80263 Omega=List([20328, 16387])
Cyclotomic invariants=2,1 Omega invariants=3,1
Orders of components of cl(Lell)=List([1, 7, 7])
              (...)
ell=329281 Omega=List([311136, 189770])
```

```
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=331339 Omega=List([157696, 276465])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=343687 Omega=List([174391, 82173])
Cyclotomic invariants=2,1 Omega invariants=2,2
Orders of components of cl(Lell)=List([7, 7, 7])

ell=363581 Omega=List([204974, 276584])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=384847 Omega=List([254100, 68887])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=396509 Omega=List([114947, 1540])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=403369 Omega=List([11361, 206458])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=408857 Omega=List([364287, 259343])
Cyclotomic invariants=2,1 Omega invariants=5,1
Orders of components of cl(Lell)=List([7, 7, 1])

ell=415717 Omega=List([239225, 363657])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 1, 7])

ell=417089 Omega=List([327908, 33957])
Cyclotomic invariants=2,1 Omega invariants=3,4
Orders of components of cl(Lell)=List([1, 7, 7])

ell=419147 Omega=List([17059, 339451])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([1, 1, 1])

ell=426007 Omega=List([161434, 215859])
Cyclotomic invariants=2,1 Omega invariants=2,1
Orders of components of cl(Lell)=List([7, 7, 7])

ell=456877 Omega=List([361697, 10010])
Cyclotomic invariants=2,1 Omega invariants=3,1
Orders of components of cl(Lell)=List([7, 7, 7])
```

For $\ell = 419147$, one gets the first example where any prime ideal $\mathfrak{l} \mid \ell$ is principal:

```
bnfisprincipal(K,Lell)=
```

```
[0,0,0],[1311001361541054679,35057663364174,1019317530188062]
```

but the invariants of Ω_ℓ are still (2,1) giving $\#\mathscr{H}_{\varphi_1} = 7^2$ and $\#\mathscr{H}_{\varphi_2} = 7$.

A.6 Illustrations of the FAMC

We intend to illustrate the FAMC with cyclic cubic fields and $p \equiv 1 \pmod 3$ giving two p-adic characters (of course, it is now a Theorem and we shall speak of the "Finite Abelian Main Theorem"); then statistics may have some interest.

The general PARI program

The program is the following and we explain, with some examples, how to use the numerical results checking the Finite Abelian Main Theorem; hmin = p^{vp} means that the program only computes fields with p-class groups CKp of order at least p^{vp}; then bf, Bf define an interval for the conductors f of the cyclic cubic field. Other indications are given in the text of the program:

```
\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)))))}
```

Numerical examples

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

$e_1 \approx 3062171948818717694.348000505806$ and $e_2 \approx 1.221295564694E-69$.

Galois structure of $\mathscr{E}_K/\mathscr{F}_K$. Let ε be the $\mathbb{Z}[G_K]$-generator of $\mathbf{E}_K$ and let η that of the subgroup $\mathbf{F}_K$ of Leopoldt's cyclotomic units; thus we have $\eta = \varepsilon^{\alpha+\beta\sigma}$ and obtain $\mathbf{E}_K/\mathbf{F}_K \simeq \mathbb{Z}[j]/(\alpha + j\beta)\mathbb{Z}[j]$, where j is a root of $S := y^2 + y + 1$.

In all the sequel, from a factorization $p = (r_1 + j r_1') \times (r_2 + j r_2')$ giving the ideal product $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[j]$, we associate, regarding the exponent p^e, the two annihilators $c_i + \sigma$ such that $(c_i + j) = \mathfrak{p}_i^e$ (up to a prime-to-p ideal); this preserves the definition of the φ_1 and φ_2-components.

For instance, for $p = 7$, $\mathfrak{p}_1 := (-2+j)\mathbb{Z}[j]$ and $\mathfrak{p}_2 := (3+j)\mathbb{Z}[j]$; writing $(\alpha + j\,\beta) =: \mathfrak{p}_1^u \times \mathfrak{p}_2^v \times \mathfrak{a}$, $\mathfrak{a}$ prime to 7, we get immediately the two φ-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 $-22 + j$).

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 $\{h_1, \dots, h_r\}$ 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 following instructions, where G[2] gives the σ-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 $\mathbb{Z}[j]/\mathfrak{p}_1^v \times \mathfrak{p}_2^0$ 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)=(-3.0000000,-2.0000000)  Index [E_K:C_K]=7.0000000
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 $\mathscr{T}_K = \mathscr{H}_K \bigoplus \mathscr{R}_K$.

```
P=x^3+x^2-2450*x-1089  f=7351=Mat([7351,1])  (a,b)=(-1,33)
Class group=[49]  sigma=4
(alpha,beta)=(5.0000000,8.0000000)  Index [E_K:C_K]=49.0000000
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 φ_2-components are trivial. Since $\mathscr{T}_K \simeq \mathbb{Z}/7^4\mathbb{Z}$, $\mathscr{R}_K = \mathscr{T}_K^{7^2}$, $\mathscr{H}_K \simeq \mathscr{T}_K/\mathscr{R}_K \simeq \mathbb{Z}/7^2\mathbb{Z}$.

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)=(19.0000000,18.0000000)  Index [E_K:C_K]=343.0000000
h=[1],  sigma(h)=[18]
0  3   P1 and P2-valuations for alpha+j*beta
0  3   P1 and P2-valuations for  H
Structure of the 7-torsion group: List([343,7])
```

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

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

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

this means that the corresponding generating classes h, h', fulfill the relations (regarding the basis $\{h_1, h_2\}$ of the class group) $h = h_1^a h_2^b$ and $h^\sigma = h_1^c \times h_2^d$, then $h' = h_1^{a'} \times h_2^{b'}$ and $h'^\sigma = h_1^{c'} \times h_2^{d'}$. Thus we compute the conditions $H^{c_i+\sigma} = 1$, $i = 1, 2$, for $H := h^x \times h'^y$; this gives the relations R11, R21 (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 they have been computed for verification and are not printed.

```
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)=(-7.0000000,-7.0000000)  Index [E_K:C_K]=49.0000000
h=[1,0],  sigma(h)=[0,1]
h'=[0,1], sigma(h')=[6,6]
1  1   P1 and P2-valuations for alpha+j*beta
R11=3*X+6*Y  R12=1*X+2*Y
R21=5*X+6*Y  R22=1*X+4*Y
Structure of the 7-torsion group: List([49,7])
```

This case means that $\widetilde{\mathscr{E}}_K \simeq \mathbb{Z}[j]/(7)$, giving the two non-trivial φ-components of order 7. The relations, for $\mathscr{H}_K$, reduce to R11 and R21 Thus $\mathscr{H}_K = \mathscr{H}_{\varphi_1} \bigoplus \mathscr{H}_{\varphi_2} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, $\mathscr{R}_K = \mathscr{T}_K^7 \simeq \mathbb{Z}/7\mathbb{Z}$.

```
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)=(-32.0000000,-20.0000000) Index [E_K:C_K]=784.0000000
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)=(42.0000000,28.0000000) Index [E_K:C_K]=1372.0000000
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 $(\alpha + \beta j) = 2 \cdot 7 \cdot (3 + 2j)$ giving the annihilator $\mathfrak{p}_1^2\mathfrak{p}_2$ which is also the annihilator of $\mathscr{H}_K$. The structure is $\mathscr{T}_K = \mathscr{H}_K \bigoplus \mathscr{R}_K$.

```
P=x^3+x^2-884540*x-393129  f=2653621=Mat([2653621,1])  (a,b)=(-1,627)
Class group=[686,14]  sigma=2
(alpha,beta)=(-112.0000000,-70.0000000)  Index [E_K:C_K]=9604.0000000
h=[2,0],  sigma(h)=[36,2]
h'=[0,2], sigma(h')=[0,4]
1   3   P1 and P2-valuations for alpha+j*beta
R11=74*X+0*Y  R12=2*X+42*Y
R21=0*X+0*Y  R22=2*X+311*Y
Structure of the 7-torsion group: List([343,49])
```

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

(**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)=(-7.0000000,-21.0000000) Index [E_K:C_K]=343.0000000
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 α and β, we obtain, for $\widetilde{\mathscr{E}}_K = \mathscr{E}_K/\mathscr{F}_K$:

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

where $\mathfrak{p}_1 = (-2+j)$ and $\mathfrak{p}_2 = (3+j)$. We get the φ-components:

$$\widetilde{\mathscr{E}}_{\varphi_1} \simeq (\mathbb{Z}[j]/\mathfrak{p}_1^2)\otimes\mathbb{Z}_7 \simeq \mathbb{Z}/7^2\mathbb{Z} \quad \text{and} \quad \widetilde{\mathscr{E}}_{\varphi_2} \simeq (\mathbb{Z}[j]/\mathfrak{p}_2)\otimes\mathbb{Z}_7 \simeq \mathbb{Z}/7\mathbb{Z}.$$

To obtain the two φ-components of $\mathscr{H}_K = \mathscr{T}_K$, we put $H = h^x h'^y h''^z$ and we determine the solutions of the two relations$H^{P_{\varphi_i}(\sigma)} = 1$, $i = 1,2$, 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, of ranks 1 and 2, respectively:

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

They are equivalent to:

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

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

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

We have indeed equalities for the orders of the φ-components relative to $\widetilde{\mathscr{E}}_K$ and $\mathscr{H}_K$, respectively, but of course with different structures of $\mathbb{Z}_7[j]$-modules since:

$$\widetilde{\mathscr{E}}_{\varphi_1} \simeq \mathbb{Z}/7^2\mathbb{Z} \ \ \&\ \ \mathscr{H}_{\varphi_1} \simeq [\mathbb{Z}/7\mathbb{Z}]^2.$$

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)=(28.0000000,-7.0000000) Index [E_K:C_K]=1029.0000000
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)=(42.0000000,77.0000000) Index [E_K:C_K]=4459.0000000
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)=(15.0000000,8.0000000) Index [E_K:C_K]=169.0000000
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)=(7.0000000,-8.0000000) Index [E_K:C_K]=169.0000000
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)=(-21.0000000,-5.0000000) Index [E_K:C_K]=361.0000000
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)=(19.0000000,4.19514516 E-69) Index [E_K:C_K]=361.0000000
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)=(31.0000000,-4.10842850 E-69) Index [E_K:C_K]=961.0000000
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)=(-11.0000000,-35.0000000) Index [E_K:C_K]=961.0000000
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])
```

Acknowledgments

I would like to warmly thank the anonymous Referee for a large number of comments and suggestions which have improved the readability of this survey and enabled clarifications and corrections, as about a false remark about monogenicity of unit groups that is explained in the new Remark 6 with the counterexample of the Referee.
I sincerely thank Philippe Heinrich for his offer to put the paper into the final format for the NWEJM, and the Editors, Pierre Dèbes and Olivier Goubet, for their support.

References

All, T. (2013). "On p-adic annihilators of real ideal classes". *J. Number Theory* **133** (7), pp. 2324–2338. DOI: 10.1016/j.jnt.2012.12.013 (cit. on pp. 114, 146).

All, T. (2017). "Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups". *Acta Arithmetica* **178**, pp. 273–299. DOI: 10.4064/aa8537-2-2017 (cit. on pp. 114, 146).

Amice, Y. and J. Fresnel (1972). "Fonctions zêta p-adiques des corps de nombres abéliens réels". French. *Acta Arithmetica* **20** (4), pp. 353–384. URL: http://matwbn.icm.edu.pl/ksiazki/aa/aa20/aa2043.pdf (cit. on p. 151).

Ankeny, N., E. Artin, and S. Chowla (1952). "The class number of real quadratic fields". *Ann. Math.(2)* **56** (3), pp. 479–493. DOI: 10.2307/1969656 (cit. on p. 111).

Belliard, J.-R. and A. Martin (2014). "Annihilation of real classes", 10 pp. URL: http://jrbelliard.perso.math.cnrs.fr/BM1.pdf (cit. on p. 114).

Belliard, J.-R. and T. Nguyen Quang Do (2005). "On modified circular units and annihilation of real classes". *Nagoya Math. J.* **177**, pp. 77–115. DOI: 10.1017/S0027763000009065 (cit. on p. 114).

Bertrandias, F. and J.-J. Payan (1972). "Γ-extensions et invariants cyclotomiques". French. *Ann. Sci. Ec. Norm. Sup., 4e série* **5** (4), pp. 517–548. DOI: 10.24033/asens.1236 (cit. on p. 150).

Bullach, D. et al. (2021). "Dirichlet L-series at $s = 0$ and the scarcity of Euler systems". URL: https://arxiv.org/abs/2111.14689 (cit. on p. 115).

Burns, D. et al. (2023). "On Euler systems for the multiplicative group over general number fields". *Publ. Mat., Barc.* **67** (1), pp. 89–126. DOI: 10.5565/publmat6712302 (cit. on p. 115).

Chevalley, C. (1933). "Sur la théorie du corps de classes dans les corps finis et les corps locaux". French. *J. Fac. Sci., Univ. Tokyo, Sect. I* **2**, pp. 365–476. URL: http://archive.numdam.org/item/THESE_1934__155__365_0/ (cit. on p. 161).

Coates, J. (1977). *p-adic L-functions and Iwasawa's theory*. Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975). DOI: 10.17863/CAM.72005 (cit. on pp. 117, 146, 151).

Coates, J. and Y. Li (2020). "Non-vanishing theorems for central *L*-values of some elliptic curves with complex multiplication". *Proceedings of the London Math. Soc. (3)* **121** (6), pp. 1531–1578. DOI: 10.1112/plms.12379 (cit. on p. 115).

Coates, J. and R. Sujatha (2006). *Cyclotomic Fields and Zeta Values*. Springer Monogr. Math. Berlin: Springer, pp. 89–99. ISBN: 3-540-33068-2. DOI: 10.1007/978-3-540-33069-1 (cit. on p. 115).

Darmon, H. (1995). "Thaine's method for circular units and a conjecture of Gross". *Canad. J. Math.* **47** (2), pp. 302–317. DOI: 10.4153/CJM-1995-016-6 (cit. on p. 115).

Dasgupta, S. and M. Kakde (2023). "On the Brumer-Stark Conjecture". *Ann. Math. (2)* **197** (1), pp. 289–388. DOI: 10.4007/annals.2023.197.1.5 (cit. on p. 115).

Dasgupta, S., M. Kakde, et al. (2023). "The residually indistinguishable case of Ribet's method for GL_2". URL: https://arxiv.org/pdf/2310.16396.pdf (cit. on p. 115).

Fresnel, J. (1967). *Nombres de Bernoulli et fonctions L p-adiques*. Séminaire Delange–Pisot–Poitou (Théorie des nombres) (1965/1966). URL: http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A3_0 (cit. on p. 117).

Gillard, R. (1974). *Relations de Stickelberger*. Séminaire de théorie des nombres de Grenoble (1974–1975). URL: http://www.numdam.org/item/?id=STNG_1974-1975__4__A1_0 (cit. on p. 146).

Gillard, R. (1976). *Sur le groupe des classes des extensions abéliennes réelles*. Séminaire de théorie des nombres de Grenoble (1975–1977). URL: http://eudml.org/doc/275207 (cit. on p. 114).

Grandet, M. and J.-F. Jaulent (1985). "Sur la capitulation dans une $\mathbb{Z}_\ell$-extension". *J. reine angew. Math.* **362**, pp. 213–217. DOI: 10.1515/crll.1985.362.213 (cit. on p. 113).

Gras, G. (1976). "Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes". *PMB (Algèbre et théorie des nombres)* **2** (1). DOI: 10.5802/pmb.a-10 (cit. on pp. 110, 146, 148, 149, 154–156, 166, 167, 169, 170).

Gras, G. (1977a). "Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés". *Ann. Inst. Fourier* **27** (1), pp. 1–66. DOI: 10.5802/aif.641 (cit. on pp. 110, 114).

Gras, G. (1977b). "Étude d'invariants relatifs aux groupes des classes des corps abéliens". **41–42**, pp. 35–53. URL: http://www.numdam.org/item/AST_1977__41-42__35_0.pdf (cit. on pp. 110, 118, 157, 166, 167).

Gras, G. (1978). "Sommes de Gauss sur les corps finis". *PMB (Algèbre et théorie des nombres)* **1** (2), 72 pp. DOI: 10.5802/pmb.a-16 (cit. on pp. 146, 150).

Gras, G. (1979a). "Annulation du groupe des ℓ-classes généralisées d'une extension abélienne réelle de degré premier à ℓ". *Ann. Inst. Fourier* **29** (1), pp. 15–32. URL: http://www.numdam.org/item?id=AIF_1979__29_1_15_0 (cit. on pp. 114, 152).

Gras, G. (1979b). *Sur l'annulation en 2 des classes relatives des corps abéliens*. Math. Rep. Acad. Sci., R. Soc. Can. URL: https://mathreports.ca/article/sur-lannulation-en-2-des-classes-relatives-des-corps-abeliens/ (cit. on p. 150).

Gras, G. (1980). *Sur la construction des fonctions L p-adiques abéliennes*. Séminaire Delange-Pisot-Poitou (Théorie des nombres) (1978–1979). URL: http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A1_0 (cit. on pp. 117, 146, 151, 170).

Gras, G. (1982). "Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres". *J. reine angew. Math.* **333**, pp. 86–132. DOI: 10.1515/crll.1982.333.86 (cit. on p. 117).

Gras, G. (1983). "Logarithme p-adique et groupes de Galois". *J. reine angew. Math.* **343**, pp. 64–80. DOI: 10.1515/crll.1983.343.64 (cit. on p. 117).

Gras, G. (1986). "Théorie des genres analytique des fonctions L p-adiques des corps totalement réels". *Invent. math.* **86**, pp. 1–17. DOI: 10.1007/BF01391492 (cit. on pp. 111, 117, 153).

Gras, G. (1987). "Pseudo-mesures associées aux fonctions L de $\mathbb{Q}$". *manuscr. math.* **57**, pp. 373–415. DOI: 10.1007/BF01168668 (cit. on pp. 111, 117, 153).

Gras, G. (1998). "Théorèmes de réflexion". *J. Théorie Nombres Bordeaux* **10** (2), pp. 399–499. URL: http://eudml.org/doc/248168 (cit. on p. 168).

Gras, G. (2005). *Class Field Theory: from theory to practice, corr. 2nd ed.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, pp. xiii+507. DOI: 10.1007/978-3-662-11323-3 (cit. on pp. 117, 151, 157, 158, 164, 167, 168).

Gras, G. (2016). "Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques; english translation: = https://arxiv.org/abs/1701.02618". *Canad. J. Math.* **68** (3), pp. 571–624. DOI: 10.4153/CJM-2015-026-3 (cit. on p. 117).

Gras, G. (2017). "Invariant generalized ideal classes – Structure theorems for p-class groups in p-extensions". *Proc. Indian Acad. Sci. (Math. Sci.)* **127** (1), pp. 1–34. DOI: 10.1007/s12044-016-0324-1 (cit. on p. 173).

Gras, G. (2018a). "Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ for real abelian extensions $K/\mathbb{Q}$". *Communications in Advanced Mathematical Sciences* **1** (1), pp. 5–34. URL: https://dergipark.org.tr/tr/download/article-file/543993 (cit. on pp. 114, 149, 152, 159).

Gras, G. (2018b). "The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator". *Int. J. Number Theory* **14** (2), pp. 329–337. DOI: 10.1142/S1793042118500203 (cit. on pp. 117, 151, 163).

Gras, G. (2019a). "Heuristics and conjectures in direction of a p-adic Brauer-Siegel theorem". *Math. Comput.* **88** (318), pp. 1929–1965. DOI: 10.1090/mcom/3395 (cit. on pp. 117, 151, 170, 171).

Gras, G. (2019b). "Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg". *Ann. Math. Qué.* **43** (2), pp. 249–280. DOI: 10.1007/s40316-018-0108-3 (cit. on p. 163).

Gras, G. (2019c). "Practice of the Incomplete p-Ramification Over a Number Field – History of Abelian p-Ramification". *Communications in Advanced Mathematical Sciences* **2** (4), pp. 251–280. DOI: 10.33434/cams.573729 (cit. on p. 112).

Gras, G. (2021). "Algorithmic complexity of Greenberg's conjecture". *Arch. Math.* **117** (3), pp. 277–289. DOI: 10.1007/s00013-021-01618-9 (cit. on p. 158).

Gras, G. (2022). "On the λ-stability of p-class groups along cyclic p-towers of a number field". *Int. J. Number Theory* **18** (10), pp. 2241–2263. DOI: 10.1142/S1793042122501147 (cit. on pp. 169, 175).

Gras, G. (2023a). "Algebraic norm and capitulation of p-class groups in ramified cyclic p-extensions". *Math. of Computation*, 56 pp. DOI: doi.org/10.1090/mcom/3920 (cit. on pp. 112, 120, 157).

Gras, G. (2023b). "The Chevalley–Herbrand formula and the real abelian Main Conjecture (New criterion using capitulation of the class group)". *J. Number Theory* **248**, pp. 78–119. DOI: 10.1016/j.jnt.2023.01.002 (cit. on pp. 112, 120, 157, 163, 164).

Gras, G. (2024a). "Genus theory of p-adic pseudo-measures – Tame kernels & abelian p-ramification", 29 pp. URL: https://arxiv.org/abs/2310.10112 (cit. on p. 153).

Gras, G. (2024b). "The real abelian main conjecture in the non semi-simple case". *Beiträge zur Algebra und Geometrie*, 29 pp. DOI: 10.1007/s13366-023-00725-8 (cit. on pp. 112, 120, 157, 163, 164).

Greenberg, R. (1975). "On p-adic L-functions and cyclotomic fields". *Nagoya Math. J.* **56**, pp. 61–77. DOI: 10.1017/S002776300001638X (cit. on pp. 113, 117).

Greenberg, R. (1977). "On p-adic L-functions and cyclotomic fields. II". *Nagoya Math. J.* **67**, pp. 139–158. DOI: 10.1017/S0027763000022583 (cit. on pp. 113, 117).

Greither, C. (1992). "Class groups of abelian fields, and the main conjecture". *Ann. Inst. Fourier* **42** (3), pp. 449–499. DOI: 10.5802/aif.1299 (cit. on pp. 114, 117, 129, 156, 166–168).

Greither, C. and R. Kučera (2014). "Eigenspaces of the ideal class group". *Ann. Inst. Fourier* **64** (5), pp. 2165–2203. DOI: 10.5802/aif.2908 (cit. on pp. 114, 160, 168).

Greither, C. and R. Kučera (2015). "Annihilators for the class group of a cyclic field of prime power degree III". *Publicationes Mathematicae Debrecen* **86** (11), pp. 401–421. DOI: 10.5486/PMD.2015.7029 (cit. on pp. 114, 160, 168).

Greither, C. and R. Kučera (2021). "Washington units, semispecial units, and annihilation of class groups". *Manuscr. Math.* **166** (1–2), pp. 277–286. DOI: 10.1007/s00229-020-01241-y (cit. on pp. 114, 160).

Group, T. P. (2016). *PARI/GP, version 2.9.0*. Université de Bordeaux. URL: https://pari.math.u-bordeaux.fr/ (cit. on p. 110).

Hasse, H. (1985). *Über die Klassenzahl abelscher Zahlkörper. Mit einer Einleitung zur Reprintausgabe von Jacques Martinet.* **1**. Math. Lehrbücher Monogr., II. Abt., Math. Monogr. Akademie-Verlag, Berlin (cit. on pp. 141, 142, 144, 145, 154).

Iwasawa, K. (1962). "A class number formula for cyclotomic fields". *Ann. Math. (2)* **76** (1), pp. 171–179. DOI: 10.2307/1970270 (cit. on p. 146).

Iwasawa, K. (1964). "On some modules in the theory of cyclotomic fields". *J. Math. Soc. Japan* **16** (1), pp. 42–82. DOI: 10.2969/jmsj/01610042 (cit. on p. 117).

Jaulent, J.-F. (1981). "Unités et classes dans les extensions métabéliennes de degré $n\ell^s$ sur un corps de nombres algébriques". *Ann. Inst. Fourier* **31** (1), pp. 39–62. DOI: 10.5802/aif.816 (cit. on p. 115).

Jaulent, J.-F. (1984). "Représentations ℓ-adiques et invariants cyclotomiques". *PMB (Algèbre et téorie des nombres)* **3**, 41 pp. DOI: 10.5802/pmb.a-39 (cit. on p. 115).

Jaulent, J.-F. (1986). "L'arithmétique des ℓ-extensions (Thèse d'état)". *PMB (Algèbre et téorie des nombres)* **1** (1), pp. 1–357. DOI: 10.5802/pmb.a-42 (cit. on pp. 115, 117, 163).

Jaulent, J.-F. (1990). "La théorie de Kummer et le K_2 des corps de nombres". *J. Théorie Nombres Bordeaux* **2** (2), pp. 377–411. DOI: 10.5802/jtnb.34 (cit. on p. 150).

Jaulent, J.-F. (1998). "Théorie ℓ-adique globale du corps de classes". *J. Théorie Nombres Bordeaux* **10** (2), pp. 355–397. DOI: 10.5802/jtnb.233 (cit. on p. 117).

Jaulent, J.-F. (2021). "Annulateurs de Stickelberger des groupes de classes logarithmiques". *Acta Arithmetica* **201**, pp. 241–253. DOI: 10.4064/aa201127-22-6 (cit. on pp. 114, 153).

Jaulent, J.-F. (2023). "Annulateurs circulaires des groupes de classes logarithmiques". *Ann. Inst. Fourier*. URL: https://hal.archives-ouvertes.fr/hal-02519397 (cit. on pp. 114, 153).

Kezuka, Y. and Y. Li (2023). "Non-vanishing of central L-values of the Gross family of elliptic curves", 17 pp. DOI: 10.48550/arXiv.2305.08689 (cit. on p. 115).

Kolyvagin, V. (2007). *Euler Systems*. Ed. by P. Cartier et al. Birkhäuser Boston, pp. 435–483. DOI: 10.1007/978-0-8176-4575-5_11 (cit. on pp. 114, 164).

Koymans, P. and C. Pagano (2022). "On the distribution of $Cl(K)[\ell^\infty]$ for degree ℓ cyclic fields". *J. Eur. Math. Soc.* **24** (4), pp. 1189–1283. DOI: 10.4171/JEMS/1112 (cit. on p. 173).

Kraft, J. and R. Schoof (1995). "Computing Iwasawa modules of real quadratic number fields". *Compositio Math. (Erratum: Compositio Math. **103**(2) (1996), p. 241.)* **97** (1-2), pp. 135–155. URL: http://eudml.org/doc/90370 (cit. on p. 113).

Kubota, T. and H. Leopoldt (1964). "Eine p-adische Theorie der Zetawerte. I: Einführung der p-adischen Dirichletschen L-Funktionen". *J. reine angew. Math.* **214/215**, pp. 328–339. URL: http://eudml.org/doc/150624 (cit. on p. 151).

Kudo, A. (1975). "On a class number relation of imaginary abelian fields". *J. Math. Soc. Japan* **27** (1), pp. 150–159. DOI: 10.2969/jmsj/02710150 (cit. on p. 111).

Kummer, E. (1855). "Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke". *J. reine angew. Math.* **50**, pp. 212–232. URL: http://eudml.org/doc/147605 (cit. on p. 161).

Lang, S. (1990). *Cyclotomic fields. I and II. With an appendix by Karl Rubin: The main conjecture*. **121**. Graduate Texts in Mathematics (Combined 2nd ed.) New York etc.: Springer-Verlag. URL: https://link.springer.com/content/pdf/bbm%5C%3A978-1-4612-0987-4%5C%2F1 (cit. on p. 114).

Lecouturier, E. (2018). "On the Galois structure of the class group of certain Kummer extensions". *J. London Math. Soc.* **98** (1), pp. 35–58. DOI: 10.1112/jlms.12123 (cit. on p. 115).

Leopoldt, H. (1954). "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper". *Abh. Deutsch. Akad. Wiss. Berlin, Math.-Naturw. Kl.* **1953** (2), pp. 1–48 (cit. on pp. 110, 118, 119, 131, 138, 145, 153–155).

Leopoldt, H. (1962). "Zur Arithmetik in abelschen Zahlkörpern". *J. reine angew. Math.* **209**, pp. 54–71. DOI: 10.1515/crll.1962.209.54 (cit. on pp. 110, 118, 131, 146, 153).

Mazigh, Y. (2017). "Unités de Stark et théorie d'Iwasawa (Thèse), Université Bourgogne Franche–Comté, Besançon". PhD thesis, 73 pp. URL: https://theses.hal.science/tel-01795150 (cit. on p. 129).

Mazur, B. and K. Rubin (2011). "Refined class number formulas and Kolyvagin systems". *Compositio Math.* **147** (1), pp. 56–74. DOI: 10.1112/S0010437X1000494X (cit. on p. 115).

Mazur, B. and A. Wiles (1984). "Class fields of abelian extensions of $\mathbb{Q}$". *Invent. Math.* **76**, pp. 179–330. DOI: 10.1007/BF01388599 (cit. on p. 114).

Nguyen Quang Do, T. (1986). "Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens". *Ann. Inst. Fourier* **36** (2), pp. 27–46. DOI: 10.5802/aif.1045 (cit. on pp. 117, 150).

Nguyen Quang Do, T. and M. Lescop (2006). "Iwasawa Descent and Co-descent for Units modulo Circular Units (with an appendix by Belliard, J-R.)" *Pure Appl. Math. Q.* **2** (2), pp. 465–496. DOI: 10.4310/PAMQ.2006.v2.n2.a4 (cit. on p. 157).

Oriat, B. (1975a). "Quelques caractères utiles en arithmétique". *PMB (Algèbre et téorie des nombres)* **4**, 27 pp. DOI: 10.5802/pmb.a-4 (cit. on pp. 118, 137, 155).

Oriat, B. (1975b). "Sur l'article de Leopoldt "Über Einheintengruppe und Klassenzahl reeller abelscher Zahlkörper"". *PMB (Algèbre et téorie des nombres)* **5**, pp. 1–35. DOI: 10.5802/pmb.a-5 (cit. on pp. 118, 145, 153–155).

Oriat, B. (1981). "Annulation de groupes de classes réelles". *Nagoya Math. J.* **81**, pp. 45–56. URL: https://projecteuclid.org/download/pdf_1/euclid.nmj/1118786304 (cit. on pp. 114, 152, 168).

Oriat, B. (1986). "Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens". *Acta Arithmetica* **46**, pp. 331–354. DOI: 10.4064/aa-46-4-331-354 (cit. on pp. 114, 168).

Pagani, L. (2022). "Greenberg's conjecture for real quadratic fields and the cyclotomic $\mathbb{Z}_2$-extension". *Math. Comput.* **91** (335), pp. 1437–1467. DOI: 10.1090/mcom/3712 (cit. on p. 113).

Perrin-Riou, B. (1990). *Travaux de Kolyvagin et Rubin*. Sémin. Bourbaki, Vol. 1989/90, 42ème année, Astérisque 189-190, Exp. No. 717. URL: http://www.numdam.org/item/SB_1989-1990__32__69_0/ (cit. on pp. 114, 129, 164).

Perrin-Riou, B. (1998). "Systèmes d'Euler p-adiques et théorie d'Iwasawa". *Ann. Inst. Fourier* **48** (5), pp. 1231–1307. DOI: 10.5802/aif.1655 (cit. on pp. 114, 164).

Ribet, K. (1979). "Fonctions L p-adiques et théorie d'Iwasawa (par P. Satgé, d'après un cours de K. Ribet 1977/78)". *Pub. Math. d'Orsay*, 92 pp. URL: https://www.imo.universite-paris-saclay.fr/~biblio/cours-m2/Fonctions_L_p-adiques_et_theorie_Iwasawa.pdf (cit. on p. 117).

Ribet, K. (2008a). "Bernoulli numbers and ideal classes". *SMF, Gazette* **118**, pp. 42–49. URL: https://smf.emath.fr/system/files/filepdf/gaz-118.pdf (cit. on pp. 110, 113).

Ribet, K. (2008b). *Modular constructions of unramified extensions and their relation with a theorem of Herbrand (Class groups and Galois representations)*. ENS., J. Herbrand centennaire. URL: https://math.berkeley.edu/~ribet/herbrand.pdf (cit. on p. 113).

Rubin, K. (1990). *The main conjecture, Appendix to Cyclotomic fields I, II, by Lang, S.* **121**. Grad. Texts Math. Pp. 397–419. URL: https://link.springer.com/content/pdf/bbm%5C%3A978-1-4612-0987-4%5C%2F1.pdf (cit. on p. 114).

Rubin, K. (2000). *Euler Systems (Hermann–Weyl lectures)*. **147**. Ann. Math. Stud. Princeton, NJ: Princeton University Press, 230 pp. DOI: 10.1515/9781400865208. URL: https://swc-math.github.io/notes/files/99RubinES.pdf (cit. on p. 114).

Schaefer, K. and E. E. Stubley (2019). "Class groups of Kummer extensions via cup products in Galois cohomology". *Trans. Amer. Math. Soc.* **372**, pp. 6927–6980. DOI: 10.1090/tran/7746 (cit. on p. 115).

Serre, J.-P. (1978). "Sur le résidu de la fonction zêta p-adique d'un corps de nombres". *C.R. Acad. Sci. Paris, Série A* **287**, pp. 183–188 (cit. on p. 117).

Serre, J.-P. (1998). *Représentations linéaires des groupes finis, 5ième éd., corr. et augm. de nouveaux exercices*. Hermann 1998, 182 pp. (Cit. on p. 124).

Sinnott, W. (1980). "On the Stickelberger ideal and the circular units of an abelian field". *Invent. Math.* **62**, pp. 181–234. DOI: 10.1007/BF01389158 (cit. on p. 146).

Smith, A. (2022). "The distribution of ℓ^∞-Selmer groups in degree ℓ twist families". URL: https://doi.org/10.48550/arXiv.2207.05674 (cit. on p. 173).

Solomon, D. (1990). "On the class groups of imaginary abelian fields". *Ann. Inst. Fourier* **40** (3), pp. 467–492. DOI: 10.5802/aif.1221 (cit. on pp. 110, 114, 129, 166).

Solomon, D. (1992). "On a construction of p-units in abelian fields". *Invent. Math.* **109** (2), pp. 329–350. URL: http://eudml.org/doc/144024 (cit. on p. 159).

Thaine, F. (1988). "On the ideal class groups of real abelian number fields". *Ann. Math. (2)* **128** (1), pp. 1–18. DOI: 10.2307/1971460 (cit. on pp. 112, 159).

Viguié, S. (2011). "Contribution à l'étude de la conjecture de Gras et de la conjecture principale d'Iwasawa, par les systèmes d'Euler (Thèse: Université de Franche–Comté)". PhD thesis. URL: https://theses.hal.science/tel-00839919/file/these_A_VIGUIE_Stephane_2011.pdf (cit. on p. 115).

Washington, L. (1997). *Introduction to Cyclotomic Fields*. 2nd ed. **83**. Grad. Texts Math. New York, NY: Springer (cit. on pp. 111, 113, 144, 146, 151, 159, 161, 163, 170).

Contents