Invariant generalized ideal classes – structure theorems for p-class groups in p-extensions

Georges Gras

INVARIANT GENERALIZED IDEAL CLASSES STRUCTURE THEOREMS FOR p-CLASS GROUPS IN p-EXTENSIONS

A SURVEY

GEORGES GRAS

Abstract. We give, in Sections 2 and 3, an english translation of: *Classes généralisées invariantes*, J. Math. Soc. Japan, 46, 3 (1994), with some improvements and with notations and definitions in accordance with our book: *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2nd corrected printing 2005. We recall, in Section 4, some structure theorems for finite $\mathbb{Z}_p[G]$-modules ($G \simeq \mathbb{Z}/p\mathbb{Z}$) obtained in: *Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ*, Annales de l'Institut Fourier, 23, 3 (1973). Then we recall the algorithm of local normic computations which allows to obtain the order and (potentially) the structure of a p-class group in a cyclic extension of degree p.

In Section 5, we apply this to the study of the structure of relative p-class groups of Abelian extensions of prime to p degree, using the Thaine–Ribet–Mazur–Wiles–Kolyvagin "principal theorem", and the notion of "admissible sets of prime numbers" in a cyclic extension of degree p, from: *Sur la structure des groupes de classes relatives*, Annales de l'Institut Fourier, 43, 1 (1993).

In conclusion, we suggest the study, in the same spirit, of some deep invariants attached to the p-ramification theory (as dual form of non-ramification theory) and which have become standard in a p-adic framework.

Since some of these techniques have often been rediscovered, we give a substantial (but certainly incomplete) bibliography which may be used to have a broad view on the subject.

1. Introduction – Generalities

Let K/k be a cyclic extension of algebraic number fields, with Galois group G, and let L be a finite Abelian extension of K; we suppose that L/k is Galois, so that G operates by conjugation on $\mathrm{Gal}(L/K)$.

We shall see the field L given, via Class Field Theory, by some Artin group of K (e.g., the Hilbert class field H_K^+ of K associated with the group of principal ideals, in the narrow sense, any ray class field $H_{K,\mathfrak{m}}^+$ associated with a ray group modulo a modulus $\mathfrak{m}$ of k, in the narrow sense, or more generally any subfield L of these canonical fields, defining $\mathrm{Gal}(H_{K,\mathfrak{m}}^+/L)$ by means of a sub-G-module $\mathcal{H}$ of the generalized class group $\mathcal{C}\ell_{K,\mathfrak{m}}^+ \simeq \mathrm{Gal}(H_{K,\mathfrak{m}}^+/K)$).

We intend to give, from the arithmetic of k and elementary local normic computations in K/k, an explicit formula for

$$\#\mathrm{Gal}(L/K)^G = \#(\mathcal{C}\ell_{K,\mathfrak{m}}^+/\mathcal{H})^G.$$

This order is the degree, over K, of the maximal subfield of L (denoted L^{ab}) which is Abelian over k.

Date: October 14, 2016.

2020 *Mathematics Subject Classification.* Primary 11R29; 11R37.

Key words and phrases. number fields; class field theory; p-class groups; p-extensions; generalized classes; ambiguous classes; Chevalley's formula.

Indeed, since G is cyclic, it is not difficult to see that the commutator subgroup $[\Gamma,\Gamma]$ of $\Gamma := \mathrm{Gal}(L/k)$ is equal to $\mathrm{Gal}(L/K)^{1-\sigma} \simeq (\mathcal{C}\ell^+_{K,\mathfrak{m}}/\mathcal{H})^{1-\sigma}$, where σ is a generator of G (or an extension in Γ). So we have the exact sequences

$$(1)\qquad \begin{array}{l} 1 \longrightarrow \mathrm{Gal}(L/K)^{1-\sigma} \longrightarrow \Gamma \longrightarrow \Gamma^{\mathrm{ab}} = \Gamma/[\Gamma,\Gamma] = \mathrm{Gal}(L^{\mathrm{ab}}/k) \longrightarrow 1, \\ 1 \longrightarrow \mathrm{Gal}(L/K)^{G} \longrightarrow \mathrm{Gal}(L/K) \xrightarrow{1-\sigma} \mathrm{Gal}(L/K)^{1-\sigma} \longrightarrow 1. \end{array}$$

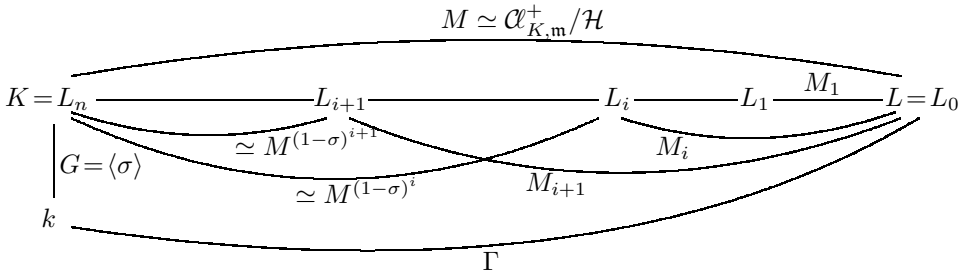
Hence $\#\mathrm{Gal}(L/K)^G = [L:K] \cdot \dfrac{\#\Gamma^{\mathrm{ab}}}{\#\Gamma} = [L:K] \cdot \dfrac{[L^{\mathrm{ab}}:k]}{[L:K][K:k]} = [L^{\mathrm{ab}}:K]$. The study of the structure of $\mathrm{Gal}(L/K)$ as G-module (or at least the computation of its order) is based under the study of the following filtration:

Definition 1.1. Let $M := \mathrm{Gal}(L/K)$ and let $(M_i)_{i\geq 0}$ be the increasing sequence of sub-G-modules defined (with $M_0 := 1$) by

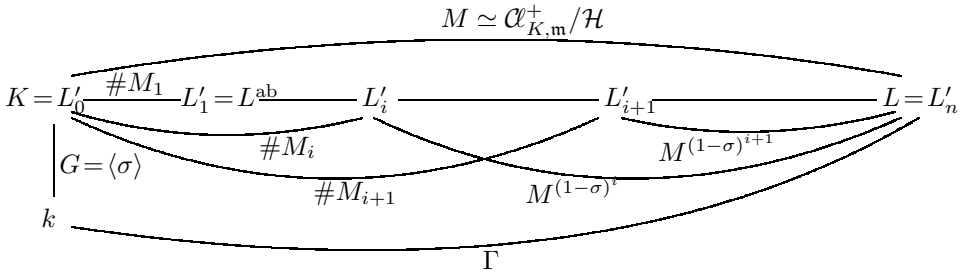
$$M_{i+1}/M_i := (M/M_i)^G, \ \text{ for } 0 \leq i \leq n,$$

where n is the least integer i such that $M_i = M$.

For $i = 0$, we get $M_1 = M^G$. We have equivalently $M_{i+1} = \{h \in M,\ h^{1-\sigma} \in M_i\}$. Thus $M_i = \{h \in M,\ h^{(1-\sigma)^i} = 1\}$ and $(1-\sigma)^n$ is the anihilator of M.
If L_i is the subfield of L fixed by M_i, this yields the following tower of fields, Galois over k, from the exact sequences $1 \to M_i \longrightarrow M \xrightarrow{(1-\sigma)^i} M^{(1-\sigma)^i} \to 1$ such that $[L_i : L_{i+1}] = (M_{i+1} : M_i)$ which can be computed from local arithmetical tools in K/k as described in the Sections 3 and 4:



In a dual manner, we have the following tower of fields where L'_i is the subfield of L fixed by $M^{(1-\sigma)^i}$, whence $[L'_i : K] = \#M_i$:



Our method to compute $\#(M_{i+1}/M_i)$ differs from classical ones by "translating" the well-known Chevalley's formula giving the number of ambiguous classes, see (28), Remark 3.10), by means of the exact sequence of Theorem 3.3 applied to a suitable $\mathcal{H} = \mathcal{H}_0$.

The main application is the case where G is cyclic of order a prime p and when L/K is an Abelian finite p-extension defined via class field theory (e.g., various p-Hilbert class fields in most classical practices). So, when the M_i are computed, it is possible to give, under some assumptions (like $M^{1+\sigma+\cdots+\sigma^{p-1}} = 1$ and/or $\#M^G = p$), the structure of $\mathrm{Gal}(L/K)$ as $\mathbb{Z}_p[G]$-module or at least as Abelian p-group.

In the above example, this will give for instance the structure of the p-class group in the restricted sense from the knowledge of the p-class group of k and some local normic computations in K/k.

Remarks 1.2. (i) In some french papers, we find the terminology *sens restreint* vs *sens ordinaire* which was introduced by J. Herbrand in [H, VII, §4], and we have used in [Gr1] the upperscripts $^{\rm res}$ and $^{\rm ord}$ to specify the sense; to be consistent with many of today's publications, we shall use here the words *narrow sense* instead of *restricted sense* and use the upperscript $^{+}$. However, we utilize S-objects, where S is a suitable set of places (S-units, S-class groups, S-class fields, etc.), so that $S = \emptyset$ corresponds to the restricted sense and totally positive elements ; the ordinary (or wide) sense corresponds to the choice of the set S of real infinite places of the field, thus, for the ordinary sense, we must keep the upperscript $^{\rm ord}$ (see §§2.1, 2.2).

We shall consider generalized S-class groups modulo $\mathfrak{m}$ since any situation is available by choosing suitable $\mathfrak{m}$ and S (including the case $p = 2$ with ordinary and narrow senses).

(ii) It is clear that the study of p-class groups in p-extensions K/k is rather easy compared to the "semi-simple" case (i.e., when $p \nmid \mathrm{Gal}(K/k)$); see, e.g., an overview in [St1], and an extensive algebraic study in [L1] via representation theory, then in [Ku], [Sch1], [Sch2], [Sch3], [SW], and in [Wa] for cyclotomic fields.

Indeed, the semi-simple case is of a more Diophantine framework and is part of an analytic setting leading to difficult well-known questions in Iwasawa theory [Iw], then in p-adic L-functions that we had conjectured in [Gr14, (1977)], and which were initiated with the Thaine–Ribet–Mazur–Wiles–Kolyvagin "principal theorem" [MW, (1984)] with significant developments by C. Greither and R. Kučera (e.g., [GK1], [GK2], [GK3], [GK4]), which have in general no connection with the present text, part of the so called "genera theory" (except for the method of Section 5 in which we obtain informations on the semi-simple case).

2. Class field theory – Generalized ideal class groups

We use, for some technical aspects, the principles defined in [Gr2]; one can also use the works of Jaulent as [Ja1], [Ja2], of the same kind. For instance, for a real infinite place which becomes complex in an extension, we speak of *complexification* instead of *ramification*, and the corresponding *inertia* subgroup of order 2 is called the *decomposition group* of the place; in other words this place has a *residue degree* 2 instead of a *ramification index* 2. If the real place remains real by extension, we say as usual that this place splits (of course into two real places above) and that its residue degree is 1. The great advantage is that the moduli $\mathfrak{m}$ of class field theory are ordinary integer ideals, any situation being obtained from the choice of S.

A consequence of this viewpoint is that the pivotal notion is the narrow sense.

2.1. Numbers – Ideals – Ideal classes.

Let F be any number field (this will apply to K and k). We denote by:

(i) $Pl_F = Pl_{F,0} \cup Pl_{F,\infty}$, the set of finite and infinite places of F. The places (finite or infinite) are given as symbols $\mathfrak{p}$; the finite places are the prime ideals; the infinite places may be real or complex and are associated with the $r_1 + r_2$ embeddings of F into $\mathbb{R}$ and $\mathbb{C}$ as usual (with $r_1 + 2\,r_2 = [F : \mathbb{Q}]$);

(ii) T & S, two disjoint sets of places of F. We suppose that T has only finite places and that $S =: S_0 \cup S_\infty$, $S_0 \subset Pl_{F,0}$, $S_\infty \subset Pl_{F,\infty}$, where S_∞ does not contain any complex place;

(iii) $\mathfrak{m}$, a modulus of F with support T (i.e., a nonzero integral ideal of F divisible by each of the prime ideals $\mathfrak{p} \in T$ and not by any $\mathfrak{p} \notin T$);

(iv) $v_{\mathfrak{p}} : F^\times \to \mathbb{Z}$ is the normalized $\mathfrak{p}$-adic valuation when $\mathfrak{p}$ is a prime ideal; if $\mathfrak{p}$ is a real infinite place, then $v_{\mathfrak{p}} : F^\times \to \mathbb{Z}/2\,\mathbb{Z}$ is defined by $v_{\mathfrak{p}}(x) = 0$ (resp. $v_{\mathfrak{p}}(x) = 1$) if $\sigma_{\mathfrak{p}}(x) > 0$ (resp. $\sigma_{\mathfrak{p}}(x) < 0$) where $\sigma_{\mathfrak{p}}$ is the corresponding embedding $F \to \mathbb{R}$ associated with $\mathfrak{p}$; if $\mathfrak{p}$ is complex (thus corresponding to a pair of conjugated embeddings $F \to \mathbb{C}$), then $v_{\mathfrak{p}} = 0$.

(v) $F^{\times +} = \{x \in F^\times,\ v_{\mathfrak{p}}(x) = 0,\ \forall \mathfrak{p} \in Pl_{F,\infty}\}$, group of totally positive elements;
$U_{F,T} = \{x \in F^\times,\ v_{\mathfrak{p}}(x) = 0,\ \forall \mathfrak{p} \in T\}$; $U^+_{F,T} = U_{F,T} \cap F^{\times +}$;
$U_{F,\mathfrak{m}} = \{x \in U_{F,T},\ x \equiv 1 \pmod{\mathfrak{m}}\}$; $U^+_{F,\mathfrak{m}} = U_{F,\mathfrak{m}} \cap F^{\times +}$;

(vi) $E^S_F = \{x \in F^\times,\ v_{\mathfrak{p}}(x) = 0,\ \forall \mathfrak{p} \notin S\}$, group of S-units of F;
$E^S_{F,\mathfrak{m}} = \{x \in E^S_F,\ x \equiv 1 \pmod{\mathfrak{m}}\}$;
$E^{Pl_\infty}_{F,\mathfrak{m}} =: E^{\rm ord}_{F,\mathfrak{m}}$, group of units (in the ordinary sense) $\varepsilon \equiv 1 \pmod{\mathfrak{m}}$;
$E^{\emptyset}_{F,\mathfrak{m}} =: E^+_{F,\mathfrak{m}}$, group of totally positive units $\varepsilon \equiv 1 \pmod{\mathfrak{m}}$;

(vii) I_F, group of fractional ideals of F;
P_F, group of principal ideals (x), $x \in F^\times$ (ordinary sense);
P^+_F, group of principal ideals (x), $x \in F^{\times +}$ (narrow sense);
$I_{F,T} = \{\mathfrak{a} \in I_F,\ v_{\mathfrak{p}}(\mathfrak{a}) = 0,\ \forall \mathfrak{p} \in T\}$; $P_{F,T} = P_F \cap I_{F,T}$; $P^+_{F,T} = P^+_F \cap I_{F,T}$;
$P_{F,\mathfrak{m}} = \{(x),\ x \in U_{F,\mathfrak{m}}\}$, ray group modulo $\mathfrak{m}$ in the ordinary sense;
$P^+_{F,\mathfrak{m}} = \{(x),\ x \in U^+_{F,\mathfrak{m}}\}$, ray group modulo $\mathfrak{m}$ in the narrow sense;

(viii) $\mathcal{C}\ell^{\rm ord}_{F,\mathfrak{m}} = I_{F,T}/P_{F,\mathfrak{m}}$, generalized ray class group modulo $\mathfrak{m}$ (ordinary sense);
$\mathcal{C}\ell^+_{F,\mathfrak{m}} = I_{F,T}/P^+_{F,\mathfrak{m}}$, generalized ray class group modulo $\mathfrak{m}$ (narrow sense);
$\mathcal{C}\ell^S_{F,\mathfrak{m}} := \mathcal{C}\ell^+_{F,\mathfrak{m}}/\langle cl(S)\rangle_{\mathbb{Z}}$, S-class group modulo $\mathfrak{m}$ where $\langle cl(S)\rangle_{\mathbb{Z}}$ is the subgroup of $\mathcal{C}\ell^+_{F,\mathfrak{m}}$ generated by the classes of $\mathfrak{p} \in S_0$ and, for real $\mathfrak{p} \in S_\infty$, by the classes of the principal ideals $(x^{\mathfrak{m}}_{\mathfrak{p}})$ where the $x^{\mathfrak{m}}_{\mathfrak{p}} \in F^\times$ satisfy to the following congruences and signatures:

$$x^{\mathfrak{m}}_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{m}},\ \ \sigma_{\mathfrak{p}}(x^{\mathfrak{m}}_{\mathfrak{p}}) < 0\ \ \&\ \ \sigma_{\mathfrak{q}}(x^{\mathfrak{m}}_{\mathfrak{p}}) > 0\ \forall \mathfrak{q} \in Pl_{F,\infty} \setminus \{\mathfrak{p}\};$$

we have $P_F = \langle\, (x_{\mathfrak{p}})\,\rangle_{\mathfrak{p} \in Pl_{F,\infty}} \cdot P^+_F \quad \& \quad P_{F,\mathfrak{m}} = \langle\, (x^{\mathfrak{m}}_{\mathfrak{p}})\,\rangle_{\mathfrak{p} \in Pl_{F,\infty}} \cdot P^+_{F,\mathfrak{m}}$.

Taking $S = \emptyset$, then $S = Pl_{F,\infty}$, we find again

$$\mathcal{C}\ell^{\emptyset}_{F,\mathfrak{m}} = \mathcal{C}\ell^+_{F,\mathfrak{m}},\ \text{then}\ \mathcal{C}\ell^{Pl_{F,\infty}}_{F,\mathfrak{m}} = \mathcal{C}\ell^+_{F,\mathfrak{m}}/cl(\langle\, (x^{\mathfrak{m}}_{\mathfrak{p}})\,\rangle_{\mathfrak{p} \in Pl_{F,\infty}}) = \mathcal{C}\ell^{\rm ord}_{F,\mathfrak{m}}.$$

(ix) $cl_F : I_{F,T} \longrightarrow \mathcal{C}\ell^S_{F,\mathfrak{m}}$, canonical map which must be read as $cl^S_{F,\mathfrak{m}}$ for suitable $\mathfrak{m}$ and S, according to the case of class group considered, when there is no ambiguity.

2.2. **Class fields and corresponding class groups.** We define the generalized Hilbert class fields as follows:

(i) H^+_F is the Hilbert class field in the narrow sense (maximal Abelian extension of F unramified for prime ideals and possibly complexified at ∞, which means that the field H^+_F may be non-real even if F is totally real); we have

$$\mathrm{Gal}(H^+_F/F) \simeq \mathcal{C}\ell^+_F = I_F/P^+_F;$$

(ii) $H^{Pl_\infty}_F = H^{\rm ord}_F \subseteq H^+_F$ is the Hilbert class field in the ordinary sense (maximal Abelian extension of F, unramified for prime ideals, and splitted at ∞); we have

$$\mathrm{Gal}(H^{\rm ord}_F/F) \simeq \mathcal{C}\ell^{\rm ord}_F = I_F/P_F;$$

(iii) $H^S_F \subseteq H^+_F$ is the S-split Hilbert class field (maximal Abelian extension of F unramified for prime ideals and splitted at S); we have

$$\mathrm{Gal}(H^S_F/F) \simeq \mathcal{C}\ell^S_F = \mathcal{C}\ell^+_F/\langle cl_F(S)\rangle_{\mathbb{Z}};$$

recall that the decomposition group of $\mathfrak{p} \in S_0$ (resp. S_∞) is given, in $\mathcal{C}\ell_F^+$, by the cyclic group generated by the class of $\mathfrak{p}$ (resp. $(x_\mathfrak{p})$); hence $\mathrm{Gal}(H_F^+/H_F^S)$, generated by these decomposition groups, is isomorphic to $\langle \mathcal{cl}_F(S)\rangle_\mathbb{Z}$.

(iv) $H_{F,\mathfrak{m}}^+$ is the $\mathfrak{m}$-ray class field in the narrow sense,

$H_{F,\mathfrak{m}}^{\mathrm{ord}}$ is the $\mathfrak{m}$-ray class field in the ordinary sense,

$H_{F,\mathfrak{m}}^S$ is the S-split $\mathfrak{m}$-ray class field of F (denoted $F_{(\mathfrak{m})}{}^S$ in [Gr2]); we have

$$\mathrm{Gal}(H_{F,\mathfrak{m}}^S/F) \simeq \mathcal{C}\ell_{F,\mathfrak{m}}^S = \mathcal{C}\ell_{F,\mathfrak{m}}^+/\langle \mathcal{cl}_F(S)\rangle_\mathbb{Z}$$

(see (viii) and (ix) for the suitable definitions of $\mathcal{cl}_F$ depending on the class group considered). In other words, $H_{F,\mathfrak{m}}^S$ is the maximal subextension of $H_{F,\mathfrak{m}}^+$ in which the (finite and infinite) places of S are totally split.

For instance, for a prime p, the p-Sylow subgroups of $\mathcal{C}\ell_F^{\mathrm{ord}}$ and $\mathcal{C}\ell_F^{Pl_p}$, for the set $S = Pl_p := \{\mathfrak{p},\ \ \mathfrak{p} \mid p\}$, have a significant meaning in some duality theorems.

3. Computation for the order of $\left(\mathcal{C}\ell_{K,\mathfrak{m}}^+/\mathcal{H}\right)^G$

Let K/k be any cyclic extension of number fields, of degree d, of Galois group G, and let σ be a fixed generator of G. We fix a modulus $\mathfrak{m}$ of k with support T which implies that $H_{K,\mathfrak{m}}^+/k$ is Galois (by abuse we keep the same notation for the extensions of $\mathfrak{m}$ and T in K). Then let

$$\mathcal{H} \subseteq \mathcal{C}\ell_{K,\mathfrak{m}}^+$$

be an arbitrary sub-G-module of $\mathcal{C}\ell_{K,\mathfrak{m}}^+$.

Remarks 3.1. (i) The group G acts on $\mathcal{C}\ell_{K,\mathfrak{m}}^+$, hence on $\mathrm{Gal}(H_{K,\mathfrak{m}}^+/K)$ by conjugation via the Artin isomorphism $\mathfrak{A} \mapsto \left(\frac{H_{K,\mathfrak{m}}^+/K}{\mathfrak{A}}\right) \in \mathrm{Gal}(H_{K,\mathfrak{m}}^+/K)$, for all $\mathfrak{A} \in I_{K,T}$ (modulo $P_{K,\mathfrak{m}}^+$), for which

$$\left(\frac{H_{K,\mathfrak{m}}^+/K}{\mathfrak{A}^\tau}\right) = \tau \cdot \left(\frac{H_{K,\mathfrak{m}}^+/K}{\mathfrak{A}}\right) \cdot \tau^{-1}, \text{ for all } \tau \in G.$$

(ii) The sub-G-module $\mathcal{H}$ fixes a field $L \subseteq H_{K,\mathfrak{m}}^+$ which is Galois over k and in the same way, $\mathrm{Gal}(L/K) \simeq \mathcal{C}\ell_{K,\mathfrak{m}}^+/\mathcal{H}$ is a G-module.

(iii) Taking $\mathcal{H} = \langle \mathcal{cl}_K(S)\rangle_\mathbb{Z}$, $S \subset Pl_K$ (see (viii)) leads to $\mathcal{C}\ell_{K,\mathfrak{m}}^+/\mathcal{H} = \mathcal{C}\ell_{K,\mathfrak{m}}^S$ & $L = H_{K,\mathfrak{m}}^S$ (assuming that $\mathcal{cl}_K(S)$ is a sub-G-module).

(iv) If we take, more generally, a modulus $\mathfrak{M}$ of K "above $\mathfrak{m}$", it must be invariant by G; so necessarily, $\mathfrak{M} = (\mathfrak{m})$ extended to K, except if some $\mathfrak{P} \mid \mathfrak{M}$ is ramified since $(\mathfrak{p}) = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{p}}$. But in class field theory, it is always possible to work with a multiple $\mathfrak{M}'$ of $\mathfrak{M}$ (because $H_{K,\mathfrak{M}}^+ \subseteq H_{K,\mathfrak{M}'}^+$), so that the case $\mathfrak{M} = (\mathfrak{m})$ is universal for our purpose and is, in practice, any multiple of the conductor $\mathfrak{f}_{L/K}$ of L/K.

We intend to compute $\#(\mathcal{C}\ell_{K,\mathfrak{m}}^+/\mathcal{H})^G = \#\mathrm{Gal}(L/K)^G$, which is equivalent, from exact sequences (1), to obtain the degree $[L^{\mathrm{ab}} : K]$, where L^{ab} is the maximal subextension of L, Abelian over k.

Our method is straightforward and is based on the well-known "ambiguous class number formula" given by Chevalley [Ch1, (1933)], and used in any work on class field theory (e.g., [Ch2], [AT], [L], [Ja1, Chap. 3], [L3]), often in a hidden manner, since it is absolutely necessary for the interpretation, in the cyclic case, of the famous idelic index $(J_k : k^\times \mathrm{N}_{K/k}(J_K)) = [K^{\mathrm{ab}} : k]$, valid for any finite extension K/k and which gives the *product formula* between normic symbols in view of the Hasse norm theorem (in the cyclic case).

This formula has also some importance for Greenberg's conjectures [Gre2] on Iwasawa's λ, μ invariants for the $\mathbb{Z}_p$-extensions of a totally real number field [Gr15].

Chevalley's formula in the cyclic case is based on (and roughly speaking equivalent to) the nontrivial computation of the Herbrand quotient $\frac{(E_k:\mathrm{N}_{K/k}(E_K))}{({}_{\mathrm{N}}E_K:E_K^{1-\sigma})}=\frac{2^{\mathrm{rc}}}{[K:k]}$ of the group of units E_K, where ${}_{\mathrm{N}}E_K$ is the subgroup of units of norm 1 in K/k and where rc is the number of real places of k, complexified in K. Chevalley's formula was established first by Takagi for cyclic extensions of prime degree p; the generalization to arbitrary cyclic case by Chevalley was possible due to the so called "Herbrand theorem on units" [H].

Many fixed point formulas where given in the same framwork for other notions of classes (e.g., logarithmic class groups, [Ja3], [So], p-ramification torsion groups, [Gr2, Theorem IV.3.3], [MoNg]).

3.1. The main exact sequence and the computation of $\#(\mathcal{C}\ell^+_{K,\mathfrak{m}}/\mathcal{H})^G$.

3.1.1. *Global computations.* Recall that $\mathcal{H}$ is a sub-G-module of $\mathcal{C}\ell^+_{K,\mathfrak{m}}=I_{K,T}/P^+_{K,\mathfrak{m}}$. Put

$$\widetilde{\mathcal{H}}=\{h\in\mathcal{C}\ell^+_{K,\mathfrak{m}},\ \ h^{1-\sigma}\in\mathcal{H}\};\tag{2}$$

it is obvious that

$$\big(\mathcal{C}\ell^+_{K,\mathfrak{m}}/\mathcal{H}\big)^G=\widetilde{\mathcal{H}}/\mathcal{H}.\tag{3}$$

We have the exact sequences

$$\begin{aligned}1\longrightarrow\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}}\longrightarrow\widetilde{\mathcal{H}}\xrightarrow{1-\sigma}(\widetilde{\mathcal{H}})^{1-\sigma}\longrightarrow 1\\ 1\longrightarrow{}_{\mathrm{N}}\mathcal{H}\longrightarrow\mathcal{H}\xrightarrow{\mathrm{N}_{K/k}}\mathrm{N}_{K/k}(\mathcal{H})\longrightarrow 1,\end{aligned}\tag{4}$$

with ${}_{\mathrm{N}}\mathcal{H}=\mathrm{Ker}(\mathrm{N}_{K/k})$, where $\mathrm{N}_{K/k}$ denotes the *arithmetical norm*[1] as opposed to the *algebraic norm* defined in $\mathbb{Z}[G]$ by $\nu_{K/k}=1+\sigma+\cdots+\sigma^{d-1}$, and for which we have the relation $\nu_{K/k}=j_{K/k}\circ\mathrm{N}_{K/k}$, where $j_{K/k}$ is the map of extension of ideals from k to K (it corresponds, via the Artin map, to the transfer map for Galois groups); for a prime ideal $\mathfrak{P}$ of K, $j_{K/k}\circ\mathrm{N}_{K/k}(\mathfrak{P})=j_{K/k}(\mathfrak{p}^{f_\mathfrak{p}})=(\prod_{\mathfrak{P}'\mid\mathfrak{p}}\mathfrak{P}'^{e_\mathfrak{p}})^{f_\mathfrak{p}}$ (where $e_\mathfrak{p}$ is the ramification index), which is indeed $\mathfrak{P}^{\nu_{K/k}}$ since G operates transitively on the $\mathfrak{P}'\mid\mathfrak{p}$ with a decomposition group of order $\frac{[K:k]}{e_\mathfrak{p}\,f_\mathfrak{p}}$.

By definition, for an ideal $\mathfrak{A}$ of K, we have $\mathrm{N}_{K/k}(\mathscr{A}_K(\mathfrak{A}))=\mathscr{A}_k(\mathrm{N}_{K/k}(\mathfrak{A}))$, and for any ideal $\mathfrak{a}$ of k, we have $j_{K/k}(\mathscr{A}_k(\mathfrak{a}))=\mathscr{A}_K(j_{K/k}(\mathfrak{a}))$, which makes sense since $\mathrm{N}_{K/k}(P^+_{K,\mathfrak{m}})\subseteq P^+_{k,\mathfrak{m}}$ and $j_{K/k}(P^+_{k,\mathfrak{m}})\subseteq P^+_{K,\mathfrak{m}}$, seeing the modulus $\mathfrak{m}$ of k extended in K in some writings.

To simplify the formulas, we write N for $\mathrm{N}_{K/k}$.

Recall that for ℓ prime, such that $\ell\nmid d=[K:k]$, the ℓ-Sylow subgroup $\mathcal{C}\ell^+_{k,\mathfrak{m}}\otimes\mathbb{Z}_\ell$ is isomorphic to $(\mathcal{C}\ell^+_{K,\mathfrak{m}}\otimes\mathbb{Z}_\ell)^G$ since the map $j_{K/k}:\mathcal{C}\ell^+_{k,\mathfrak{m}}\otimes\mathbb{Z}_\ell\longrightarrow\mathcal{C}\ell^+_{K,\mathfrak{m}}\otimes\mathbb{Z}_\ell$ is injective, and the map $\mathrm{N}_{K/k}:\mathcal{C}\ell^+_{K,\mathfrak{m}}\otimes\mathbb{Z}_\ell\longrightarrow\mathcal{C}\ell^+_{k,\mathfrak{m}}\otimes\mathbb{Z}_\ell$ is surjective.

Let $\mathcal{I}$ be any *subgroup* of $I_{K,T}$ such that $\mathscr{A}_K(\mathcal{I})=\mathcal{H}$, i.e.,

$$\mathcal{I}\cdot P^+_{K,\mathfrak{m}}\,/P^+_{K,\mathfrak{m}}=\mathcal{H};\tag{5}$$

the group $\mathcal{I}\cdot P^+_{K,\mathfrak{m}}$ is unique and we then have

$$\mathrm{N}(\mathcal{H})=\mathrm{N}(\mathcal{I})\cdot P^+_{k,\mathfrak{m}}\,/P^+_{k,\mathfrak{m}}\simeq\mathrm{N}(\mathcal{I})/\mathrm{N}(\mathcal{I})\cap P^+_{k,\mathfrak{m}}.\tag{6}$$

[1] For K/k Galois, the arithmetical norm $\mathrm{N}_{K/k}$ is defined multiplicatively on the group of ideals of K by $\mathrm{N}_{K/k}(\mathfrak{P})=\mathfrak{p}^{f_\mathfrak{p}}$ for prime ideals $\mathfrak{P}$ of K, where $\mathfrak{p}$ is the prime ideal of k under $\mathfrak{P}$ and $f_\mathfrak{p}$ its residue degree in K/k. If $\mathfrak{A}=(\alpha)$ is principal in K, then $\mathrm{N}_{K/k}(\mathfrak{A})=(\mathrm{N}_{K/k}(\alpha))$ in k.

Remark 3.2. The generalized class groups being finite and since any ideal class can be represented by a finite or infinite place, we can find a finite set $S_K = S_{K,0} \cup S_{K,\infty}$ of non-complex places such that the classes $\mathfrak{P} \cdot P_{K,\mathfrak{m}}^+$ (for $\mathfrak{P} \in S_{K,0}$) and $(x_{\mathfrak{P}}^{\mathfrak{m}}) \cdot P_{K,\mathfrak{m}}^+$ (for $\mathfrak{P} \in S_{K,\infty}$) generate $\mathcal{H}$, so that we can take $\mathcal{I} = \bigoplus\limits_{\mathfrak{P} \in S_{K,0}} \langle \mathfrak{P} \rangle_{\mathbb{Z}} \cdot \bigoplus\limits_{\mathfrak{P} \in S_{K,\infty}} \langle (x_{\mathfrak{P}}^{\mathfrak{m}}) \rangle_{\mathbb{Z}}$ as canonical subgroup of $I_{K,T}$ defining $\mathcal{H}$. Thus $\mathcal{C}\ell_{K,\mathfrak{m}}^+ / \mathcal{H} = \mathcal{C}\ell_{K,\mathfrak{m}}^{S_K}$ in the meaning of § 2.1 (viii). But, to ease the forthcoming computations, we keep the writing with the subgroup $\mathcal{I}$.

Note that we do not assume that $\mathcal{I}$ or S_K are invariant under G contrary to $\mathcal{H}$ and $\mathcal{I} \cdot P_{K,\mathfrak{m}}^+$; so, if for instance $\mathfrak{P} \in S_{K,0}$, for any $\tau \in G$ we have, $\mathcal{cl}_K(\mathfrak{P}^\tau) = \mathcal{cl}_K(\mathfrak{P}')$ for some $\mathfrak{P}' \in S_K$, whence $\mathfrak{P}^\tau = \mathfrak{P}'\,(x)$, $x \in U_{K,\mathfrak{m}}^+$.

From the exact sequence, where $\psi(u) = (u)$ for all $u \in U_{k,\mathfrak{m}}^+$,

$$1 \longrightarrow E_{k,\mathfrak{m}}^+ \longrightarrow U_{k,\mathfrak{m}}^+ \xrightarrow{\ \psi\ } P_{k,\mathfrak{m}}^+ \longrightarrow 1, \tag{7}$$

we then put

$$\Lambda := \psi^{-1}\big(\mathrm{N}(\mathcal{I}) \cap P_{k,\mathfrak{m}}^+\big) = \{x \in U_{k,\mathfrak{m}}^+,\ (x) \in \mathrm{N}(\mathcal{I})\}; \tag{8}$$

we have the obvious inclusions $E_{k,\mathfrak{m}}^+ \subseteq \Lambda \subseteq U_{k,\mathfrak{m}}^+$.

We can state (fundamental exact sequence):

Theorem 3.3. *Let K/k be any cyclic extension, of Galois group $G =: \langle \sigma \rangle$. Let $\mathcal{H} = \mathcal{I} \cdot P_{K,\mathfrak{m}}^+ \big/ P_{K,\mathfrak{m}}^+$ be a sub-G-module of $\mathcal{C}\ell_{K,\mathfrak{m}}^+$, where $\mathcal{I}$ is a subgroup of $I_{K,T}$, and let*

$$\widetilde{\mathcal{H}} = \{h \in \mathcal{C}\ell_{K,\mathfrak{m}}^+,\ \ h^{1-\sigma} \in \mathcal{H}\}.$$

We have $(\widetilde{\mathcal{H}})^{1-\sigma} \subseteq {}_{\mathrm{N}}\mathcal{H}$ and the exact sequence (see (2) and (5) to (8)):

$$1 \longrightarrow \big(E_{k,\mathfrak{m}}^+ \mathrm{N}(U_{K,\mathfrak{m}}^+)\big) \cap \Lambda \longrightarrow \Lambda \xrightarrow{\ \varphi\ } {}_{\mathrm{N}}\mathcal{H} / (\widetilde{\mathcal{H}})^{1-\sigma} \longrightarrow 1, \tag{9}$$

where, for all $x \in \Lambda$, $\varphi(x) = \mathcal{cl}_K(\mathfrak{A}) \cdot (\widetilde{\mathcal{H}})^{1-\sigma}$, for any $\mathfrak{A} \in \mathcal{I}$ such that $\mathrm{N}(\mathfrak{A}) = (x)$.

Proof. If $x \in \Lambda$, we have $(x) \in P_{k,\mathfrak{m}}^+$ and by definition (x) is of the form $\mathrm{N}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}$, and thus $\mathcal{cl}_K(\mathfrak{A}) \in {}_{\mathrm{N}}\mathcal{H}$; if $(x) = \mathrm{N}(\mathfrak{B})$, $\mathfrak{B} \in \mathcal{I}$, there exists $\mathfrak{C} \in I_K$ such that $\mathfrak{B} \cdot \mathfrak{A}^{-1} = \mathfrak{C}^{1-\sigma}$. It is known that $I_{K,T}$ is a $\mathbb{Z}[G]$-module (and a free $\mathbb{Z}$-module) such that $\mathrm{H}^1(G, I_{K,T}) = 0$; since $\mathfrak{B} \cdot \mathfrak{A}^{-1} \in I_{K,T}$ is of norm 1, it is of the required form with $\mathfrak{C} \in I_{K,T}$. Then

$$(\mathcal{cl}_K(\mathfrak{C}))^{1-\sigma} = \mathcal{cl}_K(\mathfrak{C}^{1-\sigma}) = \mathcal{cl}_K(\mathfrak{B} \cdot \mathfrak{A}^{-1}) \in \mathcal{cl}_K(\mathcal{I}) = \mathcal{H},$$

and by definition $\mathcal{cl}_K(\mathfrak{C}) \in \widetilde{\mathcal{H}}$, which implies $(\mathcal{cl}_K(\mathfrak{C}))^{1-\sigma} \in (\widetilde{\mathcal{H}})^{1-\sigma}$. Hence the fact that the map φ is well defined.

If $\mathfrak{A} \in \mathcal{I}$ is such that $\mathcal{cl}_K(\mathfrak{A}) \in {}_{\mathrm{N}}\mathcal{H}$, then $\mathrm{N}(\mathfrak{A}) = (x)$, $x \in U_{k,\mathfrak{m}}^+$, thus $x \in \Lambda$ and it is a preimage; hence the surjectivity of φ.

We now compute $\mathrm{Ker}(\varphi)$: if $x \in \Lambda$, $(x) = \mathrm{N}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}$, and if $\mathcal{cl}_K(\mathfrak{A}) \in (\widetilde{\mathcal{H}})^{1-\sigma}$, there exists $\mathfrak{B} \in I_{K,T}$ such that $\mathcal{cl}_K(\mathfrak{B}) \in \widetilde{\mathcal{H}}$ and $\mathcal{cl}_K(\mathfrak{A}) = \mathcal{cl}_K(\mathfrak{B})^{1-\sigma}$; so there exists $u \in U_{K,\mathfrak{m}}^+$ such that $\mathfrak{A} = \mathfrak{B}^{1-\sigma} \cdot (u)$, giving $(x) = \mathrm{N}(\mathfrak{A}) = (\mathrm{N}(u))$, hence

$$x = \varepsilon \cdot \mathrm{N}(u), \quad \varepsilon \in E_k^{\mathrm{ord}};$$

since x and $\mathrm{N}(u)$ are in $U_{k,\mathfrak{m}}^+$, we get $\varepsilon \in E_{k,\mathfrak{m}}^+$ and $x \in E_{k,\mathfrak{m}}^+ \mathrm{N}(U_{K,\mathfrak{m}}^+)$.

Reciprocally, if $x \in \Lambda$ is of the form $\varepsilon \cdot \mathrm{N}(u)$, $\varepsilon \in E_{k,\mathfrak{m}}^+$ and $u \in U_{K,\mathfrak{m}}^+$, this yields

$$(x) = \mathrm{N}(u) = \mathrm{N}(\mathfrak{A}), \quad \mathfrak{A} \in \mathcal{I},$$

which leads to the relation $\mathfrak{A} = (u) \cdot \mathfrak{B}^{1-\sigma}$ where, as we know, we can choose $\mathfrak{B} \in I_{K,T}$ since $\mathfrak{A}\,(u)^{-1} \in I_{K,T}$. Since $(u) \in P_{K,\mathfrak{m}}^+$, $\mathcal{cl}_K(\mathfrak{B})^{1-\sigma} = \mathcal{cl}_K(\mathfrak{A}) \in \mathcal{H}$, hence $\mathcal{cl}_K(\mathfrak{B}) \in \widetilde{\mathcal{H}}$, and we obtain $\mathcal{cl}_K(\mathfrak{A}) \in (\widetilde{\mathcal{H}})^{1-\sigma}$. □

We deduce from (4),

$$(\widetilde{\mathcal{H}} : \mathcal{H}) = \frac{\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}} \cdot \#(\widetilde{\mathcal{H}})^{1-\sigma}}{\#\mathrm{N}(\mathcal{H}) \cdot \#_{\mathrm{N}}\mathcal{H}} = \frac{\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}}}{\#\mathrm{N}(\mathcal{H}) \cdot ({}_{\mathrm{N}}\mathcal{H} : (\widetilde{\mathcal{H}})^{1-\sigma})}; \tag{10}$$

thus from (3), (9) and (10),

$$\begin{aligned} \#\big(\mathcal{C}\ell^{+}_{K,\mathfrak{m}}/\mathcal{H}\big)^{G} &= \frac{\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}}}{\#\mathrm{N}(\mathcal{H}) \cdot (\Lambda : (E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}})) \cap \Lambda)} \\ &= \frac{\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}}}{\#\mathrm{N}(\mathcal{H}) \cdot (\Lambda\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}) : E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}))}. \end{aligned} \tag{11}$$

We first apply this formula to

$$\mathcal{H}_0 = P^{+}_{K,T}/P^{+}_{K,\mathfrak{m}} \simeq (U^{+}_{K,T}/U^{+}_{K,\mathfrak{m}})/(E^{+}_{K}/E^{+}_{K,\mathfrak{m}})$$

which is the sub-module of $\mathcal{C}\ell^{+}_{K,\mathfrak{m}}$ corresponding to the Hilbert class field H^{+}_{K} since, using the idélic Chinese remainder theorem (cf. [Gr2, Remark I.5.1.2]), or the well-known fact that any class contains a representative prime to T, we get the surjection $I_{K,T}/P^{+}_{K,T} \to I_K/P^{+}_K$ giving an isomorphisme, whence

$$\big(\mathcal{C}\ell^{+}_{K,\mathfrak{m}}/\mathcal{H}_0\big)^{G} \simeq (I_{K,T}/P^{+}_{K,T})^{G} \simeq (I_K/P^{+}_K)^{G} \simeq \mathcal{C}\ell^{+\,G}_{K}. \tag{12}$$

Take $\mathcal{I}_0 := P^{+}_{K,T}$; then

$$\mathrm{N}(\mathcal{I}_0) = \mathrm{N}(P^{+}_{K,T}) \ \ \&\ \ \mathrm{N}(\mathcal{H}_0) = \mathrm{N}(P^{+}_{K,T}) \cdot P^{+}_{k,\mathfrak{m}}/P^{+}_{k,\mathfrak{m}}, \tag{13}$$

and

$$\Lambda_0 = \{x \in U^{+}_{k,\mathfrak{m}},\ \ (x) \in \mathrm{N}(P^{+}_{K,T})\} = (E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T})) \cap U^{+}_{k,\mathfrak{m}}. \tag{14}$$

It follows, from (11) applied to $\mathcal{H}_0$, from (12), and $\mathrm{N}(U^{+}_{K,\mathfrak{m}}) \subseteq \Lambda_0$ (see (14)),

$$\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}} = \#\mathcal{C}\ell^{+\,G}_{K} \cdot \#\mathrm{N}(\mathcal{H}_0) \cdot \big((E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T})) \cap U^{+}_{k,\mathfrak{m}} : E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}})\big). \tag{15}$$

Now, $\mathrm{N}(\mathcal{H}_0)$ in (13) can be interpreted by means of the exact sequence

$$\begin{aligned} 1 \longrightarrow E^{+}_{k}U^{+}_{k,\mathfrak{m}}/U^{+}_{k,\mathfrak{m}} \longrightarrow\ & E^{+}_{k}\mathrm{N}(U^{+}_{K,T})U^{+}_{k,\mathfrak{m}}/U^{+}_{k,\mathfrak{m}} \\ & \longrightarrow \mathrm{N}(\mathcal{H}_0) = \mathrm{N}(P^{+}_{K,T}) \cdot P^{+}_{k,\mathfrak{m}}/P^{+}_{k,\mathfrak{m}} \longrightarrow 1, \end{aligned}$$

giving

$$\#\mathrm{N}(\mathcal{H}_0) = \frac{(E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T}) : (E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T})) \cap U^{+}_{k,\mathfrak{m}})}{(E^{+}_{k} : E^{+}_{k,\mathfrak{m}})}; \tag{16}$$

thus from (15) and (16),

$$\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}} = \#\mathcal{C}\ell^{+\,G}_{K} \cdot \frac{(E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T}) : E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}))}{(E^{+}_{k} : E^{+}_{k,\mathfrak{m}})}. \tag{17}$$

The inclusions $\mathrm{N}(U^{+}_{K,\mathfrak{m}}) \subseteq E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}) \subseteq E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T})$ lead from (17) to

$$\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}} = \#\mathcal{C}\ell^{+\,G}_{K} \cdot \frac{(E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T}) : \mathrm{N}(U^{+}_{K,\mathfrak{m}}))}{(E^{+}_{k} : E^{+}_{k,\mathfrak{m}}) \cdot (E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}) : \mathrm{N}(U^{+}_{K,\mathfrak{m}}))},$$

in other words

$$\#\mathcal{C}\ell^{+\,G}_{K,\mathfrak{m}} = \#\mathcal{C}\ell^{+\,G}_{K} \cdot \frac{(E^{+}_{k}\,\mathrm{N}(U^{+}_{K,T}) : \mathrm{N}(U^{+}_{K,T})) \cdot (\mathrm{N}(U^{+}_{K,T}) : \mathrm{N}(U^{+}_{K,\mathfrak{m}}))}{(E^{+}_{k} : E^{+}_{k,\mathfrak{m}}) \cdot (E^{+}_{k,\mathfrak{m}}\,\mathrm{N}(U^{+}_{K,\mathfrak{m}}) : \mathrm{N}(U^{+}_{K,\mathfrak{m}}))}. \tag{18}$$

Chevalley's formula in the narrow sense ([Gr2, Lemma II.6.1.2], [Ja1, p. 177]) is

$$\#\mathcal{C}\ell^{+\,G}_{K} = \frac{\#\mathcal{C}\ell^{+}_{k} \cdot \prod_{\mathfrak{p} \in Pl_{k,0}} e_{\mathfrak{p}}}{[K : k] \cdot (E^{+}_{k} : E^{+}_{k} \cap \mathrm{N}(K^{\times}))}, \tag{19}$$

where $e_{\mathfrak{p}}$ is the ramification index in K/k of the finite place $\mathfrak{p}$.

Lemma 3.4. *For any finite set T, we have the relation*

$$U_{k,T}^{+} \cap \mathrm{N}(K^{\times}) = \mathrm{N}(U_{K,T}^{+}). \tag{20}$$

Proof. Let $x \in U_{k,T}^{+}$ of the form $\mathrm{N}(z)$, $z \in K^{\times}$; put $(z) = \prod_{\mathfrak{p} \in Pl_{k,0}} \mathfrak{C}_{\mathfrak{p}}$ where $\mathfrak{C}_{\mathfrak{p}} = \mathfrak{P}_0^{\omega}$, for a fixed $\mathfrak{P}_0 \mid \mathfrak{p}$ and $\omega \in \mathbb{Z}[G]$ depending on $\mathfrak{p}$. Since the $\mathrm{N}(\mathfrak{C}_{\mathfrak{p}}) = \mathrm{N}(\mathfrak{P}_0^{\omega})$ must be prime to T, we have $\omega \in (1-\sigma)\cdot\omega'$, $\omega' \in \mathbb{Z}[G]$, for all $\mathfrak{p} \in T$. Hence $(z) = \mathfrak{C}\cdot\mathfrak{A}^{1-\sigma}$ with $\mathfrak{C} \in I_{K,T}$ and $\mathfrak{A} \in I_K$. We can choose in the class modulo P_K^{+} (narrow sense) of $\mathfrak{A}$ an ideal $\mathfrak{B}$ prime to T, hence $\mathfrak{B} = \mathfrak{A}\cdot(y')$, $y' \in K^{\times +}$, giving $z' := z\, y'^{1-\sigma}$ prime to T; then we can multiply y' by y'', prime to T, to obtain $y := y'\, y''$ such that the signature of $y^{1-\sigma}$ be suitable, which is possible because of the relation $\mathrm{N}(z) \gg 0$ (i.e., the signature of z is in the kernel of the norm, see [Gr3, Proposition 1.1]); then $z'' := z\, y^{1-\sigma}$ yields $\mathrm{N}(z'') = x$ with $z'' \in U_{K,T}^{+}$. □

So $(E_k^{+} : E_k^{+} \cap \mathrm{N}(U_{K,T}^{+})) = (E_k^{+} : E_k^{+} \cap \mathrm{N}(K^{\times}))$. More generally, if $x \in U_{k,T}^{+}$ must be in $\mathrm{N}(U_{K,T}^{+})$ this is equivalent to say that x must be in $\mathrm{N}(K^{\times})$ (i.e., a global norm without any supplementary condition) which is more convenient to use normic criteria (with Hasse's symbols $\left(\frac{x\,,K/k}{\mathfrak{p}}\right)$ for instance; see Remark 4.7). Recall that for $T = \emptyset$, $U_{K,T}^{+} = K^{\times +}$ and the lemma says that $k^{\times +} \cap \mathrm{N}(K^{\times}) = \mathrm{N}(K^{\times +})$.

The lemma is valid with a modulus $\mathfrak{m}$ if its support T has no ramified places.

From (18) , (19) and (20), we have obtained

$$\#\mathcal{C}\ell_{K,\mathfrak{m}}^{+\,G} = \frac{\#\mathcal{C}\ell_k^{+}\cdot\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}\cdot(\mathrm{N}(U_{K,T}^{+}) : \mathrm{N}(U_{K,\mathfrak{m}}^{+}))}{[K:k]\cdot(E_k^{+} : E_{k,\mathfrak{m}}^{+})\cdot(E_{k,\mathfrak{m}}^{+}\,\mathrm{N}(U_{K,\mathfrak{m}}^{+}) : \mathrm{N}(U_{K,\mathfrak{m}}^{+}))},$$

hence using (11)

$$\#\big(\mathcal{C}\ell_{K,\mathfrak{m}}^{+}/\mathcal{H}\big)^{G} = \frac{\#\mathcal{C}\ell_k^{+}\cdot\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}\cdot(\mathrm{N}(U_{K,T}^{+}) : \mathrm{N}(U_{K,\mathfrak{m}}^{+}))}{[K:k]\cdot\#\mathrm{N}(\mathcal{H})\cdot(E_k^{+} : E_{k,\mathfrak{m}}^{+})\cdot(\Lambda\,\mathrm{N}(U_{K,\mathfrak{m}}^{+}) : \mathrm{N}(U_{K,\mathfrak{m}}^{+}))}. \tag{21}$$

3.1.2. *Local study of* $(\mathrm{N}_{K/k}(U_{K,T}^{+}) : \mathrm{N}_{K/k}(U_{K,\mathfrak{m}}^{+}))$. For a finite place $\mathfrak{P}$ of K, let $K_{\mathfrak{P}}$ be the $\mathfrak{P}$-completion of K at $\mathfrak{P}$. Then let $\mathcal{U}_{K,\mathfrak{P}}$ be the group of local units of $K_{\mathfrak{P}}$ and $\mathcal{U}_{K,T} := \prod_{\mathfrak{P}\in T}\mathcal{U}_{K,\mathfrak{P}} \subset \prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}$; we denote by $\mathcal{U}_{K,\mathfrak{m}}$ the closure of $U_{K,\mathfrak{m}}^{+}$ in $\mathcal{U}_{K,T}$ (T and $\mathfrak{m}$ seen in K). We have analogous notations for the field k.

The arithmetical norm $\mathrm{N}_{K/k} =: \mathrm{N}$ can be extended by continuity on $\prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}$ and the groups $\mathrm{N}(\mathcal{U}_{K,T})$ and $\mathrm{N}(\mathcal{U}_{K,\mathfrak{m}})$ are open compact subgroups of $\mathcal{U}_{k,T}$. It follows that the map $\mathrm{N}(U_{K,T}^{+}) \xrightarrow{\theta} \mathrm{N}(\mathcal{U}_{K,T})/\mathrm{N}(\mathcal{U}_{K,\mathfrak{m}})$ is surjective.

Consider its kernel. Let $\mathrm{N}(u)$, $u \in U_{K,T}^{+}$, be such that $\mathrm{N}(u) = \mathrm{N}(\alpha_{\mathfrak{m}})$, $\alpha_{\mathfrak{m}} \in \mathcal{U}_{K,\mathfrak{m}}$. Since $\mathrm{H}^1(G, \prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}) = 0$ (Shapiro's Lemma and Hilbert Theorem 90), there exists $\beta \in \prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}$ such that $u = \alpha_{\mathfrak{m}}\beta^{1-\sigma}$.

We can approximate (over T) β by $v \in K^{\times +}$ and $\alpha_{\mathfrak{m}}$ by $u_{\mathfrak{m}} \in U_{K,\mathfrak{m}}^{+}$; then $u = u_{\mathfrak{m}}\, v^{1-\sigma}\cdot\xi$, with ξ near from 1 in $\prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}$ and totally positive; then let $u' = u\, v^{-(1-\sigma)}$; this leads to $u' = u_{\mathfrak{m}}\,\xi \in U_{K,\mathfrak{m}}^{+}$ and $\mathrm{N}(u') = \mathrm{N}(u) \in \mathrm{N}(U_{K,\mathfrak{m}}^{+})$. The kernel of the map θ is $\mathrm{N}(U_{K,\mathfrak{m}}^{+})$. Thus

$$\begin{aligned}(\mathrm{N}(U_{K,T}^{+}) : \mathrm{N}(U_{K,\mathfrak{m}}^{+})) = (\mathrm{N}(\mathcal{U}_{K,T}) : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}})) &= \frac{(\mathcal{U}_{k,T} : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}}))}{(\mathcal{U}_{k,T} : \mathrm{N}(\mathcal{U}_{K,T}))} \\ &= \frac{(\mathcal{U}_{k,T} : \mathcal{U}_{k,\mathfrak{m}})\cdot(\mathcal{U}_{k,\mathfrak{m}} : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}}))}{(\mathcal{U}_{k,T} : \mathrm{N}(\mathcal{U}_{K,T}))}.\end{aligned} \tag{22}$$

By local class field theory we know that $(\mathcal{U}_{k,T} : \mathrm{N}(\mathcal{U}_{K,T})) = \prod_{\mathfrak{p}\in T} e_{\mathfrak{p}}$. where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ in K/k.

Remark 3.5. The index $(\mathcal{U}_{k,\mathfrak{m}} : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}}))$ may be computed from higher ramification groups in K/k (cf. [Se1, Chapitre V]) by introduction of the usual filtration of the groups $\mathcal{U}_{k,\mathfrak{p}}$ and $\mathcal{U}_{K,\mathfrak{P}}$. If $\mathfrak{m} = \prod_{\mathfrak{p}\in T} \mathfrak{p}^{\lambda_\mathfrak{p}}$, $\lambda_\mathfrak{p} \geq 1$, then $\mathcal{U}_{k,\mathfrak{m}} = \prod_{\mathfrak{p}\in T}(1+\mathfrak{p}^{\lambda_\mathfrak{p}}\mathcal{O}_\mathfrak{p})$ and $\mathcal{U}_{K,\mathfrak{m}} = \prod_{\mathfrak{p}\in T}\prod_{\mathfrak{P}\mid\mathfrak{p}}(1+\mathfrak{P}^{\lambda_\mathfrak{p} e_\mathfrak{p}}\mathcal{O}_\mathfrak{P})$, where $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{P}$ are the local rings of integers. This local index only depends on the given extension K/k.

To go back to $\mathcal{C}\ell^+_{k,\mathfrak{m}}$, we have the following formula (cf. [Gr2, Corollary I.4.5.6 (i)])

$$\#\mathcal{C}\ell^+_{k,\mathfrak{m}} = \#\mathcal{C}\ell^+_k \cdot \frac{(U^+_{k,T} : U^+_{k,\mathfrak{m}})}{(E^+_k : E^+_{k,\mathfrak{m}})} = \#\mathcal{C}\ell^+_k \cdot \frac{(\mathcal{U}_{k,T} : \mathcal{U}_{k,\mathfrak{m}})}{(E^+_k : E^+_{k,\mathfrak{m}})}, \tag{23}$$

where the integer $(\mathcal{U}_{k,T} : \mathcal{U}_{k,\mathfrak{m}})$ is given by the generalized Euler function of $\mathfrak{m}$.
Then using (21), (22), (23), we obtain the main result:

Theorem 3.6. *Let K/k be a cyclic extension of Galois group G; let $\mathfrak{m}$ be a nonzero integer ideal of k and let T be the support of $\mathfrak{m}$. Let $e_\mathfrak{p}$ be the ramification index in K/k of any finite place $\mathfrak{p}$ of k. Then for any sub-G-module $\mathcal{H}$ of $\mathcal{C}\ell^+_{K,\mathfrak{m}}$ and any subgroup $\mathcal{I}$ of $I_{K,T}$ such that $\mathcal{I}\cdot P^+_{K,\mathfrak{m}}/P^+_{K,\mathfrak{m}} = \mathcal{H}$, we have*

$$\#\big(\mathcal{C}\ell^+_{K,\mathfrak{m}}/\mathcal{H}\big)^G = \frac{\#\mathcal{C}\ell^+_{k,\mathfrak{m}} \cdot \prod_{\mathfrak{p}\notin T} e_\mathfrak{p} \cdot (\mathcal{U}_{k,\mathfrak{m}} : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}}))}{[K:k]\cdot \#\mathrm{N}(\mathcal{H}) \cdot (\Lambda : \Lambda \cap \mathrm{N}(U^+_{K,\mathfrak{m}}))}. \tag{24}$$

where $\mathrm{N} = \mathrm{N}_{K/k}$ is the arithmetical norm and $\Lambda := \{x \in U^+_{k,\mathfrak{m}},\ \ (x) \in \mathrm{N}(\mathcal{I})\}$.

Using, where appropriate, Lemma 3.4, we get the following corollaries:

Corollary 3.7. [Gr3, Théorème 4.3, p. 41]. *Taking $T = \emptyset$, we obtain:*

$$\#\big(\mathcal{C}\ell^+_K/\mathcal{H}\big)^G = \frac{\#\mathcal{C}\ell^+_k \cdot \prod_{\mathfrak{p}\in Pl_{k,0}} e_\mathfrak{p}}{[K:k]\cdot \#\mathrm{N}(\mathcal{H}) \cdot (\Lambda : \Lambda \cap \mathrm{N}(K^\times))}, \tag{25}$$

where $\Lambda := \{x \in k^{\times +},\ \ (x) \in \mathrm{N}(\mathcal{I})\}$.

Corollary 3.8. [HL, (1990)]. *If T does not contain any prime ideal ramified in K/k, we obtain, since in the unramified case $(\mathcal{U}_{k,\mathfrak{m}} : \mathrm{N}(\mathcal{U}_{K,\mathfrak{m}})) = 1$ regardless $\mathfrak{m}$:*

$$\#\big(\mathcal{C}\ell^+_{K,\mathfrak{m}}/\mathcal{H}\big)^G = \frac{\#\mathcal{C}\ell^+_{k,\mathfrak{m}} \cdot \prod_{\mathfrak{p}\in Pl_{k,0}} e_\mathfrak{p}}{[K:k]\cdot \#\mathrm{N}(\mathcal{H}) \cdot (\Lambda : \Lambda \cap \mathrm{N}(K^\times))}. \tag{26}$$

Corollary 3.9. *If $T = \emptyset$ and if $\mathcal{H} = \mathcal{C}\ell_K(S_K)$, where S_K is any finite set of places of K, we obtain $\Lambda/\Lambda\cap\mathrm{N}(K^\times) \simeq E^{\mathrm{N}S_K}_k/E^{\mathrm{N}S_K}_k \cap \mathrm{N}(K^\times)$ (see Remark 3.2), and:*

$$\#\mathcal{C}\ell^{S_K G}_K = \frac{\#\mathcal{C}\ell^+_k \cdot \prod_{\mathfrak{p}\in Pl_{k,0}} e_\mathfrak{p}}{[K:k]\cdot \#\mathcal{C}\ell_k(\langle \mathrm{N}S_K\rangle) \cdot (E^{\mathrm{N}S_K}_k : E^{\mathrm{N}S_K}_k \cap \mathrm{N}(K^\times))}, \tag{27}$$

where the group $E^{\mathrm{N}S_K}_k$ of "$\mathrm{N}S_K$-units" is defined by:
$E^{\mathrm{N}S_K}_k = \{x \in E^{S_k}_k,\ v_\mathfrak{p}(x) \equiv 0 \pmod{f_\mathfrak{p}}\ \forall \mathfrak{p} \in S_k\ \&\ v_\mathfrak{p}(x) = 0\ \forall \mathfrak{p} \in Pl_{k,\infty} \setminus S_{k,\infty}\}$,
S_k being the set of places of k under S_K and $f_\mathfrak{p}$ the residue degree of $\mathfrak{p}$.

Proof. We have $\Lambda = \{x \in k^{\times +},\ (x) \in \mathrm{N}(\mathcal{I})\}$, where $\mathcal{I} = \langle\mathfrak{P}\rangle_{\mathfrak{P}\in S_{K,0}} \cdot \langle(y_\mathfrak{P})\rangle_{\mathfrak{P}\in S_{K,\infty}}$. If $x \in \Lambda$, then $(x) = \mathrm{N}(\mathfrak{A})\cdot\mathrm{N}(A)$, $\mathfrak{A} \in \langle\mathfrak{P}\rangle_{\mathfrak{P}\in S_{K,0}}$, $A \in \langle(y_\mathfrak{P})\rangle_{\mathfrak{P}\in S_{K,\infty}}$; hence, up to $\mathrm{N}K^\times$, x is represented by a $\mathrm{N}S_K$-unit ε. One verifies that the map which associates x with the image of ε in $E^{\mathrm{N}S_K}_k/E^{\mathrm{N}S_K}_k \cap \mathrm{N}(K^\times)$ is well-defined and leads to the isomorphism. Note that $E^+_k \subseteq E^{\mathrm{N}S_K}_k$. □

Remark 3.10. We have in [Ja1, p. 177 (1986)] another writing of this formula:

$$\#\mathcal{C}\ell^{S_K G}_K = \frac{\#\mathcal{C}\ell^{S_k}_k \cdot \prod_{\mathfrak{p}\notin S_k} e_\mathfrak{p} \cdot \prod_{\mathfrak{p}\in S_k} d_\mathfrak{p}}{[K:k]\cdot (E^{S_k}_k : E^{S_k}_k \cap \mathrm{N}(K^\times))},$$

where $d_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$ is the local degree of K/k at $\mathfrak{p}$ with $e_\mathfrak{p} = 1$ for infinite places: use the relation $E^{S_k}_k \cap \mathrm{N}(K^\times) = E^{\mathrm{N}S_K}_k \cap \mathrm{N}(K^\times)$ and the exact sequence

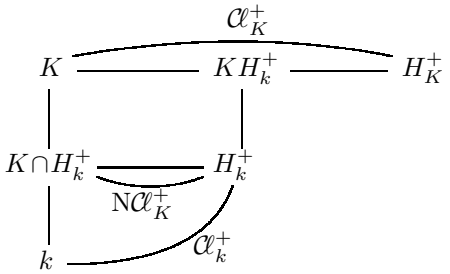
$$1 \longrightarrow E_k^{S_k}/E_k^{\mathrm{N}S_K} \longrightarrow \langle S_k\rangle_{\mathbb{Z}}/\langle \mathrm{N}S_K\rangle_{\mathbb{Z}} \longrightarrow cl_k(\langle S_k\rangle_{\mathbb{Z}})/cl_k(\langle \mathrm{N}S_K\rangle_{\mathbb{Z}}) \longrightarrow 1$$

for the comparison. Taking $S_K = Pl_{K,\infty}$ in the two formulas, we get

$$\#\mathcal{C}\ell_K^{\mathrm{ord}\,\mathrm{G}} = \frac{\#\mathcal{C}\ell_k^{\mathrm{ord}} \cdot \prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}} \cdot \prod_{\mathfrak{p}\in Pl_{k,\infty}} f_{\mathfrak{p}}}{[K:k]\cdot (E_k^{\mathrm{ord}} : E_k^{\mathrm{ord}} \cap \mathrm{N}(K^\times))}, \tag{28}$$

which is the true original Chevalley's formula (in the ordinary sense), where $f_{\mathfrak{p}} = 2$ (resp. 1) if $\mathfrak{p} \in Pl_{k,\infty}$ is complexified (resp. is not).

3.2. **Genera theory and heuristic aspects.** The usual case ($S = T = \emptyset$), in the cyclic extension K/k, can be interpreted by means of the following diagram of finite extensions:



Here $K \cap H_k^+/k$ is the maximal subextension of K/k, unramified at finite places, and the norm map $\mathrm{N}_{K/k} : \mathcal{C}\ell_K^+ \longrightarrow \mathcal{C}\ell_k^+$ is surjective if and only if $K \cap H_k^+ = k$. So formula (25) can be interpreted as follows (which will be very important for numerical computations); using the relations

$$[K:k] = [K : K\cap H_k^+]\cdot[K\cap H_k^+ : k] \quad \& \quad \#\mathcal{C}\ell_k^+ = \#\mathrm{N}(\mathcal{C}\ell_K^+)\cdot[K\cap H_k^+ : k],$$

we shall get a product of two integers

$$\#\big(\mathcal{C}\ell_K^+/\mathcal{H}\big)^G = \frac{\#\mathrm{N}(\mathcal{C}\ell_K^+)}{\#\mathrm{N}(\mathcal{H})}\cdot\frac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]\cdot(\Lambda : \Lambda\cap \mathrm{N}(K^\times))}. \tag{29}$$

Thus in the computations using a filtration M_i (see Section 4), the G-modules $\mathcal{H} = cl_K(\mathcal{I})$ are denoted $M_i = cl_K(\mathcal{I}_i)$; the M_i and $\mathrm{N}(M_i)$ will be increasing subgroups of $\mathcal{C}\ell_K^+$ and $\mathcal{C}\ell_k^+$, respectively, so that $M_n = \mathcal{C}\ell_K^+$ for some n.

Then we know that $\Lambda_i = \{x_i \in k^{\times +},\ (x_i) \in \mathrm{N}(\mathcal{I}_i)\}$, which means that x_i, being the norm of an ideal and totally positive, is a local norm at each unramified finite place and at each infinite place (from Remark 4.7, (α), (β)); so it remains to consider *the local norms at ramified prime ideals* since by the Hasse norm theorem, $x \in \mathrm{N}(K^\times)$ if and only if x is a local norm everywhere (apart from *one* place). This can be done by means of norm residue symbols computations of Remark 4.7, (γ), in the context of "genera theory" (see the abundant literature on the subject, for instance from the bibliographies of [Fr], [Fu], [Gr2], [L4]), so that the integers:

$$\frac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]\cdot(\Lambda_i : \Lambda_i\cap \mathrm{N}(K^\times))},\ \ i \geq 0,$$

are decreasing because of the injective maps

$$E_k^+/E_k^+\cap \mathrm{N}(K^\times) \hookrightarrow \cdots \hookrightarrow \Lambda_i/\Lambda_i\cap \mathrm{N}(K^\times) \hookrightarrow \Lambda_{i+1}/\Lambda_{i+1}\cap \mathrm{N}(K^\times) \hookrightarrow \cdots$$

giving increasing indices $(\Lambda_i : \Lambda_i \cap \mathrm{N}(K^\times))$.

Let $I_{\mathfrak{p}}(K/k)$ be the inertia groups (of orders $e_{\mathfrak{p}}$) of the prime ideals $\mathfrak{p}$ and put

$$\Omega(K/k) = \Big\{(\tau_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}\in Pl_0} I_{\mathfrak{p}}(K/k),\quad \prod_{\mathfrak{p}\in Pl_0}\tau_{\mathfrak{p}} = 1\Big\}; \tag{30}$$

we have the genera exact sequence of class field theory (interpreting the product formula of Hasse symbols, [Gr2, Proposition IV.4.5])

$$1 \longrightarrow E_k^+/E_k^+ \cap \mathrm{N}(K^\times) \xrightarrow{\omega} \bigoplus_{\mathfrak{p}\in Pl_0} I_{\mathfrak{p}}(K/k) \xrightarrow{\pi} \mathrm{Gal}(H_{K/k}^+/H_k^+) \longrightarrow 1,$$

where $H_{K/k}^+ := H_K^{+\,\mathrm{ab}}$ is the genera field defined as the maximal subextension of H_K^+, Abelian over k, where ω associates with $x \in E_k^+$ the family of Hasse symbols $\left(\left(\frac{x,\,K/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p}\in Pl_0}$ in $\bigoplus_{\mathfrak{p}\in Pl_0} I_{\mathfrak{p}}(K/k)$ (hence in $\Omega(K/k)$), and where π associates with $(\tau_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}\in Pl_0} I_{\mathfrak{p}}(K/k)$ the product $\prod_{\mathfrak{p}} \tau'_{\mathfrak{p}}$ of the lifts $\tau'_{\mathfrak{p}}$ of the $\tau_{\mathfrak{p}}$, in the inertia groups of $H_{K/k}^+/H_k^+$ (these inertia groups generate the group $\mathrm{Gal}(H_{K/k}^+/H_k^+)$ which is the image of π); from the product formula, if $(\tau_{\mathfrak{p}})_{\mathfrak{p}}$ is in the image of ω, then this product $\prod_{\mathfrak{p}} \tau'_{\mathfrak{p}}$ fixes both H_k^+ and K, hence KH_k^+. Thus $\pi(\Omega(K/k)) = \mathrm{Gal}(H_{K/k}^+/KH_k^+)$ with $\pi\circ\omega(E_k^+) = 1$, giving the isomorphisms

$$\Omega(K/k)/\omega(E_k^+) \simeq \mathrm{Gal}(H_{K/k}^+/KH_k^+) \;\;\&\;\; \omega(E_k^+) \simeq E_k^+/E_k^+ \cap \mathrm{N}(K^\times).$$

We have $\#\Omega(K/k) = \dfrac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]}$ and $H_{K/k}^+$ being fixed by $(\mathcal{C}\ell_K^+)^{1-\sigma}$, we get

$$[H_{K/k}^+ : K] = [H_k^+ : K\cap H_k^+] \cdot \frac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]\cdot (E_k^+ : E_k^+ \cap \mathrm{N}(K^\times))} = \#\mathcal{C}\ell_K^{+\,G}$$

as expected.

Since Λ_i contains E_k^+, we have $\pi\circ\omega(\Lambda_i/E_k^+) \subseteq \mathrm{Gal}(H_{K/k}^+/KH_k^+)$. Therefore we have at the final step $i = n$, using (29) for $\mathcal{H} = M_n = \mathcal{C}\ell_K^+$,

$$(\Lambda_n : \Lambda_n \cap \mathrm{N}(K^\times)) = \frac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]} = \#\Omega(K/k),$$

whence $\omega_n(\Lambda_n) = \Omega(K/k)$ and $\pi_n\circ\omega_n(\Lambda_n/E_k^+) = \mathrm{Gal}(H_{K/k}^+/KH_k^+)$, which explains that an obvious heuristic is that $\#\mathcal{C}\ell_K^+$ has no theoretical limitation about the integer n (but its structure may have some constraints, see Section 4).

An interesting case leading to significant simplifications is when there is a single ramified place $\mathfrak{p}_0$ in K/k; indeed, the product formula (from $\Omega(K/k) = 1$) implies $(\Lambda : \Lambda\cap\mathrm{N}(K^\times)) = 1$ and $\dfrac{e_{\mathfrak{p}_0}}{[K : K\cap H_k^+]} = 1$, so that formula (29) reduces to $\#\big(\mathcal{C}\ell_K^+/\mathcal{H}\big)^G = \dfrac{\#\mathrm{N}(\mathcal{C}\ell_K^+)}{\#\mathrm{N}(\mathcal{H})}$, where $\#\mathrm{N}(\mathcal{C}\ell_K^+) = [H_k^+ : K\cap H_k^+]$ is known. If $\mathfrak{p}_0$ is totally ramified, then $\#\big(\mathcal{C}\ell_K^+/\mathcal{H}\big)^G = \dfrac{\#\mathcal{C}\ell_k^+}{\#\mathrm{N}(\mathcal{H})}$.

From the above formulas (e.g., Formula (27)), we get some practical applications:

Theorem 3.11. *Let K/k be a cyclic p-extension of Galois group G. Let S_K be a finite set of non-complex places of K such that $\mathcal{C}\ell_K(\langle S_K\rangle)$ is a sub-G-module. Consider the p-class group $\mathcal{C}\ell_K^{S_K}$, for which we have the formula*

$$\#\mathcal{C}\ell_K^{S_K\,G} = \frac{\#\mathrm{N}(\mathcal{C}\ell_K^+)}{\#cl_k(\langle \mathrm{N}S_K\rangle)} \cdot \frac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]\cdot (E_k^{\mathrm{N}S_K} : E_k^{\mathrm{N}S_K}\cap \mathrm{N}(K^\times))}.$$

Then we have $\langle cl_K(S_K)\rangle_{\mathbb{Z}} = \mathcal{C}\ell_K^+$ (i.e., S_K generates the p-class group of K) if and only if the two following conditions are satisfied:

(i) $\mathrm{N}(\mathcal{C}\ell_K^+) = cl_k(\langle \mathrm{N}S_K\rangle)$,

(ii) $(E_k^{\mathrm{N}S_K} : E_k^{\mathrm{N}S_K}\cap\mathrm{N}(K^\times)) = \dfrac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K : K\cap H_k^+]} = \#\Omega(K/k)$ *(see (30))*.

If $K\cap H_k^+ = k$ and if all places $\mathfrak{P}\in S_K$ are unramified of residue degree 1 in K/k, the two conditions become:

(i′) $\mathcal{C}\ell_k^+ = \mathcal{C}\ell_k(\langle S_k\rangle)$, *where* S_k *is the set of places* $\mathfrak{p}$ *under* $\mathfrak{P} \in S_K$,

(ii′) $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}(K^\times)) = \dfrac{\prod_{\mathfrak{p}\in Pl_{k,0}} e_\mathfrak{p}}{[K:k]} = \#\Omega(K/k)$.

So, if the p-class group $\mathcal{C}\ell_k^+$ is numerically known, to characterize a set S_K of generators for $\mathcal{C}\ell_K^+$ needs only local normic computations with the group $E_k^{S_k}$ of S_k-units of k which are known. Moreover, we can restrict ourselves to the case of p-class groups in a cyclic extension of degree p.

Example 3.12. Consider $K = \mathbb{Q}(\sqrt{82})$, $k = \mathbb{Q}$ and $p = 2$ (the fundamental unit is of norm -1, hence ordinary and narrow senses coincide). We shall use the primes 3 and 23 which split in K, and prime ideals $\mathfrak{P}_3$ and $\mathfrak{P}_{23}$ above. It is clear that the 2-rank of the class group of K is 1 (usual Chevalley's formula (28)). The conditions of the theorem are equivalent to $(E_\mathbb{Q}^{S_\mathbb{Q}} : E_\mathbb{Q}^{S_\mathbb{Q}} \cap \mathrm{N}(K^\times)) = 2$ since the product of ramification indices is equal to 4; for instance, $E_\mathbb{Q}^{S_\mathbb{Q}} = \langle 3\rangle$ for $S_K = \{\mathfrak{P}_3\}$.

We have to compute, for some $x \in \mathbb{Q}^{\times +}$ (norm of an ideal, thus local norm at each unramified place), the Hasse symbol $\left(\dfrac{x, K/\mathbb{Q}}{41}\right)$ which is equal to 1 if and only if x is local norm at 41 (which is equivalent to be global norm in $K/\mathbb{Q}$ because of the product formula $\left(\dfrac{x, K/\mathbb{Q}}{41}\right) \cdot \left(\dfrac{x, K/\mathbb{Q}}{2}\right) = 1$ and the Hasse norm theorem).

But from the method recalled in Remark 4.7, we have to find an "associate number" x' such that $x' \equiv 1 \pmod 8$ & $x' \equiv x \pmod{41}$, then to compute the Kronecker symbol $\left(\dfrac{82}{x'}\right)$ (we have used the fact that the conductor of K is $8 \cdot 41$).

We compute that $x = 3$ is not norm of an element of $K^\times$, whence $\mathfrak{P}_3$ generates the 2-class group of K (for $x = 3$, $x' = 249$, and $\left(\frac{82}{249}\right) = -1$). We can verify that $\mathfrak{P}_3$ is of order 4 since the equation $u^2 - 82 \cdot v^2 = 3^e$ (with $\gcd(u, v) = 1$) has no solution with $e = 1$ or $e = 2$, but $\mathrm{N}(73 + 8\sqrt{82}) = 3^4$; however, the knowledge of $\#\mathcal{C}\ell_K$ is not required to generate the class group.

Now we consider $x = 23$ for which $x' = 105$ and $\left(\frac{82}{105}\right) = 1$. We compute that indeed $\frac{65+7\sqrt{82}}{3}$ is of norm 23; this is given by the PARI instruction (cf. [P]):

$$\textit{bnfisnorm(bnfinit(}x^2 - 82), 23\textit{))}.$$

Then we can verify that 23 is not the norm of an integer; so we deduce that the class of $\mathfrak{P}_{23}$ does not generate the 2-class group of K and is of order 2 (indeed, $\mathrm{N}(761 + 84\sqrt{82}) = 23^2$ giving $\mathfrak{P}_{23}^2 = (761 + 84\sqrt{82})$).

Remark 3.13. Another important fact is the relation $\nu_{K/k} = j_{K/k} \circ \mathrm{N}_{K/k}$ when some classes of k capitulate in K (i.e., $j_{K/k}$ non-injective). It is obvious that the classes of order prime to the degree d of K/k never capitulate; this explains that we shall restrict ourselves to p-class groups in p-extensions.

The generalizations of Chevalley's formula do not take into account this phenomena since they consider only groups of the form $\mathrm{N}_{K/k}(\mathcal{H})$ without mystery (when $\mathcal{C}\ell_k^+$ is well known), contrary to $\mathcal{H}^{\nu_{K/k}}$.

This property of $\mathrm{N}_{K/k}$ is valid if K/k is any Galois extension; if K/k has no unramified Abelian subextension L/K (what is immediately noticeable !) then $\mathrm{N}_{K/k}$ is surjective, but possibly not $\nu_{K/k}$. We have given in [Gr5], [Gr5′], numerical setting of this to disprove some statements concerning the propagation of p-ranks of p-class groups in p-ramified p-extensions K/k.

These local normic calculations deduced from Theorem 3.6 have been extensively studied in concrete cases from the pioneer work of Inaba [I, (1940)], in quadratic, cubic extensions, etc. and applied to non-cyclic extensions (dihedral ones, etc):

see, e.g., [Fr], [Re], [Gr3], [Gr3′], [Gr4], [HL], [L1] (in the semi-simple case of G-modules), [Bol], [L2], [L3], [L4], [Kol], [KMS], [Ge1], [Ge2], [Ge3], [Kl], [Gr5], [Y1], [Y2], and the corresponding references of all these papers !

These techniques may give information on some class field towers problems, capitulation problems, often with the use of quadratic fields ([ATZ1], [ATZ2], [Go], [GW1], [GW2], [GW3], [Su], [SW], [Ter], [Mai], [Ma1], [Ma2], [Miy1], [Miy2], [MoMo], some examples in [Gr5] and numerical computations in [Gr5′], [Gr13], [Ku] for capitulation in Abelian extensions, then many results of N. Boston, F. Hajir and Ch. Maire, and many others as these matters are too broad to be exposed here).

4. Structure of p-class groups in p-extensions

4.1. **Recalls about the filtration of a $\mathbb{Z}_p[G]$-module M, with $G \simeq \mathbb{Z}/p\mathbb{Z}$.** Let K/k be a cyclic extension of prime degree p, of Galois group $G = \langle\sigma\rangle$.

Let $\mathcal{C}\ell_K^+, \mathcal{C}\ell_k^+$ be the class groups in the narrow sense (same theory with the ordinary sense for any data). We shall look at the p-class groups $\mathcal{C}\ell_K^+ \otimes \mathbb{Z}_p$, $\mathcal{C}\ell_k^+ \otimes \mathbb{Z}_p$, still denoted $\mathcal{C}\ell_K^+, \mathcal{C}\ell_k^+$ thereafter, by abuse of notation.

We consider the $\mathbb{Z}_p[G]$-module $M := \mathcal{C}\ell_K^+$ for which we define the filtration evocated in Section 1:

$$M_{i+1}/M_i := (M/M_i)^G, \quad M_0 = 1;$$

we denote by n the least integer i such that $M_i = M$. For all $i \geq 0$ we have

$$M_{i+1}^{1-\sigma} \subseteq M_i, \;\; M_i = \big\{h \in M, \;\; h^{(1-\sigma)^i} = 1\big\}, \text{ and } \;\; \#M = \textstyle\prod_{i=0}^{n-1} \#(M_{i+1}/M_i).$$

For all $i \geq 1$, the maps $M_{i+1}/M_i \xrightarrow{1-\sigma} M_i/M_{i-1}$ are injective, giving a decreasing sequence for the orders $\#(M_{i+1}/M_i)$ as i grows, whence $\#(M_{i+1}/M_i) \leq \#M_1$.
If for instance $\#M_1 = p$, then $\#(M_{i+1}/M_i) = p$ for $0 \leq i \leq n-1$.

Remark that $\mathcal{C}\ell_k^+$ has no obvious G-module definition from M (it is not isomorphic to $M_1 = M^G$, nor to $M^{\nu_{K/k}}$ for $\nu_{K/k} := 1 + \sigma + \cdots + \sigma^{p-1}$); this is explained by the difference of nature between $\nu_{K/k}$ and the arithmetical norm $\mathrm{N}_{K/k}$ of class field theory.

4.2. **Case $M^\nu = 1$.** When $M^\nu = 1$ for $\nu := \nu_{K/k} = 1 + \sigma + \cdots + \sigma^{p-1}$, M is a $\mathbb{Z}_p[G]/(\nu)$-module and we have

$$\mathbb{Z}_p[G]/(\nu) \simeq \mathbb{Z}_p[X]/(1 + X + \cdots + X^{p-1}) \simeq \mathbb{Z}_p[\zeta],$$

where ζ is a primitive pth root of unity; then we know that

$$M \simeq \bigoplus_{j=1}^{m} \mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j}, \;\; 1 \leq n_1 \leq n_2 \leq \cdots \leq n_m, \;\; m \geq 0,$$

whose p-rank can be arbitrary. The exact sequence

$$1 \longrightarrow M_1 = M^G \longrightarrow M \xrightarrow{1-\sigma} M^{1-\sigma} \longrightarrow 1$$

becomes in the $\mathbb{Z}_p[\zeta]$-structure:

$$\begin{aligned} 1 \longrightarrow \bigoplus_{j=1}^{m} (1-\zeta)^{n_j-1}\,\mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j} \longrightarrow \\ M = \bigoplus_{j=1}^{m} \mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j} \xrightarrow{1-\zeta} \bigoplus_{j=1}^{m} (1-\zeta)\,\mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j} \longrightarrow 1, \end{aligned} \tag{31}$$

where the submodules M_i are given by $M_i = \bigoplus_{j,\, n_j \leq i} \mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j}$ (for $0 \leq i \leq n$, where $n = n_m$).

Each factor $N_j := \mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j}$ (such that $M = \bigoplus_{j=1}^{m} N_j$, not to be confused with the $M_i = \bigoplus_{j,\, n_j \leq i} N_j$) has a structure of group given by the following result:

Theorem 4.1. *Under the assumption $M^{\nu_{K/k}}=1$ in the cyclic extension K/k of degree p, put $n_j=a_j\,(p-1)+b_j$, $a_j\geq 0$ and $0\leq b_j\leq p-2$, in the decomposition of M in elementary components as above. Then*

$$N_j:=\mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j}\simeq(\mathbb{Z}/p^{a_j+1}\mathbb{Z})^{b_j}\bigoplus(\mathbb{Z}/p^{a_j}\mathbb{Z})^{p-1-b_j},\quad\forall j=1,\dots,m.$$

$$M\simeq\bigoplus_{j=1}^{m}\Big[(\mathbb{Z}/p^{a_j+1}\mathbb{Z})^{b_j}\bigoplus(\mathbb{Z}/p^{a_j}\mathbb{Z})^{p-1-b_j}\Big]. \tag{32}$$

Proof. We have $N_j:=\mathbb{Z}_p[\zeta]/(1-\zeta)^{n_j}\simeq\mathbb{Z}_p[\zeta]/p^{a_j}\,(1-\zeta)^{b_j}$. So, to have the structure of group, it is sufficient to compute the p^k-ranks for all $k\geq 1$ (i.e., the dimensions over $\mathbb{F}_p$ of $N_j^{p^{k-1}}/N_j^{p^k}$), which is immediate since this p^k-rank is $p-1$ for $k\leq a_j$, b_j for $k=a_j+1$, and 0 for $k>a_j+1$. □

This implies that the p-rank of N_j is $p-1$ if $a_j\geq 1$ and b_j if $a_j=0$ (i.e., $b_j=n_j\leq p-2$). So the parameters a_j and b_j will be important in a theoretical and numerical point of view. Put $M^{(k)}:=\big\{h\in M,\ h^{p^k}=1\big\}$, $k\geq 0$.

Lemma 4.2. *If $M^\nu=1$, then $M^{(k)}=M_{k\cdot(p-1)},\forall k\geq 0$, and the p^k-rank R_k of M is the $\mathbb{F}_p$-dimension of $M^{(k-1)}/M^{(k)}$. Then $p^{R_k}=\prod_{i=(k-1)(p-1)}^{k(p-1)-1}\#(M_{i+1}/M_i)$.*

Proof. Immediate from the $\mathbb{Z}_p[\zeta]$-structure and properties of Abelian p-groups. □

4.3. **Case $M^\nu\neq 1$.** We have, in the same framwork, the following result in the case $M^\nu\neq 1$, but $\#(M_{i+1}/M_i)=p$ [Gr2, Proposition 4.3, pp. 31–32]:

Theorem 4.3. *Let K/k be a cyclic extension of prime degree p, of Galois group $G=\langle\sigma\rangle$ and let M be a finite $\mathbb{Z}_p[G]$-module such that $M^{\nu_{K/k}}\neq 1$. Let n be the least integer i such that $M_i=M$. We assume that $\#M_1=p$.*

Put $n=a\cdot(p-1)+b$, with $a\geq 0$ and $0\leq b\leq p-2$. Then we have necessarily $n\geq 2$ and the following possibilities:

(i) Case $n<p$. Then $M\simeq\big(\mathbb{Z}/p^2\mathbb{Z}\big)\bigoplus\big(\mathbb{Z}/p\mathbb{Z}\big)^{n-2}$.

(ii) Case $n=p$. Then $M\simeq\big(\mathbb{Z}/p\mathbb{Z}\big)^p$ or $\big(\mathbb{Z}/p^2\mathbb{Z}\big)\bigoplus\big(\mathbb{Z}/p\mathbb{Z}\big)^{p-2}$.

(iii) Case $n>p$. Then $M\simeq\big(\mathbb{Z}/p^{a+1}\mathbb{Z}\big)^b\bigoplus\big(\mathbb{Z}/p^a\mathbb{Z}\big)^{p-1-b}$.

Proof. The proof needs two lemmas (in which we keep the notation M_n for M).

Lemma 4.4. *For all $k\geq 1$ we have the exact sequence*

$$1\longrightarrow M_1\cap M_n^{p^{k-1}}/M_1\cap M_n^{p^k}\longrightarrow M_n^{p^{k-1}}/M_n^{p^k}\xrightarrow{1-\sigma}M_{n-1}^{p^{k-1}}/M_{n-1}^{p^k}\longrightarrow 1. \tag{33}$$

Proof. Under the assumption $\#M_1=p$, we know fron § 4.1 that $\#(M_{i+1}/M_i)=p$, $0\leq i\leq n-1$; we have the exacte sequence $1\to M_1\longrightarrow M_{i+1}\xrightarrow{1-\sigma}M_{i+1}^{1-\sigma}\to 1$, which shows that $\#(M_{i+1}/M_{i+1}^{1-\sigma})=p$, hence $M_{i+1}^{1-\sigma}=M_i$ since $M_{i+1}^{1-\sigma}\subseteq M_i$.

Let $x\in M_n^{p^{k-1}}$ such that $x^{1-\sigma}=y^{p^k}$, $y\in M_{n-1}$. There exists $z\in M_n$ such that $y=z^{1-\sigma}$ and $x^{1-\sigma}=z^{p^k\cdot(1-\sigma)}$; thus $(x\cdot z^{-p^k})^{1-\sigma}=1$ so that $x\cdot z^{-p^k}\in M_1\cap M_n^{p^{k-1}}$, giving

$$\mathrm{Ker}(1-\sigma)\subseteq M_1\cap M_n^{p^{k-1}}/M_1\cap M_n^{p^k},$$

the opposite inclusion being obvious as well as the surjectivity. □

Lemma 4.5. *If $n\neq p$ then the p-rank of M_n is equal to the p-rank of M_{n-1}.*

Proof. From the relation $(1-\zeta)^{p-1}=p\cdot A(\zeta)$, where $A(\zeta)\equiv -1\pmod{(1-\zeta)}$, we have $\nu=(1-\sigma)^{p-1}-p\cdot A(\sigma)$, $A(\sigma)\equiv -1\pmod{(1-\sigma)}$ (i.e., $A(\sigma)$ invertible in $\mathbb{Z}_p[G]$).

(a) Case $n>p$. Let $x\in M_{n-1}\setminus M_{n-2}$ (this makes sense since $n\geq p+1\geq 3$) and let $y=x^{(1-\sigma)^{n-2}}$; then $y\in M_1$, $y\neq 1$ because of the choice of x. There exists $B(\sigma)\in\mathbb{Z}_p[G]$ such that $(1-\sigma)^{n-2}=B(\sigma)\cdot(1-\sigma)^{p-1}$ and with $z=x^{B(\sigma)}$ one

obtains $y = z^{(1-\sigma)^{p-1}}$. Since $M_{n-1} = M_n^{1-\sigma}$ one gets $M_{n-1}^{\nu} = 1$, so that $z^{\nu} = 1$ and $z^{(1-\sigma)^{p-1}} = z^{p \cdot A(\sigma)}$ which shows that $y \in M_n^p$; the assumption $\#M_1 = p$ implies the inclusion $M_1 \subseteq M_n^p$ (in fact $y \in M_{n-1}^p$). The exact sequence (33) applied with $k = 1$ leads to the isomorphism $M_n/M_n^p \simeq M_{n-1}/M_{n-1}^p$.

(b) Case $n < p$. So $M_{n-1} \simeq (\mathbb{Z}/p\,\mathbb{Z})^{n-1}$ (Theorem 4.1 applied to $M_{n-1} = M_n^{1-\sigma}$); but the relation $\nu = (1-\sigma)^{p-1} - p \cdot A(\sigma)$ leads to $M_n^{\nu} = M_n^{(1-\sigma)^{p-1} - p \cdot A(\sigma)} = M_n^p$ because $M_n^{(1-\sigma)^{p-1}} = 1$; since $M_n^{\nu} = M_1$, we get $M_n^p = M_1$ and necessarily

$$M_n \simeq \big(\mathbb{Z}/p^2\mathbb{Z}\big) \bigoplus \big(\mathbb{Z}/p\mathbb{Z}\big)^{n-2}.$$

These computations lead to the cases (i) and to a part of (ii) of the theorem since, in the case $n = p$, the exact sequence (33) for $k = 1$ is $1 \to M_1/M_1 \cap M_n^p \to M_n/M_n^p \to M_{n-1}/M_{n-1}^p \to 1$, and the structure depends on the order (1 or p) of the kernel contrary to the previous case. □

We have to prove the point (iii) of the theorem using (a) of the lemma. We then suppose $n > p$. We note that, with obvious notation, $(M_i)_j = M_j$ for $j \leq i$; so we can apply Theorem 4.1 to M_{n-1}. Lemma 4.4 shows that the p^k-rank of M_n is larger than (or equal to) that of M_{n-1}; as the p^k-rank of a group is a decreasing function of k, Lemma 4.5 and the above remark show that for $k \leq \left[\frac{n-1}{p-1}\right]$, the p^k-ranks of M_n and M_{n-1} are equal to $p-1$.

Put $n - 1 = a'\,(p-1) + b'$, $0 \leq b' \leq p-2$ (in fact $a' = \left[\frac{n-1}{p-1}\right]$).

The exact sequence of Lemma 4.4 shows a priori three possibilities:

(α) Case $b' = 0$. Necessarily, $R_{a'+1}(M_n) = 1$ and $R_{a'+1}(M_{n-1}) = 0$.

(β) Case $b' > 0$ and $R_{a'+1}(M_n) = R_{a'+1}(M_{n-1}) + 1$.

(γ) Case $b' > 0$ and $R_{a'+1}(M_n) = R_{a'+1}(M_{n-1})$ and $R_{a'+2}(M_n) = 1$.

So it remains to prove that the case (γ) is not possible. Let $x \in M_n$, $x \notin M_{n-1}$; we have $x^{\nu} \in M_1$ & $x^{\nu} = x^{(1-\sigma)^{p-1}} \cdot x^{-p \cdot A(\sigma)}$; put $x' := x^{(1-\sigma)^{p-1}}$ and $x'' = x^{-p \cdot A(\sigma)}$; we have $x' \in M_{n-(p-1)} = M_{(a'-1)(p-1)+b'+1} \subset M_{a'(p-1)}$; but $M_{a'(p-1)} = (M_{n-1})_{a'(p-1)} = (M_{n-1})^{(a')}$. As $x \notin M_{n-1}$, we have $x^{p^{a'+1}} \neq 1$, hence $x''^{p^{a'}} \neq 1$. Thus we have obtained $x' \in (M_{n-1})^{(a')}$ and $x'' \notin (M_{n-1})^{(a')}$; since $x^{\nu} \in M_1$ and $a' \neq 0$ (we have $n \geq p+1$), one has $x^{\nu} \in (M_{n-1})^{(a')}$, in other words $x'' = x^{\nu} \cdot x'^{-1} \in (M_{n-1})^{(a')}$ (absurd). □

This finishes a particular case of structure when $M^{\nu_{K/k}}$ is not specified. Of course, we have $M^{\nu_{K/k}} \subseteq M_1$ and when $\#M_1 = p$, we have $\#M^{\nu_{K/k}} = 1$ or p. It would be interesting to have more general structure theorems.

4.4. **Numerical computations for p-class groups.** Now we apply these results to the p-class group $M = \mathcal{C}\ell_K^+$ in K/k cyclic of degree p. Many cases are possible:

If the transfer map $j_{K/k}$ is injective then $(\mathcal{C}\ell_K^+)^{\nu_{K/k}} \simeq \mathrm{N}_{K/k}(\mathcal{C}\ell_K^+)$.

The map $\mathrm{N}_{K/k}$ is surjective except if K/k is unramified (i.e., $K \subset H_k^+$, the p-Hilbert class field of k); if K/k is ramified we get $\mathrm{N}_{K/k}(\mathcal{C}\ell_K^+) = \mathcal{C}\ell_k^+$.

The transfer map may be non-injective while $\mathrm{N}_{K/k}$ is surjective, which causes more intricate theoretical calculations. But as we know, if $\mathrm{N}_{K/k}$ is not surjective (unramified case), then $j_{K/k}$ is never injective (Hilbert's Theorem 94, [GW1], [GW2], [GW3], [Su], [Ter]).

To simplify, we suppose K/k cyclic of degree p and not unramified (otherwise, we get $\#M_1 = \dfrac{\#\mathcal{C}\ell_k^+}{p}$ and more generally $\#(M_{i+1}/M_i) = \dfrac{\#\mathcal{C}\ell_k^+}{p \cdot \#\mathrm{N}(M_i)}$, which can be carried out in the same way).

We suppose that K/k is ramified at some prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ of k ($t\geq 1$). We make no assumptions about $\#M_1$ and $M^{\nu_{K/k}}$. With the previous notations and definitions, we then have the simplified formulas (25) for which the submodule $\mathcal{H}$ is an element $M_i =: \mathscr{A}_K(\mathcal{I}_i)$ of the filtration of M:

$$\#\big(\mathcal{C}\ell_K^+/M_i\big)^G = \#(M_{i+1}/M_i) = \frac{\#\mathcal{C}\ell_k^+\cdot\prod_{\mathfrak{p}\in Pl_{k,0}} e_{\mathfrak{p}}}{[K:k]\cdot\#\mathrm{N}(M_i)\cdot(\Lambda_i:\Lambda_i\cap\mathrm{N}(K^\times))},$$

where $\Lambda_i=\{x_i\in k^{\times +},\ (x_i)\in\mathrm{N}(\mathcal{I}_i)\}$. If $p>2$ one can use the ordinary sense and remove the mention $^+$ in all the forthcoming expressions.

(i) Computation of $M_1=M^G$ from $M_0=1$, which means that $\mathcal{I}_0=1$, hence $\mathrm{N}(M_0)=1$ and $\Lambda_0=\{x_0\in k^{\times +},\ (x_0)\in\mathrm{N}(1)\}=E_k^+$, giving the following expression where we have put $(E_k^+:E_k^+\cap\mathrm{N}(K^\times))=:p^{\delta_0}$:

$$\begin{aligned}\#(M_1/M_0)=\#\mathcal{C}\ell_K^{+\,G}&=\frac{\#\mathcal{C}\ell_k^+\cdot p^{t-1}}{(\Lambda_0:\Lambda_0\cap\mathrm{N}(K^\times))}\\ &=:\#\mathcal{C}\ell_k^+\cdot p^{t-1-\delta_0}.\end{aligned}\tag{34}$$

First we remark that we have the isomorphism:

$$\mathcal{C}\ell_K^{+\,G}/\mathscr{A}_K(I_K^G)\simeq E_k^+\cap\mathrm{N}(K^\times)/\mathrm{N}(E_K^+),$$

which shows how to obtain $M_1=\mathcal{C}\ell_K^{+\,G}$ from $\mathscr{A}_K(I_K^G)$ (called the group of strongly ambiguous classes) and *global normic computations* with units of k. But the group $\mathrm{N}(E_K^+)$ is not effective and we must proceed otherwise. In other words, the group of strongly ambiguous classes $\mathscr{A}_K(I_K^G)$ is not a "local" invariant, contrary to $\mathcal{C}\ell_K^{+\,G}$.

So in the first step (which is a bit particular since $\mathcal{I}_0=1$ and $\Lambda_0=E_k^+$), we shall look at the $x_0\in\Lambda_0$ which are norms of some $y_1\in K^{\times +}$.

So $(x_0)=\mathrm{N}(y_1)=(1)$, $y_1\in K^{\times +}$, which yields $(y_1)\cdot\mathfrak{A}_1^{1-\sigma}=1$, where $\mathfrak{A}_1$ is defined up to an invariant ideal, so that $\mathcal{I}_1$ contains at least such non-invariants ideals $\mathfrak{A}_1^1,\dots,\mathfrak{A}_1^{r_1}$, and invariant ideals (in which are ideals $\mathfrak{a}^1,\dots,\mathfrak{a}^s$, generating $\mathcal{C}\ell_k^+$, extended to K, and ramified prime ideals $\mathfrak{P}^1,\dots,\mathfrak{P}^t$).

Reciprocally, if $\mathscr{A}_K(\mathfrak{A}_1')\in M_1$, there exists $y_1\in K^{\times +}$ such that $(y_1)\cdot\mathfrak{A}_1'^{\,1-\sigma}=(1)$, giving $\mathrm{N}(y_1)=x_0\in\Lambda_0$.

Thus, it is not difficult to see that the classes of these ideals generate M_1, whence

$$\mathcal{I}_1=\{\mathfrak{A}_1^1,\dots,\mathfrak{A}_1^{r_1}\ ;\ (\mathfrak{a}^1),\dots,(\mathfrak{a}^s)\ ;\ \mathfrak{P}^1,\dots,\mathfrak{P}^t\}.$$

This gives $\mathrm{N}(M_1)$ by means of the computation, in $\mathcal{C}\ell_k^+$, of $\mathrm{N}(\mathcal{I}_1)$ (M_1 does not need to be computed as a subgroup of $\mathcal{C}\ell_K^+$), then, with $\Lambda_1=\{x_1\in k^{\times +},\ (x_1)\in\mathrm{N}(\mathcal{I}_1)\}$:

$$\begin{aligned}\#(M_2/M_1)&=\frac{\#\mathcal{C}\ell_k^+\cdot p^{t-1}}{\#\mathrm{N}(M_1)\cdot(\Lambda_1:\Lambda_1\cap\mathrm{N}(K^\times))}\\ &=:\frac{\#\mathcal{C}\ell_k^+}{\#\mathrm{N}(M_1)}\cdot p^{t-1-\delta_1}.\end{aligned}\tag{35}$$

Remark 4.6. The p-class group $\mathcal{C}\ell_K^+$ is equal to the group of ambiguous classes if and only if $\mathscr{A}_k(\mathrm{N}\mathcal{I}_1)=\mathcal{C}\ell_k^+$ & $\delta_1=t-1$. If $\mathcal{C}\ell_k^+=1$, the group Λ_1 is easily obtained from $\mathrm{N}\mathcal{I}_1\subset P_k^+$, whence the computation of δ_1; since $\mathcal{I}_1$ only depends on $E_k^+\cap\mathrm{N}K^\times$ and the ramification in K/k, we can hope to characterize the fields K fulfilling these conditions.

(ii) For the computation of $\mathcal{I}_2$, we process from the elements of Λ_1 which are norms of some $y_2\in K^{\times +}$ and the analogous fact that if $x_1\in\Lambda_1$ is norm, then $(x_1)=\mathrm{N}(y_2)=\mathrm{N}(\mathfrak{B}_1)$, $\mathfrak{B}_1\in\mathcal{I}_1$, $y_2\in K^{\times +}$, hence there exists $\mathfrak{A}_2\in I_K$ such that $\mathfrak{B}_1=(y_2)\cdot\mathfrak{A}_2^{1-\sigma}$.

Reciprocally, let $h_2=\mathscr{A}_K(\mathfrak{A}_2')\in M_2$ for some $\mathfrak{A}_2'\in I_K$; since $h_2^{1-\sigma}\in M_1$, there exists $y_2\in K^{\times +}$ such that $(y_2)\cdot\mathfrak{A}_2'^{\,1-\sigma}=\mathfrak{A}_1'\in\mathcal{I}_1$, hence $\mathrm{N}(\mathfrak{A}_1')=\mathrm{N}(y_2)=:(x_1)$,

$x_1 \in \Lambda_1$ (since for all i, $E_k^+ \subseteq \Lambda_i$ and invariant ideals are in $\mathcal{I}_i$, the choices of x_2 and $\mathfrak{A}_2'$ do not matter).

Then these ideals of the form $\mathfrak{A}_2^1, \ldots, \mathfrak{A}_2^{r_2}$ must be added to $\mathcal{I}_1$ to create $\mathcal{I}_2$:

$$\mathcal{I}_2 = \{\mathfrak{A}_1^1, \ldots, \mathfrak{A}_1^{r_1}\ ;\ \mathfrak{A}_2^1, \ldots, \mathfrak{A}_2^{r_2}\ ;\ (\mathfrak{a}^1), \ldots, (\mathfrak{a}^s)\ ;\ \mathfrak{P}^1, \ldots, \mathfrak{P}^t\},$$

whence $\mathrm{N}(M_2)$ and

$$\Lambda_2 = \{x_2 \in k^{\times +},\ (x_2) \in \mathrm{N}(\mathcal{I}_2)\},$$

and so on. Hence, the algorithm is very systematic and the use of normic symbols to find the subgroups $\Lambda_i \cap \mathrm{N}(K^\times)$ is effective: indeed, for the most general case of computation of Hasse symbols, see the Remark 4.7 below; otherwise use Hilbert symbols $(x_i, \alpha)_\mathfrak{p}$ by adjunction to k of a primitive pth roots of unity ζ_p to obtain the Kummer extension

$$K' := K(\zeta_p) =: k'(\sqrt[p]{\alpha}), \quad \alpha \in k'^\times,$$

over $k' := k(\zeta_p)$, and use the obvious Galois structure in $K'/k'/k$ for the radical α and the decomposition of ramified prime ideals, i.e., the duality of characters given by the reflection principle [Gr2, §§ II.1.6.8, II.5.4.2, II.5.4.3, II.7.1.5, II.7.5]; this leads to generalizations of Rédei's matrices over $\mathbb{F}_p$; the rank of the matrices, denoted δ_i, may be introduced in the general formula to give:

$$\#(M_{i+1}/M_i) = \frac{\#\mathcal{C}\ell_k^+}{\#\mathrm{N}(M_i)} \cdot p^{t-1-\delta_i}, \tag{36}$$

with increasing δ_i up to the value $i = n$ giving $\delta_i = t-1$ and $\#\mathrm{N}(M_i) = \#\mathcal{C}\ell_k^+$.

This was done in [Gr3′, (1973)] essentially for $p = 2, 3$, and in [KMS, Theorem 5.16 (2015)], for $p = 5$, when the base field contains ζ_p and for particular α (essentially $k = \mathbb{Q}(\zeta_5)$ and $K = k(\sqrt[5]{q})$ where $q \in \mathbb{N}$ is for instance a prime satisfying some conditions, so that the 5-rank can be bounded explicitly by a precise computation of the filtration); this approach by [KMS] applies to the arithmetic of elliptic curves in the $\mathbb{Z}_5$-extension of k.

Remark 4.7. For convenience, recall (from [Gr2, II.4.4.3]) the hand computation of normic Hasse symbols $\left(\frac{x\,,K/k}{\mathfrak{p}}\right)$, by global means, in *any Abelian extension* K/k.

Let $\mathfrak{m}$ be a multiple of the conductor $\mathfrak{f}$ of K/k (it does not matter if the support T of $\mathfrak{m}$ strictly contains the set of (finite) places ramified in K/k, which will be the case if the conductor is not precisely known). Set $\mathfrak{m} =: \prod_{\mathfrak{p}\in T} \mathfrak{p}^{m_\mathfrak{p}}$ with $m_\mathfrak{p} > 0$.

Let $x \in k^\times$ and let $\mathfrak{p}$ be a place of k (x is not assumed to be prime to $\mathfrak{p}$); let us consider several cases, where $\left(\frac{K/k}{\mathfrak{p}}\right)$ denotes the Frobenius automorphism of $\mathfrak{p}$ in K/k (for an unramified $\mathfrak{p}$; for an infinite complexified place, the Frobenius is a complex conjugation), and let $v_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation:

(α) $\mathfrak{p} \in Pl_\infty$ (real infinite place). We have $\left(\frac{x\,,K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right)^{v_\mathfrak{p}(x)}$, where $v_\mathfrak{p}(x) = 0$ (resp. 1) if $\sigma_\mathfrak{p}(x) > 0$ (resp. $\sigma_\mathfrak{p}(x) < 0$).

(β) $\mathfrak{p} \in Pl_0 \setminus T$. Similarly, since $\mathfrak{p}$ is unramified, we have $\left(\frac{x\,,K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right)^{v_\mathfrak{p}(x)}$.

(γ) $\mathfrak{p} \in T$. Let $x' \in k^\times$ (called a $\mathfrak{p}$-associate of x) be such that (using the multiplicative Chinese remainder theorem):

(i) $x'x^{-1} \equiv 1 \pmod{\mathfrak{p}^{m_\mathfrak{p}}}$,

(ii) $x' \equiv 1 \pmod{\mathfrak{p}'^{m_{\mathfrak{p}'}}}$), for each place $\mathfrak{p}' \in T,\ \mathfrak{p}' \neq \mathfrak{p}$,

(iii) $\sigma_{\mathfrak{p}'}(x') > 0$ for each infinite place $\mathfrak{p}' \in Pl_\infty$, complexified in K/k.

Then, by the product formula, we have $\left(\frac{x'\,,K/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}'\in Pl, \mathfrak{p}'\neq\mathfrak{p}} \left(\frac{x'\,,K/k}{\mathfrak{p}'}\right)^{-1}$, and since $\left(\frac{x\,,K/k}{\mathfrak{p}}\right) = \left(\frac{x'\,,K/k}{\mathfrak{p}}\right)$ by (i) and the definition of the local $\mathfrak{p}$-conductor of K/k, we have $\left(\frac{x\,,K/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}'\in Pl, \mathfrak{p}'\neq\mathfrak{p}} \left(\frac{x'\,,K/k}{\mathfrak{p}'}\right)^{-1}$; let us compute the symbols occurring in the right hand side:

- if $\mathfrak{p}' \in T \setminus \{\mathfrak{p}\}$, $x' \equiv 1 \pmod{\mathfrak{p}'^{m_{\mathfrak{p}'}}}$ (by (ii)) and we have $\left(\frac{x',K/k}{\mathfrak{p}'}\right) = 1$,
- if $\mathfrak{p}' \in Pl_\infty$, $\left(\frac{x',K/k}{\mathfrak{p}'}\right) = 1$ since either $\left(\frac{K/k}{\mathfrak{p}'}\right) = 1$ if $\mathfrak{p}'$ is complex or non-complexified real, or $v_{\mathfrak{p}'}(x') = 0$ for $\mathfrak{p}'$ complexified real (by (iii)),
- if $\mathfrak{p}' \in Pl_0 \setminus T$, $\mathfrak{p}'$ is unramified and we know that $\left(\frac{x',K/k}{\mathfrak{p}'}\right) = \left(\frac{K/k}{\mathfrak{p}'}\right)^{v_{\mathfrak{p}'}(x')}$;

finally, we have obtained $\left(\frac{x,K/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}' \in Pl_0 \setminus T} \left(\frac{K/k}{\mathfrak{p}'}\right)^{-v_{\mathfrak{p}'}(x')}$. It follows that since $v_{\mathfrak{p}}(x') = v_{\mathfrak{p}}(x)$ by (i), we can write:

$$(x') =: \mathfrak{p}^{v_{\mathfrak{p}}(x')}\mathfrak{a} = \mathfrak{p}^{v_{\mathfrak{p}}(x)}\mathfrak{a}, \quad (\mathfrak{a} \text{ is prime to } T \text{ by (ii)}),$$

and we have obtained (for $\mathfrak{p} \in T$), $\left(\frac{x\,,\,K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{a}}\right)^{-1}$, where the Artin symbol $\left(\frac{K/k}{\mathfrak{a}}\right)$ is by definition built multiplicatively from the Frobenius automorphisms of the prime divisors of $\mathfrak{a}$. Recall that if $\mathfrak{p} \notin T$, we have $\left(\frac{x\,,\,K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(x)}$.

When we find that x is a global norm in K/k, *bnfisnorm(bnfinit* $(P), x)$ of PARI [P] (for $k = \mathbb{Q}$ and K given via the polynomial P), gives a solution y; if $x = \mathrm{N}(y)$ and $(x) = \mathrm{N}(\mathfrak{A})$ for an ideal $\mathfrak{A}$ of K, then it is immediate to get numerically $\mathfrak{B}$ such that $(y) \cdot \mathfrak{B}^{1-\sigma} = \mathfrak{A}$. This was used for the Example 3.12.

One can find numerical computations, densities results, notions of "governing fields" and heuristic principles in many papers like [Gr3′], [Mo1], [Mo2], [St2], [Wi], [Y2], [Ge4], etc. We think that the local framwork given by the algorithm may confirm these heuristic results since normic symbols are independant (up to the product formula) and take uniformly all values with standard probabilities.

4.5. **p-triviality criterion for p-class groups in a p-extension.** When K/k is cyclic of p-power degree, the triviality of $\mathcal{C}\ell_K^+$, equivalent to $\mathcal{C}\ell_K^{+\,G} = 1$, is easily characterized from the Chevalley's formula (28) and gives:

$$\frac{\#\mathcal{C}\ell_k^+ \cdot \prod_{\mathfrak{p} \in Pl_{k,0}} e_{\mathfrak{p}}}{[K:k]\,(E_k^+ : E_k^+ \cap \mathrm{N}(K^\times))} = \#\mathrm{N}(\mathcal{C}\ell_K^+) \cdot \frac{\prod_{\mathfrak{p} \in Pl_{k,0}} e_{\mathfrak{p}}}{[K:K \cap H_k^+]\,(E_k^+ : E_k^+ \cap \mathrm{N}(K^\times))} = 1,$$

which leads to the two conditions $H_k^+ \subseteq K$ & $(E_k^+ : E_k^+ \cap \mathrm{N}(K^\times)) = \#\Omega_{K/k}$, which is coherent with the fact that the genera field $H_{K/k}^+$ is K (see (29) and (30), § 3.2). Any generalization (S-class groups with modulus, quotients by a sub-module $\mathcal{H}$) is left to the reader.

The following result gives, when the p-group G is not cyclic, a charcterisation of the condition $\mathcal{C}\ell_K^S = 1$ despite the fact that the usual Chevalley's formula does not exist in the non-cyclic case; so this involves more deep invariants as the knot group κ and the p-central class field $C_{K/k}^S$ (i.e., the largest subextension of H_K^S/K, Galois over k, such that $\mathrm{Gal}(C_{K/k}^S/K)$ is contained in the center of $\mathrm{Gal}(C_{K/k}^S/k)$).

Theorem 4.8. *Let K/k be a p-extension with Galois group G (not necessarily Abelian), let S be a finite set of non-complex places of k and let $\mathcal{C}\ell_K^S$ be the p-Sylow subgroup of the S-class group of K. Then $\mathcal{C}\ell_K^S = 1$ if and only if the following three conditions are satisfied, where J_K is the idèle group of K:*
(i) $H_k^S \subseteq K$,
(ii) $(E_k^S : E_k^S \cap \mathrm{N}_{K/k}(J_K)) = \dfrac{\prod_{\mathfrak{p} \notin S}\ e_{\mathfrak{p}}^{\mathrm{ab}} \times \prod_{\mathfrak{p} \in S}\ e_{\mathfrak{p}}^{\mathrm{ab}}\, f_{\mathfrak{p}}^{\mathrm{ab}}}{[K^{\mathrm{ab}} : H_k^S]}$, where $e_{\mathfrak{p}}^{\mathrm{ab}}$ (resp. $f_{\mathfrak{p}}^{\mathrm{ab}}$) is the ramification index (resp. the residue degree) of the place $\mathfrak{p}$ of k in the maximal subextension K^{ab} of K, Abelian over k,
(iii) $\#\kappa = (E_k^S \cap \mathrm{N}_{K/k}(J_K) : E_k^S \cap \mathrm{N}_{K/k}(K^\times))$, where the knot group κ is by definition $k^\times \cap \mathrm{N}_{K/k}(J_K)/\mathrm{N}_{K/k}(K^\times)$.

The knot group, which may be nontrivial in the non-cyclic case, measures the "defect" of the Hasse principle, i.e., of local norms compared to global norms. The proof is based on the fact that $\mathcal{C}\ell_K^S = 1$ if and only if $\mathcal{C}\ell_K^S = I_G \cdot \mathcal{C}\ell_K^S$, where I_G is the augmentation ideal of G, because when G is a p-group there exists a power of I_G which is contained in $p\,\mathbb{Z}[G]$. Since by duality, $\mathrm{H}_0(G, \mathcal{C}\ell_K^S)$ and $\mathrm{H}^0(G, \mathcal{C}\ell_K^{S\,*})$ have same order, we obtain the relation $(\mathcal{C}\ell_K^S : I_G \cdot \mathcal{C}\ell_K^S) = \#(\mathcal{C}\ell_K^{S\,*})^G$, which means that $[C_{K/k}^S : K] = \#(\mathcal{C}\ell_K^{S\,*})^G$; thus we recover the condition by using the classical fixed point theorem for finite p-groups. From the formula giving $[C_{K/k}^S : K]$ (cf. [Gr2, Theorem IV.4.7]), we deduce the three conditions of the theorem.

For a detailed proof, see [Gr2, § IV.4.7.4] giving a historic of the genera and central classes theories from works of Scholz, Fröhlich, Furuta, Gold, Garbanati, Jehne, Miyake, Razar, Shirai, and many others; see [L4] for an history of genus theory and related results.

Remark 4.9. Condition (iii) is empty when G is cyclic (Hasse principle), or when $\kappa = 1$. The condition $\kappa = 1$ can be checked in the Abelian case via Razar's criterion, see [Ra]; on the contrary it becomes nontrivial in the other cases so that, in practice, there does not exist any easy numerical criterion for the triviality of the p-class group in a non-cyclic p-extension.

In the particular case $k = \mathbb{Q}$, $S = \emptyset$, condition (i) is empty, condition (ii), equivalent to $\prod_{\mathfrak{p} \in Pl_0} e_{\mathfrak{p}}^{\mathrm{ab}} = [K^{\mathrm{ab}} : \mathbb{Q}]$, is easy to check, and condition (iii) is equivalent to $\kappa = 1$; this implies that for $k = \mathbb{Q}$ with the narrow sense, the above problem is essentially reduced to that of the Hasse principle.

5. Relative p-class group of an Abelian field of prime to p degree

We fix a prime number p. To simplfy, we suppose $p > 2$.

We shall apply the above results of Sections 3 and 4 to study the Galois structure of the relative p-class group of an imaginary Abelian extension $k/\mathbb{Q}$, *of prime to p degree*, using both the genera theory with characters in a suitable extension K/k, cyclic of degree p, and the "principal theorem" of Thaine–Ribet–Mazur–Wiles–Kolyvagin in k [MW].

This section, based on [Gr11, (1993)], emphasizes an interesting phenomena which is, roughly speaking, that when one grows up in suitable p-extensions K/k, the p-class group of K becomes "more regular" and gives informations on the p-class group of the base field k; the most spectacular case being Iwasawa theory in $\mathbb{Z}_p$-extensions [Iw] giving for instance (under the nullity of the μ-invariant) Kida's formula for the λ^--invariants in finite p-extensions K/k of CM-fields, which is nothing else than a "genera theory" comparison of p-ranks of relative class groups "at infinity", i.e., in K_∞/k_∞ where k_∞ and K_∞ are the cyclotomic $\mathbb{Z}_p$-extensions of k and K, respectively (see various approaches in [Iw], [Ki], [Sin]). For instance, when K/k is cyclic of degree p one gets for the whole λ-invariants, assuming $K \cap k_\infty = k$ ([Iw, Theorem 6 (1981)]):

$$\lambda(K) - 1 = p \cdot (\lambda(k) - 1) + (p-1) \cdot (\chi(G, E_{K_\infty}) + 1) + \sum_w \big(e_w(K_\infty/k_\infty) - 1\big),$$

where w ranges over all non-p-places of K_∞, where $p^{\chi(G, E_{K_\infty})}$ is the Herbrand quotient $\frac{\mathrm{H}^2(G, E_{K_\infty})}{\mathrm{H}^1(G, E_{K_\infty})}$ of the group E_{K_∞} of units of K_∞ (similar situation as for Chevalley's formula which needs the knowledge of the Herbrand quotient of E_K) and where $e_w(K_\infty/k_\infty)$ is the ramification index of w in K_∞/k_∞.

This aspect, in p-extensions different from $\mathbb{Z}_p$-extensions, is probably not sufficiently thorough.

5.1. **Abelian extensions of $\mathbb{Q}$ and characters.** Now we fix a prime number $p > 2$. Let $\mathbb{Q}^{\rm ab}$, seen in $\mathbb{C}_p$ (the completion of an algebraic closure of $\mathbb{Q}_p$), be the maximal Abelian extension of $\mathbb{Q}$ (as we know, it is the compositum of all cyclotomic extensions of $\mathbb{Q}$), and let $G^{\rm ab} := {\rm Gal}(\mathbb{Q}^{\rm ab}/\mathbb{Q})$.

Let Ψ be the group of $\mathbb{C}_p$-irreducible characters $\psi : G^{\rm ab} \longrightarrow \mathbb{C}_p^\times$ of finite order, and let $\mathcal{X}$ be the set of $\mathbb{Q}_p$-irreducible characters χ (such a character χ is the sum of the $\mathbb{Q}_p$-conjugates ψ_i of a character $\psi \in \Psi$; then we say that these conjugates ψ_i divide χ, denoted $\psi_i \mid \chi$).

We denote by k_χ (cyclic over $\mathbb{Q}$) the subfield of $\mathbb{Q}^{\rm ab}$ fixed by the kernel ${\rm Ker}(\chi)$ of ψ and by R_χ the ring of values of ψ over $\mathbb{Z}_p$ (k_χ, ${\rm Ker}(\chi)$, R_χ do not depend on the choice of the conjugate of ψ, whence the notation); furthermore, these objects only depend on the $\mathbb{Q}$-*irreducible character* ρ above ψ or χ (ρ is the sum of all $\mathbb{Q}$-conjugates of ψ then a sum of some χ). The degree of $k_\chi/\mathbb{Q}$ is equal to the order of $\psi \mid \chi$.

The ring R_χ is a cyclotomic local ring whose maximal ideal is denoted $\mathfrak{M}_\chi$; more precisely, if $\psi \mid \chi$ is of order $d\,p^n$, $p \nmid d$, $n \geq 0$, then $R_\chi = \mathbb{Z}_p[\xi_{d\,p^n}] = \mathbb{Z}_p[\xi_d][\xi_{p^n}]$, where ξ_d and ξ_{p^n} are primitive dth and p^nth roots of unity, respectively; the prime p is unramified in $\mathbb{Q}_p(\xi_d)/\mathbb{Q}_p$ and totally ramified in $\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p$ of degree $(p-1)\,p^{n-1}$, so that we get

$$\mathfrak{M}_\chi^{(p-1)p^{n-1}} = p \cdot R_\chi.$$

Let

$$\mathcal{X}_0 := \{\chi \in \mathcal{X},\ \ \psi \mid \chi \text{ is of order prime to } p\}$$

and

$$\mathcal{X}_p := \{\chi \in \mathcal{X},\ \ \psi \mid \chi \text{ is of } p\text{-power order}\}.$$

We verify that $\mathcal{X} = \mathcal{X}_0 \cdot \mathcal{X}_p$ since for any $\chi \in \mathcal{X}$ and $\psi \mid \chi$, we have the unique factorization $\psi = \psi_0 \cdot \psi_p$ where ψ_0 is of order prime to p and ψ_p is of p-power order, then $\chi = \chi_0 \cdot \chi_p$, where $\psi_0 \mid \chi_0$ and $\psi_p \mid \chi_p$, since $\mathbb{Q}_p(\xi_d)/\mathbb{Q}_p$ and $\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p$ are linearly disjoint over $\mathbb{Q}_p$. Note that χ_p is also the $\mathbb{Q}$-irreducible character deduced from ψ_p since $\mathbb{Q}$-conjugates and $\mathbb{Q}_p$-conjugates of ψ_p coincide. The local degree $f_{\chi_0} := [\mathbb{Q}_p(\xi_d) : \mathbb{Q}_p]$ is the residue degree of p in $\mathbb{Q}(\xi_d)/\mathbb{Q}$.

We say that χ is even (resp. odd) if $\psi(s_{-1}) = 1$ (resp. $\psi(s_{-1}) = -1$), where s_{-1} is the complex conjugation. We denote by $\mathcal{X}^\pm$, $\mathcal{X}_0^\pm$ and $\mathcal{X}_p^\pm$ the corresponding sets of even or odd characters (note that since $p \neq 2$, $\mathcal{X}_p = \mathcal{X}_p^+$).

For any subfield K of $\mathbb{Q}^{\rm ab}$ we denote by $\mathcal{X}_K$ (then $\mathcal{X}_{K,0}$, $\mathcal{X}_{K,p}$) the set of characters of K (i.e., such that ${\rm Gal}(\mathbb{Q}^{\rm ab}/K) \subseteq {\rm Ker}(\chi)$ or $k_\chi \subseteq K$).

5.2. **The universal χ-class groups ($\chi \in \mathcal{X}$, $p > 2$).** Let $\mathcal{C}\ell_F$ denotes the p-class group of any field $F \subset \mathbb{Q}^{\rm ab}$ (since $p > 2$, we have implicitely the ordinary sense). Let $\chi \in \mathcal{X}$.

(i) If $\chi = \chi_0 \in \mathcal{X}_0$, let $e_{\chi_0} = \frac{1}{[k_{\chi_0}:\mathbb{Q}]} \sum\limits_{s \in {\rm Gal}(k_{\chi_0}/\mathbb{Q})} \chi_0(s^{-1})\, s$ be the idempotent of $\mathbb{Z}_p[{\rm Gal}(k_{\chi_0}/\mathbb{Q})]$ associated with $\chi = \chi_0$; so we have $\mathbb{Z}_p[{\rm Gal}(k_{\chi_0}/\mathbb{Q})] \cdot e_{\chi_0} \simeq R_{\chi_0}$.

Then we define the χ_0-class group as the corresponding semi-simple component of $\mathcal{C}\ell_{k_{\chi_0}}$ defined by

$$\mathcal{C}\ell_{\chi_0} := \mathcal{C}\ell_{k_{\chi_0}}^{e_{\chi_0}}.$$

(ii) If $\chi = \chi_0 \cdot \chi_p$ with $\chi_0 \in \mathcal{X}_0$ and $\chi_p \in \mathcal{X}_p$, $\chi_p \neq 1$, let k' be the unique subfield of k_χ such that $[k_\chi : k'] = p$ (we have $k' = k_{\chi_0}$ only if χ_p is of order p); thus the arithmetical norm ${\rm N}_{k_\chi/k'}$ induces the following exact sequence of R_{χ_0}-modules defining $\mathcal{C}\ell_\chi$:

$$1 \longrightarrow \mathcal{C}\ell_\chi \longrightarrow \mathcal{C}\ell_{k_\chi}^{e_{\chi_0}} \xrightarrow{{\rm N}_{k_\chi/k'}} \mathcal{C}\ell_{k'}^{e_{\chi_0}} \longrightarrow 1,$$

the surjectivity being obvious because k_χ is the direct compositum over $\mathbb{Q}$ of k_{χ_0} and k_{χ_p} which is a cyclic p-extension of $\mathbb{Q}$, thus totally ramified at least for a prime

number, whence k_χ/k' ramified. Since $\mathcal{C}\ell_\chi$ is anihilated by e_{χ_0} and by $\mathrm{N}_{k_\chi/k'}$ which corresponds to $1+\sigma+\cdots+\sigma^{p-1}$ in the group algebra of $\mathrm{Gal}(k_\chi/k') =: \langle\sigma\rangle$, $\mathcal{C}\ell_\chi$ is canonically a R_χ-module (and not only a R_{χ_0}-module).

This defines, by an obvious induction in k_χ/k_{χ_0}, the universal family of components $\mathcal{C}\ell_\chi$ for all $\chi \in \mathcal{X}$ for which we have the following formulas for any cyclic extension $K/\mathbb{Q}$ of degree $d\cdot p^n$, $p\nmid d$, $n\geq 0$:

$$\begin{aligned} \#\mathcal{C}\ell_K &= \prod_{\chi_0\in\mathcal{X}_{K,0}} \#\mathcal{C}\ell_K^{e_{\chi_0}},\\ \#\mathcal{C}\ell_K^{e_{\chi_0}} &= \prod_{i=0}^{n} \#\mathcal{C}\ell_{\chi_i},\quad \forall \chi_0\in\mathcal{X}_{K,0}, \end{aligned} \tag{37}$$

where, for each $\chi_0\in\mathcal{X}_{K,0}$, $\chi_i = \chi_0\cdot\chi_{p,i}$, where $\chi_{p,i}$ is above $\psi_p^{p^{n-i}}$ for $\psi_p \mid \chi_p$.

We denote by ω, of order $p-1$, the Teichmüller character for $p>2$; we have $k_\omega = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive pth root of unity and by definition $\omega(\zeta_p\to\zeta_p^a)\equiv a \pmod p$ for $a=1,\ldots,p-1$.

With these definitions, we can give the statement of the "principal theorem" of Thaine–Ribet–Mazur–Wiles–Kolyvagin [MW] in the particular context of imaginary fields K for the relative class groups $\mathcal{C}\ell_K^-$, hence with odd characters.

Theorem 5.1. *Let $p\neq 2$ and let $\chi=\chi_0\cdot\chi_p\in\mathcal{X}^-$. We assume that $\chi_0\neq\omega$ when k_χ is the cyclotomic field $\mathbb{Q}(\zeta_{p^n})$ (otherwise $\mathcal{C}\ell_\chi=1$). For $\psi\mid\chi$, let b_χ be the ideal $B_1(\psi^{-1})\cdot R_\chi$ where $B_1(\psi^{-1})$ is the generalized Bernoulli number of the character ψ. Then we have $\#\mathcal{C}\ell_\chi = \#(R_\chi/b_\chi)$.*

But as it is well known, this result does not give the structure of $\mathcal{C}\ell_\chi$ as R_χ-module; indeed, if $b_\chi=\mathfrak{M}_\chi^t$, we may have the general structure:

$$\mathcal{C}\ell_\chi \simeq \bigoplus_{i=1}^{e} R_\chi/\mathfrak{M}_\chi^{t_i},\quad 1\leq t_1\leq\cdots\leq t_e,\quad e\geq 0,\quad \sum_{i=1}^{e} t_i = t.$$

For instance, $\mathcal{C}\ell_\chi$ is R_χ-monogenic if and only if $e=1$.

5.3. **Definition of admissible sets of prime numbers.** Still for $p\neq 2$ and $\chi_0\in\mathcal{X}_0^-$, $\chi_0\neq\omega$, consider the cyclic field $k:=k_{\chi_0}$ for which $\mathcal{C}\ell_{\chi_0}=\mathcal{C}\ell_k^{e_{\chi_0}}$, where $e_{\chi_0} = \frac{1}{[k_{\chi_0}:\mathbb{Q}]}\sum\limits_{s\in\mathrm{Gal}(k_{\chi_0}/\mathbb{Q})}\chi_0(s^{-1})\,s$. We intend to apply the previous sections of this paper on genera theory to obtain informations on the structure of $\mathcal{C}\ell_{\chi_0}$.

Definitions 5.2. (i) For any $t\geq 1$, let $\mathcal{S}_t$ be the familly of sets $\{\ell_1,\ldots,\ell_t\}$ of t prime numbers fulfilling the following conditions (for given $\chi_0\in\mathcal{X}_0^-$ and $\psi_0\mid\chi_0$):

$\ell_i\equiv 1 \pmod p$, for $i=1,\ldots,t$ (i.e., $p\mid[\mathbb{Q}(\zeta_{\ell_i}):\mathbb{Q}]$);

$\psi_0(\ell_i)=1$, for $i=1,\ldots,t$ (i.e., ℓ_i totally splits in $k=k_{\chi_0}$).

(ii) For $S\in\mathcal{S}_t$, let $\Phi_S\subset\mathcal{X}_p$ be the set of characters φ, of order p, with conductor $\ell_1\cdots\ell_t$ (that is to say, $k_\varphi\subseteq\mathbb{Q}(\zeta_{\ell_1\cdot\ldots\cdot\ell_t})$ is of conductor $\ell_1\cdots\ell_t$, whence if k_i is the unique subfield of $\mathbb{Q}(\zeta_{\ell_i})$ of degree p, then k_φ is a subfield of degree p of the compositum $k_1\cdots k_t$ and k_φ is not in a compositum of less than t fields k_i).

(iii) The character $\varphi\in\Phi_S$ is said to be χ_0-*admissible* if $b_{\chi_0\cdot\varphi}=\mathfrak{M}_{\chi_0\cdot\varphi}^t$ (see Theorem 5.1 for the definition of $b_{\chi_0\cdot\varphi}$). By extension we say that $S\in\mathcal{S}_t$ is χ_0-admissible if there exists at least a χ_0-admissible character $\varphi\in\Phi_S$.

(iv) Let r_{χ_0} be the $R_{\chi_0}/p\,R_{\chi_0}$-dimension of $\mathcal{C}\ell_{\chi_0}/\mathcal{C}\ell_{\chi_0}^p$.

So the number t is known from the computation of a Bernoulli number depending on φ and it is not difficult to find χ_0-admissible characters φ. Then we have proved in [Gr11] the following effective result:

Theorem 5.3. *Let $p \neq 2$ and let $\chi_0 \in \mathcal{X}_0^-$, $\chi_0 \neq \omega$, and let $k = k_{\chi_0}$.*
Let $S = \{\ell_1, \ldots, \ell_t\} \in \mathcal{S}_t$ be a χ_0-admissible set; then for $i = 1, \ldots, t$, let $\mathfrak{l}_i$ be a prime ideal of k above ℓ_i and let $h_i := cl_k(\mathfrak{l}_i)^{e_{\chi_0}}$ be the image of $cl_k(\mathfrak{l}_i)$ in $\mathcal{C}l_k^{e_{\chi_0}}$.
Then $\mathcal{C}l_{\chi_0}$ is the R_{χ_0}-module generated by the h_i, $i = 1, \ldots, t$, and we have $r_{\chi_0} \leq t$. Taking the minimal value of t yields r_{χ_0}.

The principle of the proof is an application of the computations of invariant classes of the Section 4 in K/k where $K = k_\varphi \cdot k = k_{\chi_0 \cdot \varphi}$ and where φ is the χ_0-admissible character of order p.

$$\begin{array}{ccc} k_\varphi & \text{———} & K = k_{\chi_0 \cdot \varphi} \\ | & & | \; G \simeq \mathbb{Z}/p\mathbb{Z} \\ \mathbb{Q} & \underset{d,\ p \nmid d}{\text{———}} & k = k_{\chi_0} \end{array}$$

We consider the G-module $M = \mathcal{C}l_K^{e_{\chi_0}}$ as a component of the relative class group $\mathcal{C}l_K^-$; in other words, a semi-simple component of the p-class group of K, since from $\mathcal{C}l_K^- = \bigoplus_{\chi_0' \in \mathcal{X}_k^-} \mathcal{C}l_K^{e_{\chi_0'}}$ we have selected $\chi_0 \in \mathcal{X}_k^-$ and the associated filtration with characters of $M = \mathcal{C}l_K^{e_{\chi_0}}$ for which $M_1 = M^G = (\mathcal{C}l_K^G)^{e_{\chi_0}}$, $G := \mathrm{Gal}(K/k) \simeq \mathbb{Z}/p\mathbb{Z}$ (see [Gr12, (1978)]).

We denote by $\mathfrak{L}_i$ the ideal of K above $\mathfrak{l}_i$ (indeed, $\mathfrak{l}_i$ is totally ramified in K/k) and by $H_i := cl_K(\mathfrak{L}_i)^{e_{\chi_0}}$. Then the proof consists in proving the following lemmas (see [Gr11, Lemmes (1.2), (1.3), Corollaire (2.4)]:

Lemma 5.4. *The extension $j_{K/k} : \mathcal{C}l_k^{e_{\chi_0}} \longrightarrow \mathcal{C}l_K^{e_{\chi_0}}$ is injective.*

This comes easily from the fact that χ_0 is odd (the χ_0-components of units are trivial for $\chi_0 \neq \omega$, thus there is no capitulation of relative classes).

Lemma 5.5. *We have $M_1 = j_{K/k}(\mathcal{C}l_k^{e_{\chi_0}}) \cdot \langle H_1, \ldots, H_t \rangle_{R_{\chi_0}}$ and $M_1 / j_{K/k}(\mathcal{C}l_k^{e_{\chi_0}}) \simeq (R_{\chi_0}/p\,R_{\chi_0})^{\,t}$.*

This expression giving $\#M_1 = \#\mathcal{C}l_k^{e_{\chi_0}} \cdot p^{\,t \cdot f_{\chi_0}}$, where f_{χ_0} is the residue degree of p in $\mathbb{Q}(\xi_d)/\mathbb{Q}$, is nothing else than the χ_0-Chevalley's formula in K/k for an odd character χ_0 (cf. [Gr12]).

Lemma 5.6. *The character $\varphi \in \Phi_S$ is χ_0-admissible if and only if $M = M_1$ (in other words, if and only if there are no exceptional χ_0-classes).*

Thus, since $\mathcal{C}l_k^{e_{\chi_0}} = \mathcal{C}l_{e_{\chi_0}}$, we get $\#M := \mathcal{C}l_K^{e_{\chi_0}} = \#\mathcal{C}l_{\chi_0} \cdot \#\mathcal{C}l_{\chi_0 \cdot \varphi}$ from formula (37) with $n = 1$. From Theorem 5.1, we have $M = M_1$ if and only if $b_{\chi_0 \cdot \varphi} = \mathfrak{M}_{\chi_0 \cdot \varphi}^t$ (χ_0-admissibility). From the lemmas we get $\mathrm{N}_{K/k}(M) = \mathrm{N}_{K/k}(M_1)$, hence $\mathcal{C}l_{\chi_0} = \mathcal{C}l_{\chi_0}^p \cdot \langle h_1, \ldots, h_t \rangle_{R_{\chi_0}}$, whence $\mathcal{C}l_{\chi_0} = \langle h_1, \ldots, h_t \rangle_{R_{\chi_0}}$.

So, for practical use, we are reduced to the known algorithm which must stop at the first step. The ideals $b_{\chi_0 \cdot \varphi}$ generated by Bernoulli numbers are easily obtained from the Stickelberger element of the field K:

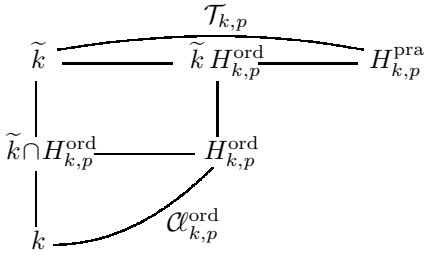
$$\mathrm{St}(K) := \sum_{a=1}^{m} \Big(\frac{K/\mathbb{Q}}{a}\Big)^{-1} \Big(\frac{a}{m} - \frac{1}{2}\Big) \in \mathrm{Gal}(K/\mathbb{Q}),$$

where m is the conductor of K and $\big(\frac{K/\mathbb{Q}}{a}\big)$ the Artin symbol (for $\gcd(a, m) = 1$).
For more details see [Gr11] where it is also proved that admissible sets have a nontrivial Chebotarev density leading to the effectivness of the detemination of the structure and where relations with some results of Schoof [Sch1] are discussed (cf. [Gr11, §§ 4, 5]).

One can then find many numerical examples in the Appendix [Gr11, (A)] by Berthier, showing some cases of non-monogenic $\mathcal{C}\ell_K^{e_{\chi_0}}$ as R_{χ_0}-modules. For instance, let $k=\mathbb{Q}\Big(\sqrt{-541\,(37+6\,\sqrt{37})}\Big)$ (quartic cyclic over $\mathbb{Q}$) and $p=5$; there exist two 5-adic characters χ_0 and χ_0' for which $\mathcal{C}\ell_k^{e_{\chi_0}} \simeq R_{\chi_0}/(2-i)R_{\chi_0} \bigoplus R_{\chi_0}/(2-i)R_{\chi_0}$ and $\mathcal{C}\ell_k^{e_{\chi_0'}}=1$ (a rare example of non-monogenic $\mathcal{C}\ell_k^{e_{\chi_0}}$). See [Ber] for numerical tables where the case of even characters χ_0 is also illustrated.

6. Conclusion and perspectives

To conclude, we can say that the p-class group is perhaps not the only object for the class field theory setting of a number field k. Indeed, we prefer the very similar finite p-group, denoted $\mathcal{T}_{k,p}$, and defined as the p-torsion subgroup of the Galois group of the maximal p-ramified (i.e., unramified outside p), non-complexified, Abelian pro-p-extension of k denoted $H_{k,p}^{\rm pra}$ in the following schema:



where $\widetilde{k}$ is the compositum of the $\mathbb{Z}_p$-extensions of k, $H_{k,p}^{\rm ord}$ the p-Hilbert class field, and $\mathcal{C}\ell_{k,p}^{\rm ord}$ is the p-class group of k (ordinary sense).

This finite group $\mathcal{T}_{k,p}$, connected with the Leopoldt conjecture at p and the residue of the p-adic zeta function, has been studied by many authors by means of algebraic and analytic viewpoints (e.g., K. Iwasawa [Iw], J. Coates [Co, Appendix], H. Koch [Ko], J-P. Serre [Se2], etc.), and we have done extensive practical studies in [Gr2] from earlier publications [Gr7], [Gr8], [Gr9], and recently in a historical overview of the Bertrandias-Payan module (a quotient of $\mathcal{T}_{k,p}$) by means of three different approaches by J-F. Jaulent, T. Nguyen Quang Do and us (see the details in [Gr6] and its bibliography).

The functorial properties of these modules $\mathcal{T}_{k,p}$ are more canonical (especially in any p-extensions K/k of Galois group G) with an explicit formula for $\#\mathcal{T}_{K,p}^G$ under the sole Leopoldt conjecture, so that a "Chevalley's formula" does exist for any p-extension K/k, see [Gr2, Theorem IV.3.3] and [MoNg]; $\mathcal{T}_{k,p}$ contains any deep information on class groups and units (using, for instance, reflection theorems to connect $\mathcal{T}_{k,p}$ and $\mathcal{C}\ell_{k,p}^{Pl_p}$ when k contains the pth roots of unity, [Gr2, Proposition III.4.2.2]); furthermore, it is a fundamental invariant concerning the structure of the Galois group of the maximal p-ramified pro-p-extension of k, saying that this pro-p-group is free if and only if $\mathcal{T}_{k,p}=1$ (fundamental notion called *p-rationality* of k; see [Gr2, Theorem III.4.2.5]).

Moreover the properties of the $\mathcal{T}_{k,p}$ in a p-extension are in relation with the notion of *p-primitive ramification* introduced in [Gr9, (1986)] and largely developed in many papers on the subject (e.g., [Ja2], [MoNg]). In a similar context, in connection with Gross's conjecture [FG], mention the *logarithmic class group* introduced by J-F. Jaulent ([Ja3], [So]) governing the *p-Hilbert kernel* and the *p-regular kernel*.

The main property concerning these groups $\mathcal{T}_{k,p}$ is that, under the Leopoldt conjecture for p in K/k (even if K/k is not Galois), the transfer map $j_{K/k}:\mathcal{T}_{k,p}\longrightarrow\mathcal{T}_{K,p}$ (corresponding as usual to extension of ideals in a broad sense) is *injective* [Gr2, Theorem IV.2.1] contrary to the case of p-class groups. Furthermore, the property of p-rationality we have mentionned above, has important consequences as is shown

by Galois representations theory (e.g., [Gre1, (2016)]) or conjectural and heuristic aspects (e.g., [Gr10, (2016)]).

So we intend to make much advertise for these $\mathcal{T}_{k,p}$ since the corresponding filtration $(M_i)_{i\geq 0}$ in a finite cyclic p-extension K/k has not been studied to our knowledge.

Acknowledgments. I thank Pr. Balasubramanian Sury for his kind interest and his valuable help for the submission of this paper. I am very grateful to the Referee for the careful reading and the suggestions for improvements of the paper.

References

[AT] Artin, E., Tate, J., *Class field theory*, Benjamin, New York, Amsterdam 1968; second edition: Advanced Book Classics, Addison-Wesley Publ. Comp., Redwood City 1990; Reprint of the 1990 second edition (2009).

[ATZ1] Azizi, A., Taous, M., Zekhnini, A., *Coclass of* $\mathrm{Gal}(k_2^2/k)$ *for some fields* $k=\mathbb{Q}(\sqrt{p_1p_2q}, \sqrt{-1})$ *with* 2*-class groups of types* $(2,2,2)$, Journal of Algebra and Its Applications 15, 2 (2016). http://scholar.google.com/citations?user=EZPtrFcAAAAJ&hl=fr

[ATZ2] Azizi, A., Taous, M., Zekhnini, A., *On the strongly ambiguous classes of some biquadratic number fields*, arXiv:1503.01992 (2015). http://arxiv.org/pdf/1503.01992.pdf

[Bau] Bauer, H., *Zur Berechnung der* 2*-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. 248 (1971), 42–46.

[Ber] Berthier, Th., *Structure et générateurs du groupe des classes des corps quartiques cycliques sur* $\mathbb{Q}$ *(tables numériques)*, Publ. Mathématiques de Besançon, Algèbre et Théorie des Nombres, Années 1992/93–1993/94, 50 pp. http://pmb.univ-fcomte.fr/1994/Berthier.pdf http://www.sudoc.abes.fr/xslt/DB=2.1//SRCH?IKT=12&TRM=043905218

[Bol] Bölling, R., *On Ranks of Class Groups of Fields in Dihedral Extensions over* $\mathbb{Q}$ *with Special Reference to Cubic Fields*, Mathematische Nachrichten 135, 1 (1988), 275–310. https://www.researchgate.net/publication/229713427

[Ch1] Chevalley, C., *Sur la théorie du corps de classes dans les corps finis et les corps locaux* (Thèse), Jour. of the Faculty of Sciences Tokyo 2 (1933), 365–476. http://archive.numdam.org/ARCHIVE/THESE/THESE_1934__155_/THESE_1934__155__365_0/THESE_1934__155__365_0.pdf

[Ch2] Chevalley, C., *La théorie du corps de classes*, Ann. of Math. II, 41 (1940), 394–418.

[Co] Coates, J., *p-adic L-functions and Iwasawa's theory*, In: *Algebraic Number Fields*, Proc. of Durham Symposium 1975, New York-London (1977), 269–353.

[FG] Federer, L.J., Gross, B.H, *Regulators and Iwasawa modules* (with an appendix by W. Sinnot, Invent. Math. 62, 3 (1981), 443–457.

[Fu] Furuta, Y., *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), 281–285. http://projecteuclid.org/download/pdf_1/euclid.nmj/1118802021

[Fr] Fröhlich, A., *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics 24, Amer. Math. Soc. 1983.

[Ge1] Gerth III, F., *On 3-class groups of certain pure cubic fields*, Bull. Austral. Math. Soc., 72, 3 (2005), 471–476. http://www.austms.org.au/Publ/Bulletin/V72P3/pdf/723-5238-GerIII.pdf

[Ge2] Gerth III, F., *On p-class groups of cyclic extensions of prime degree p of number fields*, Acta Arithmetica, LX.1 (1991), 85–92. http://matwbn.icm.edu.pl/ksiazki/aa/aa60/aa6013.pdf

[Ge3] Gerth III, F., *On p-class groups of cyclic extensions of prime degree p of quadratic fields*, Mathematika 36, 1 (1989), 89–102. http://dx.doi.org/10.1112/S0025579300013590

[Ge4] Gerth III, F., *The* 4*-class ranks of quadratic fields*, Invent. math. 77, 3 (1984), 489–515.

[GK1] Greither, C., Kučera, R., *Eigenspaces of the ideal class group*, Annales Institut Fourier 64, 5 (2014), 2165–2203. https://www.researchgate.net/publication/286369796

[GK2] Greither, C., Kučera, R., *On a conjecture concerning minus parts in the style of Gross*, Acta Arithmetica 132, 1 (2008), 1–48. http://www.muni.cz/research/publications/764249

[GK3] Greither, C., Kučera, R., *Annihilators of minus class groups of imaginary Abelian fields*, Annales Institut Fourier 5, 5 (2007), 1623–1653. https://www.researchgate.net/publication/268012963

[GK4] Greither, C., Kučera, R., *Annihilators for the Class Group of a Cyclic Field of Prime Power Degree, II*, Canad. J. Math. 58 (2006), 580-599. http://cms.math.ca/10.4153/CJM-2006-024-2

[Go] González-Avilés, C.D., *Capitulation, ambiguous classes and the cohomology of the units*, Journal für die reine und angewandte Mathematik 2007, 613 (2006), 75–97. https://www.researchgate.net/publication/2128194

[Gr1] Gras, G., *Classes généralisées invariantes*, J. Math. Soc. Japan 46, 3 (1994), 467–476.http://projecteuclid.org/euclid.jmsj/1227104692

[Gr2] Gras, G., *Class Field Theory: from theory to practice*, SMM, Springer-Verlag 2003; second corrected printing 2005.http://dx.doi.org/10.1007/978-3-662-11323-3
Private version 2016 (rooteng.pdf):

http://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[Gr3] Gras, G., *Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, I*, Annales de l'Institut Fourier, 23, 3 (1973), 1–48. http://archive.numdam.org/ARCHIVE/AIF/AIF_1973__23_3/AIF_1973__23_3_1_0/AIF_1973__23_3_1_0.pdf

[Gr3′] Gras, G., *Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, II*, Annales de l'Institut Fourier, 23, 4 (1973), 1–44. http://archive.numdam.org/ARCHIVE/AIF/AIF_1973__23_4/AIF_1973__23_4_1_0/AIF_1973__23_4_1_0.pdf

[Gr4] Gras, G., *Sur les ℓ-classes d'idéaux des extensions non galoisiennes de $\mathbb{Q}$ de degré premier impair ℓ à clôture galoisienne diédrale de degré 2ℓ*, J. Math. Soc. Japan 26 (1974), 677–685. https://www.researchgate.net/publication/238882424

[Gr5] Gras, G., *No general Riemann-Hurwitz formula for relative p-class groups*, Journal of NumberTheory 171 (2017), 213–226. https://www.researchgate.net/publication/288060081

[Gr5′] Gras, G., *Complete table concerning the paper: No general Riemann-Hurwitz formula for relative p-class groups* (2016). https://www.researchgate.net/publication/304059327

[Gr6] Gras, G., *Sur le module de Bertrandias–Payan dans une p-extension – Noyau de capitulation*, Publ. Mathématiques de Besançon, Algèbre et Théorie des Nombres(2016), 25–44. https://www.researchgate.net/publication/294194005

[Gr7] Gras, G., *Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres*, J. reine angew. Math. 333 (1982), 86–132. https://www.researchgate.net/publication/243110955

[Gr8] Gras, G., *Logarithme p-adique et groupes de Galois*, J. reine angew. Math. 343 (1983), 64–80. https://www.researchgate.net/publication/238881752

[Gr9] Gras, G., *Remarks on K_2 of number fields*, J. Number Theory 23 (1986), 322–335. https://www.researchgate.net/publication/243002782

[Gr10] Gras, G., *Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canad. J. Math. Vol. 68, 3 (2016), 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3

[Gr11] Gras, G., *Sur la structure des groupes de classes relatives. Avec un appendice d'exemples numériques par T. Berthier*, Annales de l'Institut Fourier, 43, 1 (1993), 1–20. http://archive.numdam.org/ARCHIVE/AIF/AIF_1993__43_1/AIF_1993__43_1_1_0/AIF_1993__43_1_1_0.pdf

[Gr12] Gras, G., *Nombre de φ-classes invariantes. Application aux classes des corps abéliens*, Bulletin de la Société Mathématique de France, 106 (1978), 337–364. http://archive.numdam.org/ARCHIVE/BSMF/BSMF_1978__106_/BSMF_1978__106__337_0/BSMF_1978__106__337_0.pdf

[Gr13] Gras, G., *Principalisation d'idéaux par extensions absolument abéliennes*, J. Number Theory 62 (1997), 403–421. http://www.sciencedirect.com/science/article/pii/S0022314X97920680

[Gr14] Gras, G., *Étude d'invariants relatifs aux groupes des classes des corps abéliens*, In: Astérisque 41/42, Sociéte Mathématique de France (1977), 35–53. https://www.researchgate.net/publication/267146524

[Gr15] Gras, G., *Approche p-adique de la conjecture de Greenberg (cas totalement réel p-décomposé)*, preprint (2016/2017). https://www.researchgate.net/publication/309731894

[Gre1] Greenberg, R., *Galois representations with open image*, Annales de Mathématiques du Québec, special volume in honor of Glenn Stevens 40, 1 (2016), 83–119. https://www.math.washington.edu/~greenber/GalRep.pdf

[Gre2] Greenberg, R., *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284. http://www.jstor.org/stable/2373625?seq=1#page_scan_tab_contents

[GW1] Gruenberg, K.W., Weiss, A., *Capitulation and transfer kernels*, J. Théorie des Nombres de Bordeaux 12, 1 (2000), 219–226. http://archive.numdam.org/ARCHIVE/JTNB/JTNB_2000__12_1/JTNB_2000__12_1_219_0/JTNB_2000__12_1_219_0.pdf

[GW2] Gruenberg, K.W., Weiss, A., *Capitulation and transfer triples*, Proc. London Math. Soc. 3, 87 (2003), 273–290.http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=174659

[GW3] Gruenberg, K.W., Weiss, A., *Transfer kernels for finite groups*, J. Algebra 300, 1 (2006), 35–43.http://www.sciencedirect.com/science/article/pii/S0021869305006836

[H] Herbrand, J., *Le développement moderne de la théorie des corps algébriques - Corps de classes et lois de réciprocité*, Mémorial des Sciences Mathématiques, Fasc. LXXV, Gauthier–Villars, Paris 1936. http://gallica.bnf.fr/ark:/12148/bpt6k39024r/f9.image

[HL] Harnchoowong, A., Li, W., *Sylow subgroups of ideal class group with moduli*, J. Number Theory 36, 3 (1990), 354–372. https://www.researchgate.net/publication/266920573

[I] Inaba, E., *Über die Struktur der ℓ-Klassengruppe zyklischer Zahlkörper von Primzahlgrad ℓ*, J. Fac. Sci. Tokyo I, 4 (1940), 61–115.

[Iw] Iwasawa, K., *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. 33, 2 (1981), 263–288. https://www.jstage.jst.go.jp/article/tmj1949/33/2/33_2_263/_pdf

[Ja1] Jaulent, J-F., *L'arithmétique des ℓ-extensions* (Thèse d'Etat, Université de Franche-Comté, Besançon), Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1984/86.http://pmb.univ-fcomte.fr/1986/Jaulent_these.pdf

[Ja2] Jaulent, J-F., *Théorie ℓ-adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux 10, 2 (1998), 355–397. http://www.math.u-bordeaux1.fr/~jjaulent/Articles/THCDC.pdf

[Ja3] Jaulent, J-F., *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux 6 (1994), 301–325.https://www.math.u-bordeaux.fr/~jjaulent/Articles/ClLog.pdf

[Ki] Y. Kida, *ℓ-extensions of CM-fields and cyclotomic invariants*, J. Number Theory 12 (1980), 519–528.http://www.sciencedirect.com/science/article/pii/0022314X80900426

[Kl] Klys, J., *Reflection principles for class groups* (preprint 2016). http://arxiv.org/pdf/1605.04371.pdf

[Ko] Koch, H., *Galois Theory of p-Extensions*, Springer Monographs in Mathematics, Springer 2002.

[Kol] Kolster, M., *The 2-part of the narrow class group of a quadratic number field*, Ann. Sci. Math. Québec 29, 1 (2005), 73–96.

[KMS] Kulkarni, M., Majumdar, D., Sury, B., *ℓ-Class groups of cyclic extensions of prime degree ℓ*, J. Ramanujan Math. Soc. 30, 4 (2015), 413–454. http://www.isibang.ac.in/~sury/5class.pdf

[Ku] Kurihara, M., *On the ideal class groups of the maximal real subfields of number fields with all roots of unity*, J. Eur. Math. Soc. 1 (1999), 35–49. http://link.springer.com/article/10.1007/PL00011159#page-1

[L] Lang, S., *Algebraic Number Theory*, Addison-Wesley Publ. Comp. 1970, corrected second printing 1986; second edition: Graduate Texts in Math. 110, Springer-Verlag 1994, corrected third printing 2000.

[L1] Lemmermeyer, F., *Galois action on class groups*, J. Algebra 264, 2 (2003), 553–564. http://www.sciencedirect.com/science/article/pii/S0021869303001224

[L2] Lemmermeyer, F., *Class groups of dihedral extensions*, Mathematische Nachrichten 278, 6 (2005), 679–691.http://onlinelibrary.wiley.com/doi/10.1002/mana.200310263/abstract http://www.fen.bilkent.edu.tr/~franz/publ/mndih.pdf

[L3] Lemmermeyer, F., *The ambiguous class number formula revisited*, J. Ramanujan Math. Soc. 28, 4 (2013), 415–421. http://arxiv.org/pdf/1309.1071v1.pdf

[L4] Lemmermeyer, F., *The Development of the Principal Genus Theorem*, In: The Shaping of Arithmetic after C. F. Gauss Disquisitiones Arithmeticae, chap. VIII.3, Springer 2007, 529–561.http://www.math.uiuc.edu/Algebraic-Number-Theory/0354/dpgt.pdf

[Mai] Maire, Ch., *Une remarque sur la capitulation du groupe des classes au sens restreint*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1996/97-1997/98. http://pmb.univ-fcomte.fr/1998/Maire.pdf

[Ma1] Mayer, D.C., *Principalization algorithm via class group structure*, J. Théorie des Nombres de Bordeaux 26, 2 (2014), 415–464. http://arxiv.org/pdf/1403.3839v1.pdf

[Ma2] Mayer, D.C., *The second p-class group of a number field*, Int. J. Number Theory 8, 471 (2012), 471–506.https://arxiv.org/abs/1403.3899 http://www.worldscientific.com/doi/abs/10.1142/S179304211250025X

[Miy1] Miyake, K. (Ed.), *Class field theory – Its centenary and prospect* 1998, Advanced Studies in Pure Mathematics 30, Math. Soc. Japan 2001. http://www.mathbooks.org/aspm/aspm30/aspm30-frontmatter.pdf

[Miy2] Miyake, K., *Algebraic investigations of Hilbert's theorem 94, the principal ideal theorem and the capitulation problem*, Exp. Math. 7 (1989), 289–346.

[Mo1] Morton, P., *Density results for the 2-classgroups of imaginary quadratic fields*, Journal für die reine und angewandte Mathematik, 332 (1982), 156–187. https://eudml.org/doc/152433

[Mo2] Morton, P., *Governing fields for the 2-classgroup of $\mathbb{Q}(\sqrt{-q_1\,q_2\,p})$ and a related reciprocity law*, Acta Arithmetica 55 (1990), 267–290. http://matwbn.icm.edu.pl/ksiazki/aa/aa55/aa5537.pdf

[MoMo] Mouhib, A., Movahhedi, A., *Sur le 2-groupe de classes des corps multiquadratiques réels*, Jour. de Théorie des Nombres de Bordeaux 17 (2005), 619–641. https://www.emis.de/journals/JTNB/2005-2/article12.pdf

[MoNg] Movahhedi, A., Nguyen Quang Do, T., *Sur l'arithmétique des corps de nombres p-rationnels*, Sém. Théorie des Nombres, Paris (1987/89), Progress in Math. 81, Birkhäuser (1990), 155–200. https://www.researchgate.net/publication/236865321

[MW] Mazur, B., Wiles, A., *Class fields of abelian extensions of $\mathbb{Q}$*, Inventiones Mathematicae, 76, 2 (1984), 179–330. https://eudml.org/doc/143124

[P] Belabas K. and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[Ra] Razar, M.J., *Central and genus class fields and the Hasse norm theorem*, Compositio Math. 35 (1977), 281–298.

[Re] Rédei, L., *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. Reine Angew. Math., 180 (1938), 1–43.

[Sch1] Schoof, R., *The structure of minus class groups of abelian number fields*, In: C. Goldstein (ed.), Séminaire de Théorie de Nombres, Paris 1988–1990, Progress in Math. 91, Birkhäuser 1990, 185–204. http://www.mat.uniroma2.it/~schoof/dpp.pdf

[Sch2] Schoof, R., *Computing Arakelov class groups*, "Algorithmic number theory", MSRI Publications 44, Cambridge University Press, Cambridge 2008, 447–495. http://www.mat.uniroma2.it/~schoof/14schoof.pdf

[Sch3] Schoof, R., *Class groups of real cyclotomic fields of prime conductor*, Math. Comp. 72 (2003), 913–937. http://www.mat.uniroma2.it/~schoof/realcyc.pdf

[Se1] Serre, J-P., *Corps locaux*, Actualités Scientifiques et Industrielles 1296, Hermann 1962, 1968, 1980, quatrième édition revue et corrigée 2004; English translation: *Local fields*, Graduate Texts in Math. 67, Springer-Verlag 1979, corrected second printing 1995.

[Se2] Serre, J-P., *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C.R. Acad. Sci. Paris 287, Série I (1978), 183–188.

[Sin] Sinnott, W., *On p-adic L-functions and the Riemann-Hurwitz genus formula*, Comp. Math. 53 (1984), 3–17. http://archive.numdam.org/ARCHIVE/CM/CM_1984__53_1/CM_1984__53_1_3_0/CM_1984__53_1_3_0.pdf

[So] Soriano, F., *Classes logarithmiques ambiges des corps quadratiques*, Acta Arith. LXXVIII.3 (1997), 201–219. http://matwbn.icm.edu.pl/ksiazki/aa/aa78/aa7831.pdf

[St1] Stevenhagen, P., *Rédei-matrices and applications*, Number theory (Paris, 1992–1993), 245–259, London Math. Soc. Lecture Note Ser. 215, Cambridge Univ. Press, Cambridge 1995. http://dx.doi.org/10.1017/CBO9780511661990.015

[St2] Stevenhagen, P., *Ray class groups and governing fields*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Fasc 1, Années 1988/1989. http://pmb.univ-fcomte.fr/1989/Stevenhagen.pdf

[Su] Suzuki, H., *A generalization of Hilbert's theorem 94*, Nagoya Math. J. 121 (1991), 161–169.

[SW] Schoof, R., Washington, L.C., *Visibility of ideal classes*, J. Number Theory 130, 12, 2715–2731. http://www.sciencedirect.com/science/article/pii/S0022314X1000185X

[Ter] Terada, F., *A principal ideal theorem in the genus fields*, Tohoku Math. J. 23, 2 (1971), 697–718.

[Wa] Washington, L.C., *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

[Wi] Wittmann, Ch., *p-class groups of certain extensions of degree p*, Math. of Computation 74, 250 (2004), 937–947. http://www.ams.org/journals/mcom/2005-74-250/S0025-5718-04-01725-9/

[Y1] Yue, Q., *The generalized Rédei-matrix*, Mathematische Zeitschrift 261, 1 (2008), 23–37.

[Y2] Yue, Q., 8*-ranks of class groups of quadratic number fields and their densities*, Acta Mathematica Sinica 27, 7 (2011), 1419–1434. https://www.researchgate.net/publication/226464839

Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans.
Email address: g.mn.gras@wanadoo.fr *url :* http://www.researchgate.net/profile/Georges_Gras