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

To cite this version:
Georges Gras. Invariant generalized ideal classes – structure theorems for p-class groups in p-extensions. Proceedings Mathematical Sciences, 2017, Proceedings - Mathematical Sciences, 127 (1), pp.1-34. 10.1007/s12044-016-0324-1. hal-03317756

HAL Id: hal-03317756
https://hal.science/hal-03317756
Submitted on 9 Aug 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 \((G \cong \mathbb{Z}/p\mathbb{Z})\) obtained in: Sur les \(\ell\)-classes d'idéaux dans les extensions cycliques relatives de degré premier \(\ell\), 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 \(\text{Gal}(L/K)\).

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 \(H_{K,m}^+\) associated with a ray group modulo a modulus \(m\) of \(k\), in the narrow sense, or more generally any subfield \(L\) of these canonical fields, defining \(\text{Gal}(H_{K,m}^+/L)\) by means of a sub-\(G\)-module \(\mathcal{H}\) of the generalized class group \(\mathcal{O}_{K,m}^+ \simeq \text{Gal}(H_{K,m}^+/K)\)).

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

\[
\#\text{Gal}(L/K)^G = \#(\mathcal{O}_{K,m}^+ / \mathcal{H})^G.
\]

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 \( \Gamma := \text{Gal}(L/k) \) is equal to \( \text{Gal}(L/K)^{1-\sigma} \simeq (\mathcal{O}_{K,m}^+/\mathcal{H})^{1-\sigma} \), where \( \sigma \) is a generator of \( G \) (or an extension in \( \Gamma \)). So we have the exact sequences

\[
1 \to \text{Gal}(L/K)^{1-\sigma} \to \Gamma \to \Gamma^{ab} = \Gamma/[\Gamma, \Gamma] = \text{Gal}(L^{ab}/k) \to 1,
\]

\[
1 \to \text{Gal}(L/K)^G \to \text{Gal}(L/K)^{1-\sigma} \to \text{Gal}(L/K)^{1-\sigma} \to 1.
\]

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

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

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

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 annihilator 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 \( 1 \to M_i \to M (1-\sigma)^i \to M (1-\sigma)^i \to 1 \) 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.

\[
M \simeq \mathcal{O}_{K,m}^+/\mathcal{H}
\]

\[
K = L_0 \quad \text{名为} \quad G = \langle \sigma \rangle \quad \text{名为} \quad M_{i+1} \quad \text{名为} \quad M_i \quad \text{名为} \quad L_i \quad \text{名为} \quad L_{i+1} \quad \text{名为} \quad L = L_0
\]

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 \([L'_i : K] = \#M_i\):

\[
M \simeq \mathcal{O}_{K,m}^+/\mathcal{H}
\]

\[
K = L'_{0} \quad \text{名为} \quad \#M_i \quad L'_0 = L^{ab} \quad L' = L'_1 \quad \#M_{i+1} \quad \#M_i \quad M^{(1-\sigma)^i} \quad L = L'_n
\]

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 [25], 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 \( \text{Gal}(L/K) \) 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 $\text{res}$ and $\text{ord}$ 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 $\text{ord}$ (see §2.1, 2.2).

We shall consider generalized $S$-class groups modulo $m$ since any situation is available by choosing suitable $m$ 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 $p \mid \text{Gal}(K/k)$); 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. Kucera (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 $m$ 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) $\text{Pl}_F = \text{Pl}_{F,0} \cup \text{Pl}_{F,\infty}$, the set of finite and infinite places of $F$. The places (finite or infinite) are given as symbols $p$; 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 $r_1 + 2r_2 = [F : \mathbb{Q}]$);

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

(iii) $m$, a modulus of $F$ with support $T$ (i.e., a nonzero integral ideal of $F$ divisible by each of the prime ideals $p \in T$ and not by any $p \not\in T$);
(iv) \( v_p : F^\times \to \mathbb{Z} \) is the normalized \( p \)-adic valuation when \( p \) is a prime ideal; if \( p \) is a real infinite place, then \( v_p : F^\times \to \mathbb{Z}/2\mathbb{Z} \) is defined by \( v_p(x) = 0 \) (resp. \( v_p(x) = 1 \)) if \( \sigma_p(x) > 0 \) (resp. \( \sigma_p(x) < 0 \)) where \( \sigma_p \) is the corresponding embedding \( F \to \mathbb{R} \) associated with \( p \); if \( p \) is complex (thus corresponding to a pair of conjugated embeddings \( F \to \mathbb{C} \)), then \( v_p = 0 \).

(v) \( F^\times_+ = \{ x \in F^\times, \ v_p(x) = 0, \ \forall p \in \mathcal{P}(F,\infty) \} \), group of totally positive elements;
\[ U_{F,T} = \{ x \in F^\times, \ v_p(x) = 0, \ \forall p \in T \}; U_{F,T}^+ = U_{F,T} \cap F^\times_+; \]
\[ U_{F,m} = \{ x \in U_{F,T}, \ x \equiv 1 \pmod{m} \}; \]
\[ U_{F,m}^+ = U_{F,m} \cap F^\times_+; \]

(vi) \( E_F^S = \{ x \in F^\times, \ v_p(x) = 0, \ \forall p \notin S \} \), group of \( S \)-units of \( F \);
\[ E_{F,m}^S = \{ x \in E_F^S, \ x \equiv 1 \pmod{m} \}; \]
\[ E_{F,m}^{\text{ord}} = E_{F,m} \text{, group of units (in the ordinary sense) } \epsilon \equiv 1 \pmod{m}; \]
\[ E_{F,m}^{\text{ord}+} = E_{F,m}^+ \text{, group of totally positive units } \epsilon \equiv 1 \pmod{m}; \]

(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);
\[ I_{F,T} = \{ a \in I_F, \ v_p(a) = 0, \ \forall p \in T \}; P_{F,T} = P_F \cap I_{F,T}; P_{F,T}^+ = P_F^+ \cap I_{F,T}; \]
\[ P_{F,m} = \{ (x), x \in U_{F,m} \}, \text{ ray group modulo } m \text{ in the ordinary sense}; \]
\[ P_{F,m}^+ = \{ (x), x \in U_{F,m}^+ \}, \text{ ray group modulo } m \text{ in the narrow sense}; \]

(viii) \( \mathcal{O}_{F,m}^{\text{ord}} = I_{F,T}/P_{F,m} \), generalized ray class group modulo \( m \) (ordinary sense);
\[ \mathcal{O}_{F,m}^+ = I_{F,T}/P_{F,m}^+ \text{, generalized ray class group modulo } m \text{ (narrow sense)}; \]
\[ \mathcal{O}_{F,m}^S = \mathcal{O}_{F,m}^+/(\mathcal{O}(S))_\mathbb{Z}, S \text{-class group modulo } m \text{ where } (\mathcal{O}(S))_\mathbb{Z} \text{ is the subgroup of } \mathcal{O}_{F,m}^+ \text{ generated by the classes of } p \in S_0 \text{ and, for real } p \in S_\infty, \text{ by the classes of the principal ideals } (x_p^m) \text{ where the } x_p^m \in F^\times \text{ satisfy to the following congruences and signatures:} \]
\[ x_p^m \equiv 1 \pmod{m}, \ \sigma_p(x_p^m) < 0 \ \& \ \sigma_q(x_p^m) > 0 \ \forall q \in \mathcal{P}(F,\infty) \setminus \{p\}; \]
we have \( P_F = \{(x_p)_{p \in \mathcal{P}(F,\infty)} \cdot P_F^+ \) \& \( P_{F,m} = \{(x_p^m)_{p \in \mathcal{P}(F,\infty)} \cdot P_{F,m}^+ \). \]

Taking \( S = \emptyset \), then \( S = \mathcal{P}(F,\infty) \), we find again
\[ \mathcal{O}_{F,m}^S = \mathcal{O}_{F,m}^+; \]
then \( \mathcal{O}_{F,m}^{\text{ord}+} = \mathcal{O}_{F,m}^+/(\mathcal{O}(S))_\mathbb{Z} = \mathcal{O}_{F,m}^{\text{ord}}; \]

(ix) \( \mathcal{O}_F : I_{F,T} \to \mathcal{O}_{F,m}^S \), canonical map which must be read as \( \mathcal{O}_{F,m}^{\text{ord}} \) for suitable \( m \) 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 \( \infty \), which means that the field \( H_F^+ \) may be non-real even if \( F \) is totally real); we have
\[ \text{Gal}(H_F^+/F) \simeq \mathcal{O}_F^+ = I_F/P_F^+; \]

(ii) \( H_F^{\text{ord}+}_\infty = H_F^{\text{ord}} \subseteq H_F^+ \) is the Hilbert class field in the ordinary sense (maximal Abelian extension of \( F \), unramified for prime ideals, and splitted at \( \infty \)); we have
\[ \text{Gal}(H_F^{\text{ord}+}_\infty/F) \simeq \mathcal{O}_F^{\text{ord}} = I_F/P_F; \]

(iii) \( H_F^S \subseteq H_F^+ \) is the \( S \)-split Hilbert class field (maximal Abelian extension of \( F \) unramified for prime ideals and splitted at \( S \)); we have
\[ \text{Gal}(H_F^S/F) \simeq \mathcal{O}_F^S = \mathcal{O}_F^+/(\mathcal{O}_F(S))_\mathbb{Z}; \]
recall that the decomposition group of $p \in S_0$ (resp. $S_{\infty}$) is given, in $G$, by the cyclic group generated by the class of $p$ (resp. $(x_p)$); hence $\text{Gal}(H^+_{F, m}/H^+_F)$, generated by these decomposition groups, is isomorphic to $(\alpha_F(S))_\mathbb{Z}$.

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

$H^{SD}_{F, m}$ is the m-ray class field in the ordinary sense,

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

$$\text{Gal}(H^{S}_{F, m}/F) \cong \mathcal{A}^S_{F, m} = \mathcal{A}^+_F/(\alpha_F(S))_\mathbb{Z}$$

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

For instance, for a prime $p$, the $p$-Sylow subgroups of $\mathcal{A}^ord_F$ and $\mathcal{A}^{Pr}_F$, for the set $S = Pl_p := \{p, \ p \mid p\}$, have a significant meaning in some duality theorems.

3. Computation for the Order of $(\mathcal{A}^+_K, \mathcal{H})^G$

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

$$\mathcal{H} \subseteq \mathcal{A}^+_K$$

be an arbitrary sub-$G$-module of $\mathcal{A}^+_K$.

Remarks 3.1. (i) The group $G$ acts on $\mathcal{A}^+_K$, hence on $\text{Gal}(H^+_{K, m}/K)$ by conjugation via the Artin isomorphism $A \mapsto \left(\frac{H^+_{K, m}/K}{A}\right) \in \text{Gal}(H^+_{K, m}/K)$, for all $A \in I_{K,T}$ (modulo $P^+_K$), for which

$$\left(\frac{H^+_{K, m}/K}{A}\right) = \tau \cdot \left(\frac{H^+_{K, m}/K}{A}\right) \cdot \tau^{-1},$$

for all $\tau \in G$.

(ii) The sub-$G$-module $\mathcal{H}$ fixes a field $L \subseteq H^+_{K, m}$ which is Galois over $k$ and in the same way, $\text{Gal}(L/K) \cong \mathcal{A}^+_K/\mathcal{H}$ is a $G$-module.

(iii) Taking $\mathcal{H} = (\alpha_K(S))_\mathbb{Z}, S \subseteq Pl_K$ (see (viii)) leads to $\mathcal{A}^+_K/\mathcal{H} = \mathcal{A}^S_K$ & $L = H^+_S$, (assuming that $\alpha_K(S)$ is a sub-$G$-module).

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

We intend to compute $\#(\mathcal{A}^+_K, \mathcal{H})^G = \#(\text{Gal}(L/K))^G$, which is equivalent, from exact sequences (1), to obtain the degree $[L^{ab} : K]$, 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, $[La]$), often in a hidden manner, since it is absolutely necessary for the interpretation, in the cyclic case, of the famous idelic index $(J_K : k^sN_K/k(J_K)) = [K^{ab} : k]$, 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 $\lambda, \mu$ invariants for the $\mathbb{Z}_p$-extensions of a totally real number field $[Gr13]$. 
Chevalley’s formula in the cyclic case is based on (and roughly speaking equivalent to) the nontrivial computation of the Herbrand quotient \( \frac{(\xi_K: N_{K/k}(\xi_K))}{(\xi_K: E_K)} = 2^e \) of the group of units \( E_K \), where \( N_{K/k} \) is the subgroup of units of norm 1 in \( K/k \) and where \( e \) 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” \([1]\).

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

3. The main exact sequence and the computation of \( \#(\mathcal{O}_{K,m}^+ / \mathcal{H})^G \).

3.1. Global computations. Recall that \( \mathcal{H} \) is a sub-\(G\)-module of \( \mathcal{O}_{K,m}^+ = I_{K,T} / P_{K,m}^+ \). Put

\[
(2) \quad \mathcal{H} = \{ h \in \mathcal{O}_{K,m}^+, \ h^{1-\sigma} \in \mathcal{H} \};
\]

it is obvious that

\[
(3) \quad (\mathcal{O}_{K,m}^+ / \mathcal{H})^G = \mathcal{H} / \mathcal{H}.
\]

We have the exact sequences

\[
(4) \quad 1 \longrightarrow \mathcal{O}_{K,m}^+ \longrightarrow \mathcal{H} \longrightarrow \mathcal{H} / \mathcal{H} \longrightarrow 1
\]

with \( \mathcal{H} = \text{Ker}(N_{K/k}) \), where \( N_{K/k} \) 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 \( \nu_{K/k} = j_{K/k} \circ N_{K/k} \), 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 \( K \), \( j_{K/k} \circ N_{K/k}(\mathfrak{P}) = j_{K/k}(\mathfrak{P}/\mathfrak{p}) = (\prod_{\mathfrak{p} \in \mathfrak{P} / \mathfrak{p}} \mathfrak{P}^{ef}) / \mathfrak{p} \) (where \( \mathfrak{p} \) is the ramification index), which is indeed \( \mathfrak{P}^{ef} / \mathfrak{p} \) since \( G \) operates transitively on the \( \mathfrak{P} \setminus \mathfrak{P} \cup \mathfrak{p} \) with a decomposition group of order \( [K:k] / e / f \).

By definition, for an ideal \( \mathfrak{a} \) of \( K \), we have \( N_{K/k}(\mathfrak{a} K(\mathfrak{a})) = \mathfrak{a} K(\mathfrak{a}) \), and for any ideal \( \mathfrak{a} \) of \( k \), we have \( j_{K/k}(\mathfrak{a} K(\mathfrak{a})) = \mathfrak{a} K(\mathfrak{a}) \), which makes sense since \( N_{K/k}(P_{K,m}^+) \subseteq P_{K,m}^+ \) and \( j_{K/k}(P_{K,m}^+) \subseteq P_{K,m}^+ \), seeing the modulus \( m \) of \( k \) extended in \( K \) in some writings.

To simplify the formulas, we write \( N \) for \( N_{K/k} \).

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

Let \( I \) be any subgroup of \( I_{K,T} \) such that \( \sigma_{\ell K}(I) = \mathcal{H} \), i.e.,

\[
(5) \quad I \cdot P_{K,m}^+ / P_{K,m}^+ = \mathcal{H}.
\]

the group \( I \cdot P_{K,m}^+ \) is unique and we then have

\[
(6) \quad N(\mathcal{H}) = N(I) \cdot P_{K,m}^+ / P_{K,m}^+ \simeq N(I) / N(I) \cap P_{K,m}^+.
\]

\(^1\)For \( K/k \) Galois, the arithmetical norm \( N_{K/k} \) is defined multiplicatively on the group of ideals of \( K \) by \( N_{K/k}(\mathfrak{g}) = p^{ef} \) for prime ideals \( \mathfrak{g} \) of \( K \), where \( p \) is the prime ideal of \( k \) under \( \mathfrak{g} \) and \( f \) its residue degree in \( K/k \). If \( \mathfrak{a} = (\alpha) \) is principal in \( K \), then \( N_{K/k}(\mathfrak{a}) = N_{K/k}(\alpha) \) 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 $\mathfrak{P} \cdot P_{K,m}^+$ (for $\mathfrak{P} \in S_{K,0}$) and $(x^m \mathfrak{P}) \cdot P_{K,m}^+$ (for $\mathfrak{P} \in S_{K,\infty}$) generate $\mathcal{H}$, so that we can take $\mathcal{I} = \mathfrak{P} \in S_{K,0} \mathfrak{P} \in S_{K,\infty}$ as canonical subgroup of $I_{K,T}$ defining $\mathcal{H}$. Thus $\mathcal{O}^+_{K,m}/\mathcal{H} = \mathcal{O}_{K,m}$ 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 $I \cdot P_{K,m}^+$, so, if for instance $\mathfrak{P} \in S_{K,0}$, for any $r \in G$ we have, $\varphi_K(\mathfrak{P}) = \varphi_K(\mathfrak{P}^r)$ for some $\mathfrak{P}^r \in S_K$, whence $\mathfrak{P}^r = \mathfrak{P}^r(x)$, $x \in U_{K,m}^+$.

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

$$1 \longrightarrow E_{k,m}^+ \longrightarrow U_{k,m}^+ \overset{\psi}{\longrightarrow} P_{K,m}^+ \longrightarrow 1,$$

we then put

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

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

We can state (fundamental exact sequence):

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

$$\widetilde{\mathcal{H}} = \{ h \in \mathcal{O}^+_{K,m}, h^{1-\sigma} \in \mathcal{H} \}.$$ 

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

$$1 \longrightarrow (E_{k,m}^+ N(U_{k,m}^+)) \cap \Lambda \longrightarrow \Lambda \overset{\varphi}{\longrightarrow} \mathcal{N}(\mathcal{H})/\mathcal{H}^{1-\sigma} \longrightarrow 1,$$

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

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

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

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

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

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

$$x = \varepsilon \cdot N(u), \quad \varepsilon \in E_{k,m}^{\text{ord}};$$

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

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

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

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 $(u) \in P_{K,m}^+$, $\varphi_K(\mathfrak{B})^{1-\sigma} = \varphi_K(\mathfrak{A}) \in \mathcal{H}$, hence $\varphi_K(\mathfrak{B}) \in \mathcal{H}$, and we obtain $\varphi_K(\mathfrak{A}) \in (\widetilde{\mathcal{H}})^{1-\sigma}$. $\square$
We deduce from (11),

\[(\mathcal{H} : \mathcal{H}) = \frac{\# \mathcal{O}_{K,m}^+ \cdot \#(\mathcal{H})^{1-\sigma}}{\# \mathcal{N}(\mathcal{H}) \cdot \# \mathcal{N}(\mathcal{H})} = \frac{\# \mathcal{O}_{K,m}^+}{\# \mathcal{N}(\mathcal{H}) \cdot (\mathcal{H} : \mathcal{H})^{1-\sigma}};\]
thus from (9), (9) and (10),

\[\# (\mathcal{O}_{K,m}^+ / \mathcal{H})^G = \frac{\# \mathcal{O}_{K,m}^+}{\# \mathcal{N}(\mathcal{H}) \cdot (\Lambda : (E_{k,m}^+ C N(U_{K,m}^+)) \cap \Lambda)} = \frac{\# \mathcal{O}_{K,m}^+}{\# \mathcal{N}(\mathcal{H}) \cdot (\Lambda N(U_{K,m}^+ : E_{k,m}^+ N(U_{K,m}^+))};\]

We first apply this formula to

\[\mathcal{H}_0 = P_{K,T}^+ / P_{K,m}^+ \simeq (U_{K,T}^+ / U_{k,m}^+) / (E_K^+ / E_{K,m}^+),\]
which is the sub-module of \(\mathcal{O}_{K,m}^+\) corresponding to the Hilbert class field \(H_K\) since, using the idelic 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 \(I_{K,T}^+ / P_{K,m}^+ \rightarrow I_K^+ / P_K^+\) giving an isomorphism, whence

\[( \mathcal{O}_{K,m}^+ / \mathcal{H}_0 )^G \simeq (I_{K,T}^+ / P_{K,T}^+)^G \simeq (I_K^+ / P_K^+)^G \simeq \mathcal{O}_{K,m}^+;\]

Take \(I_0 := P_{K,T}^+\); then

\[N(I_0) = N(P_{K,T}^+) \& N(\mathcal{H}_0) = N(P_{K,T}^+) \cdot P_{k,m}^+ / P_{K,m}^+;\]
and

\[\Lambda_0 = \{ x \in U_{k,m}^+, (x) \in N(P_{K,T}^+) \} = (E_k^+ C N(U_{K,T}^+)) \cap U_{k,m}^+;\]
It follows from (11) applied to \(\mathcal{H}_0\), from (12), and \(N(U_{K,m}^+) \subseteq \Lambda_0\) (see (14)),

\[\# \mathcal{O}_{K,m}^+ \cdot \#(\mathcal{H}_0) = (E_k^+ N(U_{K,T}^+) \cap U_{k,m}^+ : E_{k,m}^+ N(U_{K,m}^+)).\]

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

\[1 \rightarrow E_k^+ U_{k,m}^+ / U_{k,m}^+ \rightarrow E_k^+ N(U_{K,T}^+) U_{k,m}^+ / U_{k,m}^+ \rightarrow N(\mathcal{H}_0) = N(P_{K,T}^+) \cdot P_{k,m}^+ / P_{K,m}^+ \rightarrow 1,\]
giving

\[\# N(\mathcal{H}_0) = \frac{(E_k^+ N(U_{K,T}^+) : (E_k^+ N(U_{K,T}^+) \cap U_{k,m}^+))}{(E_k^+ : E_{k,m}^+)};\]
thus from (15) and (16),

\[\# \mathcal{O}_{K,m}^+ = \# \mathcal{O}_{K,m}^+ \cdot \frac{(E_k^+ N(U_{K,T}^+) : (E_{k,m}^+ N(U_{K,m}^+))}{(E_k^+ : E_{k,m}^+)};\]

The inclusions \(N(U_{K,m}^+) \subseteq E_{k,m}^+ N(U_{K,m}^+) \subseteq E_k^+ N(U_{K,m}^+)\) lead from (17) to

\[\# \mathcal{O}_{K,m}^+ = \# \mathcal{O}_{K,m}^+ \cdot \frac{(E_k^+ N(U_{K,T}^+) : N(U_{K,m}^+))}{(E_k^+ : E_{k,m}^+) \cdot (E_{k,m}^+ N(U_{K,m}^+) : N(U_{K,m}^+))};\]
in other words

\[\# \mathcal{O}_{K,m}^+ = \# \mathcal{O}_{K,m}^+ \cdot \frac{(E_k^+ N(U_{K,T}^+) : N(U_{K,m}^+))}{(E_k^+ : E_{k,m}^+) \cdot (E_{k,m}^+ N(U_{K,m}^+) : N(U_{K,m}^+))};\]

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

\[\# \mathcal{O}_K^+ = \# \mathcal{O}_k^+ \cdot \prod_{p \in \mathcal{P}_{K,m}} e_p \frac{1}{[K : k \cdot (E_k \cdot E_k^+ \cap N(K^+))];\]
where \(e_p\) is the ramification index in \(K/k\) of the finite place \(p\).
Lemma 3.4. For any finite set $T$, we have the relation
\[ U_{k,T}^+ \cap N(K^\times) = N(U_{K,T}^+). \]

Proof. Let $x \in U_{k,T}^+$ of the form $N(z)$, $z \in K^\times$; put $(z) = \prod_{p \in \mathfrak{P}_{k,0}} e_p \mathfrak{c}_p$ where $\mathfrak{c}_p = \mathfrak{P}_p^\omega$, for a fixed $\mathfrak{P}_0$ and $\omega \in \mathbb{Z}[G]$ depending on $p$. Since the $N(\mathfrak{c}_p) = N(\mathfrak{P}_p^\omega)$ must be prime to $T$, we have $\omega \in (1 - \sigma) \cdot \omega'$, $\omega' \in \mathbb{Z}[G]$, for all $p \in T$. 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 $F_K^+$ (narrow sense) of $\mathfrak{c}$ an ideal $\mathfrak{B}$ prime to $T$, hence $\mathfrak{B} = \mathfrak{A} \cdot (y')$, $y' \in K^{\times+}$, giving $z' := z \cdot y'^{1 - \sigma}$ 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 $N(z) \gg 0$ (i.e., the signature of $z$ is in the kernel of the norm, see [Gr3, Proposition 1.1]); then $z'' := z \cdot y^{1 - \sigma}$ yields $N(z'') = x$ with $z'' \in U_{K,T}^+$.

So $(E_k^+ : E_k^+ \cap N(U_{K,T}^+)) = (E_k^+ : E_k^+ \cap N(K^\times))$. More generally, if $x \in U_{k,T}^+$ must be in $N(U_{K,T}^+)$ this is equivalent to say that $x$ must be in $N(K^\times)$ (i.e., a global norm without any supplementary condition) which is more convenient to use normic criteria (with Hasse’s symbols $(\frac{x \cdot K/k}{p})$ for instance; see Remark [47]). Recall that for $T = \emptyset, U_{K,T}^+ = K^{\times+}$ and the lemma says that $K^{\times+} \cap N(K^\times) = N(K^{\times+})$.

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

From [18], [19] and (20), we have obtained
\[ \#Q_{K,m}^{+} = \frac{\#Q_k^{+} \cdot \prod_{p \in \mathfrak{P}_{k,0}} e_p \cdot (N(U_{K,T}^+) : N(U_{K,m}^+))}{[K : k] \cdot (E_k^+ : E_k^{+}) \cdot (E_k^{+} : N(U_{K,m}^+) : N(U_{K,m}^+))}. \]

hence using (11)
\[ (\#Q_{K,m}^{+}/\mathcal{H})^{G} = \frac{\#Q_k^{+} \cdot \prod_{p \in \mathfrak{P}_{k,0}} e_p \cdot (N(U_{K,T}^+) : N(U_{K,m}^+))}{[K : k] \cdot \#\mathcal{H} \cdot (E_k^+ : E_k^{+}) \cdot (\mathcal{A} \cdot N(U_{K,m}^+) : N(U_{K,m}^+))}. \]

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

The arithmetical norm $N_{K/k} = N$ can be extended by continuity on $\prod_{\mathfrak{P}\in T} K_{\mathfrak{P}}^{\times}$ and the groups $N(U_{K,T}^{\mathfrak{P}})$ and $N(U_{K,m})$ are open compact subgroups of $U_{K,T}$.

It follows that the map $N(U_{K,T}^{\mathfrak{P}}) \xrightarrow{\phi} N(U_{K,T})/N(U_{K,m})$ is surjective.

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

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

Thus
\[ (N(U_{K,T}^{\mathfrak{P}}) : N(U_{K,m}^{\mathfrak{P}})) = (N(U_{K,T} : N(U_{K,m}^{\mathfrak{P}})) = \frac{(U_{k,T} : N(U_{K,m}^{\mathfrak{P}}))}{(U_{k,T} : N(U_{K,m}^{\mathfrak{P}}))}. \]

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


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

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

\[
\#(\mathcal{O}_{k,m}^+ / \mathcal{O}_{k,m}^+) = \frac{\#(\mathcal{O}_{k,m}^+ / \mathcal{O}_{k,m}^+) \cdot \prod_{p \in \mathcal{T}} e_p \cdot (\mathcal{U}_{k,m} : N(\mathcal{U}_{k,m}))}{[K : k] \cdot #N(\mathcal{H}) \cdot (\Lambda : \Lambda \cap N(\mathcal{U}_{k,m}))},
\]

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

Using, where appropriate, Lemma [5.4] we get the following corollaries:

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

\[
\#(\mathcal{O}_{K,m}^+ / \mathcal{O}_{K,m}^+) = \frac{\#(\mathcal{O}_{k,m}^+ \prod_{p \in \mathcal{M}_{k,0}} e_p)}{[K : k] \cdot #N(\mathcal{H}) \cdot (\Lambda : \Lambda \cap N(\mathcal{K}^\times))},
\]

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

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

\[
\#(\mathcal{O}_{K,m}^+ / \mathcal{O}_{K,m}^+) = \frac{\#(\mathcal{O}_{k,m}^+ \prod_{p \in \mathcal{M}_{k,0}} e_p)}{[K : k] \cdot #N(\mathcal{H}) \cdot (\Lambda : \Lambda \cap N(\mathcal{K}^\times))},
\]

where the group \(E_{NSK}^+\) of “\(NSK\)-units” is defined by:

\[
E_{NSK}^+ = \{x \in E_{NSK}, v_p(x) \equiv 0 \pmod{f_p} \forall p \in S_k & v_p(x) = 0 \forall p \in P_{k,\infty} \setminus S_{k,\infty}\},
\]

where \(S_k\) is the set of places of \(k\) under \(S_{\infty}\) and \(f_p\) the residue degree of \(p\).

Proof. We have \(\Lambda = \{x \in k^{\times,+}, (x) \in N(\mathcal{I})\}\), where \(\mathcal{I} = \langle \mathcal{P}_q \rangle_{q \in S_{k,0}} \cdot \langle (\mathcal{P}_q) \rangle_{q \in S_{k,\infty}}\). If \(x \in \Lambda\), then \((x) = N(A)\), \(A \in \langle \mathcal{P}_q \rangle_{q \in S_{k,0}}\), \(A \in \langle (\mathcal{P}_q) \rangle_{q \in S_{k,\infty}}\); hence, up to \(N(K^\times)\), \(x\) is represented by a \(NSK\)-unit \(\varepsilon\). One verifies that the map which associates \(x\) with the image of \(\varepsilon\) in \(E_{NSK}^+ / E_{NSK}^+ \cap N(K^\times)\) is well-defined and leads to the isomorphism. Note that \(E_{NSK}^+ \subset E_{NSK}^+\).

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

\[
\#(\mathcal{O}_{K,m}^+ / \mathcal{O}_{K,m}^+) = \frac{\#(\mathcal{O}_{k,m}^+ \prod_{p \in \mathcal{M}_{k,0}} e_p \prod_{p \in S_{k,0}} d_p)}{[K : k] \cdot (E_{NSK}^+ / E_{NSK}^+ \cap N(K^\times))},
\]

where \(d_p = e_p f_p\) is the local degree of \(K/k\) at \(p\) with \(e_p = 1\) for infinite places: use the relation \(E_{NSK}^+ \cap N(K^\times) = E_{NSK}^+ \cap N(K^\times)\) and the exact sequence.
we shall get a product of two integers numerical computations); using the relations So formula (25) can be interpreted as follows (which will be very important for $C_p$ (resp. 1) if the cyclic extension $K/k$, can be interpreted by means of the following diagram of finite extensions:

$$
\begin{array}{c}
K \\
\downarrow \\
K \cap H^+_k \\
\uparrow \\
\O^+_K \\
\downarrow \\
H^+_K \\
\downarrow \\
H^+_k \\
\downarrow \\
\O^+_k
\end{array}
$$

Here $K \cap H^+_k/k$ is the maximal subextension of $K/k$, unramified at finite places, and the norm map $N_{K/k}: \O^+_K \rightarrow \O^+_k$ is surjective if and only if $K \cap H^+_k = k$. So formula (24) can be interpreted as follows (which will be very important for numerical computations); using the relations

$$[K : k] = [K : K \cap H^+_k] \cdot [K \cap H^+_k : k] \quad \& \quad \#\O^+_k = \#N(\O^+_K) \cdot [K \cap H^+_k : k],$$

we shall get a product of two integers

$$
\#(\O^+_K/H)^G = \frac{\#N(\O^+_K)}{\#N(H)} \cdot \prod_{p \in \mathcal{P}_{k,0}} e_p \cdot \frac{\prod_{p \in \mathcal{P}_{k,\infty}} f_p}{[K : k] \cdot (E^\text{ord}_k : E^\text{ord}_k \cap N(K^\times))}.
$$

Thus in the computations using a filtration $M_i$ (see Section 3), the $G$-modules $H = \delta_K(T)$ are denoted $M_i = \delta_K(I_i)$; the $M_i$ and $N(M_i)$ will be increasing subgroups of $\O^+_K$ and $\O^+_k$, respectively, so that $M_n = \O^+_k$ for some $n$.

Then we know that $A_i = \{x_i \in k^\times, \ (x_i) \in N(I_i)\}$, 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 2.7 (a), (b)); so it remains to consider the local norms at ramified prime ideals since by the Hasse norm theorem, $x \in N(K^\times)$ 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], [L3]), so that the integers:

$$\prod_{p \in \mathcal{P}_{k,0}} e_p \cdot \frac{\prod_{p \in \mathcal{P}_{k,\infty}} f_p}{[K : k \cap H^+_k] \cdot (A_i : A_i \cap N(K^\times))} \cdot i \geq 0,$$

are decreasing because of the injective maps

$$E^+_k/E^+_k \cap N(K^\times) \hookrightarrow \cdots \hookrightarrow A_i/A_i \cap N(K^\times) \hookrightarrow A_{i+1}/A_{i+1} \cap N(K^\times) \hookrightarrow \cdots$$

giving increasing indices $(A_i : A_i \cap N(K^\times))$.

Let $I_p(K/k)$ be the inertia groups (of orders $e_p$) of the prime ideals $p$ and put

$$\Omega(K/k) = \left\{ \left( \tau_p \right)_{p \in \mathcal{P}_0} \in \bigoplus_{p \in \mathcal{P}_0} I_p(K/k), \ \prod_{p \in \mathcal{P}_0} \tau_p = 1 \right\};$$
we have the genera exact sequence of class field theory (interpreting the product formula of Hasse symbols, \cite{Gr2} Proposition IV.4.5)

\[ 1 \to E_k^+ / E_k^+ \cap N(K^\times) \xrightarrow{\omega} \bigoplus_{p \in \mathcal{P}_0} I_p(K/k) \xrightarrow{\pi} \text{Gal}(H^+/H^+_k) \to 1, \]

where \( H^+_k := H^+_K \) is the genera field defined as the maximal subextension of \( H_K^+ \), Abelian over \( k \), where \( \omega \) associates with \( x \in E_k^+ \) the family of Hasse symbols \( \left( \frac{x}{K/k} \right)_p \) in \( \bigoplus_{p \in \mathcal{P}_0} I_p(K/k) \) (hence in \( \Omega(K/k) \)), and \( \pi \) associates with \( \prod_p \tau'_p \) the product \( \prod_p \pi_p \tau'_p \) of the lifts \( \tau'_p \) of the \( \pi_p \), in the inertia groups of \( H^+_K/k \) (these inertia groups generate the group \( \text{Gal}(H^+_K/kH^+_K) \) which is the image of \( \pi \)); from the product formula, if \( \pi_p(k) \) is in the image of \( \omega \), then this product \( \prod_p \tau'_p \) fixes both \( H^+_k \) and \( K \), hence \( KH^+_K \). Thus \( \pi(\Omega(K/k)) = \text{Gal}(H^+_K/kH^+_K) \) with \( \pi \circ \omega(E_k^+) = 1 \), giving the isomorphisms

\[ \Omega(K/k) / \omega(E_k^+ \cap N(K^\times)) \cong Gal(H^+_K/kH^+_K) \quad \text{and} \quad \omega(E_k^+ \cap N(K^\times)) \cong E_k^+ / E_k^+ \cap N(K^\times). \]

We have \( \#\Omega(K/k) = \prod_{p \in \mathcal{P}_0} e_p \) and \( H^+_K \) being fixed by \( \Omega(K/k) \), we get

\[ [H^+_K : K] = \frac{\prod_{p \in \mathcal{P}_0} e_p}{[K : K \cap H^+_K]} \cdot \frac{[K : K \cap H^+_K] \cdot (E_k^+ \cap N(K^\times))}{[K : K \cap H^+_K]} = \#\Omega(K/k), \]

as expected.

Since \( \Lambda_i \) contains \( E_k^+ \), we have \( \pi \circ \omega(\Lambda_i/E_k^+) \subseteq \text{Gal}(H^+_K/kH^+_K) \). Therefore we have at the final step \( i = n \), using \( \text{(29)} \) for \( H = M_n = \Omega_K \),

\[ \left( \Lambda_n : \Lambda_n \cap N(K^\times) \right) = \frac{\prod_{p \in \mathcal{P}_0} e_p}{[K : K \cap H^+_K]} = \#\Omega(K/k), \]

whence \( \omega_n(\Lambda_n) = \Omega(K/k) \) and \( \pi_n \circ \omega_n(\Lambda_n/E_k^+) = \text{Gal}(H^+_K/kH^+_K) \), which explains that an obvious heuristic is that \( \#\Omega_K \) has no theoretical limitation about the integer \( n \) (but its structure may have some constraints, see Section \([3]\)).

An interesting case leading to significant simplifications is when there is a single ramified place \( p_0 \) in \( K/k \); indeed, the product formula (from \( \Omega(K/k) = 1 \)) implies \( \left( \Lambda : \Lambda \cap N(K^\times) \right) = 1 \) and \( \frac{e_{p_0}}{[K : K \cap H^+_K]} = 1 \), so that formula \( \text{(29)} \) reduces to

\[ \#(\Omega^+_k/H) = \frac{\#N(\Omega^+_k)}{\#N(H)}, \]

where \( \#N(\Omega^+_k) = [H^+_k : K \cap H^+_k] \) is known. If \( p_0 \) is totally ramified, then \( \#(\Omega^+_k/H) = \frac{\#\Omega^+_k}{\#N(H)} \).

From the above formulas (e.g., Formula \( \text{(27)} \)), 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 \( \sigma_K((S_K)) \) is a sub-\( G \)-module.

Consider the \( p \)-class group \( \Omega_{SK}^+ \), for which we have the formula

\[ \#\Omega_{SK}^+ = \frac{\#N(\Omega^+_k)}{\#\sigma_K((NS_K))} \cdot \prod_{p \in \mathcal{P}_0} e_p \]

Then we have \( \left( \sigma_K(S_K)) = \Omega^+_K \) (i.e., \( S_K \) generates the \( p \)-class group of \( K \)) if and only if the two following conditions are satisfied:

(i) \( N(\Omega^+_K) = \sigma_K((NS_K)) \),

(ii) \( E^{NS}_K : E^{NS}_k \cap N(K^\times) = \frac{\prod_{p \in \mathcal{P}_0} e_p}{[K : K \cap H^+_K]} = \#\Omega(K/k) \) (see \( \text{(31)} \)).

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') $\mathcal{O}_k^+ = \alpha_k(⟨S_k⟩)$, where $S_k$ is the set of places $p$ under $\mathfrak{p} \in S_K$.

(ii') $(E_k^{S_0} : E_k^{S_0} \cap N(K^\times)) = \prod_{p \in P_{k,0}} e_p \frac{[K : k]}{[k : k']} = \#\Omega(K/k)$.

So, if the $p$-class group $\mathcal{O}_k^+$ is numerically known, to characterize a set $S_K$ of generators for $\mathcal{O}_k^+$ needs only local normic computations with the group $E_k^{S_0}$ 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 $(E_q^{S_0} : E_q^{S_0} \cap N(K^\times)) = 2$ since the product of ramification indices is equal to $4$; for instance, $E_q^{S_0} = \langle 3 \rangle$ for $S_K = \{\mathfrak{p}_3\}$.

We have to compute, for some $x \in \mathbb{Q}_0^+$ (norm of an ideal, thus local norm at each unramified place), the Hasse symbol $(x, K/41)$ 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 $\left(\frac{x}{K/41}\right) \cdot \left(\frac{x}{K/2}\right) = 1$ 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 $(\frac{82}{x'})$ (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 $(\frac{82}{249}) = -1$). We can verify that $\mathfrak{p}_3$ is of order 4 since the equation $v^2 - 82 \cdot v^2 = 3^e$ (with $\gcd(u, v) = 1$) has no solution with $e = 1$ or $e = 2$, but $N(73 + 8\sqrt{82}) = 3^2$; however, the knowledge of $\#\mathcal{O}_K$ is not required to generate the class group.

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

```
bnfisnorm(bnfinit(x^2 - 82, 23)).
```

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, $N(761 + 84\sqrt{82}) = 23^2$ giving $E_q^{S_0} = (761 + 84\sqrt{82})$).

**Remark 3.13.** Another important fact is the relation $\nu_{K/k} = j_{K/k} \circ N_{K/k}$ 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 $N_{K/k}(H)$ without mystery (when $\mathcal{O}_k^+$ is well known), contrary to $H^{(K/k)}$.

This property of $N_{K/k}$ is valid if $K/k$ is any Galois extension; if $K/k$ has no unramified Abelian subextension $L/K$ (what is immediately noticeable !) then $N_{K/k}$ is surjective, but possibly not $\nu_{K/k}$. We have given in [Gr5], [Gr57], 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 5.6 have been extensively studied in concrete cases from the pioneer work of Inaba [11] (1940)], in quadratic, cubic extensions, etc. and applied to non-cyclic extensions (dihedral ones, etc):
see, e.g., [Fr], [Re], [Gr3], [Gr4], [HL], [L1] (in the semi-simple case of $G$-modules), [Bo1], [L2], [L3], [L4], [Ko1], [Ko2], [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], [Tec], [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 $\mathcal{O}_K^+, \mathcal{O}_k^+$ 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 $\mathcal{O}_K^+ \otimes \mathbb{Z}_p$, $\mathcal{O}_k^+ \otimes \mathbb{Z}_p$, still denoted $\mathcal{O}_K^+, \mathcal{O}_k^+$ thereafter, by abuse of notation.

We consider the $\mathbb{Z}_p[G]$-module $M := \mathcal{O}_K^+$ for which we define the filtration evoked 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

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

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 $\#(M_{i+1}/M_i) \leq \#M_i$.

If for instance $\#M_1 = p$, then $\#(M_{i+1}/M_i) = p$ for $0 \leq i \leq n - 1$.

Remark that $\mathcal{O}_k^+$ has no obvious $G$-module definition from $M$ (it is not isomorphic to $M^G$, 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 $N_{K/k}$ 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 $\zeta$ is a primitive $p$th root of unity; then we know that

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

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:

$$1 \longrightarrow \bigoplus_{j=1}^m (1 - \zeta)^{n_j-1} \mathbb{Z}_p[\zeta]/(1 - \zeta)^{n_j} \longrightarrow \bigoplus_{j=1}^m (1 - \zeta) \mathbb{Z}_p[\zeta]/(1 - \zeta)^{n_j} \longrightarrow 1,$$

(31)

where the submodules $M_i$ are given by $M_i = \bigoplus_{j \leq i} \mathbb{Z}_p[\zeta]/(1 - \zeta)^{n_j}$ (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 $M^{p/k} = 1$ 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
\[
N_j := \mathbb{Z}_p[\zeta]/(1 - \zeta)^{n_j} \simeq (\mathbb{Z}/p^{a_j+1}\mathbb{Z})^{b_j} \bigoplus (\mathbb{Z}/p^{b_j}\mathbb{Z})^{p-1-b_j}, \quad \forall j = 1, \ldots, m.
\]

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

Proof. We have $N_j := \mathbb{Z}_p[\zeta]/(1 - \zeta)^{n_j} \simeq (\mathbb{Z}/p^{a_j}(1 - \zeta)^{b_j})$. 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 $N_j^{p^{k-1}}/N_j$), 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 $M^{(k)} := \{ h \in M, \ h^{p^k} = 1 \}, \ k \geq 0$.

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

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

4.3. Case $M^p \neq 1$. We have, in the same framework, the following result in the case $M^p \neq 1$, 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 $M^{p^k/k} \neq 1$. 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 $M \simeq (\mathbb{Z}/p^2\mathbb{Z}) \bigoplus (\mathbb{Z}/p\mathbb{Z})^{n-2}$.

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

(iii) Case $n > p$. Then $M \simeq (\mathbb{Z}/p^{a+1}\mathbb{Z})^{b} \bigoplus (\mathbb{Z}/p^2\mathbb{Z})^{p-1-b}$.

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
\[
1 \rightarrow M_1 \cap M_n^{p-1} / M_1 \cap M_n \rightarrow M_n^{p-1} / M_n \rightarrow M_n^{p-1} / M_n^{p-1} 
\]

\[ \rightarrow 1. \]

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

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

\[ \text{Ker}(1 - \sigma) \subseteq M_1 \cap M_n^{p-1} / M_1 \cap M_n. \]

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

(b) Case \( n < p \). So \( M_{n-1} \cong (\mathbb{Z}/p\mathbb{Z})^{n-1} \) (Theorem 4.1 applied to \( M_{n-1} = M_1^{1-\sigma} \)); but the relation \( \nu = (1-\sigma)r-1 - p \cdot A(\sigma) \) leads to \( M_n^\nu = M_1^{(1-\sigma)r-1 - p \cdot A(\sigma)} = M_n^p \) because \( M_n^{(1-\sigma)r-1} = 1 \); since \( M_n^\nu = M_1 \), we get \( M_n^p = M_1 \) and necessarily
\[
M_n \cong (\mathbb{Z}/p^2\mathbb{Z}) \bigoplus (\mathbb{Z}/p\mathbb{Z})^{n-2}.
\]
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 \( 1 \rightarrow M_1/M_1 \cap M_n^p \rightarrow M_n/M_n^p \rightarrow M_{n-1}/M_{n-1}^p \rightarrow 1 \), 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, \( (M_1)_j = M_j \) for \( j \leq i \); so we can apply Theorem 4.1 to \( M_{n-1} \). Lemma 4.3 shows that the \( p \)-rank of \( M_1 \) is larger than (or equal to) that of \( M_{n-1} \); as the \( p \)-rank of a group is a decreasing function of \( k \), Lemma 4.3 and the above remark show that for \( k \leq \left\lfloor \frac{n-1}{p-1} \right\rfloor \), the \( p \)-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 \( a' = \left\lfloor \frac{n-1}{p-1} \right\rfloor \)).

The exact sequence of Lemma 4.3 shows a priori three possibilities:

\begin{itemize}
  \item[(α)] Case \( b' = 0 \). Necessarily, \( R_{a'+1}(M_n) = 1 \) and \( R_{a'+1}(M_{n-1}) = 0 \).
  \item[(β)] Case \( b' > 0 \) and \( R_{a'+1}(M_n) = R_{a'+1}(M_{n-1}) + 1 \).
  \item[(γ)] Case \( b' > 0 \) and \( R_{a'+1}(M_n) = R_{a'+1}(M_{n-1}) \) and \( R_{a'+2}(M_n) = 1 \).
\end{itemize}

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

This finishes a particular case of structure when \( M_{pK/k} \) is not specified. Of course, we have \( M_{pK/k} \subseteq M_1 \) and when \( \#M_1 = p \), we have \( \#M_{pK/k} = 1 \) 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 \( M = \mathcal{G}_K^+ \) in \( K/k \) cyclic of degree \( p \). Many cases are possible: If the transfer map \( j_{K/k} \) is injective then \( (\mathcal{G}_K^+)_{pK/k} \cong N_{K/k}(\mathcal{G}_K^+) \).

The map \( N_{K/k} \) 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 \( N_{K/k}(\mathcal{G}_K^+) = \mathcal{G}_K^+ \).

The transfer map may be non-injective while \( N_{K/k} \) is surjective, which causes more intricate theoretical calculations. But as we know, if \( N_{K/k} \) 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 \( \#M_1 = \frac{\#\mathcal{G}_K^+}{p} \)) and more generally \( \#(M_{i+1}/M_i) = \frac{\#\mathcal{G}_K^+}{p \cdot \#N(M_i)} \), which can be carried out in the same way).
We suppose that $K/k$ is ramified at some prime ideals $p_1, \ldots, p_t$ of $k$ ($t \geq 1$). We make no assumptions about $\#M_1$ and $M^{e_{K/k}}$. With the previous notations and definitions, we then have the simplified formulas (23) for which the submodule $H$ is an element $M_{i} =: \sigma_K(I_i)$ of the filtration of $M$:

$$\#(\mathcal{O}_K^{+}/M_i)^G = \#(M_{i+1}/M_i) = \frac{\#\mathcal{O}_K^{+} \cdot \prod_{p \in \mathcal{P}_{K/k} \cup \mathcal{P}_p} \varepsilon_p}{[K : k] \cdot \#N(M_i) \cdot (\Lambda_i : \Lambda_i \cap N(K^x))},$$

where $\Lambda_i = \{x_i \in K^{\times}, (x_i) \in N(I_i)\}$. If $p > 2$ one can use the ordinary sense and remove the mention $\varepsilon$ in all the forthcoming expressions.

(i) Computation of $M_1 = M^G$ from $M_0 = 1$, which means that $I_0 = 1$, hence $N(M_0) = 1$ and $\Lambda_0 = \{x_0 \in k^{\times}, (x_0) \in N(1)\} = E_k^+$, giving the following expression where we have put $(E_k^+: E_k^+ \cap N(K^x)) =: p_0$:

$$\#(M_1/M_0) = \#\mathcal{O}_K^{+G} = \frac{\#\mathcal{O}_K^{+} \cdot p_1^{-1}}{(\Lambda_0 : \Lambda_0 \cap N(K^x))}$$

$$=: \frac{\#\mathcal{O}_K^{+} \cdot p_1^{-1}}{(\Lambda_0 : \Lambda_0 \cap N(K^x))}.$$  

First we remark that we have the isomorphism:

$$\mathcal{O}_K^{+G}/\sigma_K(I_0^G) \simeq E_k^+ \cap N(K^x)/N(E_k^+),$$

which shows how to obtain $M_1 = \mathcal{O}_K^{+G}$ from $\sigma_K(I_0^G)$ (called the group of strongly ambiguous classes) and global normic computations with units of $k$. But the group $N(E_k^+)$ is not effective and we must proceed otherwise. In other words, the group of strongly ambiguous classes $\sigma_K(I_0^G)$ is not a “local” invariant, contrary to $\mathcal{O}_K^{+G}$.

So in the first step (which is a bit particular since $I_0 = 1$ 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 $(x_0) = N(y_1) = (1), y_1 \in K^{\times}$, which yields $(y_1) \cdot \mathfrak{a}_1^{1-\sigma} = 1$, where $\mathfrak{a}_1$ is defined up to an invariant ideal, so that $I_1$ contains at least such non-invariants ideals $\mathfrak{a}_1^1, \ldots, \mathfrak{a}_1^r$, and invariant ideals (in which are ideals $\mathfrak{a}^s, \ldots, \mathfrak{a}^s$, generating $\mathcal{O}_K^{+}$, extended to $K$, and ramified prime ideals $\mathfrak{p}_1^1, \ldots, \mathfrak{p}_1^t$).

Reciprocally, if $\sigma_K(I_0^G) \in M_1$, there exists $y_1 \in K^{\times}$ such that $(y_1) \cdot \mathfrak{a}_1^{1-\sigma} = (1)$, giving $N(y_1) = x_0 \in \Lambda_0$.

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

$$I_1 = \{\mathfrak{a}_1^1, \ldots, \mathfrak{a}_1^r ; (\mathfrak{a}_1), \ldots, (\mathfrak{a}_s) ; \mathfrak{p}_1^1, \ldots, \mathfrak{p}_1^t\}. $$

This gives $N(M_1)$ by means of the computation, in $\mathcal{O}_k^{+}$, of $N(I_1)$. $M_1$ does not need to be computed as a subgroup of $\mathcal{O}_K^{+}$, then, with $\Lambda_1 = \{x_1 \in K^{\times}, (x_1) \in N(I_1)\}$:

$$\#(M_2/M_1) = \frac{\#\mathcal{O}_K^{+} \cdot p_1^{-1}}{\#N(M_1) \cdot (\Lambda_1 : \Lambda_1 \cap N(K^x))}$$

$$=: \frac{\#\mathcal{O}_K^{+} \cdot p_1^{-1}}{\#N(M_1) \cdot (\Lambda_1 : \Lambda_1 \cap N(K^x))}.$$  

Remark 4.6. The $p$-group class $\mathcal{O}_K^{+}$ is equal to the group of ambiguous classes if and only if $\sigma_K(N(I_1)) = \mathcal{O}_K^{+}$ & $\delta_1 = t - 1$. If $\mathcal{O}_K^{+} = 1$, the group $\Lambda_1$ is easily obtained from $N(I_1) \subset P_k^+$, whence the computation of $\delta_1$; since $I_1$ only depends on $E_k^+ \cap N(K^x)$ and the ramification in $K/k$, we can hope to characterize the fields $K$ fulfilling these conditions.

(ii) For the computation of $I_2$, we process from the elements of $\Lambda_1$ which are norms of some $y_2 \in K^{\times}$ and the analogous fact that if $x_1 \in \Lambda_1$ is norm, then $(x_1) = N(y_2) = N(\mathfrak{b}_1), \mathfrak{b}_1 \in I_1, y_2 \in K^{\times}$, hence there exists $\mathfrak{a}_2 \in I_K$ such that $\mathfrak{b}_1 = (y_2) \cdot \mathfrak{a}_2^{1-\sigma}$.

Reciprocally, let $h_2 = \sigma_K(\mathfrak{a}_2^t) \in M_2$ for some $\mathfrak{a}_2^t \in I_K$; since $h_2^{1-\sigma} \in M_1$, there exists $y_2 \in K^{\times}$ such that $(y_2) \cdot \mathfrak{a}_2^{1-\sigma} = \mathfrak{a}_2^t \in I_1$, hence $N(\mathfrak{a}_2^t) = N(y_2) =: (x_1)$,
Let \( x \in \Lambda_1 \) (since for all \( i, E_i^+ \subseteq \Lambda_i \) and invariant ideals are in \( T_i \), the choices of \( x_2 \) and \( \mathfrak{A}_2^+ \) do not matter). Then these ideals of the form \( \mathfrak{A}_1^1, \ldots, \mathfrak{A}_2^2 \) must be added to \( T_1 \) to create \( T_2 \):

\[
T_2 = \{ \mathfrak{A}_1^1, \ldots, \mathfrak{A}_1^m ; \mathfrak{A}_2^1, \ldots, \mathfrak{A}_2^2 ; (a^1), \ldots, (a^s) ; \mathfrak{Y}_1^1, \ldots, \mathfrak{Y}_m^1 \},
\]

whence \( N(M_2) \) and

\[
\Lambda_2 = \{ x_2 \in k^+, \ (x_2) \in N(T_2) \},
\]

and so on. Hence, the algorithm is very systematic and the use of normic symbols (of computation of Hasse symbols, see the Remark 4.7 below; otherwise use Hilbert symbols \((x, \alpha)_p\) by adjunction to \( k \) of a primitive \( p \)th roots of unity \( \zeta_p \) to obtain the Kummer extension

\[
K' := K(\zeta_p) =: k'(\sqrt[5]{\alpha}), \ \alpha \in k'^\times,
\]

over \( k' := k(\zeta_p) \), and use the obvious Galois structure in \( K'/k'/k \) for the radical \( \alpha \) 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 \( \delta_i \), may be introduced in the general formula to give:

\[
\#(M_{i+1}/M_i) = \#Q^+_k/\#(N(M_i)) \cdot p^{i-1-\delta_i},
\]

with increasing \( \delta_i \) up to the value \( i = n \) giving \( \delta_i = t - 1 \) and \( \#N(M_i) = \#Q^+_k \).

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 \( \zeta_p \) and for particular \( \alpha \) (essentially \( k = \mathbb{Q}(\zeta_5) \) and \( K = k(\sqrt[5]{\alpha}) \) 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 \( \mathcal{Z}_5 \)-extension of \( k \).

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

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

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

\( (\alpha) \ p \in P_{\infty} \) (real infinite place). We have \((x, K/k)_p = (K/k)_p^{v_p(x)}(\mathfrak{M})\), where \( v_p(x) = 0 \) (resp. 1) if \( \sigma_p(x) > 0 \) (resp. \( \sigma_p(x) < 0 \)).

\( (\beta) \ p \in P_0 \setminus T \). Similarly, since \( p \) is unramified, we have \((x, K/k)_p = (K/k)_p^{v_p(x)}\).

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

\( (i) \ x'x^{-1} \equiv 1 \pmod{p^{m_p}} \),

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

\( (iii) \ \sigma_p(x') > 0 \) for each infinite place \( p' \in P_{\infty} \), complexified in \( K/k \).

Then, by the product formula, we have \((x', K/k)_p = \prod_{p' \in T, p' \neq p} (x', K/k)_{p'}^{-1} \) and since \((x', K/k)_p = (x', K/k)_p^{v_p(x')}\) by (i) and the definition of the local \( p \)-conductor of \( K/k \), we have \((x, K/k)_p = \prod_{p' \in T, p' \neq p} (x', K/k)_{p'}^{-1} \); let us compute the symbols occurring in the right hand side:
The following result gives, when the left to the reader.

\[ \kappa \]

exist in the non-cyclic case; so this involves more deep invariants as the knot group \( \kappa \) and the condition

\[ S \]

is coherent with the fact that the genera field \( H \) (i)

\[ H \]

characterized from the Chevalley’s formula (28) and gives:

\[ 4.5. \]

One can find numerical computations, densities results, notions of “governing fields” and heuristic principles in many papers like [Gr3], [Mo1], [Mo2], [St2], [W1], [Y2], [Ge4], etc. We think that the local framework given by the algorithm may confirm these heuristic results since normic symbols are independent (up to the product formula) and take uniformly all values with standard probabilities.

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

\[ \frac{\# \Omega_{K}^{+} \cdot \prod_{p \in \mathcal{P}_{0,k,0}} e_{p}}{[K : k] \left( E_{k}^{+} : E_{k}^{+} \cap N(K^{\times}) \right) \prod_{p \in \mathcal{P}_{0,k,0}} e_{p}} = \frac{\# \Omega_{K}^{+} \cdot \prod_{p \in \mathcal{P}_{0,k,0}} e_{p}}{[K : k] \left( E_{k}^{+} : E_{k}^{+} \cap N(K^{\times}) \right) \prod_{p \in \mathcal{P}_{0,k,0}} e_{p}} = 1, \]

which leads to the two conditions \( H_{k}^{+} \subseteq K \) \& \( (E_{k}^{+} : E_{k}^{+} \cap N(K^{\times})) \) 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 characterisation of the condition \( \Omega_{K}^{+} = 1 \) 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 \( \kappa \) and the \( p \)-central class field \( C_{K/k}^{S} \) (i.e., the largest subextension of \( H_{K/k}^{S} \) of \( K \)), Galois over \( k \), such that \( \text{Gal}(C_{K/k}^{S}/K) \) is contained in the center of \( \text{Gal}(C_{K/k}^{S}/K) \).

\textbf{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 \( \Omega_{K}^{S} \) be the \( p \)-Sylow subgroup of the \( S \)-class group of \( K \). Then \( \Omega_{K}^{S} = 1 \) 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) \( (E_{k}^{S} : E_{k}^{S} \cap N_{K/k}(J_{K})) = \frac{\prod_{p \in S} e^{ab}_{p} \times \prod_{p \in S} f^{ab}_{p}}{[K^{ab} : H_{k}^{S}]} \) where \( e^{ab}_{p} \) (resp. \( f^{ab}_{p} \)) is the ramification index (resp. the residue degree) of the place \( p \) of \( k \) in the maximal subextension \( K^{ab} \) of \( K \), Abelian over \( k \),

(iii) \( \# \kappa = (E_{k}^{S} \cap N_{K/k}(J_{K}) : E_{k}^{S} \cap N_{K/k}(K^{\times})) \), where the knot group \( \kappa \) is by definition \( k^{\times} \cap N_{K/k}(J_{K})/N_{K/k}(K^{\times}) \).
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 $X_G^S = 1$ if and only if $X_G^S = I_G \cdot X_K^S$, 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, $H_0(G, \mathcal{A}_K^S)$ and $H^0(G, \mathcal{A}_K^S)$ have the same order, we obtain the relation $(\mathcal{A}_K^S : I_G \cdot \mathcal{A}_K^S) = \#(\mathcal{A}_K^S)^G$, which means that $\left[C_{K/k}^S : K\right] = \#(\mathcal{A}_K^S)^G$; thus we recover the condition by using the classical fixed point theorem for finite $p$-groups. From the formula giving $\left[C_{K/k}^S : K\right]$ (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 [Ka]; 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 $\prod_{\mathfrak{p} \not\in P_k} e_{\mathfrak{p}} = [K^{ab} : \mathbb{Q}]$, 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 simplify, 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 genus 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 [lw] giving for instance (under the nullity of the $\mu$-invariant) Kidâ’s formula for the $\lambda$-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 $K_\infty/k_\infty$ where $k_\infty$ and $K_\infty$ are the cyclotomic $\mathbb{Z}_p$-extensions of $k$ and $K$, respectively (see various approaches in [lw, Ki, Sin]). For instance, when $K/k$ is cyclic of degree $p$ one gets for the whole $\lambda$-invariants, assuming $K \cap k_\infty = k$ ([lw Theorem 6 (1981)]):

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

where $w$ ranges over all non-$p$-places of $K_\infty$, where $p^{\lambda(G, E_{K_\infty})}$ is the Herbrand quotient $H^2(G, E_{K_\infty})$ of the group $E_{K_\infty}$ of units of $K_\infty$ (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 $K_\infty/k_\infty$.

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 $\mathbb{Q}^{ab}$, 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 $G^{ab} := \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$.

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

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

The ring $R_\chi$ 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 $R_\chi = \mathbb{Z}_p[\xi_d, \xi_{p^n}] = \mathbb{Z}_p[\xi_d][\xi_{p^n}]$, where $\xi_d$ and $\xi_{p^n}$ are primitive $d$th and $p^n$th 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 $p-1$ and $p^{n-1}$, 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 $\mathcal{X} = \mathcal{X}_0 \cup \mathcal{X}_p$ since for any $\chi \in \mathcal{X}$ and $\psi \mid \chi$, we have the unique factorization $\psi = \psi_0 \cdot \psi_p$ where $\psi_0$ is of order prime to $p$ and $\psi_p$ 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 $\chi_p$ is also the $\mathbb{Q}$-irreducible character deduced from $\psi_p$ since $\mathbb{Q}$-conjugates and $\mathbb{Q}_p$-conjugates of $\psi_p$ 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 $\chi$ is even (resp. odd) if $\psi(s_{-1}) = 1$ (resp. $\psi(s_{-1}) = -1$), where $s_{-1}$ is the complex conjugation. We denote by $\mathcal{X}_0^\pm$, $\mathcal{X}_p^\pm$ the corresponding sets of even or odd characters (note that since $p \neq 2$, $\mathcal{X}_p = \mathcal{X}_p^\pm$).

For any subfield $K$ of $\mathbb{Q}^{ab}$ 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 $\text{Gal}(\mathbb{Q}^{ab}/K) \subseteq \text{Ker}(\chi)$ or $k_\chi \subseteq K$).

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

Let $\chi \in \mathcal{X}$.

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

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

$$\mathcal{O}_{\chi_0} := \mathcal{O}_{k_{\chi_0}}^{e_{\chi_0}}.$$ 

(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 $k_\chi$ such that $[k_\chi : k'] = p$ (we have $k' = k_{\chi_0}$ only if $\chi_p$ is of order $p$); thus the arithmetical norm $N_{k_\chi/k'}$ induces the following exact sequence of $R_{\chi_0}$-modules defining $\mathcal{O}_\chi$:

$$1 \to \mathcal{O}_\chi \to \mathcal{O}_{k_{\chi_0}}^{N_{k_{\chi_0}/k'}} \to \mathcal{O}_{k'}^{e_{\chi_0}} \to 1,$$

the surjectivity being obvious because $k_\chi$ is the direct compositum over $\mathbb{Q}$ of $k_{\chi_0}$ and $k_{\chi_p}$ which is a cyclic $p$-extension of $\mathbb{Q}$, thus totally ramified at least for a prime.
number, whence $k_\chi/k'$ ramified. Since $\mathcal{O}_\chi$ is annihilated by $e_\chi_0$ and by $N_{k_\chi/k'}$, which corresponds to $1 + \sigma + \cdots + \sigma^{p-1}$ in the group algebra of $\text{Gal}(k_\chi/k') = \langle \sigma \rangle$, $\mathcal{O}_\chi$ is canonically a $R_\chi$-module (and not only a $R_{\chi_0}$-module).

This defines, by an obvious induction in $k_\chi/k_{\chi_0}$, the universal family of components $\mathcal{O}_\chi$ for all $\chi \in \mathcal{X}$ for which we have the following formulas for any cyclic extension $K/Q$ of degree $d \cdot p^n$, $p \nmid d$, $n \geq 0$:

$$\#\mathcal{O}_K = \prod_{\chi_0 \in \mathcal{X}_{K,0}} \#\mathcal{O}_K^{\chi_0},$$

$$\#\mathcal{O}_K^{\chi_0} = \prod_{i=0}^n \#\mathcal{O}_{\chi_i}, \quad \forall \chi_0 \in \mathcal{X}_{K,0},$$

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

We denote by $\omega$, of order $p - 1$, the Teichmüller character for $p > 2$; we have $k_\omega = \mathbb{Q}(\zeta_p)$ where $\zeta_p$ is a primitive $p$th root of unity and by definition $\omega : (\zeta_p \rightarrow \zeta_p^a) \equiv a (\mod p)$ 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 $\mathcal{O}_K^\chi$, hence with odd characters.

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

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

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

For instance, $\mathcal{O}_\chi$ is $R_\chi$-monogenic if and only if $e = 1$.

**5.3. Definition of admissible sets of prime numbers.** Still for $p \neq 2$ and $\chi_0 \in \mathcal{X}^\chi$, $\chi_0 \neq \omega$, consider the cyclic field $k := k_{\chi_0}$ for which $\mathcal{O}_{\chi_0} = \mathcal{O}_k^{\chi_0}$, where $\epsilon_{\chi_0} = \frac{1}{(1 + \chi_0) s_{\chi_0}(s^{-1}) s} \sum_{s \in \text{Gal}(k_{\chi_0}/\mathbb{Q})} \chi_0(s^{-1}) s$. We intend to apply the previous sections of this paper on genera theory to obtain informations on the structure of $\mathcal{O}_{\chi_0}$.

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

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

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

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

(iii) The character $\varphi \in \Phi_S$ is said to be $\chi_0$-admissible if $b_{\chi_0,\varphi} = \mathfrak{M}_{\chi_0,\varphi}^t$ (see Theorem 5.11 for the definition of $b_{\chi_0,\varphi}$). By extension we say that $S \in \mathcal{S}_t$ is $\chi_0$-admissible if there exists at least a $\chi_0$-admissible character $\varphi \in \Phi_S$.

(iv) Let $r_{\chi_0}$ be the $R_{\chi_0}/R_{\chi_0}$-dimension of $\mathcal{O}_{\chi_0}/\mathcal{O}_{\chi_0}^p$.

So the number $t$ is known from the computation of a Bernoulli number depending on $\varphi$ and it is not difficult to find $\chi_0$-admissible characters $\varphi$. 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 \( S = \{ \ell_1, \ldots, \ell_t \} \in S_t \) be a \( \chi_0 \)-admissible set; then for \( i = 1, \ldots, t \), let \( \ell_i \) be a prime ideal of \( k \) above \( \ell_i \), and let \( h_i := e_{\ell_i}(\ell_i)^{\chi_0} \) be the image of \( e_{\ell_i}(\ell_i) \) in \( \mathcal{O}^{\chi_0}_k \).
Then \( \mathcal{O}_{\chi_0} \) is the \( R_{\chi_0} \)-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 \( r_{\chi_0} \).

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

\[
\begin{array}{c}
k_{\varphi} \\
\downarrow \\
K = k_{\chi_0 \cdot \varphi} \\
\downarrow \\
G \simeq \mathbb{Z}/p\mathbb{Z} \\
\downarrow \\
k = k_{\chi_0} \\
\downarrow \\
d, p|d \\
\end{array}
\]

We consider the \( G \)-module \( M = \mathcal{O}^{\chi_0}_k \) as a component of the relative class group \( \mathcal{O}^{\chi_0}_K \); in other words, a semi-simple component of the \( p \)-class group of \( K \), since from \( \mathcal{O}^{\chi_0}_K = \bigoplus_{\chi_0 \in \mathcal{X}_0^-} \mathcal{O}^{\chi_0}_K \) we have selected \( \chi_0 \in \mathcal{X}_0^- \) and the associated filtration with characters of \( M = \mathcal{O}^{\chi_0}_k \) for which \( M_1 = M^G = (\mathcal{O}^{\chi_0}_K)^{\chi_0} \), \( G := \text{Gal}(K/k) \simeq \mathbb{Z}/p\mathbb{Z} \) (see [Gr12 (1978)]).

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

Lemma 5.4. The extension \( j_{K/k}: \mathcal{O}^{\chi_0}_k \rightarrow \mathcal{O}^{\chi_0}_K \) is injective.

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

Lemma 5.5. We have \( M_1 = j_{K/k}(\mathcal{O}^{\chi_0}_k) \cdot (H_1, \ldots, H_t)_{R_{\chi_0}} \) and \( M_1/j_{K/k}(\mathcal{O}^{\chi_0}_k) \simeq (R_{\chi_0}/p R_{\chi_0})^t \).

This expression giving \( #M_1 = #\mathcal{O}^{\chi_0}_k \cdot p^{-f_{\chi_0}}, \) where \( f_{\chi_0} \) is the residue degree of \( p \) in \( Q(\xi_d)/Q \), is nothing else than the \( \chi_0 \)-Chevalley’s formula in \( K/k \) for an odd character \( \chi_0 \) (cf. [Gr12]).

Lemma 5.6. The character \( \varphi \in \Phi_S \) is \( \chi_0 \)-admissible if and only if \( M = M_1 \) (in other words, if and only if there are no exceptional \( \chi_0 \)-classes).

Thus, since \( \mathcal{O}^{\chi_0}_k = \mathcal{O}^{\chi_0}_{e_{\chi_0} \varphi} \), we get \( #M = \#\mathcal{O}^{\chi_0}_k = \#\mathcal{O}^{\chi_0}_{\chi_0} \cdot \#(\chi_0 \cdot \varphi) \) from formula (37) with \( n = 1 \). From Theorem 5.1 we have \( M = M_1 \) if and only if \( b_{\chi_0 \cdot \varphi} = M^{t_1}_{\chi_0 \cdot \varphi} \) (\( \chi_0 \)-admissibility). From the lemmas we get \( N_{K/k}(M) = N_{K/k}(M_1) \), hence \( \mathcal{O}^{\chi_0}_{\chi_0} = \mathcal{O}^{\chi_0}_{\varphi} \cdot (h_1, \ldots, h_t)_{R_{\chi_0}}, \) whence \( \mathcal{O}^{\chi_0}_{\chi_0} = (h_1, \ldots, h_t)_{R_{\chi_0}} \).

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 \( K \):

\[
\text{St}(K) := \sum_{a=1}^{n} \left( \frac{K/Q}{a} \right)^{-1} \left( \frac{a}{m} - \frac{1}{2} \right) \in \text{Gal}(K/Q),
\]

where \( m \) is the conductor of \( K \) and \( \left( \frac{K/Q}{a} \right) \) the Artin symbol (for \( \text{gcd}(a, m) = 1 \)).

For more details see [Gr11] where it is also proved that admissible sets have a nontrivial Chebotarev density leading to the effectiveness of the determination 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-monomogenic \( \mathcal{O}_K^{x_0} \) as \( R_{x_0} \)-modules. For instance, let \( k = \mathbb{Q} \left( \sqrt{-541 (37 + 6 \sqrt{37})} \right) \) (quartic cyclic over \( \mathbb{Q} \)) and \( p = 5 \); there exist two \( 5 \)-adic characters \( \chi_0 \) and \( \chi'_0 \) for which \( \mathcal{O}_k^{x_0} \simeq R_{x_0}/(2 - i)R_{x_0} \bigoplus R_{x_0}/(2 - i)R_{x_0} \) and \( \chi_0^{x_0} = 1 \) (a rare example of non-monomogenic \( \mathcal{O}_k^{x_0} \)). See [Ber] for numerical tables where the case of even characters \( \chi_0 \) 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 \( T_{k,p} \), 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 \( H_{k,p}^{\text{pra}} \) in the following schema:

\[
\begin{array}{c}
\text{k} \\
\downarrow \\
\text{H}_{k,p}^{\text{ord}} \\
\downarrow \\
\text{H}_{k,p}^{\text{pra}} \\
\end{array}
\]

where \( \tilde{k} \) is the compositum of the \( \mathbb{Z}_p \)-extensions of \( k \), \( H_{k,p}^{\text{ord}} \) the \( p \)-Hilbert class field, and \( H_{k,p}^{\text{pra}} \) is the \( p \)-class group of \( k \) (ordinary sense).

This finite group \( T_{k,p} \), 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 \( T_{k,p} \)) 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 \( T_{k,p} \) are more canonical (especially in any \( p \)-extensions \( K/k \) of Galois group \( G \)) with an explicit formula for \( \# T_{k,p}^G \) 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 [Mon]; \( T_{k,p} \) contains any deep information on class groups and units (using, for instance, reflection theorems to connect \( T_{k,p} \) and \( \mathcal{O}_{k,p}^{\text{pl}} \) when \( k \) contains the \( p \)th 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 \( T_{k,p} = 1 \) (fundamental notion called \( p \)-rationality of \( k \); see [Gr2, Theorem III.4.2.5]).

Moreover the properties of the \( T_{k,p} \) 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], [Mon]). In a similar context, in connection with Gross’s conjecture [FG], mention the logarithmic class group introduced by J-F. Jaulent ([Ja3], [Sa]) governing the \( p \)-Hilbert kernel and the \( p \)-regular kernel.

The main property concerning these groups \( T_{k,p} \) is that, under the Leopoldt conjecture for \( p \) in \( K/k \) (even if \( K/k \) is not Galois), the transfer map \( j_{K/k} : T_{k,p} \rightarrow T_{k,p} \) (corresponding as usual to extension of ideals in a broad sense) is \( \text{injective} \) [Gr2, Theorem IV.2.1] contrary to the case of \( p \)-class groups. Furthermore, the property of \( p \)-rationality we have mentioned above, has important consequences as is shown.
by Galois representations theory (e.g., \cite{Gr1} (2016)) or conjectural and heuristic aspects (e.g., \cite{Gr10} (2016)).

So we intend to make much advertise for these $T_{k,p}$ 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

\cite{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).

\cite{ATZ1} Azizi, A., Taous, M., Zekhnini, A., *Coclass of Gal$(k^2_3/k)$ for some fields $k = \mathbb{Q}(\sqrt{p_1 p_2 q}, \sqrt{-1})$ 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

\cite{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

\cite{Bau} Bauer, H., *Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilen*, J. Reine Angew. Math. 248 (1971), 42–46.

\cite{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

\cite{Bo} Bölling, R., *On $p$-class groups of cyclic extensions of prime degree $p$ of quadratic fields*, Mathematika 36, 1 (1989), 269–353.

\cite{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_1933_2/THESE_1933_2_365-476.pdf

\cite{Ch2} Chevalley, C., *La théorie du corps de classes, Ann. of Math. II, 41 (1940), 384–418. http://www.matwbn.icm.edu.pl/ksiazki/aa/aa60/aa6013.pdf

\cite{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.

\cite{FG} Federer, L.J., Gross, B.H, *Regulators and Iwasawa modules* (with an appendix by W. Sinnott, Invent. Math. 62, 3 (1981), 443–457.

\cite{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

\cite{Fr} Fröhlich, A. *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics 24, Amer. Math. Soc. 1983.

\cite{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-GeffII.pdf

\cite{Ge2} Gerth III, F., *On $p$-class groups of cyclic extensions of prime degree $p$ of number fields*, Acta Arithmetica 64, 1 (1993), 1–48. http://matwbn.icm.edu.pl/ksiazki/aa/aa60/aa6003.pdf

\cite{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

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

\cite{GK1} Greither, C., Kučera, R., *Eigenspaces of the ideal class group*, Annales Institut Fourier 64, 5 (2014), 2165–2203. https://www.researchgate.net/publication/268369796

\cite{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

\cite{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

\cite{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://dx.doi.org/10.1007/s10114-006-024-2

\cite{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

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

\cite{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):
[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_0.pdf

[Gr4] 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_0.pdf

[Gr5] Gras, G., No general Riemann–Hurwitz formula for relative p-class groups, Journal of Number Theory 171 (2017), 213–226. https://www.researchgate.net/publication/288060881

[Gr7] Gras, G., Complete table concerning the paper: No general Riemann–Hurwitz formula for relative p-class groups (2016) https://www.researchgate.net/publication/304059327

[Gr8] 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

[Gr9] Gras, G., Logarithme p-adique et groupes de Galois, J. reine angew. Math. 343 (1983), 64–80. https://www.researchgate.net/publication/23881752

[Gr10] Gras, G., Remarks on K2 of number fields, J. Number Theory 23 (1986), 322–335. https://www.researchgate.net/publication/243002782

[Gr11] 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

[Gr12] 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_0.pdf

[Gr13] Gras, G., Principalisations d’idéaux par extensions absolument abéliennes, J. Number Theory 62 (1997), 403–421. http://www.sciencedirect.com/science/article/pii/S0022314X97020680

[Gr14] Gras, G., Etude d’invariants relatifs aux groupes des classes des corps abéliens, In: Astérisque 41/42, Société 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] Greenberg, 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_0/JTNB_2000_12_1_219_0.pdf

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

[GW3] Greenberg, 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 loi de réciprocité, Mémoire des Sciences Mathématiques, Fasc. LXXV, Gauthier-Villars, Paris 1936. http://gallica.bnf.fr/ark:/12148/bpt6k39024r/f9.image

[HL] Harnoowong, 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
[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: 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.pdf

[So] Soriano, F., Classes logarithmiques ambigues 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 GAGNÉRIE, F–38520 LE BOURG D’OISANS.

Email address: g.mn.gras@wanadoo.fr url http://www.researchgate.net/profile/Georges_Gras