UNIVERSITÀ DELLA CALABRIA

Dipartimento di Matematica e Informatica

Scuola di Dottorato ISIMR - Matematica e Informatica

XXV CICLO

Capitulation and Stabilization in various aspects of Iwasawa Theory for $\mathbb{Z}_p$-extensions

S.S.D. MAT/02 – ALGEBRA

Supervisore Dott. Andrea Bandini

Firma

Direttore Prof. Nicola Leone

Firma

Dottorando Dott. Fabio Caldarola

Firma

A.A. 2012 – 2013

Acknowledgements

First, I would like to express my sincere gratitude to my advisor, Dr. Andrea Bandini, for his guidance, his many valuable discussions, and helpful advices and encouragements.
I also want to tank Professor Jozef van Bon and Professor Nicola Leone for their support during my PhD course.
Moreover, it is a pleasure to thank Dr. Gianluigi Sechi for giving me the opportunity to attend the “Sardinian Summer School in Iwasawa Theory” in August 2012 and similarly to Professor Otmar Venjakob and Dr. Thanasis Bouganis for the opportunity to partecipate to “Iwasawa-2012” and its preparatory lecture series. I thank Satoshi Fujii for some very interesting discussions and suggestions. I also would like to thank many other people at the University of Calabria and my friends who I have been close in recent years, but they are too many to mention.

A very special thank you, I want to direct to my mother for all that I can thank. A special thought and a special thanks to my grandmother Lina who I always keep in my heart and to my grandfather Roberto who particularly liked mathematics. To them and to my mother I dedicate this my little work.

Introduction

Iwasawa Theory has been one of the richest areas of research in number theory in the last half century. Before going into the details of this thesis we provide a quick overview of the development of the theory and of its main features (for a very nice survey on the subject see [15]).

The theory was initiated by Kenkichi Iwasawa in the late 50's with the study of the cyclotomic $\mathbb{Z}_p$-extensions $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$, i.e., the field obtained adding all p-power roots of unity to $\mathbb{Q}$. The study of cyclotomic extensions has always been an important topic in number theory; as examples of their relevance one can think about the Kronecker-Weber theorem or at the proof of Fermat Last Theorem for regular primes. Iwasawa proposed to consider all p-power roots of unity at once and studied the infinite extension generated by them. Infinite Galois theory shows that $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \simeq \mathbb{Z}_p$ (the ring of p-adic integers, which gives the name to all this type of extensions), so Iwasawa quickly generalized his ideas to consider the whole family of $\mathbb{Z}_p$-extensions of a number field.

The main object of his research was the following: given a (general) $\mathbb{Z}_p$-extension K/k, consider its finite subextensions which form a tower

$$k = k_0 \subseteq k_1 \ldots \subseteq k_n \subseteq \ldots K = \bigcup_n k_n$$

and let $A(k_n)$ be the p-Sylow of the ideal class group of k_n. Let $X(K/k)$ be the inverse limit of the $A(k_n)$'s with respect to the natural norm maps. Studying the structure of $X(K/k)$ as a module over the ring $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$, Iwasawa was able to prove (among other things) his celebrated formula for the order of $A(k_n)$. If $|A(k_n)| = p^{e_n}$, then, for n large enough,

$$e_n = \mu(K/k)p^n + \lambda(K/k)n + \nu(K/k)$$

for some constants $\mu(K/k)$, $\lambda(K/k)$ and $\nu(K/k)$ usually called the *Iwasawa invariants* of the extension K/k (see Theorem 1.3.1).

Moreover, the well known analogy between number fields and function fields in one variable over finite fields and the results of Weil which link the zeta

function of an algebraic curve (over a finite field) to the characteristic polynomial of the Frobenius acting on its Jacobian (see for example [49]), provided good reasons for Iwasawa to imagine a similar relation for number fields: this is what he called the *Main Conjecture*.
The module $X(K/k)$ (a purely algebraic object) defines a principal *characteristic ideal* in $\Lambda \simeq \mathbb{Z}_p[[T]]$ (for a precise definition see Definition 1.2.4), call it $(f_X(T))$. Let ω be the Teichmüller character at p and let

$$e_i := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})} \omega^i \sigma^{-1}$$

be the idempotent associated to ω^i. Then the same reasoning associates to $e_i X(K/k)$ a characteristic polynomial $f_{e_i X}(T)$. On the other hand Iwasawa (and, before him, Kubota and Leopoldt, see [25]) used distributions on the rings $\mathbb{Z}_p[\mathrm{Gal}(k_n/k)]$ to define a measure as a limit of those distributions and, associated to that measure, a p-adic L-function $L_p(s, \omega^i)$ (an analytic object). This function can be pushed to Λ to define a series $\mathcal{L}(T, \omega^i)$. The Main Conjecture asserts (roughly speaking) the equality between the ideals generated by $f_{e_{1-i}X}(T)$ and the one generated by $\mathcal{L}(T, \omega^{1-i})$ for any odd i with $3 \leqslant i \leqslant p-2$.
Instances of the Main Conjecture have been proved for the $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{Q}(\mu_p)$ by Iwasawa himself for regular primes p (see [17]) and by B. Mazur and A. Wiles for every prime p (see [32]). Today there are many more formulations of the Main Conjecture and extensions to more general fields k. For instance A. Wiles proved the conjecture for totally real fields (see [50]) and K. Rubin used Kolyvagin's Euler systems to provide a simpler proof of the already known cases and some generalizations to imaginary quadratic fields (see [44] and [45]).
This beautiful link between analytic and arithmetic (or algebraic) objects lies at the heart of Iwasawa theory and has inspired many generalizations. We only mention (for its relevance) the study of Iwasawa theory for elliptic curves started by B. Mazur and others in the 70's (see [29], [30] and [31]). The Main Conjecture relating the p-adic L-function associated to some $\mathbb{Z}_p$-extensions K/k (which interpolates the L-function associated to the elliptic curve) and the characteristic ideal of the Pontrjagin dual of the Selmer group of the curve over K, has led to many results in the direction of the Birch and Swinnerton-Dyer Conjecture (see, for example, [23] and [3]).

Recently M. Ozaki (in [40]) has developed a nonabelian Iwasawa theory for number fields to study the maximal unramified (not necessarily abelian) pro-p extension $\widetilde{L}(K)$ of a $\mathbb{Z}_p$-extension K/k. The author breaks such a big Galois group into smaller pieces using the lower central series, which lead to the definition of higher Iwasawa modules $X^{(i)}(K/k)$ (the original Iwasawa module is $X^{(1)}(K/k)$ in this new setting), we refer to Section 2.1 for precise definitions and more details. The study of $\mathrm{Gal}(\widetilde{L}(K)/K)$ relates Iwasawa theory to the problem of studying the class field tower of number fields. For some examples in this direction see [35], [34], [37], [9] (and several others).

In this thesis we address some classical phenomenons of Iwasawa theory like capitulation and stabilization both in the abelian and nonabelian setting. The $A(k_n)$ come equipped with another natural map $i_{n,m} : A(k_n) \to A(k_m)$ (for any $m \geqslant n$) arising from the inclusion of ideals. The ideal classes in $H_{n,m} := \mathrm{Ker}(i_{n,m})$ are said to *capitulate* in k_m and those in $H_n := \bigcup_{m \geqslant n} H_{n,m}$ are said to capitulate in K. Capitulation is strictly connected to the finiteness of the Iwasawa module $X(K/k)$: indeed R. Greenberg has shown that

$$X(K/k) \text{ is finite (i.e., } \lambda(K/k) = \mu(K/k) = 0) \iff A(k_n) = H_n \text{ for any } n$$

(see [14] or Proposition 1.5.1).
In Theorem 3.2.4 we give a description of the $H_{n,m}$'s and the H_n's in terms of the maximal finite submodule $D(K/k)$ of $X(K/k)$. We use this description to provide stabilization properties in Theorem 3.2.9. In Iwasawa theory is quite usual for the order of modules like $A(k_n)$ to *stabilize* (i.e., to become constant) at the very first level in which it does not increase (if such a level exists), i.e.,

$$|A(k_n)| = |A(k_{n+1})| \Longrightarrow |A(k_n)| = |A(k_m)| \ \ \forall\, m \geqslant n,$$

and the same holds for the p-ranks. We show that the H_n's enjoy a similar property while the $H_{n,m}$'s do not. Encouraged by that we go on studying (and proving) stabilization properties for other related modules like the kernels of the norm maps or the cokernels of the inclusions. In Theorem 3.4.2 (resp. Theorem 3.4.4)) we show how the stabilization of orders (resp. of p-ranks) of those modules is deeply related with the vanishing of the λ-invariant (resp. the μ-invariant) of the Iwasawa module $X(K/k)$.
In the last chapter we do the same for the modules of Galois invariants and coinvariants of $A(k_n)$ (see Theorem 4.1.2).
We also tried to extend this type of results to the nonabelian setting and, in particular, to the higher Iwasawa modules $X^{(i)}(K/k)$ (or, more precisely, to the $A^{(i)}(k_n)$'s) defined by Ozaki, but we soon found an example (see Section 2.2.1) in which the starting levels $A^{(j)}(k)$ and $A^{(j)}(k_1)$ were trivial for some $j \geqslant 2$, while $A^{(j)}(k_4) \neq 0$. It turns out that to establish stabilization properties in this setting one needs more stringent hypotheses: namely stabilization for the i-th Iwasawa module requires stabilization at all the previous levels as shown in Theorem 2.2.11.

Now we give a brief overview of the contents of this thesis. In the first chapter we open with some examples and explicit calculations on cyclotomic $\mathbb{Z}_p$-extensions. In the following two sections we recall definitions, properties, some

basic theorems and classical conjectures (still open) on $\mathbb{Z}_p$ and $\mathbb{Z}_p^d$-extensions. Sections 1.4 and 1.5 introduce the phenomenons of stabilization and capitulation of ideals recalling some of the classical and/or more recent results.
Chapter 2 is devoted to nonabelian Iwasawa Theory. Section 2.1 describes Ozaki's work, establishing definitions, notations and recalling the properties and the main theorems. Section 2.2 first shows how the same type of stabilization (both for the orders and for the p-ranks) we had in the classical theory, is no longer valid in this new context. In fact, the stabilization theorems that follow require stronger assumptions.
The third chapter was the first to be completed: and its results have been presented as a contributed talk at the "28-th Journées Arithmétiques" held in Grenoble, in July 2013.
The chapter goes back to the classical case of $\mathbb{Z}_p$-extensions. After some preliminary results, in Section 3.2, we will begin a detailed study of the maximal finite submodule $D(K/k)$ of $X(K/k)$. We shall consider the sequences of the *absolute capitulation kernels* (the H_n 's) and of the *relative capitulation kernels* (the $H_{n,m}$'s) and we will get some formulas (depending on certain parameters linked to $D(K/k)$) for their sizes, which describe accurately the growth of their orders and p-ranks. Moreover we get positive answers to questions related to the stabilization of the two sequences mentioned above and, in Section 3.3, we will discuss the problem of finding bounds for the delay of capitulation. In Section 3.4 we provide several new conditions (based on the properties arising from the phenomena of stabilization and capitulation) which will be shown to be equivalent to the vanishing of the Iwasawa invariants $\lambda(K/k)$ and/or $\mu(K/k)$.
In Chapter 4 we consider Galois invariants and coinvariants of the $A(k_n)$'s. In particular, in Section 4.1, we treat inverse and direct limits for them and study stabilization and capitulation with their consequences. In Sections 4.2 and 4.3 we provide two new criterions for the finiteness of $X(K/k)$. The first is based only on the capitulation of the invariants subgroups and the second is based on the nilpotency of the Galois group $\mathrm{Gal}(L(K)/k)$ (where $L(K)$ is the maximal abelian unramified pro-p extension of K). Finally, in Section 4.5, we show two results on the vanishing of the Iwasawa μ-invariant: in particular we study the connection between the vanishing of $\mu(F_\infty/F)$ and $\mu(kF_\infty/k)$, where F_∞/F is a $\mathbb{Z}_p$-extension of a number field F and $k \supset F$ is a Galois extension of degree p, or of degree a prime q different from p.

Contents

Acknowledgements **1**

Introduction **3**

1 Classical Iwasawa Theory **9**

1.1 $\mathbb{Z}_p$-extensions 9

1.2 Multiple $\mathbb{Z}_p$-extensions and Λ_d-modules 12

1.3 Iwasawa's Theorem 15

1.4 Stabilization 17

1.5 Capitulation 18

2 Non-abelian Iwasawa Theory **20**

2.1 Introduction 20

2.2 Stabilization for the order of $X_n^{(i)}$ 25

2.2.1 Counterexample 25

2.2.2 Stabilization 26

2.3 On the p-ranks of $X_n^{(i)}$ 30

3 Stabilization and capitulation **33**

3.1 Introduction 33

3.1.1 Preliminaries 35

3.2 The maximal finite submodule 36

3.2.1 Relation between $\mathrm{rk}_p(H_n)$, $\widetilde{\lambda}_n$ and $X \sim_\Lambda 0$ 45

3.3 Bounds for $\rho(m) - \rho(n)$ 45

3.3.1 Sharpness of the bounds 48

3.4 Finiteness of the Iwasawa module 50

3.4.1 The kernel of the norm map 52

3.4.2 The cokernel of the inclusion maps 55

3.4.3 Proofs of the opening Theorems 58

4 Invariants and coinvariants **60**

4.1 Stabilization for invariants and coinvariants of A_n 60

4.2 The modules B_n and the pseudo-nullity of X (I) 65

4.3 The modules B_n and the pseudo-nullity of X (II) 68

4.4 $\mu(F_\infty/F)$ vanishes for certain families of number fields 70

4.4.1 Finite p-extensions 71

4.4.2 Galois extensions of prime degree $q \neq p$ 72

Bibliography **78**

Compendio (abstract in Italian) **83**

Chapter 1

Classical Iwasawa Theory

In this section we give a brief account of the basic facts about Iwasawa Theory for number fields. One can find more detailed treatments of the content of this chapter in the books [48], [26], [36] or in the original papers of Iwasawa [21], [20] or in [15].

1.1 $\mathbb{Z}_p$-extensions

Let p be a prime number and let k be a number field, i.e., a finite extension of $\mathbb{Q}$. We say that a Galois extension K of k is a $\mathbb{Z}_p$*-extension* if its Galois group is topologically isomorphic to $\mathbb{Z}_p$, the additive group of p-adic integers and, in this case, we denote $\mathrm{Gal}(K/k)$ by Γ. Since every closed subgroup of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ we have that, for every $n \geqslant 0$, there exist a unique subfield of K of degree p^n over k: we call it the *n-th layer* of the $\mathbb{Z}_p$-extension K/k and denote it by k_n. In other words the subfields between k and K form a tower

$$k = k_0 \subset k_1 \subset k_2 \ldots\ldots \subset k_n \subset \ldots \subset K = \bigcup_{n=0}^{\infty} k_n \ ,$$

and the Galois group $\mathrm{Gal}(k_n/k) \simeq \Gamma/\Gamma^{p^n} =: \Gamma_n$ is isomorphic to $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.
We recall other basic properties for a $\mathbb{Z}_p$-extension:

- K/k is unramified outside p;
- there exist at least a prime of k (over p) which ramifies in K/k.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ be the primes of k which ramify in K/k and let $I(\mathfrak{p}_1), I(\mathfrak{p}_2), \ldots, I(\mathfrak{p}_t)$ be their inertia groups in $\mathrm{Gal}(K/k)$. Then $I(\mathfrak{p}_i) \simeq \Gamma^{p^{n_i}}$ for some $n_i \geqslant 0$ and we define

$$n_0 = n_0(K/k) := \max\{n_i \,:\, i = 1, \ldots, t\} \ .$$

The index $n_0(K/k)$ is the minimal $n \geqslant 0$ such that every prime which ramifies in the extension K/k_n is totally ramified. Moreover we define

$$s = s(K) = s(K/k) := \text{the number of ramified prime ideals in } K/k_{n_0} \quad (1.1)$$

and

$$s(k_n) := \text{ the number of the prime ideals of } k_n \text{ which are ramified in } K/k_n \ . \quad (1.2)$$

Remark 1.1.1. We remark that, throughout the thesis, when we type "s", we always refer to definition (1.1), which is undoubtedly the most important. The notations "s" and "$s(K/k)$" are the one used originally by Iwasawa (see [20]) and they do not say anything about the number of primes in k (or k_n) lying above p (i.e., $s = 1$ means that, even if there might be several primes in k above p, only one of them is ramified in K/k). Finally, note that s=$s(k_{n_0})$.

Example 1.1.2. Let $q = p$ if p is odd and $q = 4$ if $p = 2$. For every $n \geqslant 0$, $\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q}) \simeq (\mathbb{Z}/qp^n\mathbb{Z})^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})$. Let $\mathbb{Q}_n$ be the fixed field of $(\mathbb{Z}/q\mathbb{Z})^\times$, then we have

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \ldots \subset \mathbb{Q}_n \subset \ldots \subset \mathbb{Q}_{cyc} := \bigcup_{n=0}^{\infty} \mathbb{Q}_n \ ,$$

and we call $\mathbb{Q}_{cyc}$ the *cyclotomic $\mathbb{Z}_p$-extension* of $\mathbb{Q}$. If k is any number field, then $k_{cyc} := k\mathbb{Q}_{cyc}$ is a $\mathbb{Z}_p$-extension of k and we call it the *cyclotomic $\mathbb{Z}_p$-extension* of k. Let $t \in \mathbb{N}$ be such that $\mathbb{Q}_t = k \cap \mathbb{Q}_{cyc}$, then $k_n = k\mathbb{Q}_{t+n}$ is the n-th layer of k_{cyc}/k (for all $n \geqslant 0$). This also shows that every number field k has at least a $\mathbb{Z}_p$-extension, namely the cyclotomic one.

Example 1.1.3. If $p = 2$, then the first layers of $\mathbb{Q}_{cyc}/\mathbb{Q}$ are:

- $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(X^2 - 2)$,
- $\mathbb{Q}_2 = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) \simeq \mathbb{Q}[X]/(X^4 - 4X^2 + 2)$,
- $\mathbb{Q}_3 = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right) \simeq \mathbb{Q}[X]/(X^8 - 8X^6 + 20X^4 - 16X^2 + 2)$,
- $\mathbb{Q}_4 = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}\right)$

  $\simeq \mathbb{Q}[X]/(X^{16} - 16X^{14} + 104X^{12} - 352X^{10} + 660X^8 - 672X^6 + 336X^4 - 64X^2 + 2)$.

If $p = 3$, then the first layers of $\mathbb{Q}_{cyc}/\mathbb{Q}$ are:

- $\mathbb{Q}_1 \simeq \mathbb{Q}[X]/(X^3 - 3X + 1)$,
- $\mathbb{Q}_2 \simeq \mathbb{Q}[X]/(X^9 - 9X^7 + 27X^5 - 30X^3 + 9X + 1)$.
- $\mathbb{Q}_3 \simeq \mathbb{Q}[X]/(X^{27} - 27X^{25} + 324X^{23} - 2277X^{21} + 10395X^{19} - 32319X^{17} + 69768X^{15} - 104652X^{13} + 107406X^{11} - 72930X^9 + 30888X^7 - 7371X^5 + 819X^3 - 27X + 1)$.

Other polynomials for higher indices can be found, for example, in [1]. Once a number field k is given, using a Computer Algebra System as PARI/GP or MAGMA one can easily calculate $k \cap \mathbb{Q}_{cyc}$ and consequently the n-th layer of k_{cyc}/k (if the base field k is not too large and for small values of n).

Example 1.1.4. A particular feature of the cyclotomic $\mathbb{Z}_p$-extension is that every prime of k lying over p is ramified in k_{cyc}. But it is not totally ramified in general, in fact to have $n_0 = 0$ we need some additional hypothesis. For example, it is easy to see that, if one of the following holds

(a) $[k : \mathbb{Q}] < p$;

(b) p is unramified in $k/\mathbb{Q}$;

(c) $p \nmid [k : \mathbb{Q}]$ and $k/\mathbb{Q}$ is a Galois extension,

then $n_0(k_{cyc}/k) = 0$.
To give an explicit example we show that the condition $p \nmid [k : \mathbb{Q}]$, mentioned in **(c)**, is not sufficient to guarantee that $n_0(k_{cyc}/k) = 0$.
Let $p = 2$, let α be a root of the irreducible polynomial $P(X) = X^3 + X^2 + 8 \in \mathbb{Q}[X]$ and $k = \mathbb{Q}(\alpha)$. Using PARI/GP we can find the composite of $P(X)$ with the polynomials given in the example 1.1.3, obtaining the early layers of the cyclotomic $\mathbb{Z}_2$-extension k_{cyc}/k. In particular the first layer

$$k_1 = \mathbb{Q}(\alpha, \sqrt{2}) \simeq \mathbb{Q}[X]/(X^6 - 2X^5 - 5X^4 - 8X^3 + 24X^2 - 104X + 92)\ .$$

Computing the decomposition of 2 in k and k_1, we obtain $2\mathcal{O}_k = \mathfrak{q}_0(\mathfrak{q}_0')^2$, $\mathfrak{q}_0\mathcal{O}_{k_1} = \mathfrak{q}_1^2$, $\mathfrak{q}_0'\mathcal{O}_{k_1} = \mathfrak{q}_1'\mathfrak{q}_1''$ and $2\mathcal{O}_{\mathbb{Q}_1} = \mathfrak{p}_1^2$ (where, for any field L, we denote with $\mathcal{O}_L$ its ring of integers). The situation is pictured in the following diagram

$$\begin{tikzcd}
 & k_2 \\
\mathbb{Q}_2 \arrow[ur, dash] & k_1 \arrow[u, dash] \\
\mathbb{Q}_1 \arrow[u, dash] \arrow[ur, dash] & k \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & \mathfrak{q}_2^2(\mathfrak{q}_2')^2(\mathfrak{q}_2'')^2 \\
\mathfrak{p}_2^4 \arrow[ur, dash] & \mathfrak{q}_1^2(\mathfrak{q}_1')^2(\mathfrak{q}_1'')^2 \arrow[u, dash] \\
\mathfrak{p}_1^2 \arrow[u, dash] \arrow[ur, dash] & \mathfrak{q}_0(\mathfrak{q}_0')^2 \arrow[u, dash] \\
2\mathbb{Z} \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

where the symbols $\mathfrak{p}_2$, $\mathfrak{q}_2$, $\mathfrak{q}_2'$ and $\mathfrak{q}_2''$ have an obvious meaning. We can conclude that $n_0(k_{cyc}/k) = 1$ and this yields the desired counterexample.

1.2 Multiple $\mathbb{Z}_p$-extensions and Λ_d-modules

An extension K/k is called $\mathbb{Z}_p^d$*-extension* if it is Galois and $\mathrm{Gal}(K/k)$ is topologically isomorphic to $\mathbb{Z}_p^d$ (for some $d \in \mathbb{N}$). Let k be of degree $[k : \mathbb{Q}] = r_1 + 2r_2$ (where r_1 and r_2 denote the number of real and of pairs of complex embeddings of k in $\mathbb{C}$, respectively), let K_d/K be a $\mathbb{Z}_p^d$-extension and denote by $\widetilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of k. In accordance to what we have already seen in the case $d = 1$, we have that

- K_d/k is unramified outside p ;
- there exists an integer d_k, with $r_2 + 1 \leqslant d_k \leqslant r_1 + 2r_2$, such that $\mathrm{Gal}(\widetilde{k}/k) \simeq \mathbb{Z}_p^{d_k}$;
- Leopold's Conjecture for k is equivalent to $d_k = r_2 + 1$.

Recall that Leopold's conjecture is true for abelian extension of $\mathbb{Q}$ or of a quadratic imaginary field (see [6]).
Before proceeding further, we fix some standard notations in Iwasawa theory which we will be used throughout this thesis:

- for any algebraic extension E of $\mathbb{Q}$ (of finite or infinite degree) we denote by $L(E)$ the maximal abelian unramified pro-p-extension of E (in a fixed algebraic closure of $\mathbb{Q}$) and by $X(E)$ the Galois group $\mathrm{Gal}(L(E)/E)$;
- for any number field F we denote its ideal class group by $Cl(F)$ and the p-part of it by $A(F)$;
- if K/k is a fixed $\mathbb{Z}_p$-extension of a number field k, to shorten notations, we shall indicate $L(K)$, $L(k_n)$ and $A(k_n)$ simply by L, L_n and A_n (for every $n \geqslant 0$): moreover we let $X_n := \mathrm{Gal}(L_n/k_n)$ and $X := \mathrm{Gal}(L/K)$.

With these notations the Artin map provides a canonical isomorphism $A_n \simeq X_n$ for any $n \in \mathbb{N}$. We also have canonical maps $N_{m,n} : X_m \to X_n$ and $i_{n,m} : X_n \to X_m$ (for any $m \geqslant n$) induced (respectively) by the norm and the inclusion of ideals.
For any $\mathbb{Z}_p^d$-extension K_d/k ($d \geqslant 1$) we pose $\mathcal{G}(K_d) := \mathrm{Gal}(L(K_d)/k)$ and $X(K_d) = \mathrm{Gal}(L(K_d)/K_d)$: hence $\mathcal{G}(K_d)$ is obtained by a group extension of $\mathrm{Gal}(K_d/k)$ by $X(K_d)$.
The most important (for us) feature of $X(K_d) = \mathrm{Gal}(L(K_d)/K_d)$ is that it is a $\mathbb{Z}_p$-module on which $\mathrm{Gal}(K_d/k)$ acts in a natural way via conjugation. In particular, for every $n \geqslant 0$, let k_n' be the fixed field of $(p^n\mathbb{Z}_p)^d$ (i.e.,

$\mathrm{Gal}(k'_n/k) \simeq (\mathbb{Z}_p/p^n\mathbb{Z}_p)^d$), then $X(k'_n) = \mathrm{Gal}(L(k'_n)/k'_n)$ is a $\mathbb{Z}_p[\mathrm{Gal}(k'_n/k)]$-module and, taking inverse limits with respect to the norm maps, we have that

$$X(K_d) \simeq \lim_{\leftarrow} X(k'_n)$$

is a module over the completed group ring

$$\mathbb{Z}_p[[\mathrm{Gal}(K_d/k)]] := \lim_{\leftarrow} \mathbb{Z}_p[\mathrm{Gal}(K_d/k)/\mathrm{Gal}(K_d/k'_n)] \simeq \lim_{\leftarrow} \mathbb{Z}_p[\mathrm{Gal}(k'_n/k)] \ .$$

Choosing d independent topological generators $\sigma_1, \dots, \sigma_d$ of $\mathrm{Gal}(K_d/k)$, we have a noncanonical isomorphism

$$Z_p[[\mathrm{Gal}(K_d/k)]] \stackrel{\sim}{\longrightarrow} \Lambda_d := \mathbb{Z}_p[[T_1, \dots, T_d]] \tag{1.3}$$

(Λ_d is the formal power series ring in d variables over $\mathbb{Z}_p$) which sends σ_i to $T_i + 1$ for every $i = 1, \dots, d$. We call $\mathbb{Z}_p[[\mathrm{Gal}(K_d/k)]]$ the *Iwasawa algebra* of K_d and, since it is easier to investigate its properties by studying the ring Λ_d , we shall always tacitly use the isomorphism above to picture its elements as formal power series.

It is well known that Λ_d is a complete regular local ring of dimension $d + 1$, hence a noetherian factorial domain (in particular a noetherian integrally closed domain in which every prime ideal of height one is principal).

A finitely generated torsion Λ_d-module M is said to be *pseudo-null* if there are at least two relatively prime elements of Λ_d which annihilate M (in particular, in the case $d = 1$, this is equivalent to the finiteness of M). A Λ_d-homomorphism $\varphi : M \to N$ is called *pseudo-isomorphism* if both $\mathrm{Ker}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are pseudo-null. In this case we write $\varphi : M \sim_\Lambda N$ (or simply $M \sim_\Lambda N$) and we say that M is *pseudo-isomorphic* to N. It is important to remark that the relation $\sim_\Lambda$ is transitive, but in general, is not symmetric: the existence of a pseudo-isomorphism $\varphi : M \longrightarrow N$ in one direction, does not guarantee the existence of a pseudo-isomorphism in the opposite direction. For example consider the natural inclusion $(p, T_1) \hookrightarrow \Lambda_1$: it is obviously a pseudo-isomorphism but there is no such map from Λ_1 to (p, T_1). Nevertheless being pseudo-isomorphic is an equivalence relation between finitely generated *torsion* Λ_d-modules.

For other details one can see for example [5, Chapter VII], [36, Chapter V] or [48, Chapter 13].

The starting point for the study of the Iwasawa module $X(K_d)$ is the following

Theorem 1.2.1. ([13, Theorem 1]) *For every number field k and every $\mathbb{Z}_p^d$-extension K_d/k, $X(K_d)$ is a finitely generated torsion Λ_d-module.*

Conjecture 1.2.2. (Generalized Greenberg Conjecture - GGC - [15, Conjecture 3.5]) *For every number field k, the Λ_{d_k}-module $X(\widetilde{k})$ is pseudo-null.*

Now we give the following structure theorem for Λ_d-modules.

Theorem 1.2.3. ([5, Ch. VII §4.4, Theorems 4 and 5]) *Let M be a finitely generated Λ_d-module, then there exist an integer $r \geqslant 0$ and two finite families $\{f_i : i = 1, \ldots, s\}$ of irreducible elements of Λ_d and $\{n_i : i = 1, \ldots, s\}$ of positive integers such that M is pseudo-isomorphic to*

$$\Lambda_d^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda_d/(f_i^{n_i}) \right) . \tag{1.4}$$

Moreover r, the family of ideals $\{(f_i) : i = 1, \ldots, s\}$ and the n_i's are uniquely determined by M modulo a bijection of the indexing set.

A Λ_d-module of the form (1.4) (for some $r, s, \{f_i\}_i$ and $\{n_i\}_i$ as above) is called *elementary Λ_d-module*. For any finitely generated Λ_d module, we write $E(M)$ to denote the elementary module E associated with M.

Definition 1.2.4. *The* characteristic polynomial *of M is*

$$f_M(T) = f_{E(M)}(T) := \begin{cases} 0 & \text{if } r \neq 0 \\ \prod_{i=1}^{s} f_i^{n_i} & \text{if } r = 0 \end{cases} .$$

Note that the characteristic polynomial is well defined only up to a unit in Λ_d and, in particular, M is pseudo-null (i.e., $M \sim_{\Lambda_d} 0$) if and only if $f_M(T) \in \Lambda_d^*$.

Since it will be of particular importance in what follows, we restate the previous theorem for the case $d = 1$ (this structure will lead to the definition of the Iwasawa invariants for a $\mathbb{Z}_p$-extension).

Corollary 1.2.5. *Let M be a finitely generated $\Lambda := \Lambda_1$-module, then there exist integers $r, s, t \geqslant 0$, finite families $\{m_i : i = 1, \ldots, s\}$, $\{l_j : j = 1, \ldots, t\}$ of positive integers and $\{f_j(T) : j = 1, \ldots, t\}$ of irreducible distinguished polynomials of Λ such that M is pseudo-isomorphic to*

$$\Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}) \right) . \tag{1.5}$$

Moreover, r, s, t, the family of ideals $\{(f_j(T)) : j = 1, \ldots, s\}$ and the families of integers $\{m_i : i = 1, \ldots, s\}$, $\{l_j : j = 1, \ldots, t\}$ are uniquely determined by M modulo a bijection of the indexing sets.

1.3 Iwasawa's Theorem

The following celebrated Theorem 1.3.1 was announced by K. Iwasawa during a conference in Seattle in 1956. The details of the proof appeared in [21] in 1959. In the same year J. P. Serre gave a Bourbaki Seminar on Iwasawa's result and introduced a different approach which Iwasawa soon adopted (see [46] or [20]).

Theorem 1.3.1. (Iwasawa's growth formula) *Let K/k be a $\mathbb{Z}_p$-extension of a number field k. Then there exists integers $\underline{n}(K/k), \mu(K/k), \lambda(K/k) \geqslant 0$ and $\nu(K/k)$, all independent from n, such that*

$$|A_n| = p^{\mu(K/k)p^n + \lambda(K/k)n + \nu(K/k)}$$

for every $n \geqslant \underline{n}(K/k)$.

Proof. See, for example, [48, Theorem 13.13]. □

Definition 1.3.2. *The parameters $\mu(K/k)$ and $\lambda(K/k)$ of the previous theorem are the* Iwasawa μ-invariant *and the* Iwasawa λ-invariant *for K/k. Looking at* (1.5) *they can be written as*

$$\mu(K/k) = \sum_{i=1}^{s} m_i \quad \textit{and} \quad \lambda(K/k) = \sum_{j=1}^{t} \deg(f_j(T))l_j \ .$$

There is a vast literature on these invariants and many conjectures regarding their values (or how those values should vary in different families of extensions) are still open. Iwasawa himself proposed the following:

Conjecture 1.3.3. (Iwasawa's μ-Conjecture) *For every number field k and for every prime number p, the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension $\mu_p(k_{cyc}/k)$ is zero.*

It was proved for abelian number field by B. Ferrero and L. C. Washington in 1979 (see [8] or [48, Theorem 7.15]). For totally real number fields Greenberg's Conjecture (originally stated in [13]) predicts also the vanishing of the λ-invariant. We write it separately for future references.

Conjecture 1.3.4. (Greenberg's Conjecture) *For every totally real number field k and for every prime number p both the μ-invariant and the λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension vanish, i.e., $X(k_{cyc}/k)$ is finite.*

Assuming Leopoldt's conjecture, this is now just a particular version of Conjecture 1.2.2, since a totally real number field has $r_2 = 0$ (hence has a unique $\mathbb{Z}_p$-extension, namely the cyclotomic one, i.e., $\tilde{k} = k_{cyc}$ in this case).

We end this section providing some more classical notations for the basic objects of Iwasawa Theory.
Let γ be a fixed topological generator of $\Gamma = \mathrm{Gal}(K/k)$ (i.e., $\overline{\langle \gamma \rangle} = \Gamma$): we recall the identification $\gamma \leftrightarrow T+1$ in the isomorphism (1.3). There are some elements in $\Lambda := \mathbb{Z}_p[[T]]$ which play an important role in the study of the class groups A_n .

Definition 1.3.5. *For every $m \geqslant n \geqslant 0$, we put*

- $\omega_n := \gamma^{p^n} - 1 = (1+T)^{p^n} - 1$,
- $\nu_{n,m} := 1 + \gamma^{p^n} + \gamma^{2p^n} + \ldots + \gamma^{p^m - p^n}$
  $= \frac{\omega_m}{\omega_n} = \frac{(1+T)^{p^m}-1}{(1+T)^{p^n}-1} = 1 + (1+T)^{p^n} + ... + ((1+T)^{p^n})^{p^{m-n}-1}$.

For simplicity we write ν_n in place of $\nu_{0,n}$: hence $\nu_n = 1 + \gamma + \gamma^2 + \ldots + \gamma^{p^n - 1} = \frac{\omega_n}{\omega_0} = \frac{(1+T)^{p^n}-1}{T}$ and $\nu_{n,m} = \frac{\nu_m}{\nu_n}$ as well. Note that ω_n and $\nu_{n,m}$ are distinguished polynomials of Λ and $\nu_{n,m}$ is Eisenstein (hence irreducible) if $m = n+1$.

Proposition 1.3.6. *For any $m \geqslant n \geqslant 0$ we have*

$$\nu_{n,m} \equiv p^{m-n} \pmod{T\nu_n} \ . \tag{1.6}$$

The proof of the previous formula is immediate (see, e.g., [10, Lemma]): it suffices to note that $\nu_{n,m} = \frac{((1+T)^{p^n}-1)+1)^{p^{m-n}}-1}{(1+T)^{p^n}-1}$.
Now let $Y_{n_0} := Y_{n_0}(K/k)$ be the Λ-submodule of $X := X(K/k)$ generated by the commutators of $\mathcal{G}(K)$ and by all its inertia subgroups. Then A_{n_0} is isomorphic to X/Y_{n_0} . Using the polynomials above, we define $Y_n := \nu_{n_0,n} Y_{n_0}$ (for all $n \geqslant n_0$) and one can prove the following

Proposition 1.3.7. ([48, Lemma 13.18]) *$A_n \simeq X/Y_n$ for all $n \geqslant n_0$.*

Finally we introduce our definition of p-rank and recall a criterion for the nullity of the μ-invariant related to that.

Definition 1.3.8. *For any finitely generated $\mathbb{Z}_p$-module A, we define its p-*rank *as*

$$\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/pA) \ .$$

Moreover we shall denote by $\widetilde{\lambda}_n$ the p-rank of A_n .

Remark 1.3.9. The previous notation is in accordance with the one usually found in the literature for torsion $\mathbb{Z}_p$-modules (like the A_n's), but we remark that in this thesis we apply it to any finitely generated $\mathbb{Z}_p$-module M for which we obtain

$$\mathrm{rk}_p(M) := \mathrm{rk}_{\mathbb{Z}_p}(M) + \mathrm{rk}_p(\mathrm{Tor}(M))$$

(for an interpretation like this see, for example, [42, Section 8.2]).

Proposition 1.3.10. ([48, Proposition 13.23]) *Let K/k be a $\mathbb{Z}_p$-extension of a number field k, then*

$$\mu(K/k) = 0 \Leftrightarrow \{\widetilde{\lambda}_n\}_{n\geqslant n_0} \textit{ is bounded .}$$

1.4 Stabilization

The term "stabilization" has the expected obvious meaning: given a sequence of finite p-groups $\{M_n\}_{n\in\mathbb{N}}$, we say that their orders stabilize at an index $q \in \mathbb{N}$ if $|M_n| = |M_q|$ for all $n \geqslant q$. In the same way, we say that their p-ranks stabilize at $q' \in \mathbb{N}$ if $\mathrm{rk}_p(M_n) = \mathrm{rk}_p(M_{q'})$ for all $n \geqslant q'$.
Stabilization is quite natural in Iwasawa Theory even if there are not many results in this direction. We have stabilization theorems for $\{|A_n|\}_{n\in\mathbb{N}}$ and for $\{\mathrm{rk}_p(A_n)\}_{n\in\mathbb{N}}$ but not much else. Usually Iwasawa modules tend to stabilize at the very first level in which they do not grow (i.e., if we have no growth from n to $n+1$, we are not going to have any growth at all from n on).
The references for the following theorems are [10], [2] and [24] (we provide just a short proof for the second one to illustrate some of the techniques we are going to encounter in the next chapters).

Theorem 1.4.1. *If $|A_n| = |A_{n+1}|$ for some $n \geqslant n_0$, then $A_m \simeq A_n \simeq X$ for all $m \geqslant n$.*

Theorem 1.4.2. *If $\mathrm{rk}_p(A_n) = \mathrm{rk}_p(A_{n+1})$ for some $n \geqslant n_0$, then $\mathrm{rk}_p(A_m) = \mathrm{rk}_p(A_n)$ for all $m \geqslant n$ (hence $\mu(K/k) = 0$ and $\mathrm{rk}_p(A_n) = \mathrm{rk}_p(X)$).*

Proof. Without loss of generality we can assume $n = 0$ (hence $n_0 = 0$ too) so our hypothesis is $\widetilde{\lambda}_0 = \widetilde{\lambda}_1$. First we show that $\forall t \geqslant 0$ one has

$$Y_t + pX = T^{p^t-1}Y_0 + pX \ .$$

Indeed

$$\begin{aligned} Y_t &= \nu_t Y_0 = (1+\gamma_0+\gamma_0^2+\ldots+\gamma_0^{p^t-1})Y_0 \\ &\leftrightarrow (1+(1+T)+(1+T)^2+\ldots+(1+T)^{p^t-1})Y_0 = \tfrac{(1+T)^{p^t}-1}{(1+T)-1}Y_0 \\ &= \frac{\displaystyle\sum_{i=0}^{p^t}\binom{p^t}{i}T^i - 1}{T}\,Y_0 = \left(\textstyle\sum_{i=1}^{p^t}\binom{p^t}{i}T^{i-1}\right)Y_0 \\ &= (T^{p^t-1} + p\cdot(\text{polynomial}))Y_0 \ . \end{aligned}$$

Hence

$$Y_t + pX = T^{p^t-1}Y_0 + pX \quad \text{for any } t \geqslant 0 \ . \tag{1.7}$$

Now the hypothesis $\widetilde{\lambda}_0 = \widetilde{\lambda}_1$ means $Y_0 + pX = Y_1 + pX$ and, by what we just proved, $Y_1 + pX = T^{p-1}Y_0 + pX$. Obviously $Y_0 + pX \supseteq TY_0 + pX \supseteq T^{p-1}Y_0 + pX$, hence the equality of the first and last terms implies

$$Y_0 + pX = TY_0 + pX \ . \tag{1.8}$$

An immediate consequence is that $Y_0 + pX = T^a Y_0 + pX$ for any $a \geqslant 0$. Indeed, it is obvious for $a = 0$ and we use induction, assuming it is true for $a - 1$, to prove it for $a \geqslant 1$. We have

$$\begin{aligned} Y_0 + pX \quad &= T^{a-1}Y_0 + pX = T^{a-1}(Y_0 + pX) + pX \\ &= T^{a-1}(TY_0 + pX) + pX \quad \text{(by (1.8))} \\ &= T^a Y_0 + pX \ . \end{aligned}$$

Therefore, choosing $a = p^h - 1$, we get

$$Y_0 + pX = T^{p^h - 1}Y_0 + pX = Y_h + pX \ ,$$

(the second equality comes from (1.7)) and this is precisely the claim for $n = 0$. $\square$

1.5 Capitulation

From Corollary 1.2.5 we have an exact sequence

$$0 \to D(X) \to X \xrightarrow{\varphi} E(X) \to B(X) \to 0 \tag{1.9}$$

where φ is a pseudo-isomorphism and $D(X)$, $B(X)$ are finite. Note that $D(X)$ is the maximal finite submodule of X and to simplify the notations we shall simply write D from now on.
For all $m \geqslant n \geqslant 0$, let $N_{m,n} : A_m \to A_n$ be the norm map and $i_{n,m} : A_n \to A_m$ be the natural map induced by extension of ideals. We put

$$A := \lim_{\to} A_n \quad \text{and} \quad i_n : A_n \to A$$

as the natural map. Moreover let $H_{n,m}$ be the kernel of $i_{n,m}$ and H_n be the kernel of i_n , i.e.,

$$H_n = \bigcup_{m \geq n} H_{n,m} \ .$$

The $H_{n,m}$'s and the H_n's are often called *capitulation kernels* and are very important in Iwasawa theory, for example because of the following proposition which links them to Greenberg's Conjecture.

Proposition 1.5.1. ([14, Proposition 2]) *We have that $\lambda(K/k) = \mu(K/k) = 0$ if and only if $H_n = A_n$ for every $n \geq 0$.*

In the following theorem the statement is not exactly the original one appearing in [14], but it can be easily derived from it because the proof only uses the hypothesis $s(K/k) = 1$.

Theorem 1.5.2. ([14, Theorem 1]) *Let $n_0 = 0$ and $s(K/k) = 1$ (i.e., there is only one prime in k which ramifies in K), then X is pseudo-null if and only if $H_0 = A_0$.*

A very important remark is that, in the previous theorem, the hypothesis $n_0 = 0$ can be easily suppressed. This has been showed by J. Minardi and we write down it separately for future reference.

Corollary 1.5.3. ([33, Proposition 1.B]) *Assume $s = 1$, then X is pseudo-null if and only if $H_0 = A_0$.*

Corollary 1.5.4. *If there is only one prime in k dividing p and it generates the whole A_0 , then $X(K/k)$ is pseudo-null for every $\mathbb{Z}_p$-extension K/k.*

Statement **(a)** of the next theorem provides a stronger result and it was proved by T. Fukuda in 1994 in a very elegant way. Indeed Theorem 1.5.5 **(a)** gives the precise layer k_m for which $X \simeq A_m$, but there is a price to pay: with this kind of proof the hypothesis $n_0 = 0$ acquires a crucial role and it cannot be removed anymore.

Theorem 1.5.5. ([10, Theorem 2]) *Let $s(K/k) = 1$ and $n_0(K/k) = 0$.*

(a) *If $H_{0,n} = A_0$ for some $n \geqslant 1$, then $|A_m| = |A_n| = |X|$ for all $m \geqslant n$.*

(b) *If $|A_{n+1}| = |A_n|$ for some $n \geqslant 0$ and the exponent of A_n is p^t, then $H_{n,n+t} = A_n$.*

In Lemma 4.2.1 we will provide a Criterion which yields a generalization of part **(a)** of the previous theorem. We conclude this section recalling

Theorem 1.5.6. ([38, Theorem]) *Let $n_0(K/k) = 0$, then $X(K/k)$ is pseudo-null if and only if* $\ker N_{1,0} \subseteq H_1$ *.*

Not much more is known about the $H_{n,m}$'s, in particular regarding their orders and their stabilization properties. For example, Iwasawa proved that $H_{n,m}$ is bounded by $|D| \cdot |B(X)| \cdot |A_{n_0}|$ independently from n and m (see e.g. [20] or [36]) and M. Ozaki showed in [38] a relation between the H_n's and the maximal finite submodule d of X. We will go deeper in this direction in Chapter 3 studying the submodule D, providing some results on these topics and describing some consequences of the phenomenons of stabilization and capitulation in a general $\mathbb{Z}_p$-extension.

Chapter 2

Stabilization in Ozaki's non-abelian Iwasawa Theory

In this chapter we want to expose some results obtained in non-abelian Iwasawa Theory (as developed by M. Ozaki in [40]). In the introduction we recall the basic objects and facts of the theory, for more details and complete proofs see [40].

2.1 Introduction

For any algebraic extension E of $\mathbb{Q}$ (not necessarily finite) we denote by $\widetilde{L}(E)$ the maximal unramified (not necessary abelian) pro-p extension of E (where, as in the previous chapter, p is any prime). Let k be a number field, K any $\mathbb{Z}_p$-extension of k and, to simplify the notations, we put $\widetilde{L} := \widetilde{L}(K)$ and $\widetilde{L}_n := \widetilde{L}(k_n)$ for every $n \geqslant 0$. To study the non abelian extensions $\widetilde{L}_n/k_n$ and $\widetilde{L}/K$, the method is to break these extensions into smaller (abelian) pieces. Before doing this, we give some notations and definitions.
Let H be a group. For all $a, b \in H$ we put $a^b = b^{-1}ab$ and $[a,b] = a^{-1}b^{-1}ab$. If H_1, H_2 are subgroups of H we denote the *commutator group of* H_1 *and* H_2 by

$$[H_1, H_2] := \langle [h_1, h_2] \,:\, h_1 \in H_1,\, h_2 \in H_2 \rangle \tag{2.1}$$

When H is a topological group we refer to $\overline{[H_1, H_2]}$ (the topological closure of $[H_1, H_2]$) as the *topological commutator group of* H_1 *and* H_2. Moreover we pose

$$C_1(H) := H \quad \text{and} \quad C_i(H) := \overline{[H, C_{i-1}(H)]} \quad (\text{for any } i \geqslant 2) \tag{2.2}$$

and

$$D_0(H) := H \quad \text{and} \quad D_i(H) := \overline{[D_{i-1}(H), D_{i-1}(H)]} \quad (\text{for any } i \geqslant 1)\ . \tag{2.3}$$

We call them the *lower central series* and the *derived series* of H respectively. If H is an abstract group, $C_i(H)$ and $D_i(H)$ have the obvious meaning.
Let $\widetilde{G} := \mathrm{Gal}(\widetilde{L}/K)$: in the following pages we will consider both these series for $\widetilde{G}$

$$\widetilde{G} = C_1(\widetilde{G}) \supseteq C_2(\widetilde{G}) \supseteq C_3(\widetilde{G}) \supseteq \dots\ , \tag{2.4}$$

$$\widetilde{G} = D_0(\widetilde{G}) \supseteq D_1(\widetilde{G}) \supseteq D_2(\widetilde{G}) \supseteq \dots\ . \tag{2.5}$$

A well known relation is that $D_i(H) \subseteq C_{2^i}(H)$ (which holds for every abstract group H), i.e., the i-th term of the derived series is contained in the 2^i-th term of the lower central series. For more details see, for example, [4, Ch. I §6.3]. The derived series of $\widetilde{G}$ is naturally related with the class field tower of K, while the lower central series is less intuitive so we give here notations and properties for the fields it is related with.

Definition 2.1.1. *For every $i \geqslant 1$, we pose*

(a) $L^{(i)} :=$ *the subfield of $\widetilde{L}$ fixed by $C_{i+1}(\widetilde{G})$;*

(b) $G^{(i)} := \widetilde{G}/C_{i+1}(\widetilde{G}) \simeq \mathrm{Gal}(L^{(i)}/K)$ *;*

(c) $X^{(i)} := C_i(\widetilde{G})/C_{i+1}(\widetilde{G}) = C_i(G^{(i)}) \simeq \mathrm{Gal}(L^{(i)}/L^{(i-1)})$.

*The group $X^{(i)}$ will be called the i-*th Iwasawa module *of K/k.*

We have analogous notations/definitions for groups related with the fields k_n for every $n \geqslant 0$. Let $\widetilde{G}_n := \mathrm{Gal}(\widetilde{L}_n/k_n)$ and consider, as above, the lower central (and the derived) series of $\widetilde{G}_n$:

$$\widetilde{G}_n = C_1(\widetilde{G}_n) \supseteq C_2(\widetilde{G}_n) \supseteq C_3(\widetilde{G}_n) \supseteq \dots\ . \tag{2.6}$$

$$\widetilde{G}_n = D_0(\widetilde{G}_n) \supseteq D_1(\widetilde{G}_n) \supseteq D_2(\widetilde{G}_n) \supseteq \dots\ . \tag{2.7}$$

Definition 2.1.2. *For every $i \geqslant 1$ and $n \geqslant 0$, we pose*

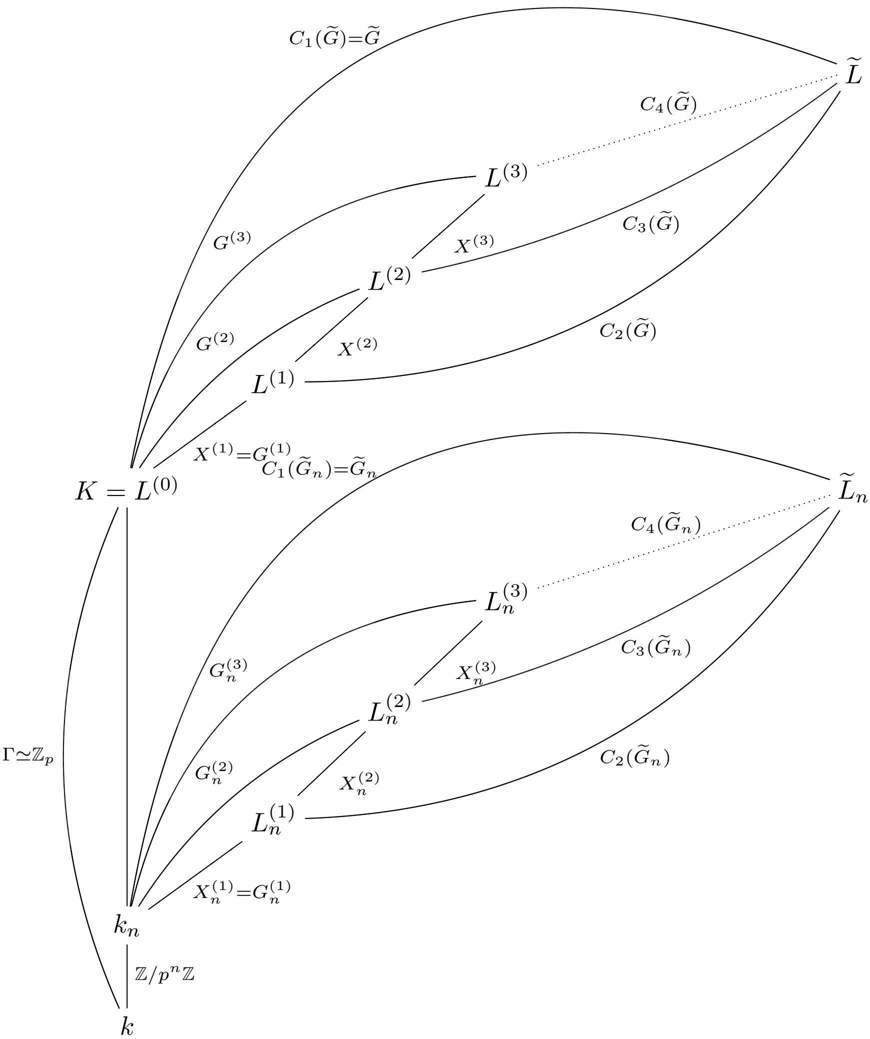
(a) $L_n^{(i)} :=$ *the subfield of $\widetilde{L}_n$ fixed by $C_{i+1}(\widetilde{G}_n)$;*

(b) $G_n^{(i)} := \widetilde{G}_n/C_{i+1}(\widetilde{G}_n) \simeq \mathrm{Gal}(L_n^{(i)}/k_n)$*;*

(c) $X_n^{(i)} := C_i(\widetilde{G}_n)/C_{i+1}(\widetilde{G}_n) = C_i(G_n^{(i)}) \simeq \mathrm{Gal}(L_n^{(i)}/L_n^{(i-1)})$.

If $F^{(i)}(k_n)$ is the i-th term of the class field tower of k_n (i.e., the maximal abelian unramified p-extension of $F^{(i-1)}(k_n)$), then, from the relation above, $L^{(2^i-1)}(k_n) \subseteq F^{(i)}(k_n)$. Note that for $i = 1$ we get $L^{(1)} = L(K)$, $X^{(1)} = X(K/k)$ and $\lambda^{(1)} = \lambda(K/k)$ (the same holds for the groups related with the layers k_n), so we shall often use the same notation of Chapter 1 for them dropping the exponent $^{(1)}$.

The above setting for the central lower series is summarized by the following diagram



Now we proceed to give an account of the principal facts of this "non-abelian setting" giving references to the main results of [40]. Recall that if F is a number field, $A(F)$ stands for the p-part of the ideal class group $Cl(F)$.

Proposition 2.1.3. ([40, Lemma 1])

(a) *For all* $i \geqslant 1$, $X^{(i)}$ *has a natural* Λ*-module structure;*

(b) *for all* $i \geqslant 1$ *and all* $n \geqslant 0$ *we have* $X_n^{(i)} \simeq A(L_n^{(i-1)})_{G_n^{(i-1)}}$ *(i.e., the*

$G_n^{(i-1)}$*-coinvariants of* $A(L_n^{(i-1)})$ *).*

It is well known that in the first column of nilpotency the norm map $N_{m,n} : A_m \to A_n$ is surjective for all $m \geqslant n \geqslant n_0(K/k)$ and (by Galois theory and class field theory) we have that $\varprojlim X_n \simeq X$.
The following proposition shows that the corresponding statements are true also in this new context.

Proposition 2.1.4. ([40, Lemma 2])

(a) *For all* $i \geqslant 1$ *and* $m \geqslant n \geqslant n_0(K/k)$ *the natural restriction map* $\pi_{m,n} : X_m^{(i)} \to X_n^{(i)}$ *is surjective;*

(b) *for all* $i \geqslant 1$ *we have* $\varprojlim X_n^{(i)} \simeq X^{(i)}$ *and* $\varprojlim G_n^{(i)} \simeq G^{(i)}$.

The following proposition provides the structure for $X^{(i)}$ viewed as a $\mathbb{Z}_p$-module. Moreover we remark that if M is a module over a (complete) discrete valuation ring R (e.g. a $\mathbb{Z}_p$-module) and it is not finitely generated, then, in general, $\mathrm{Tor}_R M$ is not a direct summand of M. A (standard) counter-example is given by $M = \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$ as $\mathbb{Z}_p$-module (see e.g. [27, Exercise 4.37]).

Proposition 2.1.5. ([40, Proposition 3]) *Let* K/k *be any* $\mathbb{Z}_p$*-extension.*

(a) *For every* $i \geqslant 1$ *there exist an integer* $\lambda^{(i)} = \lambda^{(i)}(K/k) \geqslant 0$ *such that*

$$X^{(i)} \simeq (\mathbb{Z}_p)^{\oplus \lambda^{(i)}(K/k)} \oplus \mathrm{Tor}_{\mathbb{Z}_p} X^{(i)}$$

as $\mathbb{Z}_p$*-modules.*

(b) *There exist a power of* p *which annihilates the torsion submodule* $\mathrm{Tor}_{\mathbb{Z}_p} X^{(i)}$.

Proposition 2.1.6. ([40, Proposition 1]) *Let* $\mu(K/k) = 0$*, then, for any* $i \geqslant 1$*,* $X^{(i)}$ *is finitely generated as* $\mathbb{Z}_p$*-module and, in particular, it is a finitely generated torsion* Λ*-module.*

Proof. The proof is based on the Burniside Basis Theorem: since $X^{(1)}$ is finitely generated over $\mathbb{Z}_p$ then $\widetilde{G}$ is a finitely generated pro-p group. Let α be the minimal number of generators for $\widetilde{G}$ and consider the epimorphism $\phi : F_\alpha \twoheadrightarrow \widetilde{G}$ where F_α is the free pro-p group on α generators. We have induced isomorphisms $\phi_i : C_i(F_\alpha)/C_{i+1}(F_\alpha) \twoheadrightarrow X^{(i)}$ and, since

$$C_i(F_\alpha)/C_{i+1}(F_\alpha) \simeq \mathbb{Z}_p^{\frac{1}{i}\sum_{d|i} \mu(d)\alpha^{i/d}},$$

(see, for example, [16, §I.5], where $\mu(.)$ is the Möbius function), then $X^{(i)}$ is finitely generated over $\mathbb{Z}_p$ for every $i \geqslant 1$. ☐

Definition 2.1.7. *The invariant* $\lambda^{(1)}(K/k)$ *is equal to the familiar Iwasawa invariant* $\lambda(K/k)$. *For every* $i \geqslant 1$ *we will call* $\lambda^{(i)}(K/k)$ *the* higher Iwasawa i-th λ-invariant *for* K/k.

From the proof above and Proposition 2.1.5, one easily gets the following corollary:

Corollary 2.1.8. *For any* $i \geqslant 1$ *we have*

$$\lambda^{(i)}(K/k) \leqslant \frac{1}{i} \sum_{d|i} \mu(d)\lambda(K/k)^{i/d} .$$

Now we return to view the higher Iwasawa modules $X^{(i)}$'s as modules over Λ.

Proposition 2.1.9. ([40, Proposition 2]) *Let* $\mu(K/k) > 0$. *Then, for every* $i \geqslant 2$, $X^{(i)}$ *is not a finitely generated* Λ*-module.*

In the case $\mu(K/k) = 0$ it is possible to obtain a formula for $|X_n^{(i)}|$ which is similar to the classical Iwasawa's one which deals only with $|A_n| = |X_n^{(1)}|$.

Theorem 2.1.10. ([40, Theorem 1]) *Let* $\mu(K/k) = 0$, *then for every* $i \geqslant 1$ *there exist integers* $\nu^{(i)}(K/k)$ *and* $\underline{n}^{(i)}(K/k) \geqslant 0$ *(independent from* n*) such that*

$$|X_n^{(i)}| = p^{\lambda^{(i)}(K/k)n+\nu^{(i)}(K/k)}$$

$\forall n \geqslant \underline{n}^{(i)}(K/k)$.

Summing up for $i = 1, \ldots, n$ we obtain

Corollary 2.1.11. ([40, Theorem II]) *Let* $\mu(K/k) = 0$, *then for every* $i \geqslant 1$

$$|G_n^{(i)}| = p^{\sum_{j=1}^{i} \lambda^{(j)}(K/k)n+\sum_{j=1}^{i} \nu^{(j)}(K/k)}$$

$\forall n \geqslant \max\{\underline{n}^{(1)}(K/k), \ldots, \underline{n}^{(i)}(K/k)\}$.

We notice that in the case $\mu(K/k) > 0$ it is commonly believed that there exists a formula for $|X_n^{(i)}|$, but it is very difficult to find. One special case is described in the following

Theorem 2.1.12. ([40, Theorem 2]) *Let* p *be an odd prime and* K/k *a* $\mathbb{Z}_p$*-extension satisfying the following conditions:*

(a) *there is only one prime of* k *over* p *and it is totally ramified in* K/k;

(a) $X(K/k) \simeq (\Lambda/p)^t$ *for some* $t \geqslant 0$ *(i.e.,* $\mu(K/k) = r$ *and* $\lambda(K/k) = 0$*).*

Then there exist integers $\kappa^{(2)}(K/k)$ *and* $\nu^{(2)}(K/k)$ *such that*

$$|X_n^{(2)}| = p^{\left(\frac{tp^n-1}{2}t-\kappa^{(2)}(K/k)\right)p^n+\nu^{(2)}(K/k)}$$

for all sufficiently large n.

2.2 Stabilization for the order of $X_n^{(i)}$

From Theorem 1.4.1, we know that if $|A_n| = |A_{n+1}|$ in a $\mathbb{Z}_p$-extension (for some $n \geqslant n_0(K/k)$), then the sequence $\{|A_m|\}_{m\in\mathbb{N}}$ stabilizes for $m \geqslant n$. Recall that A_n is isomorphic to $X_n^{(1)}$, so we can reformulate this property: if $|X_n^{(1)}| = |X_{n+1}^{(1)}|$, then the sequence $\{|X_m^{(1)}|\}_{m\in\mathbb{N}}$ become constant from n on. An obvious generalization would be the following: does an analogous statement hold for $\{|X_m^{(i)}|\}_{m\in\mathbb{N}}$? That is, if we assume $|X_n^{(i)}| = |X_{n+1}^{(i)}|$ for some $n \geqslant n_0(K/k)$ and $i \geqslant 2$, can we conclude that $\{|X_m^{(i)}|\}_{m\in\mathbb{N}}$ stabilizes for $m \geqslant n$?
In the same way we know that a $\mathbb{Z}_p$-extension enjoys a similar property for the stabilization of p-ranks (see Theorem 1.4.2), hence this leads to the corresponding generalization: assume that $\mathrm{rk}_p(X_n^{(i)}) = \mathrm{rk}_p(X_{n+1}^{(i)})$ for some $n \geqslant n_0(K/k)$ and $i \geqslant 2$, can we conclude that $\{\mathrm{rk}_p(X_m^{(i)})\}_{m\in\mathbb{N}}$ stabilizes for $m \geqslant n$?
This questions turn out to be too optimistic (or naive) as the following counterexample shows.

2.2.1 Counterexample

We first recall the following group theoretical results (for the first see, for example, [47, Section III], we provide a short proof for the second for the convenience of the reader).

Theorem 2.2.1. *Let G be a finite 2-group such that $G/D_1(G) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $D_1(G)/D_2(G)$ is cyclic and $D_2(G) = 1$.*

Remark 2.2.2. We recall (for future reference as well) the definition of nilpotent group which we will use in the rest of the paper. When G is an abstract group we put

$$[G,\, {}_iG] := [\dots[[A, B], B]\dots], B]\ ,$$

where B appears i times. We say that G is *nilpotent of class* $i \geqslant 1$ if $[G,\, {}_iG] = 1$ and $[G,\, {}_{i-1}G] \neq 1$. If G is a topological group whose space is Hausdorff, the last conditions are equivalent to $C_i(G) = 1$ and $C_{i-1}(G) \neq 1$ (we shall often use this equivalent definition).

Proposition 2.2.3. *Let G be a pronilpotent group (i.e., the inverse limit of finite nilpotent groups) such that $G/C_2(G)$ is cyclic or procyclic. Then G is abelian.*

Proof. Let $H := G/C_3(G)$ and note that $C_2(H) = C_2(G)/C_3(G)$ is contained in $Z(H)$ (the center of H). This means that $H/Z(H)$ is cyclic or procyclic, hence H is abelian. Therefore $C_2(G)/C_3(G) = C_2(H) = 1$, which yields $C_2(G) = C_3(G)$ (and $C_i(G) = C_2(G)$ for all $i \geqslant 2$). Since G is pronilpotent, it is clear that $\bigcap_{i=2}^{\infty} C_i(G) = 1$. Hence $C_2(G) = \bigcap_{i=2}^{\infty} C_i(G) = 1$, which means G is abelian. $\square$

Since "pro-p" implies "pronilpotent", the previous proposition shows that if there is a cyclic or procyclic quotient in the series (2.5) or (2.7) then the series stops there.

Take $p = 2$ and consider the cyclotomic $\mathbb{Z}_2$-extension of the number field $k = \mathbb{Q}(\sqrt{5 \cdot 732678913})$ as in [41, Example 1]. In the first layer we have $k_1 = k(\sqrt{2})$. Using PARI/GP we can see that $A_0 \simeq \mathbb{Z}/2\mathbb{Z}$, which yields $X_0^{(i)} = 0$ for every $i \geqslant 2$: indeed if the p-rank of $X_0^{(1)} = \widetilde{G}_0/C_2(\widetilde{G}_0)$ is 1, then $X_0^{(2)} = 0$ (by Proposition 2.2.3). Moreover

$$k_1 \simeq \frac{\mathbb{Q}[x]}{(x^4 - 7326789134x^2 + 13420459724217960969)}$$

and $A_1 \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now let $H := \widetilde{G}_1/D_3(\widetilde{G}_1)$: since $H/D_1(H) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, Theorem 2.2.1 implies that $D_2(H) = 1$ which yields $D_2(\widetilde{G}_1) = 1$. This means that $\widetilde{G}_1$ is nilpotent of class i_1 (for some $i_1 \geqslant 2$) and $X^{(i)} = 0$ for all $i \geqslant i_1$ (in other words $\widetilde{G}_1$ has derived length at most 2 and it is nilpotent of class i_1).
Going on with the computations, one finds the 4-th layer k_4 with $A_4/A_4^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{16}$. Now we denote by ρ the number of generators of the group of units of k_4 (since k_4 is totally real and has degree 2^5 over $\mathbb{Q}$, $\rho = 2^5$ as well): we have

$$\dim_{\mathbb{F}_2} A_4 = 16 \geqslant 2 + 2\sqrt{\rho + 2} = 2 + 2\sqrt{2^5 + 2} \approx 13.662 \ .$$

Thus by Golod-Shafarevich inequality (see, for example, [36, Theorem 10.10.5], which improves a little the bound of the original article [11]), we have that k_4 has an infinite Hilbert 2-class field tower, hence, a fortiori, the lower central series has infinite length, i.e., $X_4^{(i)} \neq 0$ for any $i \geqslant 1$.
Summing up we have $X_0^{(i_1)} = X_1^{(i_1)} = 0$ but certainly $X_4^{(i_1)} \neq 0$: this give us a counterexample (for the sequence of the p-ranks as well).

2.2.2 Stabilization

Therefore we have to add other hypothesis to obtain the stabilization of the order or of the p-rank of $X_m^{(i)}$.
To simplify the notations we assume in this chapter $n_0(K/k) = 0$, i.e., every ramified prime in the $\mathbb{Z}_p$-extension K/k is totally ramified. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes of k which ramify in K/k and, for every $1 \leqslant j \leqslant s$, chose one prime of $\widetilde{L}$ lying over $\mathfrak{p}_j$. Let $I(\mathfrak{p}_1), \ldots, I(\mathfrak{p}_s) \subseteq \mathcal{G} = \mathrm{Gal}(\widetilde{L}/k)$ be the inertia subgroups of $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and observe that the natural restriction $\mathcal{G} \to \Gamma$ induces isomorphisms $I(\mathfrak{p}_j) \simeq \Gamma \simeq \mathbb{Z}_p$ for every $1 \leqslant j \leqslant s$. Now we fix a topological

generator of $I(\mathfrak{p}_1)$ and, with a little abuse of notation, we denote it also by γ. We have that there exist $g_j \in \widetilde{G}$ such that γg_j is a topological generator of $I(\mathfrak{p}_j)$ for $2 \leqslant j \leqslant s$.

Definition 2.2.4. *Let g be any element of $\widetilde{G}$. For every $m \geqslant n \geqslant 0$ we define*

$$\nu_{n,m}(g) = g^{\nu_{n,m}} := g^{\gamma^{(p^{m-n}-1)p^n}+\gamma^{(p^{m-n}-2)p^n}+\ldots+\gamma^{p^n}+1}$$

$$= (\gamma^{-(p^{m-n}-1)p^n} g\gamma^{(p^{m-n}-1)p^n})\cdot(\gamma^{-(p^{m-n}-2)p^n} g\gamma^{(p^{m-n}-2)p^n})\cdot\ldots\cdot(\gamma^{-p^n} g\gamma^{p^n})\cdot g\ .$$

As in the classical theory, we write simply ν_n to indicate $\nu_{0,n}$, i.e.,

$$\nu_n(g) = g^{\nu_n} = g^{\gamma^{(p^n-1)}+\gamma^{(p^n-2)}+\ldots+\gamma+1}$$

$$= (\gamma^{-(p^n-1)} g\gamma^{p^n-1})\cdot(\gamma^{-(p^n-2)} g\gamma^{p^n-2})\cdot\ldots\cdot(\gamma^{-1}g\gamma)\cdot g\ ,$$

(for any $g \in \widetilde{G}$).

Remark 2.2.5. Note that $\widetilde{G}$ is not a Λ-module because the "+" in the exponent is not commutative. For example, if g is a general element of $g \in \widetilde{G}$, it can happen that $g^{\gamma+1} \neq g^{1+\gamma}$ and $g^{\nu_n} = g^{\gamma^{p^n-1}+\gamma^{p^n-2}+\ldots+\gamma+1} \neq g^{1+\gamma+\ldots+\gamma^{p^n-2}+\gamma^{p^n-1}}$.

Definition 2.2.6. *For every $n \geqslant 0$ we put*

$$\widetilde{R}_n := (\nu_n([\gamma, x]), \nu_n(g_j) \mid x \in \widetilde{G},\ 2 \leqslant j \leqslant s)_{\widetilde{G}}\ ,$$

where $(.)_{\widetilde{G}}$ stands for a normally generated closed subgroup in $\widetilde{G}$ and the commutator $[x, y]$ denotes the product $x^{-1}y^{-1}xy$.

Lemma 2.2.7. *For every $n \geqslant 0$ we have $\widetilde{G}_n \simeq \widetilde{G}/\widetilde{R}_n$.*

Proof. See [40, Lemma 3]. □

Now we focus our attention on the first i columns of the tower, i.e., we consider $G^{(i)} = \widetilde{G}/C_{i+1}(\widetilde{G})$ in the place of $\widetilde{G}$. We continue to use only γ and g_j to indicate the cosets $\gamma C_{i+1}(\widetilde{G})$ and $g_j C_{i+1}(\widetilde{G})$ in $G^{(i)}$.

Definition 2.2.8. *For every $n \geqslant 0$ and $i \geqslant 1$, we put*

- **(a)** $Y_n^{(i)} := \mathrm{Ker}\{\mathrm{res} : X^{(i)} \to X_n^{(i)}\}$, *where* res *denotes the natural restriction map;*
- **(b)** $R_n^{(i)} := (\nu_n([\gamma, x]), \nu_n(g_j) \mid x \in G^{(i)},\ 2 \leqslant j \leqslant s)_{G^{(i)}}$.

Proposition 2.2.9. *For every $n \geqslant 0$ and $i \geqslant 1$ we have*

- **(a)** $G_n^{(i)} \simeq G^{(i)}/R_n^{(i)}$;

(b) $Y_n^{(i)} = (C_i(\widetilde{G}) \cap \widetilde{R}_n)C_{i+1}(\widetilde{G})/C_{i+1}(\widetilde{G}) = X^{(i)} \cap R_n^{(i)}$.

For a proof of the previous proposition see [40, Lemma 3]. Moreover, note that if $i = 1$ the characterization of $Y_n^{(i)}$ is consistent to the one of Y_n in the classical context.

Lemma 2.2.10. *For any $g \in \widetilde{G}$ and any $m \geqslant n \geqslant 0$ we have*

$$(g^{\nu_n})^{\nu_{n,m}} = g^{\nu_m} \ .$$

Proof. Note that

$$\begin{aligned}(g^{\nu_n})^{\nu_{n,m}} &= (\nu_n(g))^{\gamma^{(p^{m-n}-1)p^n}+\gamma^{(p^{m-n}-2)p^n}+\ldots+\gamma^{1\cdot p^n}+1} \\ &= \prod_{\varepsilon=p^{m-n}-1}^{0} \gamma^{-\varepsilon p^n} \cdot \nu_n(g) \cdot \gamma^{\varepsilon p^n} = \nu_m(g) = g^{\nu_m} \ .\end{aligned}$$

□

Theorem 2.2.11. *Let $i \geqslant 1$ and $n \geqslant 0$; if $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ for all $1 \leqslant j \leqslant i$, then $X_n^{(j)} \simeq X_m^{(j)} \simeq X^{(j)}$ and $Y_n^{(j)} = 0$ for every $1 \leqslant j \leqslant i$ and for all $m \geqslant n$.*

Proof. We use an induction argument on i.
If $i = 1$, Theorem 1.4.1 yields $Y_n^{(1)} = 0$ and $X_n^{(1)} \simeq X_m^{(1)}$ for all $m \geqslant n$.
Now we assume the statement true for $i \geqslant 1$ and prove it for $i + 1$. First, note that if $m \geqslant n$, then $k_m \cap L_n^{(i)} = k_n$ since k_m/k_n is totally ramified and $L_n^{(i)}/k_n$ is unramified (we recall that $n_0 = 0$ here). Thus

$$\mathrm{Gal}(k_m L_n^{(i)}/k_m) \simeq \mathrm{Gal}(L_n^{(i)}/k_n) \simeq G_n^{(i)} \ .$$

This means that the natural restriction induces an epimorphism

$$G_m^{(i)} \simeq \mathrm{Gal}(L_m^{(i)}/k_m) \twoheadrightarrow \mathrm{Gal}(k_m L_n^{(i)}/k_m) \simeq G_n^{(i)} \ . \tag{2.8}$$

By inductive hypothesis,

$$|G_m^{(i)}| = |X_m^{(1)}| \cdot |X_m^{(2)}| \cdot \ldots \cdot |X_m^{(i)}| = |X_n^{(1)}| \cdot |X_n^{(2)}| \cdot \ldots \cdot |X_n^{(i)}| = |G_n^{(i)}| \ ,$$

so (2.8) is an isomorphism. But $K \cap L_m^{(i)} = k_m$, hence $\mathrm{Gal}(L_m^{(i)}/k_m) \simeq \mathrm{Gal}(KL_m^{(i)}/K)$ and, from [40, Lemma 2 (2)], we have

$$\begin{aligned}\varprojlim_m G_m^{(i)} &\simeq \varprojlim_m \mathrm{Gal}(L_m^{(i)}/k_m) \simeq \varprojlim_m \mathrm{Gal}(KL_m^{(i)}/K) \\ &\simeq \mathrm{Gal}(\bigcup_{m\in\mathbb{N}} KL_m^{(i)}/K) \simeq \mathrm{Gal}(L^{(i)}/K) \simeq G^{(i)} \ .\end{aligned}$$

Now the isomorphism in (2.8) yields

$$\mathrm{Gal}(KL_n^{(i)}/K) \simeq G_n^{(i)} \simeq \varprojlim_m G_m^{(i)} \simeq G^{(i)} \simeq \mathrm{Gal}(L^{(i)}/K)$$

and this means that

$$KL_n^{(i)} = L^{(i)} \ . \tag{2.9}$$

Now recall that $Y_n^{(i+1)} = X^{(i+1)} \cap R_n^{(i+1)}$ and $G_n^{(i+1)} \simeq G^{(i+1)}/R_n^{(i+1)}$. So we have the following isomorphisms

$$\mathrm{Gal}(KL_n^{(i+1)}/K) \simeq \mathrm{Gal}(L_n^{(i+1)}/k_n) \simeq G_n^{(i+1)} \simeq G^{(i+1)}/R_n^{(i+1)} \tag{2.10}$$

and, from (2.9),

$$\mathrm{Gal}(KL_n^{(i)}/K) = \mathrm{Gal}(L^{(i)}/K) \simeq G^{(i)} = \widetilde{G}/C_{i+1}(\widetilde{G}) \simeq G^{(i+1)}/X^{(i+1)} \ . \tag{2.11}$$

By comparing (2.10) and (2.11) we obtain $R_n^{(i+1)} \subseteq X^{(i+1)}$, which yields $R_n^{(i+1)} = Y_n^{(i+1)}$. Since $X^{(i+1)} \subseteq Z(G^{(i+1)})$ (where Z denotes the center of the group), we can take away the "normally generated" condition in the definition of $R_n^{(i+1)}$, i.e.,

$$\begin{aligned} R_n^{(i+1)} &\stackrel{\mathrm{def}}{=} (\nu_n([\gamma,x]),\nu_n(g_j)|x\in G^{(i+1)}, 2\leqslant j\leqslant s)_{G^{(i+1)}} \\ &= \langle \nu_n([\gamma,x]),\nu_n(g_j)|x\in G^{(i+1)}, 2\leqslant j\leqslant s\rangle_{G^{(i+1)}} \ , \end{aligned}$$

where $\langle . \rangle$ stands for topologically generated subgroup. We also recall that $Y_n^{(i+1)}$ is a Λ-submodule of $X^{(i+1)}$ (as the kernel of an homomorphism or because $Y_n^{(i+1)} = \mathrm{Gal}(L^{(i+1)}/L^{(i)}L_n^{(i+1)})$ is a normal subgroup of $\mathrm{Gal}(L^{(i+1)}/k)$), so we have the following equation between Λ-modules

$$\nu_{n,n+1}Y_n^{(i+1)} = \nu_{n,n+1}R_n^{(i+1)} = R_{n+1}^{(i+1)} = Y_{n+1}^{(i+1)} \ .$$

Our final hypothesis $|X_n^{(i+1)}| = |X_{n+1}^{(i+1)}|$ implies that the natural restriction map $X_{n+1}^{(i+1)} \twoheadrightarrow X_n^{(i+1)}$ is an isomorphism, hence $Y_{n+1}^{(i+1)} = Y_n^{(i+1)}$ as well.
Thus Nakayama's Lemma yields $Y_n^{(i+1)} = R_n^{(i+1)} = 0$ and the theorem follows. □

Remark 2.2.12. The hypothesis $G_n^{(i)} \simeq G_{n+1}^{(i)}$ (or $R_n^{(i)} = R_{n+1}^{(i)}$ which is the same) is equivalent to those of the above theorem, i.e., $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ for $1 \leqslant j \leqslant i$.
In the same way it is easy to see that the condition $\widetilde{G}_n \simeq \widetilde{G}_{n+1}$ (or $\widetilde{R}_n = \widetilde{R}_{n+1}$) is equivalent to requiring $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ for any $j \geqslant 1$.

Remark 2.2.13. We write here some of the facts that were showed during the proof of Theorem 2.2.11 for emphasis (and for future reference). Observe that if $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ for any $1 \leqslant j \leqslant i$ then

(a) $k_m L_n^{(j)} = L_m^{(j)}$, for all $m \geqslant n$ and any $1 \leqslant j \leqslant i$;

(b) $KL_n^{(j)} = L^{(j)}$ for any $1 \leqslant j \leqslant i$;

(c) $\mathrm{Gal}(L^{(j)}/k_n) \simeq \mathbb{Z}_p \times G_n^{(j)}$ for any $1 \leqslant j \leqslant i$;

(d) $L^{(j)}/L_n^{(j)}$ is a $\mathbb{Z}_p$-extension of the number field $L_n^{(j)}$ and, for any $1 \leqslant j \leqslant i$, the fixed field of $\mathrm{Gal}(L^{(j)}/L_n^{(j)})^{p^h}$ is $L_{n+h}^{(j)}$.

We end this section showing that Theorem 2.2.11 can be applied even with slightly different hypotheses.

Proposition 2.2.14. *Assume that* $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ *for all* $j = 1, ..., i-1$ *and that* $|A(L_{n+1}^{(i-1)})| = |A(L_n^{(i-1)})|$. *Then* $X_n^{(i)} \simeq X_{n+1}^{(i)}$.

Proof. Recall that $X_n^{(i)} \simeq A(L_n^{(i-1)})_{G_n^{(i-1)}}$, i.e., $X_n^{(i)}$ is isomorphic to the maximal quotient of $A(L_n^{(i-1)})$ on which $G_n^{(i-1)} = \mathrm{Gal}(L_n^{(i-1)}/k_n)$ acts trivially (see Proposition 2.1.3 **(b)** or [40, Lemma 1]), and, since $L_n^{(i-1)} \cap k_{n+1} = k_n$, we have a surjection

$$\begin{aligned} G_{n+1}^{(i-1)} = \mathrm{Gal}(L_{n+1}^{(i-1)}/k_{n+1}) &\twoheadrightarrow \mathrm{Gal}(k_{n+1}L_n^{(i-1)}/k_{n+1}) \\ &\xrightarrow{\sim} \mathrm{Gal}(L_n^{(i-1)}/k_n) = G_n^{(i-1)} \end{aligned}$$

given by the natural restriction maps. The first hypothesis yields $G_{n+1}^{(i-1)} \simeq G_n^{(i-1)}$, so $A(L_{n+1}^{(i-1)}) \simeq A(L_n^{(i-1)})$, immediately implies $X_n^{(i)} \simeq X_{n+1}^{(i)}$. □

2.3 On the p-ranks of $X_n^{(i)}$

Definition 2.3.1.

(a) *For all* $i \geqslant 1$ *and* $n \geqslant 0$, *let* $\widetilde{\lambda}_n^{(i)} := \mathrm{rk}_p(X_n^{(i)}) = \dim_{\mathbb{F}_p}(X_n^{(i)}/pX_n^{(i)})$.

(b) *For every* $i \geqslant 1$, *let* $\widetilde{\lambda}^{(i)} := \mathrm{rk}_p(X^{(i)}) = \dim_{\mathbb{F}_p}(X^{(i)}/pX^{(i)})$.

The sequences $\{\widetilde{\lambda}_n^{(i)}\}_{n\in\mathbb{N}_0}$ are increasing (see Proposition 2.1.4 or [40, Lemma 2]) and their behaviour only depends on $\mu(K/k)$ (in particular it is independent from i).

Proposition 2.3.2.

(a) *If* $\mu(K/k) = 0$, *then* $\{\widetilde{\lambda}_n^{(i)}\}_{n\in\mathbb{N}_0}$ *is bounded for any* $i \geqslant 1$;

(b) *if* $\mu(K/k) > 0$, *then* $\{\widetilde{\lambda}_n^{(i)}\}_{n\in\mathbb{N}_0}$ *diverges for any* $i \geqslant 1$.

Proof. **(a)** If $\mu(K/k) = 0$, then $X^{(i)}$ is a finitely generated $\mathbb{Z}_p$-module for any i (see Proposition 2.1.6 or [40, Proposition 1]). Then, for all $n \in \mathbb{N}_0$, we have $\widetilde{\lambda}_n^{(i)} \leqslant \widetilde{\lambda}^{(i)}$ which is finite.
(b) Assume that for some $i \geqslant 1$ we have $\widetilde{\lambda}_n^{(i)} \leqslant t$ for all $n \in \mathbb{N}$. Now

$$\varprojlim_n X_n^{(i)}/pX_n^{(i)} = X^{(i)}/pX^{(i)}$$

and it is clear that $\widetilde{\lambda}^{(i)} \leqslant t$. This means that $X^{(i)}/\Phi(X^{(i)})$ is generated by (at most) t elements as an $\mathbb{F}_p$-vectorial space (where $\Phi(X^{(i)})$ is the Frattini subgroup of $X^{(i)}$). Thus, by Burnside Basis Theorem, these t elements generate $X^{(i)}$ as a topological group, or, which is the same, as a $\mathbb{Z}_p$-module. This contradicts Proposition 2.1.9 (i.e., [40, Proposition 2]). $\square$

The stabilization of p-ranks turns out to be much more complicated to obtain. Up to now we can only prove it with rather stringent hypotheses similar to those of Theorem 2.2.11 (in particular they yield $\lambda^{(i)} = 0$ for any i).

Theorem 2.3.3. *Suppose that* $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ *for all* $1 \leqslant j \leqslant i$, *and* $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+1}^{(i+1)}$. *Then* $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+2}^{(i+1)} = ... = \widetilde{\lambda}^{(i+1)}$.

Proof. In the proof of Theorem 2.2.11 we have already seen that the hypothesis on the orders yield

$$R_n^{(i+1)} \subseteq X^{(i+1)} \text{ if and only if } R_n^{(i)} = 0 \ .$$

We give here a different proof of it, using only group theory. Let $\pi : G^{(i+1)} \to G^{(i)}$ be the natural projection and observe that

$$\begin{aligned} R_n^{(i)} &= \pi(R_n^{(i+1)}) = (R_n^{(i+1)} \cdot C_{(i+1)}(G^{(i+1)}))/C_{(i+1)}(G^{(i+1)}) \\ &\simeq R_n^{(i+1)}/(R_n^{(i+1)} \cap C_{(i+1)}(G^{(i+1)})) = R_n^{(i+1)}/(R_n^{(i+1)} \cap X^{(i+1)}) \ . \end{aligned}$$

Thus the claim is clear.
Now the first hypothesis yields $R_n^{(i+1)} \subseteq X^{(i+1)}$, so $Y_m^{(i+1)} = \nu_{n,m} Y_n^{(i+1)}$ for all $m \geq n$. Moreover, from the hypothesis $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+1}^{(i+1)}$, we have

$$X^{(i+1)}/(Y_n^{(i+1)} + pX^{(i+1)}) = X^{(i+1)}/(\nu_{n,n+1} Y_n^{(i+1)} + pX^{(i+1)}) \ .$$

Then $Y_n^{(i+1)} + pX^{(i+1)} = \nu_{n,n+1} Y_n^{(i+1)} + pX^{(i+1)}$ and, moding out $pX^{(i+1)}$, we obtain

$$(Y_n^{(i+1)} + pX^{(i+1)})/pX^{(i+1)} = \nu_{n,n+1}(Y_n^{(i+1)} + pX^{(i+1)}/pX^{(i+1)}) \ .$$

Nakayama's Lemma yields

$$Y_n^{(i+1)} + pX^{(i+1)}/pX^{(i+1)} = 0 \quad , \text{ i.e.,} \quad Y_n^{(i+1)} \subseteq pX^{(i+1)} \ .$$

Thus $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}^{(i+1)}$. $\square$

Remark 2.3.4. Note that assuming $|X_n^{(1)}| = |X_{n+1}^{(1)}|$ (as in the above theorem) yields $\lambda^{(1)} = 0$ and, consequently, $\lambda^{(j)} = 0$ for all $j \geqslant 1$ (as mentioned before, see Proposition 2.1.8 or [40, Proposition 3]). Of course it is still possible for $\widetilde{\lambda}^{(j)}$ to be nonzero even if the applications of the theorem might be limited.

As seen in Proposition 2.2.14, if we replace the hypothesis $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+1}^{(i+1)}$ of the previous theorem with the corresponding one on class groups, i.e., $\mathrm{rk}_p(A(L_{n+1}^{(i)})) = \mathrm{rk}_p(A(L_n^{(i)}))$, then the claim remains true.

Proposition 2.3.5. *Assume that* $\mathrm{rk}_p(A(L_{n+1}^{(i)})) = \mathrm{rk}_p(A(L_n^{(i)}))$ *and that* $|X_n^{(j)}| = |X_{n+1}^{(j)}|$ *for all* $1 \leqslant j \leqslant i$. *Then* $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+2}^{(i+1)} = \dots = \widetilde{\lambda}^{(i+1)}$.

Proof. Put $A_{n+1}^{(i+1)} := A(L_{n+1}^{(i)})$ and let

$$B_{n+1}^{(i+1)} := \langle\, a^{g-1} \ :\ g \in G_{n+1}^{(i)},\ a \in A_{n+1}^{(i+1)} \rangle \subseteq A_{n+1}^{(i+1)} \ .$$

The hypothesis on the orders implies that $\mathrm{Gal}(L_{n+1}^{(i)}/L_n^{(i)}) \simeq \mathrm{Gal}(K_{n+1}/k_n)$ (see also Remark 2.2.13.**(d)**). Thus the action of g commutes with the norm $N_{L_{n+1}^{(i)}/L_n^{(i)}}$ and one gets $N_{L_{n+1}^{(i)}/L_n^{(i)}}(B_{n+1}^{(i+1)}) = B_n^{(i+1)}$. Hence

$$N_{L_{n+1}^{(i)}/L_n^{(i)}}(pA_{n+1}^{(i+1)} + B_{n+1}^{(i+1)}) = pA_n^{(i+1)} + B_n^{(i+1)} \ .$$

By the hypothesis on ranks, the norm map $N_{L_{n+1}^{(i)}/L_n^{(i)}} : A_{n+1}^{(i+1)} \to A_n^{(i+1)}$ induces an isomorphism

$$\overline{N} : A_{n+1}^{(i+1)}/pA_{n+1}^{(i+1)} \xrightarrow{\sim} A_n^{(i+1)}/pA_n^{(i+1)} \ ,$$

which induces the following one

$$A_{n+1}^{(i+1)}/(pA_{n+1}^{(i+1)} + B_{n+1}^{(i+1)}) \xrightarrow{\sim} A_n^{(i+1)}/(pA_n^{(i+1)} + B_n^{(i+1)}) \ .$$

But $A_n^{(i+1)}/(pA_n^{(i+1)} + B_n^{(i+1)})$ is canonically isomorphic to $X_n^{(i+1)}/pX_n^{(i+1)}$, so we have $\widetilde{\lambda}_n^{(i+1)} = \widetilde{\lambda}_{n+1}^{(i+1)}$ and we can apply Theorem 2.3.3. $\square$

Chapter 3

Stabilization and capitulation for $\mathbb{Z}_p$-extensions

In this chapter we look for stabilization properties for the capitulation kernels (and many more relevant groups in Iwasawa Theory) and for connections between them and the finiteness of the Iwasawa module $X := X(K/k)$. The notations are the ones established in the Chapter 1: since the extension K/k is fixed throughout the chapter we usually omit the reference to K/k in the Iwasawa invariants or in Iwasawa modules.

3.1 Introduction

We recall the definitions given in Chapter 1 for the main objects of this chapter.

Definition 3.1.1. *We denote by $H_{n,m}$ the kernel of the inclusion map $i_{n,m}$ and by H_n the kernel of i_n , i.e., $H_n = \bigcup_{m \geqslant n} H_{n,m}$. We will call $H_{n,m}$ the* relative capitulation kernel *and H_n the* absolute capitulation kernel.

We first focus our attention over the chains of absolute and relative capitulation kernels

$$H_{n_0},\ H_{n_0+1},\ H_{n_0+2}, \dots \tag{3.1}$$

and

$$H_{n,n+1} \subseteq H_{n,n+2} \subseteq H_{n,n+3} \subseteq \dots \ . \tag{3.2}$$

The first goal is to find an answer to following question: are there any stabilization properties for the sequence of the orders or for the one of the p-ranks

given from (3.1) and (3.2) ?
In Section 3.2, after some preliminary material, we provide statements like the ones of Theorems 1.4.1 and 1.4.2 for the modules H_n (see Theorem 3.2.9) and $H_{n,m}$. The starting point is the following description of the relative capitulation kernel $H_{n,m}$ in terms of the maximal finite submodule D of $X(K)$ (inspired by [38, Proposition])

Theorem 3.1.2. *For $n \gg 0$, $H_{n,m} \simeq \mathrm{Ker}\{\nu_{n,m} : D/(Y_n \cap D) \to D/(Y_m \cap D)\}$.*

In Section 3.3 we will consider some generalization of the following problem (often referred to as the *capitulation delay*): if $k_{\rho(n)}$ is the exact capitulation layer for H_n, when does H_{n+1} capitulate ? (For a precise definition of $\rho(n)$ see Definition 3.2.10.) A more general problem is to get a bound for the difference $\rho(m) - \rho(n)$ which is explicitly computable, for instance, in terms of $|H_{n,m}|$, $|A_n|$, $|A_m|$, or similar quantities. We will obtain precise values for this delay of capitulation, which is interesting also from a computational point of view as mentioned before.
In Section 3.3.1 we provide some explicit computations for all the modules (or parameters) defined in the previous sections. The computations rely on the knowledge of some specific modules D: there are results by Ozaki (see [39] and [41]) which lead us to believe that there exist $\mathbb{Z}_p$-extensions K/k with Iwasawa module isomorphic to the D's we use (indeed to any D one can imagine), but we did not pursue here the issue of finding explicitly the extension K.

We have already seen in Chapter 1 that capitulation, stabilization and the finiteness of the Iwasawa module $X(K/k)$ are closely tied (see Theorem 1.4.1, Proposition 1.5.1, Theorem 1.5.2, and Theorem 1.5.5): in the last section of this chapter we will investigate other conditions for the vanishing of the Iwasawa invariants $\mu(K/k)$ and $\lambda(K/k)$ involving the modules H_n , $H_{n,m}$ $\mathrm{Im}(i_{n,m})$, $\mathrm{Coker}(i_{n,m})$ and $\mathrm{Ker}(N_{m,n})$. For example, in Theorem 3.4.2 we prove

Theorem 3.1.3. *Assume that all primes which ramify in K/k are totally ramified. Then the following are equivalent:*

(a) $X(K)$ *is finite;*

(b) $\mathrm{Ker}(N_{n,n-1}) \subseteq H_n$ *for some* $n \geqslant 1$*;*

(c) $H_n + \mathrm{Ker}(N_{n,1}) = A_n$ *for some* $n \geqslant 1$*;*

(d) $\mathrm{Im}(i_{n-1,n}) + H_n = A_n$ *for some* $n \geqslant 1$*;*

(e) $\mathrm{Im}(i_{n,m}) = \mathrm{Im}(i_{n-1,m})$ *for some* $m \geqslant n \geqslant 1$*;*

(f) $\mathrm{rk}_p(H_n) = \mathrm{rk}_p(A_n) = \mathrm{rk}_p(A_{n+1})$ *for some* $n \geqslant 0$.

A similar statement for the p-ranks (leading to $\mu(K/k)=0$) is given in Theorem 3.4.4.

3.1.1 Preliminaries

We gather here a few well known statements in Iwasawa Theory which will be useful in the next sections.

Remark 3.1.4. We recall a general fact on modules over a commutative ring R. Let $N \subseteq M$ be R-modules such that $|M/N|$ is finite and let $\mathfrak{a} = (a_1, ..., a_u)$ be a finitely generated ideal of R. Then using induction on u, it is easy to see that $|\mathfrak{a}M/\mathfrak{a}N| \leqslant |M/N|^u$. Note, furthermore, that the given bound is sharp: take for example $M = R = \Lambda$ and $N = \mathfrak{a} = (p, T)$.

Proposition 3.1.5. *Let $\varphi : M \to N$ be a pseudo-isomorphism of Λ-modules, $\mathfrak{a}$ an ideal in Λ, τ a nonzero element of Λ and $M[\tau]$ (resp. $N[\tau]$) the kernel of $\tau : M \to M$ (resp. of $\tau : N \to N$). Then we have canonical pseudo-isomorphisms*

- **(a)** $\varphi|_{M[\tau]} : M[\tau] \to N[\tau]$;
- **(b)** $\varphi|_{\mathfrak{a}M} : \mathfrak{a}M \to \mathfrak{a}N$;
- **(c)** $\overline{\varphi} : M/\tau M \to N/\tau N$ *(where $\overline{\varphi}$ is induced by φ).*

Proof. For **(a)** and **(c)** just consider the Snake Lemma sequences associated to the diagrams

$$\begin{tikzcd} 0 \arrow[r] & M[\tau] \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "\varphi"] & \tau M \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & N[\tau] \arrow[r] & N \arrow[r] & \tau N \arrow[r] & 0 \end{tikzcd}$$

and

$$\begin{tikzcd} 0 \arrow[r] & \tau M \arrow[r] \arrow[d, "\varphi"] & M \arrow[r] \arrow[d, "\varphi"] & M/\tau M \arrow[r] \arrow[d, "\overline{\varphi}"] & 0 \\ 0 \arrow[r] & \tau N \arrow[r] & N \arrow[r] & N/\tau N \arrow[r] & 0 \end{tikzcd}$$

with easy estimates between the cardinalities of kernels and cokernels. For **(b)** use also the previous remark. □

Corollary 3.1.6. *Let M be a finitely generated torsion Λ-module and τ a nonzero element of Λ, then*

$$\gcd(\tau, f_M) = 1 \Leftrightarrow M[\tau] \sim_\Lambda 0 \Leftrightarrow M/\tau M \sim_\Lambda 0\ .$$

Moreover if any of the previous condition holds then, for any submodule N of M, the induced map $\overline{\tau} : M/N \to \tau M/\tau N$ has pseudo-null kernel.

Proof. The statements are obvious for an elementary torsion Λ-module E (where one actually finds $E[\tau] = 0$ and $E/N \simeq \tau E/\tau N$). For a general module M just consider a pseudo-isomorphism $\varphi : M \to E$ and apply the previous proposition. □

3.2 The maximal finite submodule

We now consider capitulation of ideals and study the maps $i_{n,m} : A_n \to A_m$ induced by inclusion (in particular their kernels denoted by $H_{n,m}$). We provide a description in terms of $D := D(X(K))$ (the maximal finite submodule of $X(K)$ appearing in the sequence (1.9)) in the spirit of the results of [38] for $H_n := \cup_{m \geq n} H_{n,m}$.

Definition 3.2.1. *We put*

(a) *for all $m \geqslant n \geqslant 0$, $D_{n,m} := \nu_{n,m} D$;*

(b) *for all $n \geqslant n_0$, $D_n := D \cap Y_n$.*

The following lemma shows that the D_n's behave well with respect to the usual Iwasawa relations.

Lemma 3.2.2. *For all $m \geqslant n \geqslant n_0$, we have $\nu_{n,m} D_n = D_m = D_{n,m} \cap Y_m$.*

Proof. The relation $\nu_{n,m} D_n \subseteq D_m$ is trivial. For the converse take $z \in D_m - \nu_{n,m} D_n$, i.e., an $y \in Y_n$ such that $z = \nu_{n,m} y \in D - \nu_{n,m} D_n$ and note that $y \notin D_n$ yields $y \notin D$. Since $|X/\nu_{n,m} X| \leqslant |X/Y_m| = |A_m|$ is finite and $X/\nu_{n,m} X \sim_\Lambda E(X)/\nu_{n,m} E(X)$ (by Proposition 3.1.5.**(c)**), Corollary 3.1.6 shows that $\nu_{n,m} : E(X) \to E(X)$ is injective. Hence the induced map $\nu_{n,m} : X/D \to X/D$ is injective as well: this contradicts our choice of $y \notin D$ with $\nu_{n,m} y \in D$.
For the last equality, observe that

$$\nu_{n,m} D_n \subseteq \nu_{n,m} Y_n = Y_m \Longrightarrow \nu_{n,m} D_n \subseteq \nu_{n,m} D \cap Y_m \subseteq D_m \ ,$$

and we have already seen that the two extremities of the chain are equal. □

Since $\nu_{n,m} \in (p, T)$ (the maximal ideal of Λ), Nakayama's Lemma and Lemma 3.2.2 show that, for $n \geqslant n_0$, $D_{n+1} \neq D_n$ unless $D_n = 0$. Moreover, since D is finite, there exists an m such that $D_m = 0$.

Definition 3.2.3. *We put*

(a) $r := r(K/k) = \min\{z \geqslant n_0 \ s.t. \ D_z = 0\}$*;*

(b) $\widetilde{r} := \widetilde{r}(K/k) = \min\{z \geqslant n_0 \ s.t. \ D_z \subseteq pD\}$.

Note that the isomorphisms $X/Y_m \simeq A_m$ induce embeddings $D/D_m \hookrightarrow A_m$ for all $m \geqslant n_0$ and, in particular, we can embed D into A_r .
Now we provide an isomorphism for the kernels $H_{n,m}$ in terms of the finite module D which leads to a description of H_n as in [38, Proposition].

Theorem 3.2.4. *With the above notations we have*

$$H_{n,m} \simeq \mathrm{Ker}\,\{\nu_{n,m} : D/D_n \longrightarrow D/D_m\} \tag{3.3}$$

and

$$H_n \simeq D + Y_n/Y_n \simeq D/D_n \tag{3.4}$$

for all $m \geqslant n \geqslant n_0$. Moreover, if $m \geqslant n \geqslant r(K/k)$, $H_{n,m} \simeq D[p^{m-n}]$ (where $D[p^{m-n}]$ is the submodule of the p^{m-n}-torsion elements of D).

Proof. From the well known commutative diagram

$$\begin{tikzcd} A_m \arrow[r, "\simeq"'] & X/Y_m \\ A_n \arrow[u, "i_{n,m}"] \arrow[r, "\simeq"'] & X/Y_n \arrow[u, "\nu_{n,m}"'] \end{tikzcd} \tag{3.5}$$

we have that $H_{n,m} \simeq \mathrm{Ker}\,\{\nu_{n,m} : X/Y_n \longrightarrow X/Y_m\}$. Now consider the diagram

$$\begin{tikzcd} D+Y_n/Y_n \arrow[r, hook] \arrow[d, "\nu^{(1)}_{n,m}"] & X/Y_n \arrow[r, two heads] \arrow[d, "\nu_{n,m}"] & X/D+Y_n \arrow[d, "\nu^{(2)}_{n,m}"] \\ D+Y_m/Y_m \arrow[r, hook] & X/Y_m \arrow[r, two heads] & X/D+Y_m \end{tikzcd} .$$

Let $\alpha \in X$ be such that $\nu_{n,m}\alpha \in D + Y_m$, i.e., $\alpha \pmod{D + Y_n} \in \mathrm{Ker}(\nu^{(2)}_{n,m})$. Then there exist $d \in D$ and $y_m \in Y_m$ such that $\nu_{n,m}\alpha = d + y_m$ and, since $Y_m = \nu_{m,n}Y_n$, $\nu_{n,m}\alpha = d + \nu_{n,m}y_n$ for some $y_n \in Y_n$. Therefore $\nu_{n,m}(\alpha - y_n) = d$ and $\alpha - y_n \in \mathrm{Ker}\{\nu_{n,m} : X \to X/D\}$. The injectivity of the map $\nu_{n,m} : X/D \to X/D$ yields $\alpha - y_n \in D$, i.e., $\alpha \in D + Y_n$, which means $\nu^{(2)}_{n,m}$ is injective. Hence

$$H_{n,m} \simeq \mathrm{Ker}(\nu_{n,m}) \simeq \mathrm{Ker}\left\{\nu^{(1)}_{n,m} : D + Y_n/Y_n \longrightarrow D + Y_m/Y_m\right\}$$

and the isomorphism $D/D_i = D/D \cap Y_i \simeq D + Y_i/Y_i$ concludes the proof of (3.3).
The second isomorphism follows easily.

For the final statement use (1.6) to get $\nu_{n,m} = p^{m-n} + g(T)T\nu_n$ (for some $g(T) \in \Lambda$). For $m \geqslant n \geqslant r$ one has

$$T\nu_n D = \nu_{n_0,n}\nu_{n_0}TD \subseteq \nu_{n_0,n}(Y_{n_0} \cap D) = \nu_{n_0,n}D_{n_0} = D_n = 0 \ .$$

Hence $\nu_{n,m}$ acts as multiplication by p^{m-n} on D. □

Remark 3.2.5. In [12] the authors treat capitulation in the case $\mu = 0$. If we consider X as a $\mathbb{Z}_p$-module, we can write $X \simeq \mathbb{Z}_p^\lambda \oplus \mathrm{Tor}_{\mathbb{Z}_p} X$ and, if $\mu = 0$, then $\mathrm{Tor}_{\mathbb{Z}_p} X = D$. The claims of [12, Theorem] follow easily from this observation and from Theorem 3.2.4. In particular

(a) for any $n \geqslant r$, the norm map $N_n : X \to A_n$ induces an isomorphism $D \simeq H_n$;

(b) for any $n \geqslant n_0$, H_n is a direct summand of A_n ;

(c) $A \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$.

Proof. **(a)** The map N_n is given by the projection $X \to X/Y_n$. Just note that

$$(N_n)_{|D} : D \to D + Y_n/Y_n \simeq D/D_n = D$$

for all $n \geqslant r$.
(b) Let $\mathscr{F} \simeq \mathbb{Z}_p^\lambda$ be the free part of the $\mathbb{Z}_p$-module X and note that

$$A_n \simeq \mathscr{F} + Y_n/Y_n \oplus D + Y_n/Y_n$$

for all $n \geqslant n_0$.
(c) Note that $A \simeq \varinjlim \mathscr{F} + Y_n/Y_n$ and that (for n big enough) $\nu_{m,n} = p^{m-n}u_{n,m}$ for some unit $u_{n,m} \in \Lambda^*$. □

Corollary 3.2.6. *For all $m \geqslant n \geqslant n_0$ we have*

(a) $|H_{n,m}| = \dfrac{|D| \cdot |D_m|}{|D_n| \cdot |D_{n,m}|}$;

(b) $|H_{n,m}| = |D + Y_n/D_{n,m} + Y_m| \cdot \dfrac{|A_n|}{|A_m|}$;

(c) *if $D \neq 0$ and $n \geqslant n_0$, then $i_n : A_n \to A$ is injective if and only if $n = n_0$ and D is contained in Y_{n_0} .*

Proof. **(a)** Follows immediately from Theorem 3.2.4, noting that $\mathrm{Im}(\nu_{n,m}) = D_{n,m}/D_m$.
(b) From Theorem 3.2.4 and the fact that $\mathrm{Im}(\nu_{n,m}^{(1)}) = D_{n,m} + Y_m/Y_m$, one finds

$$|H_{n,m}| = \frac{|D + Y_n/Y_n|}{|D_{n,m} + Y_m/Y_m|} \ .$$

Using the exact sequences

$$Y_n/Y_m \hookrightarrow D + Y_n/Y_m \twoheadrightarrow D + Y_n/Y_n \quad , \quad Y_n/Y_m \hookrightarrow X/Y_m \twoheadrightarrow X/Y_n$$

and

$$D_{n,m} + Y_m/Y_m \hookrightarrow D + Y_n/Y_m \twoheadrightarrow D + Y_n/D_{n,m} + Y_m$$

(recalling that $|X/Y_i| = |A_i|$ for any $i \geqslant n_0$), one gets

$$\begin{aligned}\frac{|D + Y_n/Y_n|}{|D_{n,m} + Y_m/Y_m|} &= \frac{|D + Y_n/Y_m|}{|Y_n/Y_m|} \cdot \frac{|D + Y_n/D_{n,m} + Y_m|}{|D + Y_n/Y_m|} \\ &= \frac{|D + Y_n/D_{n,m} + Y_m|}{|Y_n/Y_m|} = |D + Y_n/D_{n,m} + Y_m| \cdot \frac{|A_n|}{|A_m|} \ .\end{aligned}$$

(c) By Theorem 3.2.4, $H_n = 0$ implies $D \subseteq Y_n \subseteq Y_{n_0}$, then $D = D_n = D_{n_0}$. Now as remarked before Definition 3.2.3, since D is not zero, we obtain $n = n_0$ and $D \subseteq Y_{n_0}$. The converse is trivial. □

Note that from the last assertion it follows that if $D \neq 0$ and $n > n_0$, then there are at least $p - 1$ ideal classes in A_n which capitulate in some A_m .

Corollary 3.2.7. *For any $\mathbb{Z}_p$-extension K/k, the following are equivalent:*

(a) *X does not contain any nontrivial finite submodule;*

(b) *$H_{n_0+1} = 0$;*

(c) *$i_{n,m} : A_n \to A_m$ are injective for all $m \geqslant n \geqslant n_0$.*

Proof. **(a)** $\Rightarrow$ **(c)** follows from Theorem 3.2.4, **(c)** $\Rightarrow$ **(b)** is obvious and **(b)** $\Rightarrow$ **(a)** is given by Corollary 3.2.6.**(c)** . □

An example for **(a)** is provided by the minus part of the Iwasawa module for the $\mathbb{Z}_p$-cyclotomic extension of a CM field (see [48, Propositions 13.26 and 13.28]), similar results can be derived from [38].
The following corollary generalizes [10, Proposition].

Corollary 3.2.8. *Let K/k be a $\mathbb{Z}_p$-extension, assume that $A_n \neq 0$ and $i_{n,m}$ is injective for some $m > n \geqslant n_0$. Then $|A_m| \geqslant p^{m-n}|A_n|$.*

Proof. It suffices to prove that $Y_i \supsetneq Y_{i+1}$ for any $n \leqslant i \leqslant m-1$ or, equivalently, $Y_{m-1} \neq 0$. So we assume $Y_{m-1} = 0$ and look for a contradiction. Obviously

$$|A_n| = |i_{n,m-1}(A_n)| = |\nu_{n,m-1}X/Y_{m-1}| = |\nu_{n,m-1}X|$$

and

$$|A_n| = |i_{n,m}(A_n)| = |\nu_{n,m}X/Y_m| = |\nu_{n,m}X| \ .$$

This yields $\nu_{m-1,m}\nu_{n,m-1}X = \nu_{n,m-1}X$ and, by Nakayama's Lemma, $\nu_{n,m-1}X = 0$. Then $i_{n,m}$ is the zero map and this contradicts $A_n \neq 0$. □

As customary for Iwasawa modules, the H_n's verify some stabilization results.

Theorem 3.2.9. *Assume $n \geqslant n_0$:*

(a) *if $|H_n|$=$|H_{n+1}|$, then $H_m \simeq H_n \simeq D$ for all $m \geqslant n$. In particular*

$$|H_{n_0}| < |H_{n_0+1}| < \ldots < |H_r| = |H_{r+1}| = \ldots = |D| \; ; \qquad (3.6)$$

(b) *if $\mathrm{rk}_p(H_n) = \mathrm{rk}_p(H_{n+1})$, then $\mathrm{rk}_p(H_m) = \mathrm{rk}_p(H_n) = \mathrm{rk}_p(D)$ for all $m \geqslant n$. In particular*

$$\mathrm{rk}_p(H_{n_0}) < \mathrm{rk}_p(H_{n_0+1}) < \ldots < \mathrm{rk}_p(H_{\widetilde{r}}) = \mathrm{rk}_p(H_{\widetilde{r}+1}) = \ldots = \mathrm{rk}_p(D) \; . \qquad (3.7)$$

Proof. **(a)** Since $H_n \simeq D/D_n$, the hypothesis yields $D_n = D_{n+1} = \nu_{n,n+1}D_n$ (by Lemma 3.2.2). Nakayama's Lemma implies $D_n = 0$, so, for any $m \geqslant n$, $D_m = 0$ and $H_m \simeq H_n \simeq D$. The cardinalities in (3.6) follow from the definition of r.
(b) The hypothesis yields $D/D_n + pD \simeq D/D_{n+1} + pD$, i.e., $D_n + pD = D_{n+1} + pD$. Therefore $D_n + pD/pD = \nu_{n,n+1}(D_n + pD/pD)$ and, from Nakayama's Lemma, $D_n{+}pD/pD = 0$. Thus, for any $m \geqslant n$, $D_m \subseteq D_n \subseteq pD$ and $D/D_m + pD = D/D_n + pD = D/pD$, which is the claim. ☐

From Theorem 3.2.9, we have $r = \min\{z \geqslant n_0 \; s.t. \; H_z = H_{z+1}\}$ and $\widetilde{r} := \min\{z \geqslant n_0 \; s.t. \; \mathrm{rk}_p(H_z) = \mathrm{rk}_p(H_{z+1})\}$, so these two parameters indicate the stabilization of orders and p-ranks of the H_n's (even if they were at first expressed in terms of D_n's). Motivated by this, we define other parameters dealing with the stabilization of the $H_{n,m}$'s and the delay of capitulation.

Definition 3.2.10. *We put*

(a) *for any $n \geqslant 0$, $h(n) := \min\{z \geqslant n \; s.t. \; D_{n,z} = 0\}$;*

(b) *for any $n \geqslant n_0$, $\rho(n) := \min\{z \geqslant n \; s.t. \; H_{n,z} = H_z\} = \min\{z \geqslant n \; s.t. \; D_{n,z} = D_z\}$.*

(c) $\widetilde{\rho}(n) := \min\{z \geq n \; s.t. \; \mathrm{rk}_p(H_{n,z}) = \mathrm{rk}_p(H_n)\}$.

Remarks 3.2.11.

1. For notational convenience we shall also use $r_1(n) := \min\{z \geqslant n \; s.t. \; D_z = 0\}$ (for $n \geqslant n_0$). Note that, by definition,

$$r_1(n) = \begin{cases} r & \text{if } n_0 \leqslant n \leqslant r \\ n & \text{if } n \geqslant r \end{cases} \quad .$$

2. Note that the different parameters verify some obvious relations which basically derive from their definitions. In particular

$$n_0 \leqslant \widetilde{r} \leqslant r = r_1(n_0) \leqslant r_1(n)\ ,\ n_0 \leqslant n \leqslant r_1(n) \leqslant h(n)$$

and

$$n_0 \leqslant n \leqslant \widetilde{\rho}(n) \leqslant \rho(n) \leqslant h(n)$$

(the last one follows from $D_{h(n)} = \nu_{n,h(n)} D_n \subseteq D_{n,h(n)} = 0$).

3. From Theorem 3.2.4 and the definition of ρ, for any $m \geqslant \rho(n)$, one has $|H_n| = |H_{n,m}| = \dfrac{|D|}{|D_n|}$ and $\mathrm{rk}_p(H_n) = \mathrm{rk}_p(H_{n,m}) = \mathrm{rk}_p(D/D_n)$.

The following propositions (and their corollaries) emphasize similarities (and differences) between $\rho(n)$ and $h(n)$.

Proposition 3.2.12. *Let $|D| = p^\delta$ with $\delta \in \mathbb{N}$ and let $p^\varepsilon \in \mathbb{N}$ be the exponent of D (i.e., the minimum integer for which $p^\varepsilon D = 0$). Then*

(a) *for every $n \geqslant 0$, we have $h(n) - n \leqslant \delta$ and, for every $n \geqslant \delta - 1$, $h(n) - n = \varepsilon$;*

(b) *$h(n) - n = \varepsilon$ holds, also, for all $n \geqslant r$.*

Proof. **(a)** The first statement follows from Nakayama's Lemma: indeed, for any $n \geqslant 0$, $\nu_{n,n+\delta} D = 0$ (since $\nu_{n,m} P = P$ if and only if $P = 0$, the order of a nontrivial module must decrease of a factor at least p at any step, i.e., D vanishes after at most δ steps).
For the second statement, consider the action of $\Gamma = \mathrm{Gal}(K/k)$ over D and let p^Δ be the cardinality of the greatest orbit in D. Then Γ^{p^Δ} acts trivially on D, so, for all $n \geqslant \delta - 1 \geqslant \Delta$, the element $\nu_{n,n+1} = 1 + \gamma^{p^n} + \ldots + \gamma^{(p-1)p^n}$ acts on D as multiplication by p. This implies $\nu_{n,n+\varepsilon-1} D = p^{\varepsilon-1} D \neq 0$ and $\nu_{n,n+\varepsilon} D = p^\varepsilon D = 0$, i.e., $h(n) = n + \varepsilon$.
(b) As seen in the proof of Theorem 3.2.4, for $m \geqslant r$, $\nu_{m,m+1} D = pD$. This yields $h(n) = n + \varepsilon$. □

Corollary 3.2.13. *We have:*

(a) *for all $n \geqslant n_0$,*

$$\begin{aligned} 1 = |H_{n,n}| &\leqslant |H_{n,n+1}| \leqslant |H_{n,n+2}| \leqslant \cdots \leqslant |H_{n,r_1(n)}| \\ &= |H_{n,r_1(n)}| < |H_{n,r_1(n)+1}| < |H_{n,r_1(n)+2}| < \cdots < |H_{n,h(n)}| \\ &= |H_{n,h(n)}| = |H_{n,h(n)+1}| = |H_{n,h(n)+2}| = \cdots = |D/D_n|\ ; \end{aligned}$$

(b) *if $n \geqslant r$, $|H_{n,m}| = \frac{|D|}{|D_{n,m}|}$ for all $m \geqslant n$ and*

$$1 < |H_{n,n+1}| < \cdots < |H_{n,h(n)}| = |H_{n,h(n)+1}| = \cdots = |D|\ .$$

Proof. Everything follows immediately from Corollary 3.2.6. For the central line of **(a)** we just remark that, since $\nu_{n,r_1(n)+j}D_n = D_{r_1(n)+j} = 0$ for any $j \geqslant 0$, one has

$$|H_{n,r_1(n)+j}| = \frac{|D|}{|D_n| \cdot |D_{n,r_1(n)+j}|} \ .$$

Moreover, by Lemma 3.2.2 and Nakayama's Lemma, the $D_{n,r_1(n)+j}$'s stabilize (i.e., become 0) only at the level $D_{n,h(n)}$. ☐

Proposition 3.2.14.

(a) *If $n \geqslant n_0$ and $r_1(n) \neq h(n)$, then $\rho(n) = h(n)$. Moreover if $n \geqslant r$, then $\rho(n) = h(n) = n + \varepsilon$.*

(b) *For all $n \geqslant n_0$, $\rho(n) - n \leqslant \delta$.*

(c) *Assume $D \neq 0$ and $r \geqslant \delta$: moreover assume that $r = n_0 + 1$ and $D \not\subseteq Y_{n_0}$, or that $r > n_0 + 1$. Then $\rho(r-1) - (r-1) = \varepsilon$.*

(d) *For all $n \geq n_0$ we have*

$$\widetilde{\rho}(n) \begin{cases} = n+1 & \text{if } n \geq r \text{ and } D \neq 0 \\ \leq r+1 & \text{if } \widetilde{r} \leq n < r \\ \leq r & \text{if } n < \widetilde{r} \end{cases} .$$

Proof. **(a)** If $r_1(n) \neq h(n)$, then the central line in Corollary 3.2.13.**(a)** is nontrivial. Hence $H_{n,h(n)} = H_n$ and $h(n)$ is the minimal index with this property, i.e., $h(n) = \rho(n)$.
If $n \geqslant r$, then, by definition, $D_m = \nu_{r,m}D_r = 0$. Hence $0 = D_m = D_{n,m}$ if and only if $m \geqslant h(n)$ and, by the minimality of $\rho(n)$, one gets $\rho(n) = h(n)$ (in particular $\rho(n) = n + \varepsilon$ in this case).
(b) Follows easily from **(a)** and Proposition 3.2.12.
(c) By Proposition 3.2.12.**(a)** we have $h(r-1) - (r-1) = \varepsilon$, so, if $h(r-1) > r_1(r-1) = r$, the thesis follows from part **(a)**. If $h(r-1) = r_1(r-1) = r$, then the additional hypotheses ensure that $H_{r-1} \neq 0 = H_{r-1,r-1}$ (see Corollary 3.2.6.**(c)**). Thus $\rho(r-1) = h(r-1) = r$ and the statement follows (this can only happen when $\varepsilon = 1$).
(d) Observe that, if $n \geq r$, we have $D_n = 0$ and $\nu_{n,m}$ acts as p^{m-n} on D from (1.6). Hence $\widetilde{\rho}(n) = n + 1$. The other cases are clear. ☐

Remarks 3.2.15.

1. If we assume that $|A_{n+1}| = |A_n|$ for some $n \geqslant n_0$ then, $Y_n = 0$ and $X = D \simeq A_n$. Therefore $D_n = 0$ and $r \leqslant n$. Thus, for every $m \geqslant n$, $\rho(m) = m + \varepsilon$, i.e., A_m capitulates in $A_{m+\varepsilon}$ but not in $A_{m+\varepsilon-1}$.

2. We emphasize the difference between the layers n_0 and n_0+1 (already showed by Corollary 3.2.6.**(c)**, we will see similar phenomenons in Section 3.4): if $D \neq 0$, then for every $n > n_0$ there exists a non zero class of ideal in A_n which capitulates in A, while we might have no capitulation from A_{n_0} to A. It is also easy to find examples in which $A_0 = 0$ and A_1 does not capitulate. Just take $k = \mathbb{Q}(\sqrt{m})$ an imaginary quadratic field, a prime p which splits in k and does not divide the class number of k and $K = k_{cyc}$ the cyclotomic $\mathbb{Z}_p$-extension of k. Then A_1 does not capitulate because $\lambda(k_{cyc}/k) \geqslant 1$ (see Theorem 3.4.2).

From Proposition 3.2.14 we obtain equations analogous to those in Corollary 3.2.13 **(a)** and **(b)**. Now, as a further application of the theory developed until here, we can consider the sequences of the $H_{n,m}$'s but fixing m and letting the lower index vary.

Proposition 3.2.16. *Let $m \geqslant n_0$ be a fixed integer.*

(a) *If $m \geqslant r + \varepsilon$, we have*

$$|H_{n_0,m}| < \ldots < |H_{r,m}| = \ldots = |H_{m-\varepsilon,m}| > \ldots > |H_{m,m}| = 1 \ .$$

(b) *If $r < m < r + \varepsilon$, let $n_1 := \max(\{n_0\} \cup \{q \geqslant n_0 \ : \ \rho(q) \leqslant m\})$. Then we have*

$$|H_{n_0,m}| < \ldots < |H_{n_1,m}| \quad \textit{and} \quad |H_{r,m}| > \ldots > |H_{m,m}| = 1 \ .$$

Proof. **(a)** If n is contained in $\{n_0, \ldots, m-\varepsilon\}$ then, by Proposition 3.2.14**(b)**, we have $\rho(n) \leqslant \rho(m-\varepsilon) = m$ and this means $H_{n,m} = H_n$ for all $n_0 \leqslant n \leqslant m - \varepsilon$. Hence, from Theorem 3.2.9**(a)**, we obtain the first piece of our equation. The second part follows from the last statement of Theorem 3.2.4. **(b)** Note that, essentially by definition, $n_1 < r$. If $n \in \{n_0, \ldots, n_1 - 1\}$, we have $\rho(n+1) \leqslant \rho(n_1) \leqslant m$. This means $H_{n+1,m} = H_{n+1}$ and, from Theorem 3.2.9**(a)**, we obtain the first equation. The second one follows from Theorem 3.2.4 as before. ☐

In the remaining case, i.e., $m \leqslant r(K/k)$, we do not have a precise statement (except for the obvious one $|H_{n_0,m}| < \ldots < |H_{n_1,m}|$ as in the previous proposition, part **(b)**). As far as the p-ranks are concerned, we have the following corollary to Proposition 3.2.14.

Corollary 3.2.17.

(a) *If $D \neq 0$ and $m \geqslant r + 1$, we have*

$$0 \leqslant \mathrm{rk}_p(H_{n_0,m}) < \ldots < \mathrm{rk}_p(H_{\widetilde{r},m}) = \ldots$$

$$\ldots = \mathrm{rk}_p(H_{r,m}) = \ldots = \mathrm{rk}_p(H_{m-1,m}) > \mathrm{rk}_p(H_{m,m}) = 0 \ .$$

(b) *If* $m \leqslant r$, *let* $n_2 := \max(\{n_0\} \cup \{n : n_0 \leqslant n \leqslant \widetilde{r}(K/k)$ *and* $\rho(n) \leqslant m\})$. *Then*

$$\mathrm{rk}_p(H_{n_0,m}) < \ldots < \mathrm{rk}_p(H_{n_2,m}) \ .$$

Proof. The equation in **(a)** follows from Proposition 3.2.14 and Theorem 3.2.9**(b)**. The one in **(b)** is clear from the same Theorem. □

Before looking at some explicit examples we recall that, since $N_{m,n} \circ i_{n,m}$ is the multiplication by p^{m-n} map, one has $\exp(H_{n,m}) \leqslant p^{m-n}$ for all $m \geqslant n \geqslant 0$. For example, if $n \geqslant r$, then $H_{n,n+1}$ is a non-trivial elementary p-group.

Example 3.2.18. By [39, Theorem 1], for any finite $\mathbb{Z}_p[[\Gamma]]$-module D there exist a field k whose cyclotomic $\mathbb{Z}_p$-extension provides $X(k_{cyc}) \simeq D$. Take $D \simeq \Lambda/(p^u, T)$: then there exists u_0 such that $0 \leqslant u_0 \leqslant u$ and $D_0 = p^{u_0} D$. A little calculation shows that

$$|H_{n,m}| = \begin{cases} 1 & \text{if } 0 \leqslant n \leqslant m \leqslant u - u_0 \\ p^{m-u+u_0} & \text{if } n \leqslant u - u_0 \ \text{ and } \ u - u_0 < m \leqslant n + u \\ p^{m-n} & \text{if } n > u - u_0 \ \text{ and } \ n \leqslant m \leqslant n + u \\ p^u & \text{if } n > u - u_0 \ \text{ and } \ m > n + u \ . \end{cases}$$

Furthermore we can easily see that our parameters take the following values:

$$r = u - u_0 \ , \ \widetilde{r} = 0 \ \text{ and, for any } n \geqslant 0, \ \ r_1(n) = \max\{n, \ u - u_0\} \ ,$$

$$h(n) = \rho(n) = n + u \ \text{ and } \ \widetilde{\rho}(n) = \max\{n + 1, \ u - u_0 + 1\} \ .$$

In particular, if $n \leqslant u - u_0$, the equation of Corollary 3.2.13 becomes

$$1 = |H_{n,n}| = \ldots = |H_{n,u-u_0}| < \ldots < |H_{n,n+u}| = \ldots = |H_n| \ .$$

Example 3.2.19. Let $v \geqslant 1$ and $D \simeq \Lambda/(p, T^v)$. As in the previous example, there exist a number field k whose cyclotomic $\mathbb{Z}_p$-extension provides $X(k_{cyc}) \simeq D$ and, starting from some large layer, we can assume $Y_0 = 0$.
With a little computation one can show that, for all $m \geqslant n \geqslant 0$, we have

$$|H_{n,m}| = \begin{cases} p^{p^m - p^n} & \text{if } m \leqslant \lfloor \log_p(v + p^n - 1) \rfloor \\ p^v & \text{if } m > \lfloor \log_p(v + p^n - 1) \rfloor \end{cases}$$

and

$$\mathrm{rk}_p(H_{n,m}) = \begin{cases} p^m - p^n & \text{if } m \leqslant \lfloor \log_p(v + p^n - 1) \rfloor \\ v & \text{if } m > \lfloor \log_p(v + p^n - 1) \rfloor \end{cases} ,$$

where $\lfloor a \rfloor$ is the floor of $a \in \mathbb{R}$ (i.e., the largest integer less than or equal to a). Our parameters take the following values:

$$r = 0 \ , \ \widetilde{r} = 0 \ \text{ and, for any } n \geqslant 0, \ r_1(n) = n \ , h(n) = \lfloor \log_p(v + p^n - 1) \rfloor + 1 \ ,$$

$$\rho(n) = \lfloor \log_p(v + p^n - 1) \rfloor + 1 \ \text{ and } \ \widetilde{\rho}(n) = \lfloor \log_p(v + p^n - 1) \rfloor + 1 \ .$$

As a final remark, note that if we define

$$\begin{aligned} \alpha \quad &:= \max\{i \in \mathbb{N}_0 \,:\, v > p^{i+1} - p^i\} \\ &= \max\{i \in \mathbb{N}_0 \,:\, v + p^i \geqslant p^{i+1} + 1\} \\ &= \max\{i \in \mathbb{N}_0 \,:\, \lfloor \log_p(v + p^i - 1) \rfloor > i\} \end{aligned} \quad ,$$

then we have that $|H_{n,n+1}| = p^v$ if (and only if) $n \geqslant \alpha + 1$. In particular $h(n) = \rho(n) = n + 1$ when $n \geqslant \alpha + 1$.

3.2.1 Relation between $\mathrm{rk}_p(H_n)$, $\widetilde{\lambda}_n$ and $X \sim_\Lambda 0$

We conclude this section with a theorem which relates $\mathrm{rk}_p(H_n)$, $\widetilde{\lambda}_n$ and pseudo-nullity of X. To simplify notations we assume $n_0 = 0$ even if this is not a necessary condition.

Theorem 3.2.20. *If $\mathrm{rk}_p(H_n) = \widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$ for some $n \geqslant 0$, then X is pseudo-null.*

Proof. Consider the map $\psi := \pi \circ i$ given by the composition

$$D + Y_n \xhookrightarrow{\quad i \quad} X \xrightarrow{\quad \pi \quad} X/Y_n + pX \quad .$$

Since $\widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$ (i.e., $Y_n \subseteq pX$, by Theorem 1.4.1), we have the equalities

$$\mathrm{Ker}(\psi) = (D+Y_n) \cap (pX+Y_n) = (D+Y_n) \cap pX = (D \cap pX) + Y_n = pD + Y_n \ ,$$

where the last equality comes from Corollary 3.1.6 (indeed if px is an element of $D \cap pX$ of order p^β , then $x \in \mathrm{Ker}\{p^{\beta+1} : X \to X\}$ which is finite, hence contained in D, because $\mu(K/k) = 0$). So ψ induces an embedding

$$D + Y_n/pD + Y_n \xhookrightarrow{\quad \overline{\psi} \quad} X/Y_n + pX \ .$$

Now note that $D + Y_n/pD + Y_n \simeq D/(D \cap Y_n) + pD \simeq H_n/pH_n$ (by Theorem 3.2.4), hence the hypothesis $\mathrm{rk}_p(H_n) = \widetilde{\lambda}_n$ implies that $\overline{\psi}$ is an isomorphism. Then $X = D + pX$ and eventually $X = D$. □

3.3 Bounds for $\rho(m) - \rho(n)$

By definition we have that ideals in H_n capitulate exactly in $A_{\rho(n)}$ (i.e., $\rho(n) - n$ measures how much capitulation is delayed in the tower). We have given estimates for $\rho(n) - n$ in Proposition 3.2.14, now we are going to provide bounds for the rate of growth of the sequence of the $\rho(n)$'s, i.e., for $\rho(m) - \rho(n)$ when $m \geqslant n$. By Proposition 3.2.14.**(a)** we know that $\rho(n) = n + \varepsilon$ for any $n \geqslant r$, hence for any $m \geqslant n \geqslant r$ one has $\rho(m) - \rho(n) = m - n$. We now consider indices between n_0 and r and, to avoid trivialities, we assume $X \neq 0$ (while $D = 0$ is permitted even if no proofs would be needed in that case). We begin with some estimates on the growth of the parameter $h(n)$ (defined for all $n \geqslant 0$). The easiest one follows from $h(m) \leqslant m + \delta = m + \log_p(|D|)$ (Proposition 3.2.12.**(a)**) which yields

$$h(m) - h(n) \leqslant \log_p(|D|) + m - n \tag{3.8}$$

(if $D \neq 0$ one can add a -1 on the right side). The following results improve this bound and lead to an estimate for $\rho(m) - \rho(n)$. They can all be formulated (and proved) in terms of the D_n's (which provide sharper bounds), but in the main statements we prefer to use the A_n's which are more suitable for computations in explicit examples.

Proposition 3.3.1. *For all $m > n \geqslant 0$ we have*

$$h(m) - h(n) \leqslant \log_p\left(\frac{|D|}{|D_{n,m}|}\right) + \max\{0, m - h(n)\}\ . \tag{3.9}$$

Proof. If $h(n) \geqslant m$, then $\nu_{n,m} D_{m,h(n)} = \nu_{n,m}\nu_{m,h(n)} D = \nu_{n,h(n)} D = 0$. Hence $|D_{m,h(n)}| \leqslant \frac{|D|}{|D_{n,m}|}$. Now note that $\nu_{h(n),h(m)} D_{m,h(n)} = D_{m,h(m)}$ $= 0$, so, by Nakayama's Lemma and the minimality of $h(m)$, we have that $|D_{m,h(n)}| \geqslant p^{h(m)-h(n)}$. Therefore

$$h(m) - h(n) \leqslant \log_p\left(\frac{|D|}{|D_{n,m}|}\right)\ .$$

If $m > h(n)$, then $D_{n,m} = 0$ and we write $h(m) - h(n) = h(m) - m + (m - h(n))$. One has

$$h(m) - h(n) \leqslant \log_p(|D|) + m - h(n) = \log_p\left(\frac{|D|}{|D_{n,m}|}\right) + m - h(n)\ .$$

□

Note that if $h(n) \geqslant m$, then the last term in (3.9) (i.e., $\max\{0, m - h(n)\}$) disappears: this certainly happens, for example, when $m = n + 1$.

Theorem 3.3.2. *For all $m \geqslant n \geqslant n_0$ we have*

$$h(m) - h(n) \leqslant \log_p\left(\frac{|A_m|}{|A_n|}\right) + \log_p(|H_{n,m}|) + m - n\ . \tag{3.10}$$

and

$$h(m) - h(n) \leqslant \log_p\left(\frac{|A_m|}{|A_n|}\right) + \sum_{i=1}^{m-n} \log_p(|H_{n+i-1,n+i}|)\ . \tag{3.11}$$

Proof. The first equation follows from Proposition 3.3.1 and Corollary 3.2.6.**(a)**, which yields

$$h(m)-h(n)\leqslant \log_p\left(\frac{|D|}{|D_{n,m}|}\right)+m-n=\log_p\left(\frac{|D_n|}{|D_m|}\right)+\log_p(|H_{n,m}|)+m-n\ .$$

Now note that we can embed D_n/D_m into Y_n/Y_m and (as seen in the proof of Corollary 3.2.6.**(b)**) we have $|Y_n/Y_m|=\frac{|A_m|}{|A_n|}$.
If $D\neq 0$, take any $i\in\{1,\dots,m-n\}$ and use (3.9) to get

$$h(n+i)-h(n+i-1)\leqslant \log_p\left(\frac{|D|}{|D_{n+i-1,n+i}|}\right)$$

(note that if $D\neq 0$ then $h(n+i-1)\geqslant n+i$). Summing up one finds

$$h(m)-h(n)\leqslant \sum_{i=1}^{m-n}\log_p\left(\frac{|D|}{|D_{n+i-1,n+i}|}\right)=\log_p\left(\frac{|D|^{m-n}}{\prod_{i=1}^{m-n}|D_{n+i-1,n+i}|}\right)\ .$$

Using again Corollary 3.2.6.**(a)**, we have

$$\begin{aligned}\log_p\left(\frac{|D|^{m-n}}{\prod_{i=1}^{m-n}|D_{n+i-1,n+i}|}\right)&=\log_p\left(\prod_{i=1}^{m-n}|H_{n+i-1,n+i}|\cdot\frac{|D_{n+i-1}|}{|D_{n+i}|}\right)\\&=\log_p\left(\frac{|D_n|}{|D_m|}\right)+\log_p\left(\prod_{i=1}^{m-n}|H_{n+i-1,n+i}|\right)\\&=\log_p\left(\frac{|D_n|}{|D_m|}\right)+\sum_{i=1}^{m-n}\log_p(|H_{n+i-1,n+i}|)\ .\end{aligned}$$

We have already seen that $|D_n/D_m|\leqslant\frac{|A_m|}{|A_n|}$, so the proof is complete. □

Now we use the previous results to achieve the bounds for $\rho(m)-\rho(n)$ when $m\geqslant n\geqslant n_0$. The easiest one, coming from (3.8), is

$$\rho(m)-\rho(n)\leqslant\delta+m-n\ . \tag{3.12}$$

Corollary 3.3.3. *For all $m\geqslant n\geqslant n_0$, we have*

$$\rho(m)-\rho(n)\leqslant\log_p\left(\frac{|D|}{|D_{n,m}|}\right)+\max\{0,m-h(n)\}+(h(n)-\rho(n))\ , \tag{3.13}$$

$$\rho(m)-\rho(n)\leqslant\log_p\left(\frac{|A_m|}{|A_n|}\right)+\log_p(|H_{n,m}|)+m-n+\max\{0,r-\rho(n)\} \tag{3.14}$$

and

$$\rho(m)-\rho(n)\leqslant\log_p\left(\frac{|A_m|}{|A_n|}\right)+\sum_{i=1}^{m-n}\log_p(|H_{n+i-1,n+i}|)+\max\{0,r-\rho(n)\}\ . \tag{3.15}$$

Proof. Just note that $\rho(m)-\rho(n) \leqslant h(m)-\rho(n) = h(m)-h(n)+h(n)-\rho(n)$ and use the bounds of Proposition 3.3.1 and Theorem 3.3.2. $\square$

We remark that the last two bounds are not completely independent from D, since it implicitly appears in the constant r.

Remark 3.3.4. The bound given in (3.13) is always better or equal to the one given in (3.12). The proof is an easy computation for which we have only to distinguish the following four cases: (1) $n \geqslant r$, (2) $n < r$, $m \leqslant h(n)$ and $m \geqslant r$, (3) $n < r$ and $m \geqslant h(n)$, (4) $m < r$.
We prove (1) as an example: we have $\log_p\left(\frac{|D|}{|D_{n,m}|}\right) \leqslant \delta$, $h(n) = \rho(n) = n+\varepsilon$ and $\max\{0, m-h(n)\} = \max\{0, m-n-\varepsilon\}$. Then

$$\begin{aligned} &\log_p\left(\frac{|D|}{|D_{n,m}|}\right) + \max\{0, m-h(n)\} \\ +h(n)-\rho(n) &\leqslant \begin{cases} \delta + m - h(n) & \text{if } m \geqslant h(n) \\ \delta & \text{if } m < h(n) \end{cases} \\ &\leqslant \delta + m - n\ . \end{aligned}$$

The proofs of the other cases are similar.

3.3.1 Sharpness of the bounds

Ozaki proved that for every prime p and every finite Λ-module D there exists a totally real field k whose cyclotomic $\mathbb{Z}_p$-extension has Iwasawa module isomorphic to D (see [39, Theorem 1]) as we already mentioned in Examples 3.2.18 and 3.2.19. For an explicit computation of all our parameters we need to know the module Y_0 as well. There are easy cases in which $Y_0 = X$ or $Y_0 = TX$ but they depend on the class group of k or on the number (and behaviour) of the primes of k above p and Ozaki's results give no informations about them.
To speculate on the possible values of our parameters it seems reasonable to assume the following (it can be considered as a conjecture generalizing Ozaki's results):

Assumption 3.3.5. *Let Γ be a (multiplicative) topological group isomorphic to $\mathbb{Z}_p$ and let $D_0 \subseteq D$ be two finite $\mathbb{Z}_p[[\Gamma]]$-modules. Then there exists a number field k and a $\mathbb{Z}_p$-extension K of k such that*

- $n_0(K/k) = 0$;
- *the Iwasawa module $X(K/k)$ is isomorphic to D;*
- *the submodule $Y_0(K/k)$ is isomorphic to D_0 ,*

via the isomorphism induced by $\Gamma \simeq \mathrm{Gal}(K/k)$.

The following proposition provides a strategy (and the explicit modules) to prove the sharpness of some of the previous bounds.

Proposition 3.3.6. *Assume Assumption 3.3.5, then for any* $0 \leqslant r' \leqslant h'$ *and for every finite sequence of integers* $\{t_i\}_{1\leqslant i\leqslant h'}$ *such that*

$$\begin{cases} t_i \geqslant 0 & \text{if } 1 \leqslant i \leqslant r' \\ t_{r'+1} \geqslant t_{r'+2} \geqslant \ldots \geqslant t_{h'} \geqslant 1 \end{cases},$$

there exist a number field k *and a* $\mathbb{Z}_p$*-extension* K/k *such that*

$$n_0(K/k) = 0\ ,\ r(K/k) = r'\ ,\ h(0) = h'\ ,\ \frac{|H_{0,i}|}{|H_{0,i-1}|} = p^{t_i} \text{ for all } 1 \leqslant i \leqslant h'$$

and

$$|H_{0,j}| = p^{\sum_{i=1}^{h'} t_i} \text{ for any } j \geqslant h'\ .$$

Proof. Let

$$D = \bigoplus_{i=1}^{r'} (\Lambda/(p^i,T))^{t_i} \oplus \Lambda/(p^{r'},T) \oplus \bigoplus_{i=r'+1}^{h'-1} (\Lambda/(p^i,T))^{t_i-t_{i+1}} \oplus (\Lambda/(p^{h'},T))^{t_{h'}}$$

and

$$D_0 = \bigoplus_{i=1}^{r'} ((p,T)/(p^i,T))^{t_i} \oplus \Lambda/(p^{r'},T)$$

$$\oplus \bigoplus_{i=r'+1}^{h-1} ((p^{i-r'},T)/(p^i,T))^{t_i-t_{i+1}} \oplus ((p^{h'-r'},T)/(p^{h'},T))^{t_{h'}}\ .$$

There are four summands both in D and D_0: the first one influences the part $|H_{0,0}| \leqslant |H_{0,1}| \leqslant \ldots \leqslant |H_{0,r'}|$, the second one is the same for D and D_0 and it guarantees that $r(K/k) = r'$, the last two affect the part $|H_{0,r'}| < |H_{0,r'+1}| < \ldots < |H_{0,h'}|$. The checking of the claim is just a matter of direct (even if a bit involved) calculation. □

Looking at Corollary 3.2.13, we see that the previous proposition shows that every possibility for the part $|H_{n,n}| \leqslant |H_{n,n+1}| \leqslant \ldots \leqslant |H_{n,r}|$ (when $n \leqslant r$) is realizable. In particular if $|H_{n,q}|$ stabilizes at a certain index m, i.e., $|H_{n,m}| = |H_{n,m+1}| = \ldots = |H_{n,t}|$ for some $n \leqslant m < r$, then this does not guarantee a definitive stabilization, i.e., we can still have $|H_{n,t}| < |H_{n,t+1}|$.
Furthermore note that if $h(n) = r+1$ for some $n \geqslant n_0$, then Proposition 3.3.6 can take the following form: *every situation not explicitly prohibited by Corollary 3.2.13 is realizable.* Nevertheless Proposition 3.3.6 does not describe all possible situations: for example a case in which $t_{r'+1} < t_{r'+2} < \ldots < t_{h'}$ can be easily realized (a particular case is provided by Example 3.2.19), but involves a more complicated (and not particularly enlightening) computation.

3.4 Finiteness of the Iwasawa module

In this final section to simplify notations we assume the following

Assumption 3.4.1. All primes which ramify in K/k are totally ramified, i.e., $n_0 = 0$.

We remark that all statements can be proved for a general n_0 with no relevant modifications.

Theorem 3.4.2. *The following are equivalent:*

(a) $\lambda(K/k) = \mu(K/k) = 0$*;*

(b) $H_n = A_n$ *for all* $n \geqslant 0$*;*

(c) $H_n = A_n$ *for some* $n \geqslant 1$*;*

(d) $\mathrm{Ker}(N_{n,n-1}) \subseteq H_n$ *for some* $n \geqslant 1$*;*

(e) $H_n + \mathrm{Ker}(N_{n,1}) = A_n$ *for some* $n \geqslant 1$*;*

(f) $\mathrm{Im}(i_{n-1,n}) + H_n = A_n$ *for some* $n \geqslant 1$*;*

(g) $\mathrm{Im}(i_{n,m}) = \mathrm{Im}(i_{n-1,m})$ *for some* $m \geqslant n \geqslant 1$*;*

(h) $\mathrm{rk}_p(H_n) = \widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$ *for some* $n \geqslant 0$*.*

Note that if **(c)**, **(d)**, **(e)** or **(f)** are true for a certain suitable n, then they are true for all $n \geqslant 0$ (because of **(b)**).
We mention that one can find several other equivalences (mainly dealing with inverse images of norms and inclusions, but see also the beginning of Sections 3.4.1 and 3.4.2), but we decided to include only kernels, cokernels and images since they are more commonly used in the theory (see, e.g., [12] or [28]) and they give a full account of the techniques used in the proofs.
We can include the level $n_0 = 0$ if we add some hypotheses.

Theorem 3.4.3. *Assume that one of the following holds:*

(i) $\widetilde{\lambda}_0 = \widetilde{\lambda}_1$*;*

(ii) $|A_1^\Gamma| = |A_0|$*.*

Then the following statements are equivalent:

(a) $\lambda(K/k) = \mu(K/k) = 0$*;*

(c′) $H_n = A_n$ *for some* $n \geqslant 0$*;*

(e′) $H_n + \mathrm{Ker}(N_{n,0}) = A_n$ *for some* $n \geqslant 0$*.*

The final theorem only deals with the triviality of the μ-invariant which is related to the stabilization of the p-ranks of kernels and cokernels of natural maps.

Theorem 3.4.4. *The following are equivalent:*

- **(a)** $\mu(K/k) = 0$;
- **(b)** $\widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$ *for some* $n \geqslant 0$;
- **(c)** $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n})) = \mathrm{rk}_p(\mathrm{Ker}(N_{m+1,n}))$ *for some* $m \geqslant n \geqslant 0$;
- **(d)** $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n})) = \mathrm{rk}_p(\mathrm{Ker}(N_{m,n-1}))$ *for some* $m \geqslant n \geqslant 1$;
- **(e)** $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1}))$ *for some* $m \geqslant n \geqslant 0$;
- **(f)** $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n-1,m}))$ *for some* $m \geqslant n \geqslant 1$;
- **(g)** $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \widetilde{\lambda}_m$ *for some* $m \geqslant n \geqslant 1$.

Remark 3.4.5. If in k there is only one prime over p, then $Y_0 = TX$ and this is equivalent to $|A_1^\Gamma| = |A_0|$ (see Proposition 3.4.6 below). In particular [14, Theorem 1] and [10, Theorem 2] can be seen as a special cases of our Proposition 3.4.6.

The proofs will be divided in various propositions whose results we regroup in Section 3.4.3. Here we just give a generalization of [10, Theorem 2], useful for Theorem 3.4.3.

Proposition 3.4.6. *We have* $|A_1^\Gamma| = |A_0|$ *if and only if* $Y_0 = TX$. *Moreover, if* $|A_1^\Gamma| = |A_0|$ *and* $H_{0,n} = A_0$ *for some* $n \geqslant 1$, *then* $A_n \simeq X$.

Proof. From the exact sequence

$$1 \longrightarrow A_1^\Gamma \longrightarrow A_1 \xrightarrow{\gamma-1} A_1 \longrightarrow (A_1)_\Gamma \longrightarrow 1$$

we have $|A_1^\Gamma| = |(A_1)_\Gamma| = |X/Y_1 + TX|$. Hence $|X/Y_0| = |X/TX + Y_1|$ which yields $Y_0 = TX + Y_1$. Therefore $\nu_1(Y_0/TX) = TX + Y_1/TX = Y_0/TX$ and, by Nakayama's Lemma, $Y_0/TX = 0$. The converse is obvious.
To prove the last statement note that, from the hypothesis $H_{0,n} = A_0$, we have $\nu_{0,n}X \subseteq Y_n = \nu_{0,n}Y_0 = \nu_{0,n}TX$. By Nakayama's Lemma, we get $\nu_{0,n}X = 0$, i.e., $Y_n = 0$. $\square$

The last claim of the previous proposition is a particular case of a criterion we shall show in Chapter 4 on the Γ-invariant subgroup of A_n^Γ: more precisely it can be seen as a corollary of Lemma 4.2.1.
Now, before going to the details of the proofs of the previous theorems, we provide here an application of Theorem 3.4.2. For every $n \geqslant 0$, we define l_n as the minimum $q \in \mathbb{N}$ such that A_n can be generated by the prime divisors (in k_n) of $2, ..., q$.

Theorem 3.4.7. *Let k be a totally real number field for which Leopold's Conjecture holds and let k_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of k. Then Greenberg's Conjecture holds for k if and only if the sequence $\{l_n\}_{n\in\mathbb{N}}$ is bounded as $n \to \infty$.*

Proof. The "only if" direction is trivial. For the other implication, assume that $\{l_n\}_{n\in\mathbb{N}}$ is bounded and let $\bar{l}$ be the maximum of the l_n's. Therefore, for any $n \geqslant 0$, the group A_n is generated by the primes lying above $2, \ldots, \bar{l}$. We know that every prime of $\mathbb{N}$ is finitely decomposed in k_{cyc} , hence all primes $\leqslant \bar{l}$ are totally ramified or unramified (and non-split) in k_{cyc}/k_{m_0} for a large enough m_0.
Let now $m \geqslant m_0$ and note that the subgroup of A_m generated by the primes of k_m which are inert in k_{cyc}/k_m is obviously contained in $\mathrm{Ker}(N_{m,1})$ (if $m \gg m_0$).
Let $M(k)$ be the maximal abelian pro-p extension of k unramified outside (primes dividing) p and recall that Leopold's Conjecture implies $\widetilde{k} = k_{cyc}$ (see the beginning of the Section 1.2). Thus class field theory yields $[M(k) : k_{cyc}]$ is finite (see, for example, the proof of [48, Theorem 13.4]).
Let $n \geqslant m$ and denote by $E_{m,n}$, the maximal abelian extension of k_m contained in L_n . Following the proof of [48, Lemma 13.14] it is easy to see that $(\gamma^{p^m} - 1)A_n = ((1 + T)^{p^m} - 1)A_n$ corresponds, via the Artin map, to the commutator subgroup of $\mathrm{Gal}(L_n/k_m)$, i.e., to $\mathrm{Gal}(L_n/E_{m,n})$. Thus for the subgroup of A_n fixed by Γ^{p^m} we have

$$|A_n^{\Gamma^{p^m}}| = [A_n : ((1 + T)^{p^m} - 1)A_n] = [E_{m,n} : k_n] \ .$$

Since $E_{m,n} \cap k_{cyc} = k_n$, by Galois theory we have $[E_{m,n} : k_n] = [k_{cyc}E_{m,n} : k_{cyc}]$ which is bounded by $[M(k) : k_{cyc}]$.
Therefore we have that $|A_n^{\Gamma^{p^m}}|$ is bounded as $n \to \infty$. Hence, if $n \gg m$, the subgroup of A_m generated by the primes of k_m which are ramified in k_{cyc}/k_m is contained in H_m . Since the subgroups generated by inert and ramified primes less than or equal to $\tilde{l}$ generate the whole A_m , we obtain $A_m = H_m + \mathrm{Ker}(N_{m,1})$, i.e., condition **(e)** of Theorem 3.4.2 holds. □

3.4.1 The kernel of the norm map

Since the extension K/k is totally ramified at some prime, the maps $N_{m,n}$ have trivial cokernels, hence we only focus on stabilization properties of their kernels. The stabilization of the $\mathrm{Ker}(N_{m,n})$'s is easily seen to imply the finiteness of X (just like the stabilization of the A_n's). For example (noting that $\mathrm{Ker}(N_{n,m}) \simeq Y_n/Y_m$, see diagram (3.16) below), $\mathrm{Ker}(N_{m,n}) = \mathrm{Ker}(N_{m,n-1})$ is equivalent to $Y_{n-1}/Y_m = Y_n/Y_m = \nu_{n-1,n}Y_{n-1}/Y_m$, i.e., $Y_{n-1} = Y_m = \nu_{n-1,m}Y_{n-1}$. Hence $Y_{n-1} = 0$ and $X \simeq A_{n-1}$ (and $\mathrm{Ker}(N_{b,a}) = 0$ for all $b \geqslant a \geqslant n-1$). In a similar way $\mathrm{Ker}(N_{m,n}) = \mathrm{Ker}(N_{m+1,n})$ is equivalent to

$X \simeq A_m$ (and yields $\mathrm{Ker}(N_{b,n}) = \mathrm{Ker}(N_{m,n})$ for all $b \geqslant m$). Hence (after some results on the relation between $\mathrm{Ker}(N_{m,n})$, H_m and X) we focus on the stabilization properties for the $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n}))$'s to emphasize their link with the stabilization of the $\widetilde{\lambda}_n$'s.

Proposition 3.4.8. *The following hold*

(a) *assume that* $H_{n,m} = A_n$ *for some* $m \geqslant n \geqslant 1$, *then* $X \simeq A_m$.

(b) *if* $\mathrm{Ker}(N_{n,n-1}) \subseteq H_{n,m}$ *for some* $m \geqslant n \geqslant 1$, *then* $X \simeq A_m$.

Proof. **(a)** Note that $H_{n,m} = A_n$ implies $H_{1,m} = A_1$, so we only consider the case $n = 1$. From diagram (3.5) and the hypothesis one gets $\nu_{1,m}X \subseteq Y_m = \nu_{0,1}\nu_{1,m}Y_0 \subseteq \nu_{0,1}\nu_{1,m}X$. Nakayama's Lemma yields $\nu_{1,m}X = 0$, thus $Y_m = 0$ and $X \simeq A_m$.
(b) The norm map fits in the following commutative diagram

$$\begin{tikzcd} A_m \arrow[rr, "\simeq"'] \arrow[d, "N_{m,n}"] & & X_m \simeq X/Y_m \arrow[d, "\pi_{m,n}"'] \\ A_n \arrow[rr, "\simeq"'] & & X_n \simeq X/Y_n \end{tikzcd} \tag{3.16}$$

(where $\pi_{m,n}$ is the natural projection). So $\mathrm{Ker}(N_{m,n}) \simeq Y_n/Y_m$ and the hypothesis yields $Y_{n-1}/Y_n \subseteq \mathrm{Ker}(\nu_{n,m})$, i.e., $\nu_{n,m}Y_{n-1} \subseteq Y_m$. Since $Y_m = \nu_{n,m}Y_n \subseteq \nu_{n,m}Y_{n-1}$, we have $\nu_{n,m}Y_{n-1} = Y_m$. Multiplying by $\nu_{n-1,n}$, one has $Y_m = \nu_{n-1,n}Y_m$, which yields $Y_m = 0$ and $X \simeq A_m$. □

The following corollary improves the range of Proposition 3.2.14 for a bound for the delay of capitulation.

Corollary 3.4.9. *Assume that* $\mathrm{Ker}(N_{n,b}) \subseteq H_{n,m}$ *for some* $m \geqslant n > b \geqslant 0$. *Then* $A_n = H_{n,m+\varepsilon_b}$ *and, in particular,* $n + \varepsilon_n \leqslant \rho(n) \leqslant m + \varepsilon_b$ *(*p^{ε_j} *is the exponent of* A_j*).*

Proof. As in Proposition 3.4.8.**(b)**, we obtain $\nu_{n,m}Y_b = Y_m = 0$. By (1.6), $\nu_{m,m+\varepsilon_b}X \subseteq p^{\varepsilon_b}X + T\nu_m X \subseteq Y_b$. Therefore $\nu_{n,m+\varepsilon_b}X = \nu_{n,m}\nu_{m,m+\varepsilon_b}X \subseteq \nu_{n,m}Y_b = 0$, i.e., $i_{n,m+\varepsilon_b}A_n = 0$.
For the inequality $n + \varepsilon_n \leqslant \rho(n)$ it suffices to note that $A_n \nsubseteq H_{n,n+\varepsilon_n-1}$ is always true (e.g., because the map $N_{n+\varepsilon_n-1,n} \circ i_{n,n+\varepsilon_n-1} = p^{\varepsilon_n-1}$ cannot be 0). □

We recall that $\rho(n) \leqslant m + \varepsilon_b$ does not mean $A_n = H_{n,m+\varepsilon_b}$ but only $H_n = H_{n,m+\varepsilon_b}$.
Having seen that $\mathrm{Ker}(N_{m,n}) \subseteq H_m$ is equivalent to the finiteness of X, we now point out that the reverse inclusions hold if and only if $D = 0$.

Proposition 3.4.10. *The following hold*

(a) *if* $m \geqslant n \geqslant 1$*, then* $H_m \subseteq \mathrm{Ker}(N_{m,n})$ *if and only if* $D = 0$*;*

(b) *if* $n \geqslant 0$*, then* $H_n \subseteq \mathrm{Ker}(N_{n,0})$ *if and only if* $H_0 = 0$*.*

Proof. Note that $H_m \subseteq \mathrm{Ker}(N_{m,n}) \iff D = D_n$. Then **(b)** follows from (3.4), while, in case **(a)**, $n \geqslant 1$ yields $D = D_n = D_{n-1}$ and finally $D = 0$. □

The following proposition can be compared with [38, Theorem].

Proposition 3.4.11. *Assume* $p^{m-a-1}A_n = 0$ *and* $\mathrm{Ker}(N_{m,n}) \subseteq \mathrm{Im}(i_{a,m})$ *for some* $m > a \geqslant n$ *(if* $p = 2$ *we require* $a > n$*). Then* $A_n \simeq X$*.*

Proof. From the inclusion $\mathrm{Ker}(N_{m,n}) \subseteq \mathrm{Im}(i_{a,m})$ it follows that $Y_n \subseteq \nu_{a,m}X$ and the hypothesis yields $p^{m-a-1}X \subseteq Y_n$. Since, by (1.6), $\nu_{a,m} = p^{m-a} + q\nu_a T$ for some $q \in \Lambda$, we have

$$Y_n \subseteq p^{m-a}X + q\nu_{n,a}\nu_n TX \subseteq pY_n + q\nu_{n,a}Y_n \subseteq (p,T)Y_n$$

(note that if $p \neq 2$ the explicit formulas yields $q \in (p,T)$, whereas if $p = 2$ we have $\nu_{n,a} \in (p,T)$ from $n < a$). Now Nakayama's Lemma yields $Y_n = 0$. □

Theorem 3.4.12. *Assume that* $\widetilde{\lambda}_0 = \widetilde{\lambda}_1$*.*

(a) *If* $H_{0,n} = A_0$ *for some* $n \geqslant 0$*, then* $X \simeq A_n$*;*

(b) *if* $H_n + \mathrm{Ker}(N_{n,0}) = A_n$ *for some* $n \geqslant 0$*, then* X *is finite.*

Proof. The hypothesis on p-ranks yields $Y_0 \subseteq pX$.
(a) If $H_{0,n} = A_0$, then $\nu_n X \subseteq Y_n = \nu_n Y_0$, so we obtain $\nu_n X \subseteq p\nu_n X$. By Nakayama's Lemma we have $\nu_n X = 0$ and $Y_n = \nu_n Y_0 = 0$ as well.
(b) If $H_n + \mathrm{Ker}(N_{n,0}) = A_n$, then, by Theorem 3.2.4, $(D + Y_n/Y_n) + Y_0/Y_n = X/Y_n$. Hence $X = D + Y_0 \subseteq D + pX$ and X is contained in D, i.e., X is pseudo-null. □

Now we start considering results on p-ranks which appear in Theorem 3.4.4.

Theorem 3.4.13. *Let* K/k *be as above.*

(a) *If* $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n,l-1}))$ *for some* $n \geqslant l \geqslant 1$*, then* $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{m,l})) = \mathrm{rk}_p(Y_l)$ *and* $\widetilde{\lambda}_m = \widetilde{\lambda}_n$ *for all* $m \geqslant n$*;*

(b) *if* $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n+1,l}))$ *for some* $n \geqslant l \geqslant 0$*, then* $\mathrm{rk}_p(\mathrm{Ker}(N_{m,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(Y_l)$ *and* $\widetilde{\lambda}_m = \widetilde{\lambda}_n$ *for all* $m \geqslant n$*.*

Proof. **(a)** Since $\mathrm{Ker}\{\nu_{l-1,l} : Y_{l-1} \to Y_l/Y_n\} \supseteq \nu_{l,n}Y_{l-1}$ one has a surjective map

$$Y_{l-1}/Y_n \xrightarrow{\pi} Y_{l-1}/\nu_{l,n}Y_{l-1} \xrightarrow{\nu_{l-1,l}} Y_l/Y_n$$

(where π is the natural projection). This map $\upsilon := \nu_{l-1,l} \circ \pi$ induces a surjection $\overline{\upsilon} : Y_{l-1}/Y_n + pY_{l-1} \to Y_l/Y_n + pY_l$. By hypothesis

$$\mathrm{rk}_p(Y_{l-1}/Y_n) = \mathrm{rk}_p(\mathrm{Ker}(N_{n,l-1})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(Y_l/Y_n) ,$$

thus both $\overline{\upsilon}$ and $\overline{\pi} : Y_{l-1}/Y_n + pY_{l-1} \to Y_{l-1}/\nu_{l,n}Y_{l-1} + pY_{l-1}$ are isomorphisms. This means that $Y_n + pY_{l-1} = \nu_{l,n}Y_{l-1} + pY_{l-1}$ and, if we consider the quotient module $M := \nu_{l,n}Y_{l-1} + pY_{l-1}/pY_{l-1}$, we have that $\nu_{l-1,l}M = M$. Nakayama's Lemma yields $M = 0$ and $\nu_{l,n}Y_{l-1} \subseteq pY_{l-1}$. Therefore $Y_n \subseteq pY_l$ and, in general, $Y_m \subseteq pY_l \subseteq pX$ for any $m \geqslant n$. Hence

$$\mathrm{rk}_p(\mathrm{Ker}(N_{m,l})) = \dim_{\mathbb{F}_p}(Y_l/Y_m + pY_l) = \dim_{\mathbb{F}_p}(Y_l/pY_l) = \mathrm{rk}_p(Y_l)$$

and

$$\widetilde{\lambda}_m = \dim_{\mathbb{F}_p}(X/Y_m + pX) = \dim_{\mathbb{F}_p}(X/pX)$$

for any $m \geqslant n$ (note that, in particular, the last equality implies $\mu(K/k) = 0$).
(b) From the hypothesis we have $Y_l/Y_n + pY_l \simeq Y_l/Y_{n+1} + pY_l$, then $Y_n + pY_l = Y_{n+1} + pY_l$. As in part **(a)**, letting $M := Y_n + pY_l/pY_l$, one gets $M = 0$, i.e., $Y_n \subseteq pY_l$ and, in general, $Y_m \subseteq pY_l \subseteq pX$ for any $m \geqslant n$. □

Remark 3.4.14. As the proof shows, $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n,l-1}))$ is a stronger condition than $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n+1,l}))$. Moreover, both statements of Theorem 3.4.13 cannot be reversed, i.e., if $\widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$ for some $n \geqslant l \geqslant 0$, we cannot conclude that $\mathrm{rk}_p(\mathrm{Ker}(N_{n,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n+1,l}))$. But with the following proposition we can give a bound for the delay of the stabilization of the $\mathrm{rk}_p(\mathrm{Ker}(N_{m,l}))$'s.

Proposition 3.4.15. *Let $n \geqslant 0$ be such that $\widetilde{\lambda}_n = \widetilde{\lambda}_{n+1}$. Then, if $l \in \{0, 1, ..., n\}$, we have*

$$\mathrm{rk}_p(\mathrm{Ker}(N_{m,l})) = \mathrm{rk}_p(\mathrm{Ker}(N_{n+\varepsilon_l,l}))$$

for all $m \geqslant n + \varepsilon_l$.

Proof. The hypothesis yields $Y_n \subseteq pX$. Now $\exp(A_l) = p^{\varepsilon_l}$ and Proposition 1.3.6 imply $\nu_{n,n+\varepsilon_l}X \subseteq Y_l$. Thus

$$Y_{n+\varepsilon_l} = \nu_{n,n+\varepsilon_l}Y_n \subseteq \nu_{n,n+\varepsilon_l}pX \subseteq pY_l \ .$$

Since $\mathrm{rk}_p(\mathrm{Ker}(N_{n+\varepsilon_l,l})) = \mathrm{rk}_p(Y_l/Y_{n+\varepsilon_l} + pY_l)$, the statement follows. □

3.4.2 The cokernel of the inclusion maps

We recall that $\mathrm{Coker}(i_{n,m}) \simeq X/\nu_{n,m}X$, hence $\mathrm{Coker}(i_{n,m}) = \mathrm{Coker}(i_{n,m+1})$ yields $\nu_{m,m+1}\nu_{n,m}X = \nu_{n,m}X$. Thus $\nu_{n,m}X = 0$, $Y_m = 0$ and $X \simeq A_m$. The same holds if $\mathrm{Coker}(i_{n-1,m}) = \mathrm{Coker}(i_{n,m})$. The stabilization of the

$\mathrm{rk}_p(\mathrm{Coker}(i_{n,m}))$'s are more interesting and are related with the stabilization of the $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n}))$'s and of the $\widetilde{\lambda}_n$'s. First of all observe that, once n and m are fixed, we have increasing sequences

$$\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) \leqslant \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1})) \leqslant \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+2})) \leqslant \dots \quad (3.17)$$

and

$$\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) \leqslant \mathrm{rk}_p(\mathrm{Coker}(i_{n-1,m})) \leqslant \mathrm{rk}_p(\mathrm{Coker}(i_{n-2,m})) \leqslant \dots . \quad (3.18)$$

Theorem 3.4.16. *Let $m \geqslant n \geqslant 0$ be such that $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1}))$ (or $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n-1,m}))$ which is equivalent when $n \geqslant 1$). Then*

- **(a)** $\mathrm{rk}_p(\mathrm{Coker}(i_{l,q})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m}))$ *for all $l \leqslant n \leqslant m \leqslant q$;*
- **(b)** $\widetilde{\lambda}_q = \widetilde{\lambda}_m$ *for all $q \geqslant m$.*

Proof. **(a)** By hypothesis $X/\nu_{n,m}X + pX \simeq X/\nu_{n,m+1}X + pX$, hence $pX + \nu_{n,m}X = pX + \nu_{n,m+1}X$ and $\nu_{m,m+1}(\nu_{n,m}X + pX/pX) = \nu_{n,m+1}X + pX/pX$. By Nakayama's Lemma $\nu_{n,m}X + pX/pX = 0$, thus $\nu_{n,m}X \subseteq pX$ and $\nu_{l,q}X \subseteq pX$ for any $l \leqslant n \leqslant m \leqslant q$.
(b) Just note that $\nu_{n,m}X \subseteq pX$ implies $Y_q \subseteq Y_m \subseteq pX$ for all $q \geqslant m$. ☐

Remark 3.4.17. An immediate consequence of the previous theorem (resp. of Theorem 3.4.13) and of Theorem 3.2.20 is that if $\mathrm{rk}_p(\mathrm{Coker}(i_{a,n}))$ (resp. $\mathrm{rk}_p(\mathrm{Ker}(N_{n,a}))$) stabilizes and is equal to $\mathrm{rk}_p(H_n)$, then X is pseudo-null. Note also that $\widetilde{\lambda}_m = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m})$ is easily seen to imply $\nu_{n,m}X \subseteq pX$, which is equivalent to the stabilization of $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m}))$.

Corollary 3.4.18. *Assume that $|A_1^\Gamma| = |A_0|$ or $A_0 = 0$. If $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1}))$ for some $m \geqslant n \geqslant 0$, then $\{\mathrm{rk}_p(\mathrm{Ker}(N_{q,n}))\}_{q \geqslant n}$ stabilizes for $q \geqslant m$.*

Proof. In the proof of Proposition 3.4.16**(a)**, we obtained $\nu_{n,m}X \subseteq pX$. Adding one of the two hypothesis $A_0 = 0$ or $|A_1^\Gamma| = |A_0|$, this implies $Y_m \subseteq pY_n$ (see also the proof of the Proposition 3.4.6). The corollary immediately follows (see, for example, the proof of Corollary 3.4.13). ☐

This corollary is another example of the relation between Theorems 3.4.2 and 3.4.3 (note also that here conditions $|A_1^\Gamma| = |A_0|$ or $A_0 = 0$ provide the same outcome). Another characterization for the stabilization of (3.17) is given by the following proposition.

Proposition 3.4.19. *Let $n \geqslant 1$ (or alternatively $n \geqslant 0$ and $|A_1^\Gamma| = |A_0|$). The sequence (3.17) stabilizes if and only if $\Omega_n := \{q \geqslant n : \mathrm{rk}_p(\mathrm{Coker}(i_{n,q})) = \widetilde{\lambda}_q\}$ is nonempty. Moreover, in this case, the precise index of stabilization is the minimum of Ω_n .*

Proof. The proof is similar to those of Proposition 3.4.16 and its Corollary 3.4.18.
If $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1}))$, then we have $\nu_{n,m}X \subseteq pX$ (see the proof of Proposition 3.4.16), hence $Y_n \subseteq pX$ which yields $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \widetilde{\lambda}_m$.
On the other hand if $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \widetilde{\lambda}_m$ for some $m \geqslant n$, then $\nu_{n,m}X + pX = Y_m + pX$ and applying Nakayama's Lemma we obtain $\nu_{n,m}X \subseteq pX$, which implies $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+1}))$. □

We can give a bound for the delay of the stabilization of the $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m}))$ analogous to the one in Proposition 3.4.15 and the proof is similar to that.

Proposition 3.4.20. *Let $m \geqslant 0$ such that $\widetilde{\lambda}_m = \widetilde{\lambda}_{m+1}$. Then, if $n \in \{0, 1, ..., m\}$, we have*

$$\mathrm{rk}_p(\mathrm{Coker}(i_{n,q})) = \mathrm{rk}_p(\mathrm{Coker}(i_{n,m+\varepsilon_n}))$$

for all $q \geqslant m + \varepsilon_n$.

Assuming $|A_1^\Gamma| = |A_0|$ (resp. $A_0 = 0$ but limiting ourselves to indices $n \geqslant 1$), one has $Y_0 = TX$ (resp. $Y_0 = X$) and it is easy to see that the stabilization of the $\mathrm{rk}_p(\mathrm{Coker}(i_{n,m}))$'s (i.e., $\nu_{n,m}X \subseteq pX$) yields stabilization of the $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n}))$'s (i.e., $Y_m \subseteq pY_n$). To obtain a relation in the other direction one needs to assume also the maximality of $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n}))$.

Theorem 3.4.21. *Assume $|A_1^\Gamma| = |A_0|$ or $A_0 = 0$ and $n \geqslant 1$.*
If $\mathrm{rk}_p(\mathrm{Ker}(N_{m,n})) = \widetilde{\lambda}_m$, then $\mathrm{rk}_p(\mathrm{Coker}(i_{n,q}))$ stabilizes for $q \geqslant m$.
Moreover $\widetilde{\lambda}_q$ and $\mathrm{rk}_p(\mathrm{Ker}(N_{q,n}))$ stabilize for $q \geqslant m$ too.

Proof. We give a proof only in the case $|A_1^\Gamma| = |A_0|$ because the other one is similar. Consider the map $\beta := \pi \circ \nu_n \circ T$ pictured as

$$X \xrightarrow{\quad T \quad} Y_0 \xrightarrow{\quad \nu_n \quad} Y_n \xrightarrow{\quad \pi \quad} Y_n/Y_m + pY_n$$

where π is the canonical projection. Since $pX + \nu_{n,m}X \subseteq \ker(\beta)$, we can consider the map

$$X/Y_m + pX \longrightarrow X/\nu_{n,m}X + pX \xrightarrow{\quad \overline{\beta} \quad} Y_n/Y_m + pY_n$$

where $\overline{\beta}$ is induced by β and the first map is again a projection. By hypothesis $X/Y_m + pX \simeq Y_n/Y_m + pY_n$, hence, from the middle term, we get $Y_m + pX = \nu_{n,m}X + pX$. Moding out by pX one has

$$T(\nu_{n,m}X + pX/pX) = \nu_{n,m}Y_0 + pX/pX \supseteq Y_m + pX/pX = \nu_{n,m}X + pX/pX \ .$$

Nakayama's Lemma yields $\nu_{n,m}X + pX/pX = 0$, i.e., $\nu_{n,m}X \subseteq pX$ and, in general, $\nu_{n,q}X \subseteq pX$ for any $q \geqslant m$. This implies

$$\mathrm{rk}_p(\mathrm{Coker}(i_{n,q})) = \dim_{\mathbb{F}_p}(X/\nu_{n,q}X + pX) = \dim_{\mathbb{F}_p}(X/pX)$$

for any $q \geqslant m$. The final statement follows from Theorem 3.4.16. □

Corollary 3.4.22. *In the setting of the previous theorem assume*

$$\mathrm{rk}_p(\mathrm{Ker}(N_{m,n})) = \mathrm{rk}_p(\mathrm{Coker}(i_{a,d}))$$

for some $0 \leqslant a \leqslant n \leqslant m \leqslant d$ *with* $a \neq n$ *or* $m \neq d$. *Then* $\mathrm{rk}_p(\mathrm{Coker}(i_{n,q}))$, $\widetilde{\lambda}_q$ *and* $\mathrm{rk}_p(\mathrm{Ker}(N_{q,n}))$ *stabilize for* $q \geqslant m$.

Proof. The proof is similar to the one of the Theorem. □

3.4.3 Proofs of the opening Theorems

Proof of Theorem 3.4.2. The equivalence **(a)** $\Leftrightarrow$ **(b)** is the content of [14, Proposition 2].
(c) $\Rightarrow$ **(a)** and **(d)** $\Rightarrow$ **(a)** are given by Proposition 3.4.8.
For **(e)** $\Rightarrow$ **(a)** note that the hypothesis yields $(D + Y_n/Y_n) + Y_1/Y_n = X/Y_n$, hence $D + Y_1 = X$. Therefore $\nu_1(X/D) = \nu_1 X + D/D \supseteq Y_1 + D/D = X/D$ and Nakayama's Lemma implies $X = D$.
For **(f)** $\Rightarrow$ **(a)** the situation is similar to the previous one: the hypothesis yields $(\nu_{n-1,n}X/Y_n) + (D + Y_n/Y_n) = X/Y_n$, hence $D + \nu_{n-1,n}X = X$, which again leads to $X = D$.
For **(g)** $\Rightarrow$ **(a)** the hypothesis yields $\nu_{n-1,m}X = \nu_{n,m}X$, hence $\nu_{n,m}X = 0$, $Y_m = 0$ and $X \simeq A_m$.
(h) $\Rightarrow$ **(a)** is given by Theorem 3.2.20.
All the remaining arrows are clear. □

Proof of Theorem 3.4.3. By Theorem 3.4.2 we only need to check the case $n = 0$.
If condition *(i)* holds, the implications **(c′)** $\Rightarrow$ **(a)** and **(e′)** $\Rightarrow$ **(a)** are given by Theorem 3.4.12.
If condition *(ii)* holds, then **(c′)** $\Rightarrow$ **(a)** is Proposition 3.4.6. For **(e′)** $\Rightarrow$ **(a)** the hypothesis yields $(D + Y_n/Y_n) + Y_0/Y_n = X/Y_n$, hence $D + Y_0 = X$. By Proposition 3.4.6 one has $Y_0 = TX$, which gives $D + TX = X$. Applying Nakayama's Lemma to X/D we find $X = D$.
The other implications are clear. □

Proof of Theorem 3.4.4. The equivalence **(a)** $\Leftrightarrow$ **(b)** is well known (see e.g. [48, Proposition 13.23]).
(c) $\Rightarrow$ **(a)** and **(d)** $\Rightarrow$ **(a)** follow from Theorem 3.4.13.
(e) $\Rightarrow$ **(a)** and **(f)** $\Rightarrow$ **(a)** follow from Theorem 3.4.16.

The equivalence **(a)** $\Leftrightarrow$ **(g)** is given by Theorem 3.4.16 (and Remark 3.4.17). The other implications are clear. $\square$

Chapter 4

Invariants and coinvariants of class groups

In this chapter we consider two more modules associated with the class groups A_n: namely their invariants and coinvariants with respect to the action of the Iwasawa algebra. In Section 4.1 we will treat stabilization properties for the sequences of the invariants and coinvariants of A_n and in Section 4.2 we will give a criterion for the pseudo-nullity of $X(K/k)$ based on the invariant subgroup of the A_n's.

4.1 Stabilization for invariants and coinvariants of A_n

Let $B_n := (A_n)^\Gamma$ be the invariant subgroup of A_n with respect to the action of Γ, i.e.,

$$B_n := \{b \in A_n \,:\, \gamma(b) = b\} \ .$$

Let I_Γ be the augmentation ideal of $\Lambda = \mathbb{Z}_p[[\Gamma]]$ (which correspond to $T\Lambda$ in the isomorphism (1.3)) and let $C_n := (A_n)_\Gamma$ be the coinvariants of A_n with respect to the same action of Γ, i.e.,

$$C_n := A_n/I_\Gamma A_n = A_n/\{a^{\gamma-1} \,:\, a \in A_n\} \ .$$

In terms of Galois groups B_n corresponds, through the Artin map, to $\mathrm{Gal}(L_n/L'_n)$, (where L'_n is the smallest extension of k_n contained in L_n such that Γ/Γ^{p^n} acts trivially on $\mathrm{Gal}(L_n/L'_n)$), while $C_n \simeq \mathrm{Gal}(L''_n/k_n)$ (where L''_n is the maximal abelian extension of k contained in L_n). Finally note that B_n and C_n appear in the exact sequence

$$B_n \hookrightarrow A_n \xrightarrow{\gamma-1} A_n \twoheadrightarrow C_n \ ,$$

hence they have the same cardinality for every n.

Lemma 4.1.1. *For all $n \geqslant 0$ we have*

(a) $N_{n+1,n}(B_{n+1}) \subseteq B_n$ *and* $i_{n,n+1}(B_n) \subseteq B_{n+1}$ *;*

(b) $N_{n+1,n}(I_\Gamma A_{n+1}) \subseteq I_\Gamma A_n$ *and* $i_{n,n+1}(I_\Gamma A_n) \subseteq I_\Gamma A_{n+1}$ *.*

Proof. All statement can be easily derived from the commutativity of the following two diagrams

$$\begin{tikzcd} A_{n+1} \arrow[r, "\gamma"] \arrow[d, "N_{n+1,n}"] & A_{n+1} \arrow[d, "N_{n+1,n}"] \\ A_n \arrow[r, "\gamma"] & A_n \end{tikzcd} \qquad \begin{tikzcd} A_n \arrow[r, "\gamma"] \arrow[d, "i_{n+1,n}"] & A_n \arrow[d, "i_{n+1,n}"] \\ A_{n+1} \arrow[r, "\gamma"] & A_{n+1} \end{tikzcd}$$

□

Therefore inclusions and norms induce well defined maps on B_n and C_n as well (we will still denote them with $i_{n,m}$ and $N_{m,n}$). We define

$$B_\infty(K/k) := \lim_{\leftarrow} B_n \ , \ B(K/k) := \lim_{\rightarrow} B_n \ ,$$

$$C_\infty(K/k) := \lim_{\leftarrow} C_n \quad \text{and} \quad C(K/k) := \lim_{\rightarrow} C_n \ .$$

As usual, since K/k will be fixed, we denote them only by B_∞ , B, C_∞ and C. Furthermore let $i_n : B_n \to B$ and $i_n : C_n \to C$ be the natural maps induced by inclusions.

Theorem 4.1.2. *Let k be any number field and K/k a $\mathbb{Z}_p$-extension (in this chapter we drop the previous hypothesis on $n_0(K/k)$). Then the following statements are equivalent:*

(a) $B_\infty(K/k) \sim_\Lambda 0$*;*

(b) $C(K/k) = 0$*;*

(c) $C_\infty(K/k) \sim_\Lambda 0$*;*

(d) $|B_n| = |B_{n+1}|$ *for some* $n \geqslant n_0$ *;*

(e) $|C_n| = |C_{n+1}|$ *for some* $n \geqslant n_0$ *;*

(f) $i_n(C_n) = 0$ *for some* $n \geqslant n_0 + 1$*;*

(g) $[L(K) \cap \widetilde{k} : K] < \infty$*, i.e., the maximal unramified extension of K contained in $\widetilde{k}$ is finite over K;*

(h) $T \nmid f_X$ *.*

Proof. First of all conditions **(d)** and **(e)** are obviously equivalent (because $|B_n| = |C_n|$ for any n), we put both just for completeness.
Since $C_\infty \simeq X/TX$ and $B_\infty = X[T]$ (the T-torsion of X), the equivalences **(c)**$\Leftrightarrow$**(h)** and **(a)**$\Leftrightarrow$**(h)** are obvious.
Now **(c)**$\Rightarrow$**(e)** is trivial and the converse will follow from Theorem 4.1.4**(a)**.
The equivalence **(f)**$\Leftrightarrow$**(e)**$\Leftrightarrow$**(b)** is proved in Proposition 4.1.6.
We are left with condition **(g)**, so we show here that **(g)**$\Leftrightarrow$**(c)**. We recall some notations: L is the maximal abelian unramified pro-p extension of K, L'' is the maximal abelian extension of k contained in L, $M(k)$ is the maximal abelian p-ramified pro-p extension of k and $\widetilde{k}$ the compositum of all the $\mathbb{Z}_p$-extensions of k. Consider the following diagram

$$\begin{tikzcd}
& & & & L \\
& & & L'' \arrow[ur, no head] \arrow[r, no head] & M(k) \\
k \arrow[r, no head] & K \arrow[r, no head] & \widetilde{k}\cap L \arrow[ur, no head] \arrow[r, no head] & \widetilde{k} \arrow[ur, no head] &
\end{tikzcd}$$

and note that, since $[M(k) : \widetilde{k}\,]$ is finite by class field theory (see for example the proof of [48, Theorem 13.4]), then $[L'' : \widetilde{k} \cap L] = [\widetilde{k}L'' : \widetilde{k}]$ is finite too. We can conclude that $[\widetilde{k} \cap L : K]$ is finite if and only if $[L'' : K] = |C_\infty|$ is finite. ☐

In the previous theorem we eluded the condition $B = 0$: it is because it is much stronger. We recover this condition in Theorem 4.2.2 from which we derive the following equivalence

$$B = 0 \Leftrightarrow A = 0 \ .$$

Remark 4.1.3. Note that if $s(K/k) = 1$, then we have $L''_m = k_m L_0$ for all $m \geqslant 0$ and $|C_m| = |\mathrm{Gal}(L''_m/k_m)| = |\mathrm{Gal}(L_0/k_0)| \leqslant |A_0|$ for all $m \geqslant n_0$. Hence condition **(e)** of Theorem 4.1.2 holds.

Now we proceed with the results on the stabilization of the groups B_n and C_n.

Theorem 4.1.4.

(a) *If* $|C_n| = |C_{n+1}|$ *for some* $n \geqslant n_0$*, then* $C_m \simeq C_n \simeq C_\infty$ *for any* $m \geqslant n$.

(b) *If* $\mathrm{rk}_p(C_n) = \mathrm{rk}_p(C_{n+1})$ *for some* $n \geqslant n_0$*, then* $\mathrm{rk}_p(C_m) = \mathrm{rk}_p(C_m)$ *for any* $m \geqslant n$.

Proof. **(a)** Since $C_n = X/TX + Y_n$, the hypothesis $|C_n| = |C_{n+1}|$ means that $TX + Y_n = TX + Y_{n+1}$. Considering the quotient module $TX + Y_n/TX$ we have $\nu_{n,n+1}(TX + Y_n/TX) = TX + Y_n/TX$ and, from Nakayama's Lemma, $Y_n \subseteq TX$. Thus the restriction map $\mathrm{Gal}(L''/K) \to \mathrm{Gal}(L''_n/k_n)$ is an isomorphism. Similarly the norm maps $N_{m,n} : C_m \to C_n$ are isomorphisms for all $m \geqslant n$.
(b) In this case $\mathrm{rk}_p(C_n) = \mathrm{rk}_p(C_{n+1})$ means $(T,p)X + Y_n = (T,p)X + Y_{n+1}$ and, considering the quotient module $(T,p)X + Y_n/(T,p)X$, we obtain $Y_n \subseteq (T,p)X$. Hence $Y_m \subseteq (T,p)X$ and consequently $\mathrm{rk}_p(C_m) = \mathrm{rk}_p(C_n)$ for every $m \geqslant n$. □

Corollary 4.1.5. *If $|B_n| = |B_{n+1}|$ for some $n \geqslant n_0$, then B_∞ is finite and $|B_m| = |B_n| \geqslant |B_\infty|$ for all $m \geqslant n$ (equality holds if and only if X is pseudo-null, see Proposition 4.1.7).*

There are obvious relations between the groups we are considering.
If $\{\mathrm{rk}_p(A_n)\}_{n\geqslant n_0}$ stabilizes at certain index m, then $\{\mathrm{rk}_p(C_n)\}_{n\geqslant n_0}$ stabilizes at most at m. Moreover if sequence $\{|A_n|\}_{n\geqslant n_0}$ stabilizes at m, then $\{|B_n|\}_{n\geqslant n_0}$ stabilizes at most at m as well. More precisely: if $N_{n+1,n} : A_{n+1} \to A_n$ is an isomorphism for some $n \geqslant n_0$, then it maps isomorphically B_{n+1} onto B_n as well. On the contrary, if we assume that B_{n+1} is isomorphic to B_n , we cannot conclude anything unless we know that the isomorphism is given by the norm map (i.e., if $N_{n+1,n} : B_{n+1} \to B_n$ is an isomorphism, then $N_{n+1,n} : A_{n+1} \to A_n$ is an isomorphism too, see Remark 4.2.4).

Proposition 4.1.6.

(a) *Assume $i_{n,m}(C_n) = 0$ for some $m \geqslant n \geqslant n_0 + 1$. Then $\{|C_q|\}_{q\geqslant n_0}$ stabilizes for $q \geqslant m$.*

(b) *Assume $|C_n| = |C_{n+1}|$ for some $n \geqslant n_0$ and let p^β be the exponent of C_n . Then C_m capitulates exactly in $C_{m+\beta}$ for all $m \geqslant n$.*

Proof. **(a)** If $i_{n,m}(C_n) = 0$, then $\nu_{n,m}X$ is contained in $Y_m + TX$ and $\nu_{n,m}X + TX = Y_m + TX$. Consider the quotient module $\nu_{n,m}X + TX/TX$ and note that

$$Y_m + TX = \nu_{n-1,m}Y_{n-1} + TX \subseteq \nu_{n-1,m}X + TX \subseteq \nu_{n,m}X + TX \ .$$

Since $n - 1 \geqslant n_0$, the above equality yields

$$\nu_{n-1,n}(\nu_{n,m}X + TX/TX) = \nu_{n,m}X + TX/TX$$

and, by Nakayama's Lemma, $\nu_{n,m}X \subseteq TX$. But this imply $Y_m \subseteq TX$: so we have $C_m \simeq C_{m+1}$ and can apply Theorem 4.1.4.**(a)**.
(b) As in the proof of Theorem 4.1.4.**(a)** we obtain $Y_n \subseteq TX$. Since p^β is the exponent of C_n, one has that $p^\beta X$ is contained in $TX + Y_n$ and so

it is contained in TX as well. Recall that $\nu_{m,m+\beta} \equiv p^\beta \pmod{T}$, hence $\nu_{m,m+\beta}X \subseteq p^\beta X + TX$ and finally $\nu_{m,m+\beta}X \subseteq TX$. This means that C_m capitulates in $C_{m+\beta}$.
For the last claim it is easy to show that if C_m capitulates in $C_{m+\beta-1}$ for some $m \geqslant n$, then, with similar arguments, we have $p^{\beta-1}C_m = 0$, from which $p^{\beta-1}C_n = 0$: a contradiction. □

We end this section noting that $|C_\infty|$ is always a bound for $|B_\infty|$: indeed if B_∞ is not pseudo-null, then they are both infinite. When B_∞ is finite we have the following statement.

Proposition 4.1.7. *Let E be the elementary module associated with X and denote by $\theta : X \to E$ a pseudo-isomorphism between them. If B_∞ is pseudo-null, then*

$$|C_\infty| = |B_\infty||E/TE| \ .$$

Proof. Recall that $B_\infty = X[T]$ and $C_\infty = X/TX$, so, in particular, $|B_\infty| < \infty$ implies $T \nmid f_X$. If X pseudo-null (i.e., $E = 0$) the statement follows immediately from the exact sequence

$$X[T] \hookrightarrow X \xrightarrow{T} X \twoheadrightarrow X/TX \ .$$

Now assume X is not pseudo-null and consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & X[T] \arrow[r] \arrow[d, "\theta'"] & X \arrow[r] \arrow[d, "\theta"] & TX \arrow[r] \arrow[d, "\theta''"] & 0 \\
0 \arrow[r] & E[T] \arrow[r] & E \arrow[r] & TE \arrow[r] & 0
\end{tikzcd}$$

where θ' and θ'' are induced by θ and $E[T] = 0$ (see Corollary 3.1.6). From the Snake Lemma exact sequence we obtain

$$|X[T]| = \frac{|\operatorname{Ker}(\theta)|}{|\operatorname{Ker}(\theta'')|} \quad \text{and} \quad |\operatorname{Coker}(\theta)| = |\operatorname{Coker}(\theta'')| \ .$$

Now consider the "other side" of the previous diagram

$$\begin{tikzcd}
0 \arrow[r] & TX \arrow[r] \arrow[d, "\theta''"] & X \arrow[r] \arrow[d, "\theta"] & X/TX \arrow[r] \arrow[d, "\theta'''"] & 0 \\
0 \arrow[r] & TE \arrow[r] & E \arrow[r] & E/TE \arrow[r] & 0
\end{tikzcd}$$

(where θ''' is induced by θ on the quotients). Its Snake Lemma sequence reads as

$$\operatorname{Ker}(\theta'') \hookrightarrow \operatorname{Ker}(\theta) \to \operatorname{Ker}(\theta''') \to \operatorname{Coker}(\theta'') \to \operatorname{Coker}(\theta) \twoheadrightarrow \operatorname{Coker}(\theta''') \ .$$

Computing orders one gets

$$\frac{|\operatorname{Ker}(\theta)|}{|\operatorname{Ker}(\theta'')|} = \frac{|\operatorname{Ker}(\theta''')||\operatorname{Coker}(\theta)|}{|\operatorname{Coker}(\theta'')||\operatorname{Coker}(\theta''')|} \ .$$

Noting that

$$\frac{|\operatorname{Ker}(\theta''')|}{|\operatorname{Coker}(\theta''')|} = \frac{|X/TX|}{|E/TE|}$$

and putting the pieces together we obtain the proposition. □

4.2 The modules B_n and the pseudo-nullity of X (I)

The following lemma gives another criterion for the pseudo-nullity of X which can be useful in specific cases (mainly when $r(K/k)$ is large, $|B_n| = |B_{n+1}|$ for a small n and B_n is generated by classes of totally ramified ideals or of ideals which totally split). We introduce a final piece of notation: we let $\xi_T : X \to X$ represent multiplication by T, this implies that, in terms of Λ-modules, we write B_n as $\xi_T^{-1}(Y_n) = \{x \in X \,:\, \xi_T(x) = Tx \in Y_n\}$ (it might seem redundant but it is useful to avoid using a possibly misleading T^{-1}).

Lemma 4.2.1. *If $|B_n| = |B_{n+1}|$ and $B_n \subseteq H_{n,m}$ for some $m \geqslant n \geqslant n_0$, then $X \simeq A_m$.*

Proof. The hypothesis of capitulation for B_n means that $\nu_{n,m}\xi_T^{-1}(Y_n)$ is contained in Y_m , so $T\nu_{n,m}\xi_T^{-1}(Y_n) \subseteq TY_m$. As we have already seen in the proof of Theorem 4.1.4, $|B_n| = |B_{n+1}|$ implies $Y_n \subseteq TX$, i.e., Y_n is contained in the image of ξ_T . Thus $T\nu_{n,m}\xi_T^{-1}(Y_n) = \nu_{n,m}Y_n = Y_m$ and $Y_m = TY_m$. Nakayama's Lemma yields $Y_m = 0$ and $X \simeq A_m$. □

If we consider the very particular situation in which $s(K/k) = 1$ (and $n_0(K/k) = 0$), we have that $|B_n| = |A_0|$ for all $n \geqslant 0$ and in particular $|B_0| = |A_0|$. Hence [14, Theorem 1] and the first statement of [10, Theorem 2] can be seen as particular cases of our criterion (to understand better the situation see Theorem 1.5.5.**(a)**: if $s = 1$, $n_0 = 0$ and $A_0 = H_{0,n}$ for some $n \geqslant 0$, then $B_0 = A_0$ is contained in $H_{0,n}$ and $|B_0| = |B_1| = |A_0|$ and we can apply our criterion). Note, furthermore, that Proposition 3.4.6 is also a particular case of Lemma 4.2.1.
Another application of the criterion (yielding the announced equivalence $B = 0 \Leftrightarrow A = 0$) is given by the following

Theorem 4.2.2. *We have*

$$B = 0 \Leftrightarrow X \sim_\Lambda 0 \ .$$

Proof. The $\Leftarrow$ direction is obvious. For the other direction if $B = 0$, then $i_{r+1}(B_{r+1}) = 0$ and this means that B_{r+1} is contained in H_{r+1}, i.e., in terms of Iwasawa modules, $\xi_T^{-1}(Y_{r+1}) \subseteq Y_{r+1} + D$. It is easy to see that $\xi_T^{-1}(Y_{r+1}) = Y_{r+1} + D[T]$, thus

$$B_{r+1} \simeq D[T] + Y_{r+1}/Y_{r+1} \simeq D[T]$$

(the last isomorphism depends on the fact that $D[T] \cap Y_{r+1} = 0$, which comes from our definition of r in Definition 3.2.3). Now consider B_r which, by hypothesis, is contained in H_r: repeating the previous argument we find $B_r \simeq D[T]$. Therefore $B_r = B_{r+1}$ and we can apply the criterion of Lemma 4.2.1 to obtain the pseudo-nullity of X. $\square$

Remark 4.2.3. For completeness we also give a direct proof of $B = 0 \Rightarrow A = 0$. Assume that $B = 0$ and that there exists $n \geqslant 0$ such that $H_n \neq A_n$. Consider the action of Γ_n on A_n/H_n: from the class orbit formula we have that there exists $[\mathfrak{a}] \in A_n - H_n$ such that $[\mathfrak{a}]H_n$ is fixed by γ. Hence $[\mathfrak{a}]^{\gamma-1} \in H_n$, i.e., there exists $m \geqslant n$ such that $i_{n,m}([\mathfrak{a}]) \in B_m$. By hypothesis $B_m \subseteq H_m$ and we have a contradiction. Therefore $H_n = A_n$ for every $n \geqslant 0$ and $A = 0$ (and X is pseudo-null).

We want to point out a final simple fact about the B_n's, in connection with the kernel of the norm maps.

Lemma 4.2.4. *Suppose that $B_{n+1} \cap \mathrm{Ker}(N_{n+1,n}) = 0$ for some $n \geqslant n_0$, then $X \simeq A_n$.*

Proof. We give two proofs (the first is more direct but the second is more in the spirit of the rest of our results).
First proof. Consider the action of Γ_{n+1} on $\mathrm{Ker}(N_{n+1,n})/\mathrm{Ker}(N_{n+1,n}) \cap B_{n+1}$ which, by hypothesis, is isomorphic to $\mathrm{Ker}(N_{n+1,n})$.
Since $\mathrm{Ker}(N_{n+1,n})/\mathrm{Ker}(N_{n+1,n}) \cap B_{n+1}$ has no fixed points, by the class orbit formula we have that $\mathrm{Ker}(N_{n+1,n})$ is trivial: hence $X \simeq A_{n+1} \simeq A_n$.
Second proof. By hypothesis $N_{n+1,n} : B_{n+1} \to B_n$ is injective. Thus it has to be surjective too and then $|B_{n+1}| = |B_n|$. But this means $\xi_T^{-1}(Y_{n+1}) + Y_n = \xi_T^{-1}(Y_n)$ and, as we have seen in the proof of Theorem 4.1.4, Y_n is contained in the image of ξ_T. Therefore $Y_{n+1} + TY_n = Y_n$, i.e., $(\nu_{n,n+1}, T)Y_n = Y_n$. By Nakayama's Lemma $Y_n = 0$ and $X \simeq A_n$. $\square$

Proposition 4.2.5. *For any $n \geqslant r$, $B_n \cap H_n$ capitulates exactly in $B_{n+\zeta}$, where p^ζ is the exponent of $D[T]$.*

Proof. In terms of Λ-modules

$$B_n \cap H_n \simeq (\xi_T^{-1}(Y_n)/Y_n) \cap (D + Y_n/Y_n) = \xi_T^{-1}(Y_n) \cap (D + Y_n)/Y_n\ ,$$

so, using the modular law, we get

$$B_n \cap H_n \simeq (\xi_T^{-1}(Y_n) \cap Y_n) + (\xi_T^{-1}(Y_n) \cap D)/Y_n = Y_n + (\xi_T^{-1}(Y_n) \cap D)/Y_n \ .$$

Since $n \geqslant r$, note that $Y_n + (\xi_T^{-1}(Y_n) \cap D)/Y_n$ is isomorphic to $\xi_T^{-1}(Y_n) \cap D = D[T]$, hence we obtain $B_n \cap H_n \simeq D[T] + Y_n/Y_n$ and, using Lemma 1.3.6, we get

$$\nu_{n,n+\zeta}(Y_n + D[T]) = Y_{n+\zeta} + \nu_{n,n+\zeta} D[T] \subseteq Y_{n+\zeta} + p^{\zeta} D[T] + T\nu_n D[T] = Y_{n+\zeta} \ .$$

This means that $B_n \cap H_n$ capitulates in $B_{n+\zeta}$ for all $n \geqslant r$.
Now assume that there exist some $m \geqslant r$ such that $B_m \cap H_m$ capitulates in $B_{m+\zeta-1}$. Working as before, one finds $\nu_{m,m+\zeta-1}(Y_m + D[T]) = Y_{m+\zeta-1}$ and, in particular, $\nu_{m,m+\zeta-1} D[T] \subseteq D_{m+\zeta-1} = 0$. Using Lemma 1.3.6, we find $p^{\zeta-1} D[T] = 0$: a contradiction. □

An immediate consequence is that if X is pseudo-null, then Propositions 4.2.5 and 3.2.14 yield that B_n capitulates exactly in $A_{n+\zeta}$ and A_n exactly in $A_{n+\varepsilon}$ independently from the value of $n \geqslant r$.
To end this section recall that (from Theorem 4.1.2) $\{|B_m|\}_{m \geqslant n_0}$ is bounded if and only if $T \nmid f_X$. The following theorem gives an expected formula for the growth of $|B_n|$ in the same spirit of Iwasawa's Theorem 1.3.1.
First recall the pseudo-isomorphism given in (1.5):

$$X \sim E = \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}) \right) \ ,$$

with $s, t \geqslant 0$, the $f_j(T)$'s irreducible distinguished polynomials of Λ and $l_j \geqslant 1$. We denote by ϑ the number of $f_j(T)$ which are equal to T.

Theorem 4.2.6. *Let K/k be a $\mathbb{Z}_p$-extension of any number field k, then there exist $n' \in \mathbb{N}$ such that*

$$|B_n| = p^{\vartheta n + \nu'}$$

for all $n \geqslant n'$.

Proof. We can write $|B_n| = |X/Y_{n_0}| \cdot |Y_{n_0}/TY_{n_0} + Y_n| \cdot |TX + Y_n/TY_{n_0} + Y_n|^{-1}$. Note that the sequence $\{|TX + Y_n/TY_{n_0} + Y_n|\}_{n \geqslant n_0}$ is increasing and bounded by $|TX/TY_{n_0}|$ which is less than or equal to $|X/Y_{n_0}| = |A_{n_0}|$. This means that there exist $n_1 \geqslant n_0$ such that the sequence stabilizes (actually we can also prove that $|TX + Y_n/TY_{n_0} + Y_n| = |TX/TY_{n_0}|$ for every $n \geqslant n_1$).
Now from Proposition 3.1.5.**(c)** we have that Y_{n_0}/TY_{n_0} is pseudo-isomorphic to E/TE which is isomorphic to $(\Lambda/(T))^{\vartheta} \oplus$ (a finite Λ-module). Now define $Y'_{n_0} := Y_{n_0}/TY_{n_0}$ and $E' := (\Lambda/(T))^{\vartheta}$, so that $Y'_{n_0} \sim_\Lambda E'$. From this we obtain $|Y'_{n_0}/\nu_{n_0,n} Y'_{n_0}| = p^{\alpha} |E'/\nu_{n_0,n} E'|$ for all n sufficiently large and for some constant α (see for example [48, Lemma 13.21]). But $Y'_{n_0}/\nu_{n_0,n} Y'_{n_0}$ is isomorphic to $Y_{n_0}/Y_n + TY_{n_0}$ and, by an easy calculation, $|E'/\nu_{n_0,n} E'| = p^{\vartheta(n-n_0)}$. Putting all the pieces together, we obtain the claim. □

4.3 The modules B_n and the pseudo-nullity of X (II)

This section is devoted to proving the following statement (for the definition of nilpotent group we refer to Remark 2.2.2.)

Theorem 4.3.1. *Let k be a totally real field for which Leopold's Conjecture holds. Then Greenberg's Conjecture is true for k if and only if* $\mathrm{Gal}(L(k_{cyc})/k)$ *is nilpotent.*

We will find this claim as a particular case of the more general Theorem 4.3.4 which gives a new criterion for the pseudo-nullity of $X(K/k)$ (where K/k is any $\mathbb{Z}_p$-extension of a, not necessarily totally real, number field k).
In this section we allow n_0 to be any non negative integer and we use the notation $H \leq_c G$ (resp. $H \leq_o G$) to indicate that H is a closed (resp. open) subgroup of a topological group G.
We begin with a simple observation: if a group G has a normal subgroup N such that $G/N \simeq \mathbb{Z}$, then there exists a subgroup H of G isomorphic to $\mathbb{Z}$ such that $G = N \rtimes H$. The following lemma deals with the case of a topological group.

Lemma 4.3.2. *Let G be a profinite group and N a closed normal subgroup such that G/N is a torsion-free procyclic group. Then there exists a procyclic subgroup H of G such that G is the topological semidirect product of H acting on N.*

Proof. Let $\alpha_1 \in G$ be a representative of a topological generator of G/N and let $H_1 := \overline{\langle\alpha_1\rangle} \leq_c G$. Note that H_1N/N, being a subgroup of G/N, is torsion-free. By the canonical isomorphism (which is also an homeomorphism, because N is compact) between H_1N/N and $H_1/N \cap H_1$, we obtain that the last is torsion-free too. Hence (see, for example [42, Section 2.7]) there exist disjoint subsets $S_1,\ S_2,\ S_3 \subseteq \{p \text{ prime} \in \mathbb{N}\}$ and an isomorphism

$$\phi : H_1 \xrightarrow{\simeq} \prod_{p\in S_1} \mathbb{Z}_p \times \prod_{p\in S_2} \mathbb{Z}_p \times \prod_{p\in S_3} \mathbb{Z}_p/p^{n(p)}\mathbb{Z}_p$$

(where $n(p)$ is a positive integer for every $p \in S_3$) such that

$$\phi(H_1 \cap N) = \prod_{p\in S_2} \mathbb{Z}_p \times \prod_{p\in S_3} \mathbb{Z}_p/p^{n(p)}\mathbb{Z}_p \ .$$

Define $H := \phi^{-1}(\prod_{p\in S_1} \mathbb{Z}_p)$ and let α be a topological generator of H: since $H \cap (H_1 \cap N) = 0$, it follows immediately that $H \cap N = 0$.
The natural projection $\pi : G \to G/N$ is a closed map since G is profinite and N is compact. Hence the equality $\alpha_1 N = \alpha N$ yields

$$G/N = \overline{\langle\alpha_1 N\rangle} = \overline{\langle\alpha N\rangle} = \overline{\langle\pi(\alpha)\rangle} = \overline{\pi(\langle\alpha\rangle)} = \pi(\overline{\langle\alpha\rangle}) = \pi(H) \ .$$

Therefore $G = HN$ and we have an isomorphism of groups between G and $N \rtimes H$. It is easy to check that the map

$$\theta : N \times H \longrightarrow G$$

given by $\theta(n, h) = nh$, is also a homeomorphism of topological spaces. □

Lemma 4.3.3. *Let G be a group and let $A \trianglelefteq G$, $B \leq G$ be abelian subgroups such that $G = A \rtimes B$. Then*

$$C_i(G) = [A,\, {}_{i-1}B]$$

for all $i \geqslant 2$ (where $[A,\, {}_{i-1}B] = [\ldots[[A, B], B]\ldots], B]$ with B appearing $i - 1$ times).

Proof. We use induction on $i \geqslant 2$. Let $i = 2$ and $a,\ a_1 \in A$, $b,\ b_1 \in B$. A simple computation shows that

$$[ab, a_1 b_1] = [a^b, b_1][(a_1^{-1})^{b_1}, b] \in [A, B] \ ,$$

so $C_2(G) = [A, B]$.
Now assume the statement true for some $i \geqslant 2$ and observe that, if E is a normal subgroup of G contained in A, then $[E, G] = [E, B]$. Thus, since $C_i(G)$ is a normal subgroup of G contained in A,

$$C_{i+1}(G) = [C_i(G), G] = [[A,\, {}_{i-1}B], G] = [[A,\, {}_{i-1}B], B] = [A,\, {}_iB] \ .$$

□

The following theorem gives a criterion (for the finiteness of the Iwasawa module $X(K/k)$) which relies on methods very different from the ones used until now.

Theorem 4.3.4. *Let K/k be a $\mathbb{Z}_p$-extensions of a number field k. The following conditions are equivalent:*

- **(a)** *$X = X(K/k)$ is finite;*
- **(b)** *the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ is bounded and $\mathcal{G} := \mathrm{Gal}(L(K)/k)$ is nilpotent.*

Proof. By Lemma 4.3.2, we can write $\mathcal{G}$ as a semidirect product $\mathcal{G} = X \rtimes \Gamma$ (where Γ is isomorphic to $\mathbb{Z}_p$). We claim that $C_{i+1}(\mathcal{G}) = T^i X$ for every $i \geqslant 1$ and prove it with an induction argument on i.
If $i = 1$ the claim is true by, for example [48, Lemma 13.14], so assume that it holds for some $i \geqslant 1$. We have

$$C_{i+2}(\mathcal{G}) = \overline{[C_{i+1}(\mathcal{G}), \mathcal{G}]} = \overline{[T^i X, \mathcal{G}]}$$

and, applying Lemma 4.3.3, we obtain

$$C_{i+2}(\mathcal{G}) = \overline{[T^i X, \Gamma]} \ .$$

It is easy to show that $[T^i X, \Gamma] = T^{i+1}X$ and $T^{i+1}X$ is closed (since it is the image of a compact set). Thus $C_{i+2}(\mathcal{G}) = T^{i+1}X$ and the claim is proved.
(b)⇒(a) Let $j \in \mathbb{N}$ be the nilpotency class of $\mathcal{G}$ (i.e., the least t such that $C_{t+1}(\mathcal{G}) = 1$). The previous claim yields $X = X[T^j]$ and, since $\{|B_n|\}_{n\in\mathbb{N}}$ is bounded, from Theorem 4.1.2 we also have $T \nmid f_X$. Hence T^j and f_X are two relatively prime annihilators of X.
(a)⇒(b) The boundness of the orders of the B_n's comes from the bound for the X_n's. Since X is finite, there exists a $j \in \mathbb{N}$ such that $T^j X = 0$ which yields $C_{j+1}(\mathcal{G}) = 1$. □

Proof of Theorem 4.3.1. As we have already seen in the proof of Theorem 4.1.2, $[M(k) : \widetilde{k}]$ is finite. Since k is a totally real field for which Leopold's Conjecture holds, then $\widetilde{k} = k_{cyc}$ and the finiteness of $[M(k) : k_{cyc}]$ gives the boundedness of the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ of the invariants. Thus the thesis follows from Theorem 4.3.4 above. □

The results of this section seem to suggest that it could be worthwhile to study the lower central series of the Galois group $\mathcal{G} := \mathrm{Gal}(L(K)/k)$. It is reasonable to expect that (at least in some cases) it could provide a different approach to results similar to those of Chapter 2.

4.4 $\mu(F_\infty/F)$ vanishes for certain families of number fields

The Iwasawa's μ-Conjecture, in Iwasawa's original papers, states that the μ-invariant is always zero for the p-primary subgroup of the ideal class group of $F(\zeta_{p^\infty})$, i.e., the field obtained by adjoining to F all p-power roots of unity (see Conjecture 1.3.3 and the papers [22], [20]). This conjecture was proved by B. Ferrero and L. C. Washington (see [8]) when F is an abelian extension of $\mathbb{Q}$ as we recalled in the first chapter, but it remains open in general.
In the following we consider a general $\mathbb{Z}_p$-extension F_∞/F, with the only exception of the cyclotomic extension which will always be written as F_{cyc}: the Iwasawa invariants will be $\mu_p(F_\infty)$ and $\lambda_p(F_\infty)$ or simply $\mu_p(F)$ and $\lambda_p(F)$ if F_∞ is clearly fixed. The modules C_n (and the others appearing here) will have the same meaning of the previous sections, whenever needed we add a reference to the $\mathbb{Z}_p$-extension they belong to, for example $C_n(F_\infty)$ will denote the coinvariants of the p-part of the class group of the n-th layer of F_∞/F.

Definition 4.4.1. *For a $\mathbb{Z}_p$-extension F_∞/F we let $n_1(F_\infty) = n_1 := \min\{n \geqslant n_0 \ : \ \mathrm{rk}_p(C_n) = \mathrm{rk}_p(C_{n+1}) \ \}$.*

Note that the sequence $\{\mathrm{rk}_p(C_n)\}_{n\geqslant n_0}$ is always bounded by $\mathrm{rk}_p(X/TX)$, so from part **(b)** of Theorem 4.1.4 we have that $\{\mathrm{rk}_p(C_n)\}_{n\geqslant n_0}$ is strictly growing between n_0 and n_1 and constant from n_1 on (in particular $C_m/pC_m \simeq X/(p,T)X$ for any $m \geqslant n_1$).
By a *finite p-extension* we mean a Galois extension whose Galois group is a finite p-group. Let k/F be a Galois extension of number fields. If the Galois group $\mathrm{Gal}(k/F)$ is of certain types we can transfer the vanishing of μ from a $\mathbb{Z}_p$-extension F_∞/F to k_∞/k, where $k_\infty = kF_\infty$ (the general result is given by Corollary 4.4.9). To obtain this we need two main ingredients: the first (see Theorem 4.4.2) deals with the case of a finite p-extension and the second (see Theorem 4.4.6) is a criterion on $C_{n_1} = C_{n_1}(k_\infty)$ to have the vanishing of $\mu(k_\infty)$ in the case in which the order of $\mathrm{Gal}(k/F)$ is a prime number q different from p.

4.4.1 Finite p-extensions

Theorem 4.4.2. *Let F_∞/F be a $\mathbb{Z}_p$-extension, k/F be a finite p-extension and put $k_\infty := kF_\infty$. If every ramified prime of k/F is finitely decomposed in F_∞/F, then*

$$\mu(F_\infty) = 0 \iff \mu(k_\infty) = 0\ .$$

Proof. The arrow "$\Leftarrow$" is clear: see for example [26, Chap. 13, § 1, Lemma 1]. For the reverse arrow assume $\mu(F_\infty/F) = 0$. Let $G := \mathrm{Gal}(L(k_\infty)/F_\infty)$ and consider its Frattini subgroup $\Phi(G)$. Since G is a pro-p group, then $\Phi(G) = \overline{[G,G]G^p}$ and, in particular, $G/\Phi(G)$ is abelian (see, for example, [42, Section 2.8]).
Let F' be the subfield of $L(k_\infty)$ fixed by $\Phi(G)$, denote $\mathrm{Gal}(F'/F_\infty)$ by H and let $t \in \mathbb{N}$ be such that $F_t = F_\infty \cap k$ (the setting is summarized in the diagram below).

$$\begin{tikzcd}
 & L(F_\infty) \arrow[r, dash] & L(k_\infty) \arrow[dl, dash, "\Phi(G)"'] \arrow[ddl, dash, "X(k_\infty)"] \\
 & F' & \\
F_\infty \arrow[uur, dash, "X(F_\infty)"] \arrow[ur, dash, "H"] \arrow[r, dash, "\Delta"] \arrow[d, dash, "\simeq\Gamma"'] \arrow[dd, dash, bend right=60, "\Gamma"'] & k_\infty = kF_\infty \arrow[d, dash, "\simeq\Gamma"'] & \\
F_t \arrow[r, dash, "\Delta"] \arrow[d, dash, "\Gamma_t"'] & k & \\
F \arrow[ur, dash, "\Theta"] & &
\end{tikzcd} \tag{4.1}$$

Let $\mathfrak{q}$ be a prime ideal of F_∞ (not necessarily lying over p) and note that if $\mathfrak{q}$ ramifies in k_∞/F_∞, then $\mathfrak{q} \cap F_t$ ramifies in k/F_t as well. Since every prime ideal of F_t which ramifies in k/F_t is finitely decomposed in F_∞/F_t by hypothesis, there are finitely many primes of F_∞ which ramify in k_∞/F_∞. Moreover, if $\mathfrak{q}_L$ is a prime of $L = L(k_\infty)$ lying over $\mathfrak{q}$ and $\mathfrak{q}_1 = \mathfrak{q}_L \cap k_\infty$, then

$$I(\mathfrak{q}_L/\mathfrak{q}) \simeq I(\mathfrak{q}_1/\mathfrak{q})$$

and so $I(\mathfrak{q}_L/\mathfrak{q})$ is finite for every $\mathfrak{q}$ in F_∞. Let S be the set of the prime ideals of F_∞ which ramify in F': since S is finite, H abelian and the groups $I(\mathfrak{q})$ are closed we have

$$I := \overline{\langle \bigcup_{\mathfrak{q}\in S} I(\mathfrak{q}) \rangle} = \prod_{\mathfrak{q}\in S} I(\mathfrak{q}) \ ,$$

(where $I(\mathfrak{q})$ stands for the inertia group of $\mathfrak{q}$ in H). Then I is a finite subgroup of H and H/I is a quotient of $X(F_\infty)$ which is a finitely generated $\mathbb{Z}_p$-module by hypothesis. Thus $H \simeq G/\Phi(G)$ is $\mathbb{Z}_p$-finitely generated (hence finite, because it is an $\mathbb{F}_p$ vector space) and this implies that G is a finitely generated pro-p group (by [42, Proposition 2.8.10]). Since $X(k_\infty)$ is a (closed) subgroup of G of finite index, it is open and this yields (see for example [7, Proposition 1.7]) that $X(k_\infty)$ is finitely generated too, i.e., $\mu(k_\infty/k) = 0$. □

The previous theorem can obviously be applied to F_{cyc}.

Corollary 4.4.3. *Let p be a prime number and F a number field such that $\mu_p(F_{cyc}) = 0$. If k is a finite p-extension of F then $\mu_p(k_{cyc}) = 0$.*

To prove the previous corollary just recall that in a cyclotomic $\mathbb{Z}_p$-extension every ideal is finitely decomposed and apply Theorem 4.4.2. Note that, in particular, if k is any finite p-extension of $\mathbb{Q}$ (not necessarily abelian), then $\mu_p(k_{cyc}) = 0$.

4.4.2 Galois extensions of prime degree $q \neq p$

We recall some standard definitions for profinite groups. A *supernatural number* is a formal product of the kind $\prod_p p^{n(p)}$ where p runs through the set $\mathcal{P}$ of all prime numbers and $n(p)$ is a non negative integer or the symbol ∞. Multiplication, divisions, greatest common divisors and least common multiples are defined between supernatural numbers in the obvious way. If G is a profinite group and H a closed subgroup of G, the *index* of H in G is defined as the supernatural number

$$[G : H] := \mathrm{lmc}\{[G/N : HN/N]\}$$

where N runs in the set of all open normal subgroups of G. The *order* $|G|$ of G is the index $[G : 1]$. Let π be a set of prime numbers (not necessarily

a finite set) and denote by π' the complement set $\pi' = \mathcal{P} - \pi$; we say that a supernatural number $n = \prod_p p^{n(p)}$ is a *π-number* if $n(p) = 0$ for all $p \in \pi'$. A closed subgroup H of G is called a *π-Hall subgroup* if $|H|$ is a π-number and $[G : H]$ is a π'-number. When π consist of only an element, i.e., $\pi = \{p\}$, we say that $n = p^{n(p)}$ is a *p-number* and call H a *p-Sylow subgroup* of G.
Now we establish a criterion of pronilpotency for profinite groups which is based on the well known criterion of nilpotency of P. Hall for finite groups (see for example [43, 5.2.10]).

Lemma 4.4.4. (Pronilpotency Criterion.) *Let G be a profinite group and H be a normal closed subgroup such that $G/C_2(H)$ and H are pronilpotent. Then G is pronilpotent.*

Proof. Let U be an open normal subgroup of G and pose $N_U = HU/U$, $G_U = G/U$. Note that $N_U \simeq H/U \cap H$ is a finite quotient of a pronilpotent group, so it is nilpotent.
Using the commutator identities $[ab, c] = [a, c]^b[b, c]$ and $[a, bc] = [a, c][a, b]^c$, we can easily show that $[HU, HU]$ can be written as $[H, H][U, H][U, U]$. This yields, recalling that U is normal in G,

$$[N_U, N_U] = [HU/U, HU/U] = [HU, HU]U/U = [H, H]U/U \ ,$$

and since $[H, H]U$ is open (hence closed) in G, then $\overline{[H, H]}U = [H, H]U$. So

$$G_U/[N_U, N_U] \simeq G/\overline{[H, H]}U \ ,$$

being a finite quotient of $G/\overline{[H, H]}$, is nilpotent and applying to the couple G_U , N_U the criterion of Hall we obtain the claim. □

The following lemma will be used in the proof of Theorem 4.4.6.

Lemma 4.4.5. *Let G be a group, N be a normal torsion subgroup of finite exponent ϵ_N, and ϕ be an automorphism of finite order of G such that* $\gcd(o(\phi),\ \epsilon_N) = 1$. *If ϕ acts trivially on N and on G/N, then it acts trivially on the whole group G.*

Proof. Denote by $\overline{\phi} : G/N \to G/N$ the automorphism on the quotient induced by ϕ. By hypothesis $\overline{\phi}$ is the identity on G/N, then for every $g \in G$ there exists $n_g \in N$ such that $\phi(g) = gn_g$. By induction it is immediate to prove that $\phi^t(g) = g(n_g)^t$ for all $t \in \mathbb{N}$. Choosing $t = o(\phi)$ we find $(n_g)^{o(\phi)} = 1$ and since $o(\phi)$ and ϵ_N are relatively prime then $n_g = 1$ for every $g \in G$, i.e., ϕ is the identity on G. □

We are now ready to examine the nullity of the μ-invariant for extensions k/F of degree prime with p: the result depends on a hypothesis on the action of $\mathrm{Gal}(k/F)$ on $C_{n_1}(k_\infty)$ (we recall that the same criterion can be formulated for $X(k_\infty)/(T)$).

Theorem 4.4.6. *Let p be a prime number and k/F an extension whose Galois group $\Delta = \mathrm{Gal}(k/F)$ has prime order $q \neq p$. Let F_∞/F be a $\mathbb{Z}_p$-extension in which every ramified prime of k/F is finitely decomposed and put $k_\infty := kF_\infty$. If Δ acts trivially on $C_{n_1}(k_\infty)/p\,C_{n_1}(k_\infty)$, then*

$$\mu(F_\infty) = 0 \iff \mu(k_\infty) = 0 \ .$$

Proof. As said in the proof of Theorem 4.4.2, the arrow "$\Leftarrow$" is clear and it holds in general.
For the reverse arrow we need some new notations: let $E(k_\infty) := L(k_\infty)^{pX(k_\infty)}$, i.e., the subfield of $L(k_\infty)$ fixed by $pX(k_\infty)$ and let $E''(k_\infty)$ be the maximal abelian extension of k contained in $E(k_\infty)$, by [48, Lemma 13.14], we have

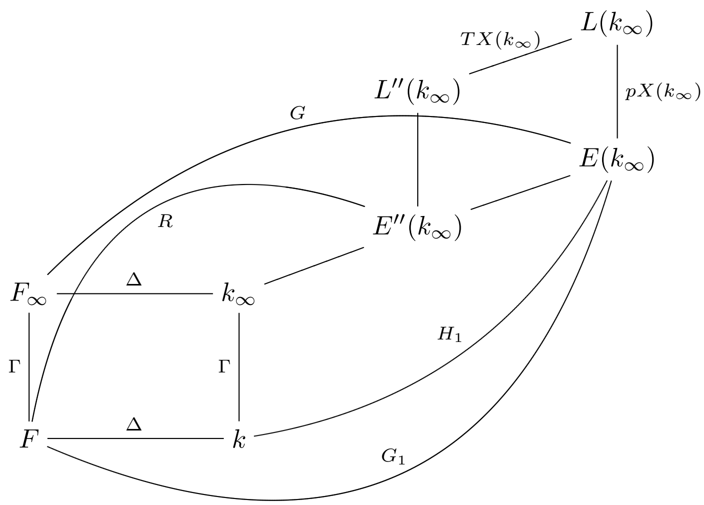
$$\mathrm{Gal}(E''(k_\infty)/k_\infty) \simeq X(k_\infty)/(p,T) \simeq C_\infty(k_\infty)/p\,C_\infty(k_\infty) \ .$$

Note that $E''(k_\infty)$ can also be visualized as $E(k_\infty) \cap L''(k_\infty)$ where $L''(k_\infty)$ is the maximal abelian extension of k contained in $L(k_\infty)$. In the same way we define $E(F_\infty) := L(F_\infty)^{pX(F_\infty)}$ and we also put

$$\mathcal{G} := \mathrm{Gal}(L(k_\infty)/k) \quad , \quad G := \mathrm{Gal}(E(k_\infty)/F_\infty) \quad , \quad G_1 := \mathrm{Gal}(E(k_\infty)/F) \ ,$$

$$H_1 := \mathrm{Gal}(E(k_\infty)/k) \quad \text{and} \quad R := \mathrm{Gal}(E''(k_\infty)/F)$$

as can be visualized in the following picture



(4.2)

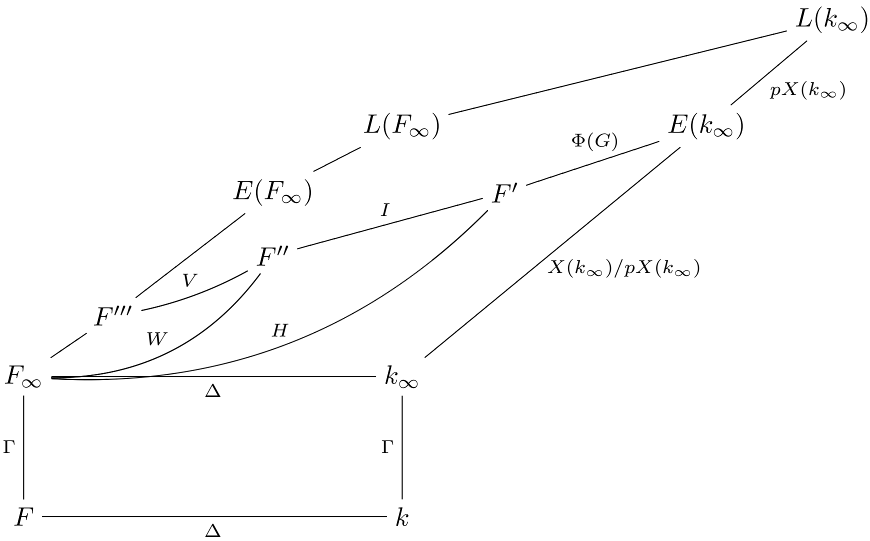
Claim: G_1 is pronilpotent.
Note that $C_2(H_1) = \overline{[H_1, H_1]} = \mathrm{Gal}(E(k_\infty)/E''(k_\infty))$, hence R is isomorphic to $G_1/C_2(H_1)$. Moreover R has only one p-Sylow subgroup, i.e., the Galois group of $E''(k_\infty)$ over k. By hypothesis Δ acts trivially over $C_{n_1}/p\,C_{n_1}$ and

consequently on $C_\infty/pC_\infty \simeq \mathrm{Gal}(E''(k_\infty)/k_\infty)$. Let δ be a generator of Δ and note that applying the Lemma 4.4.5 to the couple $\mathrm{Gal}(E''(k_\infty)/k_\infty) \lhd \mathrm{Gal}(E''(k_\infty)/k)$ and the automorphism of $\mathrm{Gal}(E''(k_\infty)/k)$ induced by δ, we obtain that Δ acts trivially on $\mathrm{Gal}(E''(k_\infty)/k)$. If Q is a q-Sylow of $R = \mathrm{Gal}(E''(k_\infty)/F)$, then it is immediate that $R = Q \times \mathrm{Gal}(E''(k_\infty)/k)$, so R is a pronilpotent group. Now note that H_1 is pronilpotent because it is a pro-p group, then, applying Lemma 4.4.4 to the closed normal subgroup H_1 of G_1, we obtain that G_1 is a pronilpotent group as claimed.

Now we continue the proof of the theorem and observe that, since $G = \mathrm{Gal}(E(k_\infty)/F_\infty)$ is a closed subgroup of G_1, G is pronilpotent as well. This implies (see [51, Proposition 2.5.1]) that $G/\Phi(G)$ is abelian (where $\Phi(G)$ is the Frattini subgroup of G). Now we put

$$F' := E(k_\infty)^{\Phi(G)} \quad \text{and} \quad H := \mathrm{Gal}(F'/F_\infty) \simeq G/\Phi(G) \ ,$$

and we consider the following diagram



(4.3)

Let S be the set of the prime ideals of F_∞ which ramify in F' and put

$$I = \overline{\langle \bigcup_{\mathfrak{q} \in S} I(\mathfrak{q}) \rangle} \ ,$$

where $I(\mathfrak{q})$ is the inertia group of $\mathfrak{q}$ in $\mathrm{Gal}(F'/F_\infty)$. Repeating the same argument of the proof of the Theorem 4.4.2, we obtain that I is a finite subgroup of $H = \mathrm{Gal}(F'/F_\infty)$. Put $F'' := (F')^I$, $W := \mathrm{Gal}(F''/F_\infty)$ and consider the q-Sylow V of W (it could be $V = 1$): let $F''' := (F'')^V$. Now, finally, F''' is contained in $L(F_\infty)$: then $\mathrm{Gal}(F'''/F_\infty)$ is finitely generated and the same holds for $H \simeq G/\Phi(G)$ because I and V are finite. Thus G is finitely generated (as profinite group, see [7, Proposition 1.9]) and $\mathrm{Gal}(E(k_\infty)/k_\infty)$ (being open in G) is finitely generated as well. But $\mathrm{Gal}(E(k_\infty)/k_\infty)$ is isomorphic to $X(k_\infty)/pX(k_\infty) = X(k_\infty)/\Phi(X(k_\infty))$, so $X(k_\infty)$ is finitely generated, i.e., $\mu(k_\infty) = 0$. □

Remark 4.4.7. We can provide an alternative proof of the previous Theorem which avoids the pronilpotency criterion of Lemma 4.4.4. We decided to use the criterion in the proof above to illustrate its possible application to the setting of Iwasawa theory hoping that it could be useful in other similar situations.
Let $\overline{X} := X(k_\infty)/pX(k_\infty)$: by the hypotheses of Theorem 4.4.6, Δ acts trivially on $C_{n_1}/p\,C_{n_1}$, hence also on $C_\infty/p\,C_\infty \simeq \overline{X}/T\overline{X}$. We only need to show that Δ acts trivially on $\overline{X}$ and, since $\bigcap_n T^n\overline{X} = 0$, it suffices to prove that Δ acts trivially on $\overline{X}/T^n\overline{X}$ for any n. We use induction: if $n = 1$ there is nothing to prove. Assume Δ acts trivially on $\overline{X}/T^n\overline{X}$, let δ be a generator of Δ and let x be an element of $\overline{X}$. Since the action of δ over $\overline{X}/T^n\overline{X}$ is trivial we have

$$(x + T^n\overline{X})^\delta = x^\delta + T^n\overline{X} = x + T^n\overline{X}\ .$$

Then there exists $x_1 \in \overline{X}$ such that

$$x^\delta = x + T^n x_1 \tag{4.4}$$

and, similarly, there exists $x_2 \in \overline{X}$ such that

$$x_1^\delta = x_1 + T x_2\ . \tag{4.5}$$

From these equations one easily gets

$$(x + T^{n+1}\overline{X})^{\delta^s} = x + sT^n x_1 + T^{n+1}\overline{X}$$

for every $s \in \mathbb{N}$. For $s = q = |\Delta|$, we find $qT^n x_1 \in T^{n+1}\overline{X}$, which yields $T^n x_1 \in T^{n+1}\overline{X}$. Thus Δ acts trivially on $\overline{X}/T^{n+1}\overline{X}$ and the induction is completed.

The following corollary for F_{cyc} is the analogue of Corollary 4.4.3.

Corollary 4.4.8. *Let F be a number field such that $\mu_p(F_{cyc}) = 0$ and k/F an extension whose Galois group $\Delta = \mathrm{Gal}(k/F)$ has prime order $q \neq p$. If Δ acts trivially on $C_{n_1}(k_{cyc})/p\,C_{n_1}(k_{cyc})$, then $\mu_p(k_{cyc}) = 0$.*

It is easy to combine Theorems 4.4.2 and 4.4.6 to get the following corollary (we write it only in the case of cyclotomic $\mathbb{Z}_p$-extensions but it has obvious generalizations).

Corollary 4.4.9. *Let k be a number field, p a fixed prime number and suppose that there exist a finite chain of number fields $\mathbb{Q} = \kappa_0 \subseteq \kappa_1 \subseteq \kappa_2 \subseteq \ldots \subseteq \kappa_n$ such that*

(i) κ_1/κ_0 *is an abelian extension (possibly trivial);*

(ii) for every $i \geqslant 2$, κ_i/κ_{i-1} *is a normal extension such that*

- *(ii.1)* $\mathrm{Gal}(\kappa_i/\kappa_{i-1})$ *is a group of p-power order or*
- *(ii.2)* $\mathrm{Gal}(\kappa_i/\kappa_{i-1})$ *is cyclic of prime order different from p and it acts trivially on* $C_{n_1}((\kappa_i)_{cyc}/\kappa_i)/p\, C_{n_1}((\kappa_i)_{cyc}/\kappa_i)$*;*

(iii) k *is contained in* κ_n *.*

Then $\mu_p(k_{cyc})$ *vanishes.*

Proof. We only have to use the Ferrero-Washington Theorem for the first step of the chain, followed by Theorems 4.4.2 and 4.4.6 in sequence as we need. Recall again that if $k \subseteq k'$ and k_∞ is any $\mathbb{Z}_p$-extension of k, then $\mu(k_\infty) \leqslant \mu(k_\infty k')$. □

Bibliography

[1] M. Aranes and A. Arenas, *On the defining polynomials of maximal cyclotomic extensions*, Rev. R. Acad. Cien. Serie A. Math. **102**(2) (2008), 183–191.

[2] A. Bandini, *A note on p-ranks of class groups in $\mathbb{Z}_p$-extensions*, JP J. Algebra Number Theory Appl. **9** (2007), 95–103.

[3] M. Bertolini and H. Darmon, *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Ann. of Math. (2) **162** (2005), 1–64.

[4] N. Bourbaki, *Algebra I. Chapters 1-3*, Spinger-Verlag (1989).

[5] N. Bourbaki, *Commutative Algebra. Chapters 1-7*, Spinger-Verlag (1989).

[6] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[7] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups - Second edition*, Cambridge stud. in advanc. math. **61**.

[8] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[9] S. Fujii, *On the depth of the relations of the maximal unramified pro-p Galois group over the cyclotomic Zp-extension*, Acta Arithmetica **149.2** (2011), 101–110.

[10] T. Fukuda, *Remark on $\mathbb{Z}_p$-extensions of Number Fields*, Proj. Japan Acad. **70** Ser. A (1994), 264–266.

[11] E.S. Golod and I.R. Shafarevich, *On class field towers (in Russian)*, Izv. Akad. Nauk SSSR **28** (1964), 261–272. English translation in Am. Math. Soc. Transl. (2) **48** (1965) 91–102.

[12] M. Grandet and J.F. Jaulent, *Sur la capitulation dans une $\mathbb{Z}_l$-extension*, J. reine angew. Math. **362** (1985), 213–217.

[13] R. Greenberg, *The Iwasawa invariants of Γ-extensions of a fixed number field*, Amer. J. Math. **95** (1973), 204–214.

[14] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[15] R. Greenberg, *Iwasawa Theory - Past and Present*, Adv. Studies in Pure Math. **30** (2001), 335–385.

[16] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. Math. **98** (1973), 246–326.

[17] K. Iwasawa, *On p-adic L-functions*, Ann. of Math. (2), **89** (1969), 198–205.

[18] K. Iwasawa, *A note on capitulation problem for number fields*, Proc. Japan Acad. **65** ser. A (1989), 59–61.

[19] K. Iwasawa, *A note on capitulation problem for number fields. II*, Proc. Japan Acad. **65** ser. A (1989), 183–186.

[20] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2), **98** (1973), 246–326.

[21] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[22] K. Iwasawa, *On the theory of cyclotomic fields*, J. Math. Soc. Japan **20** (1964), 42–82.

[23] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in "Cohomologies p-adiques et applications arithmetiques III" Asterisque **295** (2004), 117–290.

[24] J.S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.

[25] T. Kubota and H.W. Leopold, *Eine p-adische Theorie de Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen*, J. Reine Angew. Math. **214/215** (1964), 328–339.

[26] S. Lang, *Cyclotomic fields I and II - Combined second edition*, Springer-Verlag, GTM **121** (1990).

[27] T.Y. Lam, *Exercises on Modules and Ring*, Springer-Verlag (2007).

[28] M. Le Floc'h, A. Movahhedi and T. Nguyen Quang Do, *On capitulation cokernels in Iwasawa Theory*, Amer. J. Math. **127** n° 4 (2005), 851–877.

[29] B. Mazur, *Rational points of abelian varieties with values in a tower of number fields*, Invent. Math. **18** (1972), 183–266.

[30] B. Mazur and H. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[31] B. Mazur - J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[32] B. Mazur and A. Wiles, *Class fields of abelian extensions of Q*, Invent. Math. **76** (1984), 179–330.

[33] J. Minardi, *Iwasawa Modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D. Thesis, University of Washington (1986).

[34] Y. Mizusawa, *On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields II*, Acta Arithmetica **119.1** (2005), 93–107.

[35] Y. Mizusawa and M. Ozaki, *Abelian 2-class field towers over the cyclotomic Z_2-extension of imaginary quadratic fields*, Math. Annalen **347** (2010), 437–453.

[36] J. Neuchirch, A. Schmidt and K. Wingberg, *Cohomology of number fields - Second edition*, Springer-Verlag, GMW **323** (2008).

[37] K. Okano, *Abelian p-class field tower over the cyclotomic Zp-extensions of imaginary quadratic fields*, Acta Arithmetica **125.4** (2006), 363–381.

[38] M. Ozaki, *A Note on the Capitulation in $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **71** ser. A (1995), 218–219.

[39] M. Ozaki, *Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa modules*, J. Math. Soc. Japan **56** n° 3 (2004), 787–801.

[40] M. Ozaki, *Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions*, J. Reine Angew. Math. **602** (2007), 59–94.

[41] M. Ozaki, *Construction of real abelian fields of degree p with $\lambda_p = \mu_p = 0$* , Int. J. Open Problem Compt. Math. **3.2** (2009), 342–351.

[42] L. Ribes and P. Zalesskii, *Profinite Groups - Second edition*, Spinger-Verlag EMG **40**.

[43] D. J. S. Robinson, *A course in the Theory of Groups - Second edition*, Springer-Verlag, GTM 80.

[44] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **93** (1988), 701–713.

[45] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **143** (1991), 25–68.

[46] J.P. Serre, *Classes des corps cyclotomiques*, Séminaire Bourbaki, Expose **174** (1958-1959).

[47] O. Taussky, *A remark on the class field tower*, J. London Math. Soc. **12** (1937), 82–85.

[48] L.C. Washington, *Introduction to cyclotomic fields - Second edition*, Springer-Verlag, GTM **83**.

[49] A. Weil, *Courbes Algébriques et Variétiés Abéliennes*, Hermann - Paris (1971).

[50] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540.

[51] J. S. Wilson, *Profinite Groups*, Clarendon Press - Oxford.

Compendio

Nella tesi vengono trattati i fenomeni della capitolazione degli ideali e della stabilizzazione in Teoria di Iwasawa, sia in ambito non abeliano (come sviluppato di M. Ozaki in [40]), che abeliano classico.
Una breve panoramica dei contenuti: il primo capitolo si apre con esempi e calcoli espliciti sulla $\mathbb{Z}_p$-estensione ciclotomica; poi si ricordano definizioni, proprietà, alcuni teoremi fondamentali e alcune congetture classiche (ancora aperte) sulle $\mathbb{Z}_p$ e sulle $\mathbb{Z}_p^d$-estensioni. Nei paragrafi 1.4 e 1.5 si introducono i fenomeni della capitolazione degli ideali e della stabilizzazione, richiamando alcuni risultati classici e recenti.
Il Capitolo 2 è dedicato alla Teoria di Iwasawa non abeliana. Il paragrafo 2.1 descrive il lavoro di Ozaki stabilendo definizioni, proprietà e teoremi principali. Nel paragrafo 2.2 si fa vedere come lo stesso tipo di stabilizzazione (sia per gli ordini che per i p-ranghi) che vale nella teoria classica, non è più valido in questo nuovo contesto. Infatti, il teorema di stabilizzazione, in ambito non abeliano, richiede ipotesi più forti.
Il terzo capitolo torna indietro al caso delle $\mathbb{Z}_p$-estensioni: dopo alcuni risultati preliminari, nel paragrafo 3.2 si comincia uno studio dettagliato del massimo sottomodulo finito $D(K/k)$ del modulo di Iwasawa $X(K/k)$. Si considerano poi le successioni degli *absolute capitulation kernels* e dei *relative capitulation kernels* e si ottengono alcune formule (dipendenti da certi parametri legati a $D(K/k)$) che descrivono in modo accurato come crescono i loro ordini e i loro p-ranghi. Nel seguito, poi, si danno risposte affermative riguardo alla stabilizzazione delle due successioni su menzionate e nel paragrafo 3.3 si discute il problema di limitare il ritardo nella capitolazione. Infine, nel paragrafo 3.4, si ottengono diverse nuove condizioni (basate su proprietà relative a capitolazione e stabilizzazione) che si dimostrano essere equivalenti all'annullamento degli invarianti di Iwasawa $\mu(K/k)$ e/o $\lambda(K/k)$.
Nel Capitolo 4 si considerano invarianti e coinvarianti di Galois per i gruppi $A(k_n)$. In particolare, nel paragrafo 4.1 trattiamo i loro limiti diretto e inverso, e studiamo stabilizzazione e capitolazione con le loro conseguenze. Nei paragrafi 4.2 e 4.3 otteniamo due nuovi criteri per la finitezza di $X(K/k)$: il

primo è basato solo sulla capitolazione del sottogruppo degli invarianti mentre il secondo sulla nilpotenza del gruppo di Galois $\mathrm{Gal}(L(K)/k)$ (dove $L(K)$ è la massima pro-p estensione abeliana non ramificata di K). Infine, nel paragrafo 4.5, si dimostrano due risultati che pongono in relazione l'annullamento di $\mu(F_\infty/F)$ e di $\mu(kF_\infty/k)$ (dove F_∞/F è una $\mathbb{Z}_p$-estensione di un campo di numeri F) nei casi in cui $k \supset F$ è un'estensione di Galois di grado p, o di grado un primo q diverso da p.