SNOQIT I: THE $\Lambda[G]$-MODULES OF IWASAWA THEORY

PREDA MIHĂILESCU

ABSTRACT. For $\Lambda = \mathbb{Z}_p[[T]]$, the ring of formal power series in one variable, the structure of the finitely generated Λ - torsion modules is a main concern of Iwasawa theory. In this first part of Snoqit[1] we investigate some topics related to the representation of these Λ-modules as direct sums of certain elementary Λ - submodules, and the growth of the intermediate levels of modules which are projective limits.

CONTENTS

1. INTRODUCTION

Let p be an odd prime and $\Lambda = \mathbb{Z}_p[[T]]$ be the ring of formal power series in the independent variable T. Then Λ is a local ring with maximal ideal $\mathfrak{M} = (p, T)$. The maximal ideal verifies the topological condition $\cap_n \mathfrak{M}^n = \{0\}$, which allows one to induce $\mathfrak{M}$ - adic completion on Λ - modules. Therefore all the Λ-modules considered here will be assumed to be complete in the $\mathfrak{M}$ - adic topology [5], Chapter 5, §11.

In number theory, one considers extensions $\mathbb{K}_\infty/\mathbb{K}$ of finite extensions $\mathbb{K}/\mathbb{Q}$, such that $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) \cong \mathbb{Z}_p$ and $\mathbb{K}_\infty = \cup_{n\geq 0}\mathbb{K}_n, [\mathbb{K}_n : \mathbb{K}_{n-1}] =$

Date: Version 1.00 September 21, 2010.

Key words and phrases. 11R23 Iwasawa Theory, 11R27 Units.

$p, \mathbb{K}_0 = \mathbb{K}$. If A_n are the p-parts of the class groups of the intermediate fields $\mathbb{K}_n$, the fundamental Λ-module of Iwasawa theory if $A = \varprojlim_n A_n$.

Due to the intimate relation between Λ-modules and the structure of some important groups related to $\mathbb{Z}_p$ - extensions of number fields, such as A, the study of Λ-modules takes an important role in Iwasawa's seminal papers, especially [2, 3]. In [2], Iwasawa proved that the module A has a fundamental property – see property F below – which is essentially Hilbert's Theorem 90 for Λ-module, with an additionally case related to ramification of the primes above p. The Leitmotiv of this paper is to show that property F is a distinctive property for the Λ-modules of number theory, which endows them with strong additional structure, compared to the arbitrary Λ-modules, which was considered so far as "Iwasawa"-modules, thus in a certain sense the natural objects of Iwasawa theory.

One often encounters Λ-free modules in Iwasawa theory, and their quotients may have the structure of arbitrary Λ-modules. The title "Λ-modules of Iwasawa theory" therefore has some ambiguity: our position is that the specific properties of the fundamental module A are relevant for Iwasawa theory. This leads to our interest in studying modules with property F; we uncover very strong structural consequences of this property, such as the fact that they decompose in direct sums of f-primary parts, with f irreducible distinguished polynomials. Moreover, their minimal polynomial is squarefree.

In the rest of this introduction we review some classical facts about general Λ-modules and then introduce the notation used in this paper. In the second Chapter we define our Λ-modules of interest. These are all projective limits with respect to families of maps which behave like norms in galois groups of extensions of Iwasawa towers $\mathbb{K}_\infty/\mathbb{K}$; we thus consider modules $M = \varprojlim_n M_n$, with M_n abelian p-groups endowed with an action of Γ. In these modules, we introduce the Property F and, after giving some definitions and examples, deduce the main consequences of this property on the growth of the intermediate level modules M_n, in the case when $|M_n| < \infty$. These consequences are derived from the fundamental proposition 3, which generalizes a result of Fukuda for the module A of Iwasawa theory. Based on this result, some considerations of linear algebra imply the conditions of asymptotic growth of our modules.

In the third Chapter we investigate submodules of Λ-modules and questions related to their decomposition in direct sums. The modules here do not need to satisfy property F. It is in the fourth chapter that we consider the impact of property F on decompositions of Λ-modules.

The general setting of this paper is axiomatic, but the examples focus on class field theory related to Iwasawa theory. The fundamental result of Iwasawa which proves that the modules $A = \varprojlim_n A_n$ – or, likewise, the galois groups $X_n = \mathrm{Gal}(\mathbb{H}_n/\mathbb{K}_n)$ with their projective limit $X = \mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty)$ – has property F was derived using class field and Kummer theory, and the proof appears to encrypt quite precisely the property F for maximal p-abelian unramified extensions of the intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$. The same proof is encountered in text books like [6], [5], and we do not know about the existence of some alternative, module theoretic approach. While the property itself can be retained in a simple axiom, it is an important open question, to find out other examples of modules with property F, and possibly some general conditions under which a submodule of a free Λ-module has this property. As we shall see, the property implies some kind of *completion* of the given module, and fixes its structure together with the one of its submodules. In Appendix A we give, for the sake of completeness, a generalization of Iwasawa's proof to the case of submodules $M \subset A$ which have a direct complement in A. This proof illustrates the method of Iwasawa in our terminology; the result follows however directly from Iwasawa's result on A, using some simple algebraic arguments given Chapter 4.

1.1. **Classical theory of Λ-modules reviewed.** The prime ideals of Λ are generated by p and the irreducible distinguished polynomials $f(T) \in \mathbb{Z}_p[T]$; we recall that f is *distinguished* if $f(T) = T^k + \sum_{i=0}^{k-1} a_i T^i$ with $a_i \in p\mathbb{Z}_p[T]$. The Weierstrass preparation Theorem says that for each $x \in \Lambda \setminus \{0\}$ there is a $k \geq 0$ and a distinguished polynomial $f(T) \in \mathbb{Z}_p[T]$, together with an unit $u \in \Lambda$ such that

$$g(T) = p^k f(T) \cdot u(T).$$

If $f, g \in \mathbb{Z}_p[T]$ are two prime distinguished polynomials which are coprime to each other in $\mathbb{Q}_p[T]$, then the ideal $(f, g) \subset \Lambda$ has finite index, but is in general not the trivial ideal [6], Lemma 13.7. As a consequence, the notion of *pseudoisomorphism* arises as a practical notion for comparing structures of Λ-modules. Two Λ-modules X, Y are said to be pseudoisomorphic (one writes: $X \sim Y$) if there is an exact sequence

$$0 \to K_1 \to X \to Y \to K_2 \to 0,$$

in which the kernels and cokernels K_1, K_2 are finite. In particular, for f, g prime as above, we have that

$$\Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg), \tag{1}$$

but one never has isomorphism ([6], Lemma 13.8). The module X is Noetherian iff $X/\mathfrak{M}X$ is finite, that is, iff it is finitely generated as a Λ-module. Iwasawa defines [3], §1.2 elementary Λ-modules by

$$E(e_0; \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s}) = \Lambda^{e_0} \oplus \bigoplus_{i=1}^{s} \Lambda/\mathfrak{p}_i^{e_i},$$

where $e_i \geq 0$ and $\mathfrak{p}_i$ are prime ideals of height one in Λ. As a consequence of the above, he deduces that every Noetherian Λ -module X is pseudoisomorphic to some elementary Λ - module, thus

Lemma 1. *If X is a Noetherian Λ-module, then there is a collection of s (not necessarily distinct) prime ideals $\mathfrak{p}_i \subset \Lambda$ of height one together with $s+1$ integers $e_0; e_1, \ldots, e_s \geq 0$ such that*

$$X \sim E(e_0; \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s}) \tag{2}$$

For a proof, see [3], §1.2. In view of (1), one sees that the primary parts in (2) can be combined – or possibly decomposed – up to pseudoisomorphism. One may thus generalize elementary modules by allowing also products of prime powers: an elementary module is then described by the exponents $e_0, e_1, \ldots, e_{s'}$ together with the distinguished polynomials $f_i(T)$:

$$E'(e_0; f_1^{e_1}, \ldots, f_{s'}^{e_{s'}}) = \Lambda^{e_0} \oplus \bigoplus_{i=1}^{s'} \Lambda/f_i^{e_i}. \tag{3}$$

Remark 1. *Due to the phenomenon described in (1), one cannot expect in general to obtain precise descriptions of submodules of Λ-modules up to isomorphisms; therefore, the notion of pseudoisomorphism has imposed itself since the beginning of this theory on the study of arbitrary Λ-modules. However, modules that are complete in the sense of Property F are direct sums of submodules with minimal polynomials $f \in \mathbb{Z}_p[T]$ which are distinguished and irreducible.*

The consequences of Property F derived in this paper will be used in Snoqit II for the study of Kummer radicals and in particular the Iwasawa bilinear space. This is a subspace $A^{(S)} \subset A$ which acts both as radical and as galois group in a subextension of the Hilbert class field; it is the obstruction module to the Greenberg conjecture.

The module Λ can be represented in various ways as a projective limit. If one considers (see [3], §1.3) a sequence of elements $0 \neq \pi_n \in \Lambda$ with $\pi_0 \in \mathfrak{M}$ and $\pi_{n+1} \in \pi_n\mathfrak{M}$, then $\cap_n \pi_n \Lambda = 0$ and $\Lambda = \varprojlim_n \Lambda/(\pi_n\Lambda)$. If X is a Noetherian Λ - torsion module, one can always choose the π_n to be coprime to primes occurring in the representation (2) of X;

by defining $X_n = X/\pi_n X$, we obtain natural maps $X_n \to X_m$ for $n > m$ with respect to which $X = \varprojlim_n X_n$. In Section 3 we show that the polynomials $\omega_n = (T+1)^{p^n} - 1$ and the related prime polynomials $\nu_{n,n+1} = \omega_{n+1}/\omega_n$ are related to a useful additional property of Λ-modules, which is encountered in number theory and governs the asymptotic growth of the finite level submodules of projective limits.

1.1.1. *Notation.* If G is a group, which is an module over the ring R and $S \subset G$ is a finite or infinite set, we shall often use the notation $\langle S \rangle_R$ for denoting the R - submodule spanned by the set S. The *subexponent* of a finite abelian p - group X is

$$\mathrm{sexp}(X) = \min\{\mathrm{ord}(x) \ : \ x \in X \setminus pX\}.$$

The $\mathbb{Z}_p$ - torsion of a Λ module M is $M^{\dagger}$ and the maximal finite submodule of M is M°.

In Iwasawa theory, we consider an odd prime p and extensions $\mathbb{K}/\mathbb{K}_{\infty}$ which contain the p-th roots of unity, together with their cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}_{\infty} = \cup_n \mathbb{K}_n, \mathbb{K} = \mathbb{K}_1$. We let k be the least integer such that $\mu_{p^{k+1}} \not\subset \mathbb{K}$.

The units of $\mathbb{K}_n$ are denoted $E_n = (\mathcal{O}(\mathbb{K}_n))^{\times}$ and the p-units – i.e. the smallest ring contained in $\mathbb{K}_n$, in which all the primes above p are invertible – are $E'_n \supset E_n$. The *local*-units (of interest in our context) are defined by $U_n = \mathcal{O}\left(\mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p\right)^{\times}$. The maximal p-abelian unramified extension of $\mathbb{K}_n$ is $\mathbb{H}_n$ and $\mathbb{H} = \cup_n \mathbb{H}_n$. The p-parts of the class groups of $\mathbb{K}_n$ are A_n, being isomorphic to $X_n = \mathrm{Gal}(\mathbb{H}_n/\mathbb{K}_n)$ via the global Artin map φ, which extends to infinity under projective limits to a map $\varphi : A \to X$. The maximal subfield $\mathbb{H}'_n \subset \mathbb{H}$ which splits all the primes above p has galois group isomorphic to A'_n, the p-parts of the class groups of the p units $E'_n \subset E_n$; we have $\mathbb{H}' \subset \mathbb{H}$ and $A' := \varprojlim_n A'_n$. Moreover, if $\mathbf{B}_n \subset A_n$ is the subgroup spanned by the classes of powers of ramified primes above p and $\mathbf{B} = \varprojlim_n \mathbf{B}_n$, then

$$\varphi(\mathbf{B_n}) = \mathrm{Gal}(\mathbb{H}_n/\mathbb{H}'_n), \quad \varphi(\mathbf{B}) = \mathrm{Gal}(\mathbb{H}/\mathbb{H}'), \tag{4}$$

$$A'_n \cong A_n/\mathbf{B}_n \quad A' \cong A/\mathbf{B}. \tag{5}$$

We use Lang's notation Ω with various indices for *large* extensions of $\mathbb{K}_{\infty}$, with galois groups that contain non trivial free Λ-submodules. In particular Ω is the maximal p - abelian p - ramified extension of $\mathbb{K}_{\infty}$; its most important subfields are $\Omega_E = \cup_n \mathbb{K}_n[E_n^{1/p^n}]$ and $\Omega_{E'} = \cup_n \mathbb{K}_{\infty}[(E'_n)^{1/p^n}]$, with $E'_n \supset E_n$ the p - units of $\mathbb{K}_n$. The maximal p - ramified p - abelian extension of $\mathbb{K}_n$ is $\Omega_n \subset \Omega$; it contains $\mathbb{K}_{\infty}$. The extensions $\Omega_{E,n} = \mathbb{K}_n[E_n^{1/p^n}], \Omega_{E',n} = \mathbb{K}_n[(E'_n)^{1/p^n}]$. We write $\mathbb{H}_E = \mathbb{H} \cap \Omega_E$ and $\mathbb{H}_{E'} = \mathbb{H} \cap \Omega_{E'}$. If $\mathbb{F} \subset \Omega$ is a galois extension of $\mathbb{K}$ which is not completely unramified, then the finite level subextensions are induced by Ω via $\mathbb{F}_n = \Omega_n \cap \mathbb{F}$. Note that $\Omega_n \supset \mathbb{K}_\infty$ since $\mathbb{K}_\infty/\mathbb{K}_n$ is p-abelian and p-ramified, while $\mathbb{H}_n \cap \mathbb{K}_{n+1} = \mathbb{K}_n$, due to the fact that $\mathbb{H}_n$ is unramified.

The base field $\mathbb{K}$ contains the p-th root of unity, so there is a maximal integer, which will be denoted by $k \geq 1$ such that $\zeta_{p^k} \in \mathbb{K}$. We shall use from classical Iwasawa theory the following standard polynomials:

$$\begin{aligned} \omega_n &= (T+1)^{p^{n-k}} - 1 \in \mathbb{Z}_p[T], \quad n \geq k, \\ \nu_{m,n} &= \omega_m/\omega_n \in \mathbb{Z}_p[T], \quad m > n \geq k, \\ \omega_n &= \omega_k \quad \text{and} \quad \nu_{m,n} = \nu_{m,k} \quad \text{for } 0 \leq n < k. \end{aligned} \tag{6}$$

We assume for simplicity that $k = 1$, in order to simplify notations. This assumption is somewhat restrictive, since $\mathbb{K}$ may not split into linear disjoint extensions, one of which is $\mathbb{B}/\mathbb{Q}$, the cyclotomic $\mathbb{Z}_p$-extension. In Snoqit II, we shall introduce more precise notations which take this fact into consideration. The assumption is sufficient though for illustrating the main picture. Note that both ω_n and $\nu_{m,n}$ are distinguished polynomials and we may choose $\pi_n = \omega_n$ in order to organize Λ as a projective limit, as described above.

2. Property F and IW modules

In this section $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ and τ is a topological generator of Γ, while $T = \tau - 1$. The ring Λ is local and its maximal ideal is $\mathfrak{M} = (p, T)$. We shall also assume that Λ is endowed with an involution $* : \Lambda \to \Lambda$ given by $\tau^* = (p + 1 - \tau)\tau^{-1}$, the Iwasawa involution.

We consider additively written Λ-modules[1] which are projective limits $M = \varprojlim_n M_n$, and the projections $\pi_n : M \to M_n$ are defined by two sequences of maps $N_{m,n} : M_m \to M_n$ and $\iota_{n,m} : M_n \to M_m$, called *norms* and *lifts*, such that

$$N_{n+1,n} \dagger \iota_{n,n+1} = p : M_n \to M_n, \quad \text{and, possibly} \tag{7}$$

$$\iota_{n,n+1} \dagger N_{n+1,n} = \nu_{n+1,n} : M_{n+1} \to \tag{8}$$

We assume that all maps $N_{n+1.n}$ are surjective, but $\iota_{n,n+1}$ need not always be injective. For $m > n \geq 0$, the maps $N_{m,n}, \iota_{n,m}$ are defined by iteration. The property (8) is not required in general and we give below conditions under which it necessarily holds. The limit $M = \varprojlim_n M_n$ is taken with respect to $M_{m,n}$. Injective limits are related to examples from traditional approaches to Kummer theory, which will

[1] We keep additive notation for simplicity in the axiomatic approach, but the concrete modules from Iwasawa theory, which are endowed with natural multiplicative structures, will be written accordingly in a multiplicative notation

not be pursued here: we shall not consider injective limits here. If $V_n \subset M_n$ are a family of submodules, we define $V = \varprojlim_n V_n$ and $N_{\infty,n}(V) = \cap_{m>n} N_{m,n}(V_m)$ The norm from infinity is identical with the projection of M onto the n-th level:

$$N_{\infty,n}(M) = M_n = \pi_n(M).$$

In particular, the intermediate levels of M can be recovered by means of the norms or projections. The elements of M are $x = (x_n)_{n\in\mathbb{N}} \in M$ with $x_n \in M_n$; they will also be referred to as *norm coherent sequences*, and a sequence of modules $(V_n)_{n\in\mathbb{N}}$ with $V_n \subset M_n$ and $N_{m,n}(V_m) = V_n$ is a norm coherent sequence of submodules.

If $f \in \mathbb{Z}_p[T]$ is a distinguished polynomial, we define the f-primary part $A(f)$ of M and its *socle* $A[f]$ by

$$\begin{aligned} M(f) &= \{x \in M : \exists n \in \mathbb{N}, f^n A = 0\} \subset M, && (9)\\ M[f] &= \{x \in M : fx = 0\} \subset M. && (10) \end{aligned}$$

Then $M(f) = \cup_{n=1}^{\infty} M[f^n]$. The union is infinite when M is, for instance, a Λ-free module, but in the most cases of interest it will be in fact finite.

Finally, we define for $n \geq 0$ the fundamental submodules

$$Y_n = Y_n(M) = \text{ Ker } (N_{\infty,n} : M \to M_n) \subset M. \qquad (11)$$

2.1. **Definition of Property F.** With this prerequisites, we define the property F as follows:

Definition 1. 1. *Let $M = \varprojlim_n M_n$ with M_n a norm coherent sequence of Λ-modules. Suppose that there is a submodule $\mathcal{T} = \mathcal{T}(M) \subset M[T]$ which is $\mathbb{Z}_p$-free and such that the following conditions hold:*

$$\begin{aligned} Y_1(M)/TM &\cong \mathcal{T}(M) && (12)\\ Y_m(\mathcal{T}) &= \nu_{m,n}(Y_n(\mathcal{T})), && (13)\\ Y_m(M) &= \nu_{m,n}(Y_n(M)). && (14) \end{aligned}$$

Then M has Property F and the submodule $\mathcal{T}(M)$ is called the ramification of M. In particular, M is unramified iff $Y_0(M) = TM$; this can happen also when $M[T]$ is infinite.

2. *A sequence $a = (a_n)_{n\in\mathbb{N}} \in M$ is called floating of level $n_1 > 1$, if $a \notin \mathfrak{M}M$ but for $n_1 > 1$ we have $a_n = 0, \forall n < n_0$ and $a_{n_0} \neq 0$. We denote by $\mathcal{F}(M) \subset M$ the Λ-module generated by all floating elements.*

3. *We introduce the following nominations for various types of Λ-modules which posses property F: a PIW a is a module $M = \varprojlim_n M_n$ with property F. If in addition $\iota_{n,n+1}$ are injective for all $n \geq n_0$, the module is an injective PIW or an IW-module. Finally, if M is an IW which is free as a $\mathbb{Z}_p$-module and all M_n are finite and of uniformly bounded p-rank, then M is a* Weierstrass *modules. Thus Weierstrass modules are infinite Λ-torsion modules with $\lambda \neq 0$ and $\mu = 0$ and such that the lift maps are asymptotically injective; in addition, they have property F. A $\mathbb{Z}_p$-torsion IW module is called a μ-type IW, of MIW.*

Remark 2. 1. *We have already mentioned that Iwasawa proved in* [2] *that $A = \varprojlim_n A_n$, with A_n the p-parts of class groups in a $\mathbb{Z}_p$-cyclotomic towers in which all primes above p are totally ramified, enjoy Property F – see for instance* [6]*, Lemma 13.15. In this relevant context, the module*

$$\mathcal{T}(A) \cong Gal(((\Omega_1 \cdot \mathbb{K}_\infty) \cap \mathbb{H})/(\mathbb{H}_1 \cdot \mathbb{K}_\infty)),$$

*and it is spanned by the decomposition group of primes which are inert in the Hilbert class field. Thus $\mathcal{T}(A) \sim$ **B**. This explains the choice of the term ramification for $\mathcal{T}$. It follows in particular that A is unramified iff $[(\Omega_1 \cdot \mathbb{K}_\infty) \cap \mathbb{H} : \mathbb{K}_\infty] < \infty$. We shall prove later the deeper result that $A[T]$ is finite.*

2. *For unramified modules M, the property F is equivalent to Hilbert 90 for M. Furtwängler has proved in the first decade of the* 20*-th century the fact that Hilbert 90 holds for the class groups in cyclic subfields of Hilbert class fields. Using Chevalley's generalization of Furtwängler's results (see* [5]*, Chapter 13, Lemma 4.1) one may obtain an alternative proof of Iwasawa's result.*
3. *In connection with Kummer theory, one can define the duals of PIW modules, which will be projective with respect to the dual norms $N^*_{m,n}$. The property F is then conserved by duality, with respect to the action of Λ twisted by the Iwasawa convolution.*

A useful consequence of the property F is

Lemma 2. *Let M_n be a coherent sequence of Noetherian Λ-modules with the F-property and $\mathcal{F}(M) \subset \mathcal{M}$ be the module of the floating elements. Then*

$$\mathcal{F}(M) \neq \emptyset \quad \Leftrightarrow \quad Y_0(\mathcal{T}(M)) \not\subset \mathfrak{M}M.$$

Proof. Let $a = (a_n)_{n \in \mathbb{N}} \in M$ be a floating element of level 0. There is a surjective homomorphism of $\mathbb{Z}_p$-modules $t : M \rightarrow \mathcal{T}(M)$ and $M =$ Ker $(t) \oplus \mathcal{T}$, thus $a = a_u + a_t$ with $a_u \in$ Ker $(t), a_t \in \mathcal{T}$. From

(12) we gather that $Y_0(M) = TM + Y_0(\mathcal{T})$ and therefore $a \in \mathcal{F} \cap Y_0(M)$ is floating of level 0 iff $a_t \in Y_0(\mathcal{T})$ and $a_t \not\in \mathfrak{M}M$. Indeed, $TM \subset \mathfrak{M}M$ and since $a \not\in \mathfrak{M}M$, it follows that $a_t \not\in \mathfrak{M}M$. This completes the proof. We see that the existence of floating elements is controlled by ramification and in particular, unramified modules have no floating elements. □

We give some examples of projective limits and property F, which are related to the setting of cyclotomic $\mathbb{Z}_p$-extensions, with the notations introduced above.

Example 1.

1. *Let $A = \varprojlim_n A_n$. Then A is a PIW-module of finite type and A^- is an IW-module; it is the direct sum of a Weierstrass and a MIW-module, while for $\mu^- = 0$ it is a pure Weierstrass module.*

   If the primes above p are not split in $\mathbb{K}/\mathbb{K}^+$, then A^- is a torsionfree IW-module. For plus parts, A^+ is PIW but in general not IW, since it may contain finite torsion submodules. A conjecture of Greenberg implies that A^+ contains no IW - submodule.
2. *Let $\mathbb{K}_n = \mathbb{Q}[\zeta_{p^n}]$, the p^n-th cyclotomic extensions and U_n be like above. Let $e_k \in \mathbb{Z}_p[Gal(\mathbb{K}_1/\mathbb{Q})]$ be an orthogonal idempotent with odd index and $\xi_n \in e_k U_n$ be such that $[e_k U_n^- : \xi_n^{\Lambda}] = 1$; then $e_k\Omega$ is naturally defined as the fixed field of the $(1 - e_k)Gal(\Omega/\mathbb{K}_\infty)$. By class field theory,*

   $$D := Gal((e_k\Omega)/(e_k\mathbb{H})) \cong e_k U_\infty \cong \Lambda,$$

   the isomorphism being induced by the Artin map φ. Consider finally $f(T) \in \mathbb{Z}_p[T]$, any distinguished polynomial; then $f(T)D \subset D$ is a compact subgroup, with quotient $D/(fD) \cong \Lambda/(f)$. Let $\tilde{\Omega}_f = (e_k\Omega)^{fD}$ be the fixed field of this compact subgroup and $\tilde{\Omega}_{f,n} \subset \tilde{\Omega}_f$ be the maximal subextensions which contain $\mathbb{K}_n$ but not $\mathbb{K}_{n+1}$, and are galois over $\mathbb{Q}$. By construction, $M_n = Gal(\tilde{\Omega}_{f;n}/\mathbb{K}_n)$ are a coherent sequence of Λ-modules with characteristic polynomials $f(T)$ – for n sufficiently large. This example indicates that one encounters Λ-modules with arbitrary characteristic polynomials. We shall see later, that these modules cannot be IW modules.
3. *Let $\mathbb{L} \subset \mathbb{H}$ be a galois extension of $\mathbb{K}$ with group $Z = Gal(\mathbb{L}/\mathbb{K}_\infty)$ and suppose that Z is a PIW. Let $p^{m(n)} = \exp(Z_n)$ and $B_n \subset \mathbb{K}_\infty^\times$ be groups with $\mathbb{K}_\infty \cdot \mathbb{L}_n = \mathbb{K}_\infty[B_n^{1/p^{m(n)}}]$. We let $\mathcal{R}(\mathbb{L}_n/\mathbb{K}_n) = \mathbb{K}_\infty^\times \langle B_n^{1/p^{m(n)}} \rangle_{\mathbb{Z}} / \mathbb{K}_\infty^\times$; these radicals will be investigated in Snoqit*

> *II, when we discuss Kummer theory. There is a twisted action of Λ on $\mathcal{R}(\mathbb{L}_n/\mathbb{K}_n)$ which induce a projective limit $\mathcal{R}(\mathbb{L}/\mathbb{K}_\infty)$ with respect to the twisted norms $N^*_{m,n}$. Then $\mathcal{R}(\mathbb{L}/\mathbb{K}_\infty)$ is also a PIW with respect to this action of Λ.*

2.2. **Growth of IW-modules.** Our investigation of IW modules focuses on the *transitions* $M_n \to M_{n+1}$ and the growth from one module to the other. For this we define

Definition 2. *Let $(M_n)_{n\in\mathbb{N}}$ be a norm coherent sequence of Λ modules, such that $M = \varprojlim_n M_n$ is an unramified Weierstrass module. The n - transition is the module $C_n = M_{n+1}/\iota_{n,n+1}(M_n)$.*

The n - transition is an R_n-module, with $R_n = \mathbb{Z}/(p^N \cdot \mathbb{Z})[\omega_n]]/(\omega_{n+1})$-module, for a $p^N \geq \exp(M_{n+1})$. The ring R_n is local with maximal ideal (ω_n), so its annihilator is generated by a power of T. For the investigation of transitions, we shall consider in particular the case when $a = (a_n)_{n\in\mathbb{N}} \in X \setminus \mathfrak{M}X$ for an unramified Weierstrass module X and $M_n = \Lambda a_n$. In this case, the annihilator

$$C_n^\top = \{x \in R_n : xC_n = 0\} = \omega_n^{(k(n)} R_n,$$

for $k(n) \geq 1$, which is an invariant of the transition. According to its size we distinguish several cases of growth:

Definition 3. *Let C_n and $k(n)$ we like above. The exponent $k(n) \in \mathbb{N}$ is called the growth factor of the transition C_n. The transition C_n is called*

1. *Stable, if $k(n) = 1$,*
2. *Semistable, if $k(n) < p - 1$,*
3. *Tame, if $k(n) \leq p - 1$ and*
4. *Wild, if $k(n) > p - 1$.*

A module M is stable, semistable or tame if there is an n_0 depending only on M such that for all $\Lambda a \subset M$, with $a = (a_n)_{n\in\mathbb{N}} \in M \setminus \mathfrak{M}M$, all of its transitions $C_n, n \geq n_0$ have this property.

The following lemma generalizes the Theorem 1 of Fukuda in [1], showing that transitions tend to stabilize, under mild assumptions on M. The proof of Fukuda was made for the full class groups $A(\mathbb{K})$ and uses Iwasawa's result mentioned above. We show here that the proof only requires Property F.

Lemma 3. *Let $(M_n)_{n\in\mathbb{N}}$ be a norm coherent sequence such that $M = \varprojlim_n M_n$ is a PIW with finite p - rank (so M/pM is finite). Then there is an $n_0 > 0$ such that for all $n \geq n_0$ the following hold:*

1. *If $|M_n| = |M_{n+1}|$, then $M_m = M_n$ for all $m > n \geq 0$.*

2. *If p-rk$(M_n) = p$-rk(M_{n+1}) then there is a constant R with p-rk$(M_m) = p$-rk$(M_n) = R$ for all $m > n \geq 0$; furthermore there is a constant $\lambda(M) \leq R$ such that $|M_{n+1}| - |M_n| = p\lambda$ for all n sufficiently large.*

Proof. Consider $Y_n(M) = \text{ Ker } (N_{\infty,n} : M \to M_n)$; by Property F (14), we have $Y_n(M) = \nu_{m,0}Y_0(M)$. We assume without restriction of generality that 0 is the least integer n for which $|M_n| = |M_{n+1}|$, for point 1., respectively p-rk$(M_n) = p$-rk(M_{n+1}), for point 2. From the choice of Y_n, we have a commutative diagram in which $M_n \to M_0$ is induced by the map $N_{n,0}$ while the horizontal isomorphism are deduced from the definition of Y_n.

$$\begin{tikzcd} M_n \arrow[r, phantom, "\cong"] \arrow[d] & M/\nu_{n,0}Y \arrow[d] \\ M_0 \arrow[r, phantom, "\cong"] & M/Y. \end{tikzcd} \tag{15}$$

For the first point we assume $|M_1| = |M_0|$. Then $M_1 \to M_0$ is an isomorphism; therefore $\nu_{1,0}Y = Y$. Since $\mathcal{M} = (p,T) \subset \Lambda$ is the unique maximal ideal and $\nu_{1,0} \in \mathcal{M}$, and since Y is finitely generated over Λ, it follows from Nakayama's lemma that $Y = 0$. Consequently, $M \cong M_0$ is finite and $M_n \cong M_0 \cong M$ for all $n \geq 0$. This proves the assertion 1.

Suppose now that p-rk$M_1 = p$-rkM_0. Then $M_1/pM_1 \cong M_0/pM_0$ and thus $M/(\nu_{1,0}Y + pM) \cong M/(Y + pM)$ and $\nu_{1,0}Y + pM = Y + pM$. Letting $Z = (Y + pM)/pM$, we have

$$\nu_{1,0}Z = (\nu_{1,0}Y + pM)/pM = (Y + pM)/pM = Z.$$

By Nakayama's lemma, we conclude that $Z = 0$ and $Y \subset pM$. Therefore,

$$\begin{aligned} p\text{-rk}(M_n) &= p\text{-rk}(M/\nu_{n,0}Y) = p\text{-rk}(M/(\nu_{n,0}Y + pM)) \\ &= p\text{-rk}(M/pM) = \mathbb{Z}_p\text{-rk}(M), \quad \text{for all} \quad n \geq 0. \end{aligned}$$

By Iwasawa's formula, for n sufficiently large we have

$$|M_n| = p^{\mu p^n + \lambda n + \nu},$$

and since the rank stabilizes, we see that $\mu(M) = 0$ and $|M_{n+1}| - |M_n| = p^{\lambda}$. This proves assertion 2. □

Let M be an IW-module. Since $M^{\dagger}$ is a $\mathbb{Z}_p$ - torsion module its exponent is finite, say $q = p^m$. Then $M^{\dagger} = \text{ Ker } (p^m : M \to M)$ is a canonical submodule. Let $M^{\circ} \subseteq M^{\dagger}$ be the maximal submodule of finite rank. This is also a canonical module, defined as the Λ - span of all the elements $x \in M \setminus \mathcal{M}M$, such that Λx is finite.

In view of the Lemma 3, beyond a fixed n, we have $|M_m^\circ| = |M_n^\circ|, m > n$. Let $M^{(\mu)} = M^\dagger/M^\circ$ and $M^{(\lambda)} = M/M^\dagger$. Then $M^{(\lambda)}$ the Lemma implies that $M^{(\lambda)}$ is a Weierstrass module. Having split IW-modules in this way, the Lemma 3 suggests the following

Definition 4. *Let M be a PIW-module of finite p - rank. The minimal integer $n_0 = n_0(M)$ such that*

1. *The sizes $|M_n^\circ| = |M_{n_0}^\circ|$ for all $n > n_0$,*
2. *The ranks p-rk$(M_n^{(\lambda)}) =$ p-rk$(M_{n_0}^{(\lambda)}$ for all $n > n_0$,*

is called the stabilization index of M. The module M is called stable, if $n_0(M) = 0$.

Next we give an elementary, technical lemma which will allow us to draw additional information from Lemma 3;

Lemma 4. *Let A and B be finitely generated abelian $p-$groups denoted additively, with subexponents* $\mathrm{sexp}(A), \mathrm{sexp}(B) \geq p^2$ *and let $N : B \rightarrow A$, $\iota : A \rightarrow B$ two $\mathbb{Z}_p$ - linear maps such that:*

1. *N is surjective;*
2. *The $p-$ranks of A and B are both equal to r and $|B|/|A| = p^r$.*
3. *$N(\iota(a)) = pa, \forall a \in A$ and ι is rank preserving, so p-rk$(\iota(A)) =$ p-rk(A);*

Then ι is injective, $\iota(A) = pB$ and $\mathrm{ord}(x) = p \cdot \mathrm{ord}(Nx)$ *for all $x \in B$.*

Proof. We start by noting that for any finite abelian p - group A of p - rank r and any pair $\alpha_i, \beta_i;\ i = 1, 2, \ldots, r$ of minimal systems of generators there is a matrix $E \in \mathrm{Mat}(r, \mathbb{Z}_p)$ which is invertible over $\mathbb{Z}_p$, such that

$$\vec{\beta} = E\vec{\alpha}. \tag{16}$$

This can be verified either by tensoring with $\mathbb{Q}_p$, or directly by extending the map $\alpha_i \mapsto \beta_i$ linearly to A and, since $(\beta_i)_{i=1}^r$ is also a minimal system of generators, deducing that the map is invertible, thus regular. It represents a unimodular change of base in the vector space $A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The maps ι and N induce maps

$$\overline{\iota} : A/pA \rightarrow B/pB,\ \overline{N} : B/pB \rightarrow A/pA.$$

From 1, we see $\overline{N}$ is surjective and since, by 2., it is a map between finite sets of the same cardinality, it is actually an isomorphism. But 3. implies that $\overline{N}\dagger\overline{\iota} : A/pA \rightarrow A/pA$ is the trivial map and since $\overline{N}$ is an isomorphism, $\overline{\iota}$ must be the trivial map, hence $\iota(A) \subset pB$.

Assume now that ι is rank preserving and let $b_i,\ i = 1, 2, \ldots, r$ be a minimal set of generators of B: thus the images $\overline{b}_i$ of b_i in B/pB

form an $\mathbb{F}_p$ - base of this algebra. Let $a_i = N(b_i)$; since p-rk$(B/pB) =$ p-rk(A/pA), the set $(a_i)_i$ also forms a minimal set of generators for A. We claim that $|B/\iota(A)| = p^r$.

Pending the proof of this equality, we show that $\iota(A) = pB$ and ι is injective. Indeed, we have the equality of p- ranks:

$$|B/pB| = |A/pA| = |B/\iota(A)| = p^r,$$

implying that $|pB| = |\iota(A)|$; since $\iota(A) \subset pB$ and the p - ranks are equal, the two groups are equal, which is the first claim. The second claim will be proved after showing that $|B/\iota(A)| = p^r$. Since $|B|/|A| = p^r$, it follows that $|A| = |\iota(A)|$, so ι is injective.

Let $S(X)$ denote the socle of the finite abelian p - group X. There is the obvious inclusion $S(\iota(A)) \subset S(B) \subset B$ and since ι is rank preserving, p-rk$(A) = p$-rk$(S(A)) = p$-rk$(B) = p$-rk$(S(B)) = p$-rk$(S(\iota(A)))$, thus $S(B) = S(\iota(A))$. Let $(a_i)_{i=1}^r$ be a minimal set of generators for A and $a'_i = \iota(a_i) \in B, i = 1, 2, \ldots, r$; the $(a'_i)_{i=1}^r$ form a minimal set of generators for $\iota(A) \subset B$. We choose in B two systems of generators in relation to a'_i and the matrix E will map these systems according to (16).

First, let $b_i \in B$ be such that $p^{e_i} b_i = a'_i$ and $e_i > 0$ is maximal among all possible choices of b_i. From the equality of socles and p - ranks, one verifies that the set $(b_i)_{i=1}^r$ spans B as a $\mathbb{Z}_p$-module; moreover, $\iota(A) \subset pB$ implies $e_i \geq 1$. On the other hand, the norm being surjective, there is a minimal set of generators $b'_i \in B,\ i = 1, 2, \ldots, r$ such that $N(b'_i) = a_i$. Since b_i, b'_i span the same finite $\mathbb{Z}_p$-module B, (16) in which $\vec{\alpha} = \vec{b}$ and $\vec{\beta} = \vec{b'}$ defines a matrix with $\vec{b} = E \cdot \vec{b'}$. On the other hand,

$$\iota(\vec{a}) = \vec{a'} = \mathbf{Diag}(p^{e_i})\vec{b} = \mathbf{Diag}(p_i^{e_i})E \cdot \vec{b'},$$

The linear map $N : B \to A$ acts component-wise on vectors $\vec{x} \in B^r$. Therefore,

$$\begin{aligned} N\vec{b} &= \vec{Nb_i} = N(E\vec{b'}) = N\left((\prod_j b'^{\sum_j e_{i,j}}_j)_{i=1}^r \right) \\ &= \left(\prod_j (Nb'_j)^{\sum_j e_{i,j}} \right)_{i=1}^r = \left(\prod_j (a_j)^{\sum_j e_{i,j}} \right)_{i=1}^r \\ &= E(\vec{a}). \end{aligned}$$

Using the fact that the subexponent is not p, we obtain thus two expressions for $N\vec{a'}$ as follows:

$$\begin{aligned} N\vec{a}' &= p\vec{a} = pI \cdot \vec{a} \\ &= N\left(\mathbf{Diag}(p^{e_i})\vec{b}\right) = \mathbf{Diag}(p^{e_i}) \cdot N(\vec{b}) = \mathbf{Diag}(p^{e_i}) \cdot E\vec{a}, \quad \text{so} \\ \vec{a} &= \mathbf{Diag}(p^{e_i - 1}) \cdot E\vec{a} \end{aligned}$$

The a_j form a minimal system of generators and E is regular over $\mathbb{Z}_p$; therefore $\vec{(\alpha)} := (\alpha_j)_{j=1}^r = E\vec{a}$ is also minimal system of generators of A and the last identity above becomes

$$\vec{a} = \mathbf{Diag}(p^{e_i-1}) \cdot \vec{\alpha}.$$

If $e_i > 1$ for some $i \leq r$, then the right hand side is not a generating system of A while the left side is: it follows that $e_i = 1$ for all i. Therefore $|B/\iota(A)| = p^R$ and we have shown above that this implies the injectivity of ι.

Finally, let $x \in B$ and $q = \text{ord}(Nx) \geq p$. Then $qN(x) = 1 = N(qx)$, and since $qx \in \iota(A)$, it follows that $N(qx) = pqx = 1$ and thus pq annihilates x. Conversely, if $\text{ord}(x) = pq$, then $pqx = 1 = N(qx) = qN(x)$, and $\text{ord}(Nx) = q$. Thus $\text{ord}(x) = p \cdot \text{ord}(Nx)$ for all $x \in B$ with $\text{ord}(x) > p$. If $\text{ord}(x) = p$, then $x \in S(B) = S(\iota(A) \subset \iota(A)$ and $Nx = px = 1$, so the last claim holds in general. □

This small exercise in linear algebra avoids a deeper investigation of M as a sum of irreducible Λ-modules, and the afferent pseudo-isomorphisms which may arise. Of course one may identify the modules A, B in the Lemma with subsequent levels in an IW-module.

Proposition 1. *Let M be a $\mathbb{Z}_p$ - torsion free Noetherian Λ - module of finite p-rank with property F and $n_0 \in \mathbb{N}$ be the bound proved in Lemma 3, such that for all $n \geq n_0$ and for all submodules $A \subset M$ we have p-rk$(A_n) = \mathbb{Z}_p$-rk$(A) = \lambda(A)$. Then for all $n \geq n_0$ and all $x \in M_{n+1}$, the lifts $\iota_{n,n+1}$ are injective, so M is Weierstrass. Moreover and the following hold:*

$$\begin{aligned} px &= \iota(N_{n+1,n}(x)), \quad \iota(M_n) = pM_{n+1}, \\ \omega_n x &\in \iota_{n,n+1}(M_n[p]) \end{aligned} \tag{17}$$

In particular, for $n > n_0$, the transitions $C_n(M)$ are stable and

$$\nu_{n+1,n}(a_{n+1}) = pa_{n+1} = \iota_{n,n+1}(a_n). \tag{18}$$

Proof. Since M has property F, has finite p - rank and has no $\mathbb{Z}_p$ - torsion, the second point in Lemma 3 holds, thus $|M_n| > |M_{n+1}|$ for an $n_0 \in \mathbb{N}$. We let thus from now on $n > n_0$. Since M is torsion free, we may also assume also that $\operatorname{sexp}(A_n) > p$. It follows then form Lemma 4 that the lift maps are injective, so M is Weierstrass. We use the notations from this Lemma and let $\iota = \iota_{n,n+1}, N = N_{n+1,n}$ and $N' = \nu_{n+1,n}$.

For proving (18), thus $px = \iota(N(x)) = N'(x)$, we consider the development $t := \omega_n = (T+1)^{p^n} - 1$ and

$$N' = p + t \cdot v = p + t(\binom{p}{2} + tw)), \quad v, w \in \mathbb{Z}[t],$$

as follows from the Newton development of $N' = \frac{(t+1)^p - 1}{t}$. By definition, t annihilates M_n and a fortiori $\iota(M_n) \subset M_{n+1}$; therefore, for arbitrary $x \in M_{n+1}$ we have $(pt)x = t(px) = t\iota(x_1) = 0$, where the existence of x_1 in $px = \iota(x_1), x_1 \in M_n$ follows from Lemma 4. Since ι is injective and thus rank preserving, we deduce that $tx \in M_{n+1}[p] = \iota(M_n[p])$, which is the first claim in (17). Then

$$t^2x = t \cdot (tx) = tx_2 = 0, \qquad \text{since } x_2 = tx \in \iota(M_n).$$

Using $t^2x = ptx = 0$, the above development for N' plainly yields $N'x = px$, as claimed. Injectivity of the lift map then leads to (17). Indeed, for $a = (a_n)_{n\in\mathbb{N}}$ and $n > n_0$ we have

$$\begin{aligned} \operatorname{ord}(a_n) &= \operatorname{ord}(\iota_{n+1,n}(a_n)) = \operatorname{ord}(\iota_{n+1,n}\dagger N_{n+1,n}(a_{n+1})) \\ &= \operatorname{ord}(\nu_{n+1,n}a_{n+1}) = \operatorname{ord}(pa_{n+1}) = \operatorname{ord}(a_{n+1})/p. \end{aligned}$$

This completes the proof. □

As a consequence, we have

Corollary 1. *Let M be a Weierstrass module, let $n_0 = n_0(M)$ be its stabilization index and consider $x = (x_n)_{n\in\mathbb{N}} \in M \setminus M^\circ$. Then there is a constant $z(x) \in \mathbb{Z}$ such that $\operatorname{ord}(x_n) = p^{\max(0,n+1+z(x))}$ for all $n > n_0$. Furthermore, for $n > n_0$ the cyclic composition rules are*

$$\begin{aligned} N_{n+1,n}\dagger\iota_{n,n+1} &= p : M_n \to M_n \quad \textit{and} \\ \iota_{n,n+1}\dagger N_{n+1,n} &= p : M_{n+1} \to M_{n+1}. \end{aligned}$$

Proof. Let $n > n_0$ be such that $x \notin Y_n$, so $x_n \neq 0$. Then we define $z(x) = \operatorname{ord}(x_n) - (n+1)$. By Proposition 1, it follows that $z(x)$ has the desired properties, and in particular it does not depend on n. The first composition rule belongs to the definition of coherent sequences; the second is new and follows from (18). □

Definition 5. *Let M be a PIW module and $z : M \to \mathbb{Z} \cup \{-\infty\}$ be defined by $z(x) = -\infty$ if $x \in M^\dagger$, while for $x \in M \setminus M^\dagger$, the value is defined by the previous corollary. We define the order of M by $z(M) = \max\{z(x) : x \in M\}$.*

Note that since $z(x) \leq \exp(M_{n_0}) - (n+1)$ for all $x \in M$, the order $z(M)$ is an integer. Furthermore, one verifies that z verifies the ultrametric inequality $z(xy) \leq \max(z(x), z(y))$ for $x, y \in M$.

Finally, we consider the semistable transitions:

Lemma 5. *Let M be an IW module, $a \in M \setminus \mathfrak{M}M$ and $A_n = \Lambda a_n$. If $C_n = (A_{n+1})/(\iota(A_n))$ is a semistable transition, then $pA_{n+1} = \iota(A_n)$. Moreover, $pa_{n+1} = \nu_{n+1,n} a_{n+1} = v\iota_{n,n+1}(a_n)$, for $v \in R_n^\times$.*

Proof. From the definition,

$$\nu_{n+1,n} = \frac{(\omega_n+1)^p - 1}{\omega_n} = p \cdot \left(1 + \frac{p-1}{2}\omega_n + \ldots + \omega_n^{p-2})\right) + \omega_n^{p-1}.$$

Since C_n is semistable, it follows in particular that $\omega_n^{p-1} a_{n+1} = 0$ and thus

$$\iota(a_n) = \nu_{n+1,n}(a_{n+1}) = (up)a_{n+1}, \quad u \in R_n^\times.$$

But then $u^{-1}\iota(a_n) = pa_{n+1}$, which readily implies that $pA_{n+1} = \iota(A_n)$; the last claim follows with $v = u^{-1}$. Note that we do not need injectivity of the lift map for this proof. □

We have the following consequence:

Corollary 2. *Let M be a semistable PIW-module. Then for all $n \geq n_0$ and all $a \in M$ we have*

$$\begin{aligned} \iota_{n,n+1}(\Lambda a_n) &= \Lambda p a_{n+1}, \\ p a_{n+1} &= \iota_{n,n+1} v a_n, \quad v \in \Lambda^\times. \end{aligned} \tag{19}$$

If additionally $\iota_{n,n+1}$ is injective for the transitions $C(\Lambda a_n)$, then $\mathrm{ord}(a_n) = p^{n-n_0} \cdot \mathrm{ord}(a_{n_0})$.

Proof. This is a direct consequence of Lemma 5. □

Iwasawa's theory of Λ-modules holds in particular for IW - modules and the constants $\lambda(M), \mu(M), \nu(M)$ and the characteristic polynomial $f_M(T) \in \mathbb{Z}_p[T]$ are well defined for Λ - torsion IW modules. We shall show in Chapter 4, that the class groups of Iwasawa theory enjoy property F.

2.3. **Classification of PIW-modules.** The various types of PIW modules are related by:

Proposition 2. *Any PIW-module A is the direct sum $A = W \oplus M \oplus F$, with W an asymptotic Weierstrass module, M a finite sum of modules of μ - type and F finite. Moreover, $A^\dagger = M \oplus F$.*

Proof. The statement is evident. By definition $A^\dagger$, which is a canonic module, has a direct complement which must be Weierstrass. Moreover, the finite $\mathbb{Z}_p$ - torsion $F := A^\circ \subset A^\dagger$ is also canonic and it has a direct complement in $A^\dagger$ which is a sum of $\mathbb{Z}_p$ - torsion cyclic modules, none of which is finite. It must thus by a sum of modules of μ - type. □

3. Coalescence and decompositions of Λ modules

In this section we let $M = \varprojlim_n M_n$ be an arbitrary Λ-module which is projective limit of a norm coherent sequence of modules M_n; moreover, we assume that M is free as a $\mathbb{Z}_p$-module and has finite $\mathbb{Z}_p$-rank. Property F will in particular not be required. We assume that there is a finite group Δ which acts on M and endows it with a structure of $\Lambda[\Delta]$-module. We shall consider therefore M as an R-module where $R \in \{\mathbb{Z}_p, \Lambda, \Lambda[\Delta]\}$. In all of these three cases, we consider submodules $A \subset M$ with respect to the existence of direct complements, the possibility of taking "roots" in R and the R - completeness of A. We define

Definition 6. *Let M be like above and $A \subset M$ be a Λ-submodule. Let $R \in \{\mathbb{Z}_p, \Lambda, \Lambda[\Delta]$. We say that A is*

N. R - Complementable, *iff there is an R-submodule $B \subset M$ such that $M = A \bigoplus B$. Note that A is always a Λ-module, but B need not be one, if $R = \mathbb{Z}_p$.*

C. R-coalescence closed, *if for all $a \in A$ and $b \in M$ such that there exist $x, y \in R$ with $ax + by = 0$, it follows that there is a $b' \in A$ with $by = b'y$. In general, we say that two elements $u, v \in M$ are R-coalescent if there are $x, y \in R$ such that $ux + vy = 0$.*

M. R-maximal, *if for all $a \in A, b \in M$ with $a = bx$ for an $x \in R$, it follows that there is a $b' \in A$ with $b'x = a$.*

We give a simple example which will motivate the notion of coalescence and show its relation with pseudoisomorphisms.

Example 2. *Let $\mathbb{K} = \mathbb{Q}[\zeta_p]$ be the p-th cyclotomic extension, suppose that $A = A^-$ and there are two orthogonal idempotents $\varepsilon_i, \varepsilon_j \in \mathbb{Z}_p[\Delta]$ with $\varepsilon_i A \neq 0 \neq \varepsilon_j A$. Moreover, we assume that $\lambda(A) = 2$ and the minimal polynomials are $f_i = T - up, f_j = T - vp$ with $u, v \in \mathbb{Z} \setminus p\mathbb{Z}$. Let $a, b \in A$ generate $\varepsilon_i A$ and $\varepsilon_j A$, respectively and $c = a \cdot b$. Since a and b are separated by the action of $\mathbb{Z}_p[\Delta]$ - and not of Λ - it follows that $A_0 = \langle a_0, b_0 \rangle_{\mathbb{Z}_p}$ and since $f_i a_n = 0$ for all n and $n = 0$ in particular, it follows that $(T - up)a_0 = pa_0 = 1$, so $\mathrm{ord}(a_0) = p$ and the same holds for b_0. However, $(\Lambda c)_0 \subset A_0$ is a one dimensional $\mathbb{F}_p$ - space,* *and thus $\Lambda c \sim A$ but we cannot have isomorphism. The same holds for $c' = a - b$, for instance, and thus $\Lambda c \sim \Lambda c'$; one can verify even that $pc \in \Lambda c'$ and $pc' \in \Lambda c$ and $A = \Lambda c + \Lambda c'$. The relation between c and c' is a symmetric one, but we also have $pa \in \Lambda c$ while there is no p - power such that $p^n c \in \Lambda a$, the $\mathbb{Z}_p$ - ranks being different: the relation between a and c is thus an asymmetric one, although $\Lambda a + \Lambda c = \Lambda c' + \Lambda c = A$.*

In view of simplifying the consequences of pseudoisomorphisms, it is interesting to merge all submodules that are mutually pseudoisomorphic, by defining an equivalence. This is the purpose of the notion of coalescence. Maximality implies that one can take R-roots within the submodule A, and complementability is related to direct sum decompositions. The main result of this section is that the three notions coincide:

Proposition 3. *Let $M = \varprojlim_n M_n$ be like above and $A \subset M$ be a Λ-submodule. Let $R \in \{\mathbb{Z}_p, \Lambda, \mathbb{Z}_p[\Lambda]\}$ be a ring. If $R = \Lambda[\Delta]$, we assume that A is also a $\Lambda[\Delta]$-module. Then*

- (i) *The module A is R-coalescently closed iff it is R-maximal.*
- (ii) *If A is complementable, then A is coalescence closed.*
- (iii) *Suppose that A is coalescence closed and for each prime distinguished polynomial $f \in \mathbb{Z}_p[T]$, if $M(f) \cap A \neq 0$, then $M(f) \subset A$. Then A is R-complementable.*

Proof. Since maximality is the special case of coalescence in which $x = 1$, coalescence closed modules are R-maximal. Conversely, if A is R-maximal and $a \in A, b \in M$ with $xa = yb$ for $x, y \in R$, then $xa \in A$ since A is an R-module, and since it is R-maximal, it follows that $xa = yb'$ for an $b' \in Y$. Thus A is coalescence closed. This proves (i).

Suppose that A is R-complementable; let $B \subset M$ be an R-module with $M = A \oplus B$. Let $a \in A, c \in M$ with $ax + cy = 0$ for $x, y \in R$. We may decompose $a = (a_1, 0), c = (c_1, c_2)$ according to the direct sum $M = A \oplus B$; then we deduce in particular that $0x + c_2 y = 0$ and letting $c' = (c_1, 0)$ we have $cy = c'y$, while $c' \in A$. Thus A is coalescence complete and (ii) holds.

Suppose now that A is coalescence closed and the premise of (iii) holds. We consider the three cases for R independently. Since A is R-maximal, it is in particular $\mathbb{Z}_p$-maximal, so it is $\mathbb{Z}_p$-complementable, which proves the claim for $R = \mathbb{Z}_p$.

Let thus $R \neq \mathbb{Z}_p$. For $V \subseteq M$ an R-module we define the R-radical of V in M by $W = \{a \in M : \exists x \in R \text{ with } ax \in V\} \subset M$. Then one verifies that W is an R-module. Let now $\mathcal{M} = \{a_1, a_2, \ldots, a_s; a_{s+1}, \ldots, a_r\} \subset M$ be a minimal set of generators of M as an R-module, the first s of which are a minimal set of generators for A. One can construct such generators using the Nakayama lemma and the structure of $M/(\mathfrak{M}M)$ of an $\mathbb{F}_p$, resp. $\mathbb{F}_p[\Delta]$-module, according to the cases $R = \Lambda$ and $R = \Lambda[\Delta]$. We let then $B = \langle a_{s+1}, a_{s+2}, \ldots, a_s \rangle_R \subset M$, so $A + B = M$ by definition. Let now $V = A \cap B$ and $W \subset M$ be the R-radical of V. Since A is R-maximal, it follows that $W \subset A$: indeed, for $w \in W$ there is an $x \in R$ such that $v = xw \in A \cap B \subset A$, and maximality implies that there is a $w' \in A$ with $xw' = v$ and thus $x(w - w') = 0$. Let $x = F \cdot G$ be a decomposition with $F | f_A(T)$ and $(G, f_A(T)) = 1$, where $f_A(T) \in \mathbb{Z}_p[T]$ is the minimal polynomial of A. Since $w' \in A$ and $(G, f_A) = 1)$ it follows that $Gw' \in A$: indeed, there is a linear combination $uf_A + vG = p^N u', u' \in \Lambda^\times, (v, f_A) = (u, G) = 1$ and thus

$$p^N w'u' = uf_A w' + vGw' = vGw' \in A',$$

and thus $vGw' \in A$. But $(v, f_A) = 1$ implies that $Gw' \in A$. Let $w_1 = Gw \in W$ and $w_1' = Gw' \in W \cap A$. Then $F(w_1 - w_1') = 0$, so $w_1 - w_1' \in A$, since $A \cap M(f) \neq 0$ implies $M(f) \subset A$ for all $f | f_A$. Then $w_1 = w_1' + (w_1 - w_1') \in A$. Finally, since $(G, f_A) = 1$ if follows also that $w \in A$, thus $W \subset A$ as claimed. On the other hand, $W \cap B$ is a Λ-module containing the submodule $V = A \cap B$. Since $W \cap B = 0$ it follows that $V = 0$, so A is complementable. For $R = \mathbb{Z}_p[\Delta]$ the proof of (iii) is similar. Instead the minimal sets of generators for A and M are this time induced by minimal sets of generators for $A/(\mathfrak{M} \cap A)$ and $M/\mathfrak{M}$ as $\mathbb{F}_p[\Delta]$-modules. □

4. The decomposition of Weierstrass modules

In this section the module M will be an unramified Weierstrass module. It enjoys thus in particular the properties of the modules of the previous section. Conversely, not all $\mathbb{Z}_p$-free Λ-torsion modules enjoy property F: it suffices to consider $A = p^n M \subset M$ for M an unramified Weierstrass module and $n > \exp(M_1)$. Then $Y_1(A) = A$ and property F would imply $Y_1(A) = T(A) = A$, so $A \in \mathfrak{M}A$ and $A = 0$ by Nakayama's Lemma. Therefore, we shall consider $\mathbb{Z}_p$-coalescently closed submodules of M, thus submodules $A = A^{(c)} \subset M$, where the $\mathbb{Z}_p$ hull is defined by

$$A^{(c)} = \{x \in M : p^n x \in A \text{ for } n \geq 0\}.$$

The coalescent closed modules are $\mathbb{Z}_p$-complementable by Proposition 3.

The main fact of this section settles the question of ramification:

Proposition 4. *Let M be a Weierstrass module. Then $M(T) = M[T] = \mathcal{T}(M)$ and $M[T]$ is Λ-complementable.*

Proof. Since M is Weierstrass, it has finite $\mathbb{Z}_p$-rank and there is a T-exponent $k = \exp_T(M) = \min\{k : T^k M(T) = 0\}$. Suppose that $k > 1$; then there is an $a \in M(T) \setminus \mathfrak{M}M$ such that $T^{k-1}a \neq 0$. Let $q = \mathrm{ord}(a_1)$ and $b = qa \in Y_1(M) \cap M(T)$. From the property F of M we deduce that there are $y \in M, t \in \mathcal{T}(M) \subset M[T]$ with $Ty + t = b$. Then

$$T^{k+1}y = T^{k+1}y + T^k t = T^k b = T^k qa = 0,$$

and thus $y \in M(T)$. The choice of $k < 1$ implies then

$$T^k y = T^k y + T^{k-1}t = T^{k-1}b = T^{k-1}qa = 0,$$

and since M is $\mathbb{Z}_p$-torsion free, it follows that $T^{k-1}a = 0$ in contradiction with the choice of a. We must thus have $k = 1$, so $M(T) = M[T]$. Suppose now that $\mathcal{T}(M) \neq M[T]$ and let $a \in M[T] \setminus \mathcal{T}(M)$ and $b = \mathrm{ord}(a_1) \cdot a \in Y_1(M)$. Like before, $b = Ty + t$ and $Tb = T^2y = 0$ and thus $y \in M[T]$, and the previous equation yield

$$\mathrm{ord}(a_1)a = b = Ty + t = t \in \mathcal{T}(M).$$

Thus $b \in \mathcal{T}(M)$ and since this module is coalescence closed, it follows that $a \in \mathcal{T}(M)$, which completes the proof of the first statement.

Let $W = TM \subset Y_1(M)$. This is a Λ-submodule and property F implies that $W + M[T] = M$. Moreover, $W \cap M[T] = 0$, since the T - exponent of $M(T)$ is one. Let $W' = W^{(c)} \subset M$. We claim that $M = W' \oplus M[T]$ and W' is a Λ-module. It is a $\mathbb{Z}_p$-module by definition and it has a Λ-submodule W of finite index. Then $p^nW' \subset W$ and if $\overline{W}' \supset W'$ is the Λ-closure of W', then the Λ-closure of p^nW' is $\overline{p^nW'} = p^n\overline{W}' \subset W$, so $p^n\overline{W}' \subset W$. Since W' is $\mathbb{Z}_p$-coalescence closed, it follows by comparing $\mathbb{Z}_p$-ranks, that $W' = \overline{W}'$, so W' is a Λ-module. Let $I = W' \cap M[T]$. Then $p^nI \subset (p^nW') \cap M[T] \subset W \cap M[T] = 0$. The module M being $\mathbb{Z}_p$-free, it follows that $I = 0$, which completes the proof. □

This elementary computation in Weierstrass modules implies that $(A')^-[T] = 0$ in CM fields, a fact which was conjected by Gross in 1983. We shall give more details on this conjecture, together with an alternative proof, in Snoqit III.

Since the T-part of M is a direct term, we may assume from now on that M is a Weierstrass module which is free of T-parts and in particular of ramification. In particular $Y_n(M) = \omega_n M$ for all $n \geq 1$. Since $M(T) = 0$, a fortiori $M(\omega_n) = 0$, so the map $M \to \omega_n M$ is an isomorphism of Λ-modules. The following lemma describes a large class of submodules of M with property F:

Lemma 6. *Let M be a Weierstrass module with $M(T) = 0$ and $A \subset M$ be a Λ-module which is $\mathbb{Z}_p$-coalescence closed. Then A has property F. In particular, if $f \in \mathbb{Z}_p[T]$ is a polynomial dividing the minimal polynomial $f_M(T)$, then $M(f)$ and $M[f]$ have property F.*

Proof. Let $Y_1(A) = A \cap Y_1(M)$. It suffices to show that $Y_1(A) = TA$. Since $M(T) = 0$, the condition is equivalent to property F. Let $a \in A \setminus \mathfrak{A}$ and $q = \text{ord}(a_1), b = qa \in Y_1(A)$; thus $b = Ty, y \in M$. If $f_a(T)$ is the minimal polynomial of a, then $f_a(T) = p^n + Th(T)$ for an $n > 0$ and $h(T) \in \mathbb{Z}_p[T]$, and thus $p^n a = -Th(T)a \in Y_1(A)$, so $q|p^n$. Suppose that $p^n = qr$: then $rb = T(ry) \in TA$ and since the map $M \to Y_1(M)$ is injective, it follows that $ry \in A$. The module A is coalescence closed, so we must also have $y \in A$. Finally, $Y_1(A)$ is spanned, by Nakayama's lemma by elements like b, so we conclude that $Y_1(A) = TA$, as claimed.

If $f|f_M(T)$, then $M(f)$ and $M[f]$ are by definition coalescent closed: indeed if $qx \in M(f)$, then $f^k qx = 0$ for $k \geq 1$ and since M is $\mathbb{Z}_p$-torsion free, $f^k x = 0$, so $x \in M(f)$ and $M(f)$ is coalescence closed. For $M[f]$, the proof is the same, choosing $k = 1$. □

If $M = \bigoplus_{i=1}^{s} M_i$ is a Weierstrass module that decomposes in a direct sum of Λ-modules, then it follows from the definition that all M_i have property F: indeed, $Y_1(M_i) = TM \cap M_i = TM_i$, and thus M_i has property F (we already know that $\mathcal{T}(M)$ is a direct term, so we assumed it vanishes. We deduce in the Appendix below the same fact following Iwasawa's proof in [2].

5. Appendix: Property F for class groups

In this section we let $\mathbb{K}$ be a galois number field that contains the p-th roots of unity and $\mathbb{K}_n, A_n, \mathbf{B}_n$, etc. have the usual signification and $A = \varprojlim_n A_n$. We assume that the primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. Let $\mathbb{H}/\mathbb{K}_\infty$ be the maximal unramified abelian p-extension and $X = \varphi(A) = \text{Gal}(\mathbb{H}/\mathbb{K}_\infty)$, with φ the Artin symbol.

The purpose of this chapter is to prove that Property F is enjoyed by all coalescence closed submodules of A. For A itself, this fact was proved in 1959 by Iwasawa, the proof is found in all text books on cyclotomy (see references below) and it uses class field theory. Although the statement has module-theoretic flavor, even for the simple case of A, no proof is known, which relays only on module theoretic facts. A deeper reason for this fact may stem from the use of Kummer duality, which involves pairs of isomorphic Λ-modules.

We fix $\mathbb{K}_\infty \subseteq \mathbb{M} \subseteq \mathbb{H}$, an infinite extension which is galois over $\mathbb{K}$, and let for all $n \geq 0$, the field $\mathbb{M}_n = \mathbb{M} \cap \mathbb{H}_n$ be the largest subextension of $\mathbb{M}$ which intersects $\mathbb{K}_\infty$ in $\mathbb{K}_n$. Let $X = \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ and $G = \mathrm{Gal}(\mathbb{M}/\mathbb{K}), G_n = \mathrm{Gal}(\mathbb{M}/\mathbb{K}_n)$. The following classical computation yields the commutator G' (see [6], Lemma 13.14):

Lemma 7. *Notations being like above, $G' = TX$ and $G'_n = \omega_n X$.*

Proof. We may lift Γ to G for instance by identifying this group with the inertia group $I(\wp)$ of a prime $\wp \subset \mathbb{K}$ above p which ramifies completely in $\mathbb{K}_\infty/\mathbb{K}$. Since $\mathbb{M}/\mathbb{K}_\infty$ is unramified, it follows indeed that $I(\wp) \cong \Gamma$ and we let $\sigma \in I(\wp)$ be a topological generator mapping to $\tau \in \Gamma$. Then we assume that Γ acts on X via σ, so $z^\sigma = \sigma z \sigma^{-1}$ for $z \in X$. Since $G = \Gamma X$, we may represent arbitrary elements of G via this decomposition; let thus

$$a = \alpha x, b = \beta y, \quad \alpha, \beta \in \Gamma, x, y \in X.$$

Then, using the fact that Γ and thus I are abelian groups, and so is X

$$\begin{aligned}
[a,b] &= aba^{-1}b^{-1} = \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\
&= x^\alpha (yx^{-1})^{\alpha\beta} \alpha\beta\alpha^{-1} y^{-1}\beta^{-1} = x^\alpha (yx^{-1})^{\alpha\beta} \beta y^{-1} \beta^{-1} \\
&= x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \\
&= (x^\alpha)^{1-\beta} \cdot (y^\beta)^{\alpha - 1}.
\end{aligned}$$

After this cataract of algebraic transformations, we brought the commutator in a simple form, that allows to apply the structure of Λ. For this we note that, since σ is a topological generator, an arbitrary element $w \in I(\wp)$ is of the form $w = \sigma^c, c \in \mathbb{Z}_p$. We lift T to $\sigma - 1 \in \mathbb{Z}_p[I(\wp)]$; since $\cap_n T^n \Lambda = 0$, we have

$$1 - w = 1 - (T+1)^c = 1 - (1 + T \cdot \sum_{n=1}^{\infty} \binom{c}{n} T^{n-1}) \in T\mathbb{Z}_p[I(\wp)].$$

Since we defined the action of τ on X via σ, it follows that $(x^\alpha)^{1-\beta} \cdot (y^\beta)^{\alpha-1} \in TX$. But X is closed, and thus TX is closed too, so it follows that $TX \supset G'$. On the other hand, by choosing $\beta = 1, \alpha = \sigma$ in the above, we find that $y^T \in G'$ for any $y \in X$ and thus $TX \subset G'$. Consequently, $TX = G'$. The proof for G'_n follows by replacing τ with $\tau^{p^{n-k}}$, Γ by $\Gamma^{p^{n-k}}$, etc. □

In view of the previous lemma, we may define $\overline{\mathbb{L}}_n = \mathbb{M}^{\omega_n X}$; since $\omega_n X = G'_n$ is the closure of the commutator of G_n, it follows that $\overline{\mathbb{L}}_n$ is the maximal subextension of $\mathbb{M}$ which is abelian over $\mathbb{K}_n$.

Next we consider ramification and investigate the group fixing the maximal subextension of $\overline{\mathbb{L}}_n$ which is also unramified over $\mathbb{K}_n$, that is, by definition, $\mathbb{M}_n$.

Let $\Omega(\mathbb{K})$ be the product of all $\mathbb{Z}_p$ extensions of $\mathbb{K}$ and $\mathbb{H}_M = \Omega(\mathbb{K}) \cap \mathbb{M}$. Then $\mathbb{H}_M/\mathbb{K}$ is an abelian extension with galois group $\Delta \hookrightarrow A$, which is annihilated by T. Therefore $\Delta \hookrightarrow A[T]$; let s denote the number of conjugate primes above p in $\mathbb{K}$. We shall assume for simplicity that $A[\omega_n] = A[T]$; this can be achieved under eventual shift of the base field $\mathbb{K}$.

Lemma 8. *Notations being like above, let* $W_n = Gal(\mathbb{M}/\overline{\mathbb{L}}_n) \subset X$ *and* $\overline{\mathbb{M}}_n = \mathbb{K}_\infty \cdot \mathbb{M}_n$*. There is a submodule* $Z_0 \subset A[T]$ *such that* $Gal(\overline{\mathbb{L}}_0/\overline{\mathbb{M}}_0) \cong Z_0$*. Letting* $Z_n = \nu_{n,0} Z_0$*, we have for all* $n \geq k$ *that* $Gal(\overline{\mathbb{L}}_n/\overline{\mathbb{M}}_n) \cong Z_n$*. Moreover, if* $Y_n = \omega_n X \cdot Z_n$*, and* $X_n = Gal(\mathbb{M}_n/\mathbb{K}_n) = Gal(\overline{\mathbb{M}}_n/\mathbb{K}_\infty)$*, then*

$$X/Y_n = X_n, \quad \text{and} \quad Y_n = \nu_{n,0} Y_0, \quad \forall n \geq k. \tag{20}$$

Proof. We follow here Washington's presentation of Iwasawa's proof in op.cit, pp 278-279. Let $\wp_i, i = 1, 2, \ldots, s$ be the conjugate primes above p in $\mathbb{K}$ and $\tilde{\wp}$ be a prime of $\mathbb{M}$ lying above $\wp = \wp_1$. If $I \subset G$ is its inertia group, then $I \cap X = 1$ since $\mathbb{M}/\mathbb{K}_\infty$ is unramified. Total ramification of $\mathbb{K}_\infty/\mathbb{K}$ at $\wp$ implies that the map $I \hookrightarrow G/X = \Gamma$ is also surjective; it is thus bijective. Therefore $G = (\nu I)X = X(\nu I)$ for all $\nu \in C := \mathrm{Gal}(\mathbb{K}/\mathbb{Q})/D(\wp)$, the set of coset representatives mapping $\wp$ to the various $\wp_i$. Choose $\sigma(\nu) \in \nu I$ mapping to τ, so $\sigma(\nu)$ is a topological generator of I; since $\nu I \subset XI$, there is an $a_\nu \in X$ such that $\sigma(\nu) = a_\nu \cdot \sigma, \quad \sigma = \sigma(1)$. Let

$$Z_0 = \langle a_\nu : \nu \in C \setminus \{1\} \rangle_{\mathbb{Z}_p} \quad \text{and} \quad Z_n = \langle \nu_{n,0} a_\nu : \nu \in C \setminus \{1\} \rangle_{\mathbb{Z}_p}.$$

Since the primes of $\mathbb{K}$ are totally ramified, $I^T = 1$ and $a_\nu^T = 1$, so $Z_0 \subset \varphi(A[T])$. By definition of the $\mathbb{Z}_p$ - span, it is a compact subgroup of X. We prove now that $\nu_{n,0} a_\nu = a_\nu^{p^{n-k}}$; from the definition, $\nu_{n,0} = \frac{\tau^{p^{n-k}}-1}{\tau-1} = p^{n-k} + O(T)$, and since $a_\nu^T = 1$, the claim follows.

The extension $\overline{\mathbb{L}}_0$ is the maximal abelian extension of $\mathbb{K}_0$ in $\mathbb{M}_0$, and $\mathbb{M}_0$ is the maximal unramified abelian subextension. It is thus fixed by the closure $Z_0' = \langle I(\nu\wp) : \nu \in C \rangle_{\mathbb{Z}_p}$ of the group generated by the inertia of all the ramified primes above p, so $\mathbb{M}_0 = \overline{\mathbb{L}}_0^{Z_0'}$. We may identify a lift of Γ to G with $I(\wp) \subset G$, so $Z_0' = \Gamma \cdot Z_0$ and we find that $\overline{\mathbb{M}}_0 = \overline{\mathbb{L}}_0^{Z_0}$, as claimed. The proof for Z_n is similar.

Since $X_n = \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_n) = \mathrm{Gal}(\overline{\mathbb{M}}_n/\mathbb{K}_\infty)$ and by combining the previous result with the one of Lemma 7 we find that the closure $Y_n =$

$\omega_n Z_n \subset X$ is the group fixing $\overline{\mathbb{M}}_n$, it follows by galois theory that

$$X_n = \text{Gal}(\overline{\mathbb{M}}_n/\mathbb{K}_\infty) = \text{Gal}(\mathbb{M}/\mathbb{K}_\infty)/\text{Gal}(\mathbb{M}/\overline{\mathbb{M}}_n) \cong X/Y_n.$$

Since $G'_n = \omega_n X = \nu_{n,0}(TX) = \nu_{n,0}G'$ and $Z_n = \nu_{n,0}Z_0$, as we have shown above, it follows also that $Y_n = \nu_{n,0}Y_0$. This completes the proof of (20) and the lemma. □

Note that the above result, applied to $\mathbb{M} = \mathbb{H}$ readily implies that $A \cong \text{Gal}(\mathbb{H}/\mathbb{K}_\infty$ has the property F. Moreover, if $\mathbb{H}' \subset \mathbb{H}$ is the maximal subextension that splits all the primes above p, then (20) implies that A' has also the property F.

We have defined Z_0 with respect to an arbitrary choice of $\wp$, but:

Lemma 9. *Let $\mathbb{M} \subset \mathbb{H}$ be a galois extension of $\mathbb{K}$ with $X = Gal(\mathbb{M}/\mathbb{K}_\infty)$. Then there is a canonic subgroup $Z_0(\mathbb{M}) \subset A[T]$, such that $Y_n(\mathbb{M}) = Ker\ (N_{\infty,n} : X \to X_n) = \omega_n X \cdot Z_0(\mathbb{M})$.*

Proof. The existence of Z_0 was proved in the Lemma 8. We show now that this module is in fact canonic. We defined $\sigma(\nu) \in I(\nu\wp) \subset G$ as topological generators of these inertia groups and let $a_\nu = a(1,\nu) \in X$ relate the different inertias by $\sigma(\nu) = a(1,\nu)\sigma(1)$. More generally we let $a(\mu,\nu) \in X$ be such that $\sigma(\nu) = a(\mu,\nu)\sigma(\mu)$. The module $Z_0 \subset X$ is the $\mathbb{Z}_p$ span of the $a(1,\nu)$. In order to show that it does not depend on the choice of $\wp$, we show that

$$Z_0 = \langle a(\mu,\nu)\ :\ \mu,\nu \in C\rangle_{\mathbb{Z}_p} \subset X. \tag{21}$$

We have

$$\begin{aligned} a(1,\nu)\sigma(1) &= \sigma(\nu) = a(\mu,\nu)\sigma(\mu) = a(\mu,\nu)a(1,\mu)\sigma(1), \quad \text{thus} \\ 0 &= \left(a(1,\nu) - a(\mu,\nu)a(1,\mu)\right)\sigma(1). \end{aligned}$$

We have shown that $\sigma(1)$ is a lift of τ, so the second identity above implies that $\tau\left(a(1,\nu) - a(\mu,\nu)a(1,\mu)\right) = 0$. This leads to $a(1,\nu) = a(\mu,\nu)a(1,\mu)$, hence $a(\mu,\nu) \in Z_0$ and (21) is true.

□

With this we may define $\widetilde{\mathbb{H}} = \mathbb{H}^{Z_0} \subseteq \mathbb{H}'$, which is a canonic subfield of $\mathbb{H}'$, the maximal class field which splits all the primes above p. Let $\mathcal{X} = \text{Gal}(\widetilde{\mathbb{H}}/\mathbb{K}_\infty)$. Then $Y_n = Y_n(\widetilde{\mathbb{H}}) =$ Ker $(N_{\infty,n} : \mathcal{X} \to \mathcal{X}_n)$ has the simple expression $Y_n = \omega_n\mathcal{X}$ and $\widetilde{\mathbb{H}}$ was constructed to be the maximal subfield with this property.

The question whether $\widetilde{\mathbb{H}} = \mathbb{H}'$ or there is actual inclusion is intimately related to a conjecture of Gross which shall be treated in SNOQIT II. The conjecture implies that the two fields are equal.

We shall now apply (20) in order to prove, more generally, that an arbitrary Λ - submodule $M \subset A$ has the property F.

Proposition 5. *Notations being like above, let $M \subset A$ be a Λ-maximal Λ-submodule and $Y_n(M) = \ Ker\ (N_{\infty,n}M \to M_n)$. Then there is a submodule $Z_0(M) \subset M \cap A[T]$ such that*

$$(22)\quad Y_0(M) = (TM) \cdot Z_0(M), \qquad \textit{and} \qquad Y_n(M) = \nu_{n,0} Y_0(M)$$

Moreover, $M_n \cong M/Y_n(M)$ for all $n \geq k$.

Proof. Let $X = \mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty) \cong A$. Since $M \subset X$ is a Λ-module and X is abelian, it is a compact normal subgroup, and the fixed field $\mathbb{M} = \mathbb{H}^{\varphi(M)}$ is abelian over $\mathbb{K}_\infty$; let its group be $Q = \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong X/M$. The extension $\mathbb{M}/\mathbb{K}$ is galois: let $G = \mathrm{Gal}(\mathbb{H}/\mathbb{K}) = \tilde{\Gamma} \ltimes X$, where $\tilde{\Gamma} \cong \Gamma$ is a lift determined by the inertia group of some prime, like before, and its topological generator is denoted by σ. Since M is a Λ-module, we have $\sigma M = M$ and for arbitrary $a = \alpha x \in G, \alpha \in \tilde{\Gamma}, x \in X$ and $m \in M$ we have $am = \alpha x m = \alpha m x$, since X is abelian. Moreover, since M is a Λ-module, $\alpha m = m' \in M$ and we conclude that $GM = MG$, so $M \subset G$ is normal and compact therefore $\mathbb{M}/\mathbb{K}$ is galois and Q is a Λ-module.

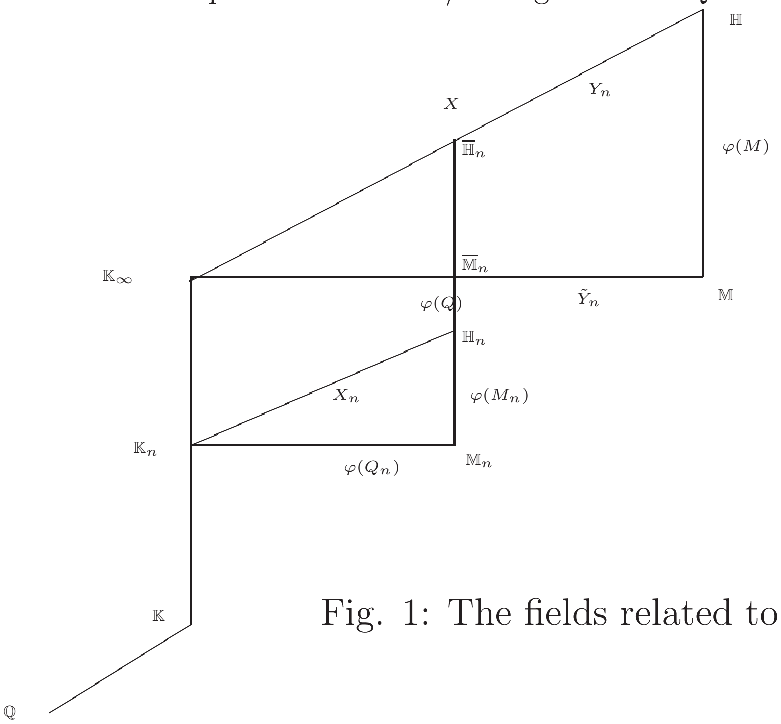

Fig. 1: The fields related to norm kernles

We can thus apply Lemma 8 to the groups A and A/M, thus to the extensions $\mathbb{M}$ and $\mathbb{H}$. Let Y_n, Z_n be defined by the lemma with respect to X and $\tilde{Y}_n, \tilde{Z}_n$ correspond to Q. We have thus by Lemma 8

$$\begin{aligned} A_n &\cong \mathrm{Gal}(\overline{\mathbb{H}}_n/\mathbb{K}_\infty) \cong A/Y_n, \\ Q_n &\cong \mathrm{Gal}(\overline{\mathbb{M}}_n/\mathbb{K}_\infty) \cong Q/\tilde{Y}_n. \end{aligned}$$

We see from the field diagram, that $\tilde{Y}_n, Y_n$ appear as natural groups, to which the Lemma 8 can be applied. There is no maximal abelian extension fixed by $Y_n(M)$ occurring in this diagram; therefore the Lemma cannot be applied directly. However, we claim that $Y_n(M) \cong Y_n/\tilde{Y}_n$, which reduces the claim (5) to the previous lemma.

For proving this claim, we note that $Y_n(M) \subset Y_n$, as the kernel of the norm $N_{\infty,0}$ on the subgroup $M \subset X$, so there is a surjective projection $Y_n \to Y_n(M)$. Furthermore, if $N_Q = (N_{\infty,0} : X \to X_n)|_Q$ then $\tilde{Y}_n = \text{ Ker } (N_Q)$, so the lift of N_Q back to X induces an injective map $\tilde{Y}_n \to Y_n$. We can then apply the 3×3 *Lemma* [4], Chapter II, Lemma 5.1 to the following diagram:

(23)
$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \tilde{Y}_n \arrow[r] \arrow[d] & Y_n \arrow[r] \arrow[d] & Y_n(M) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & Q \arrow[r] \arrow[d] & X \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & Q_n \arrow[r] \arrow[d] & X_n \arrow[r] \arrow[d] & M_n \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

in which the second and third rows are split, as a consequence of M being Λ - maximal. We deduce that the sequence

$$1 \to \tilde{Y}_n \to Y_n \to Y_n(M) \to 1 \tag{24}$$

is exact. Let $Z_0, \tilde{Z}_0$ be defined by Lemma 8 with respect to X, respectively Q. Then $\tilde{Z}_0 = \mathrm{Gal}(\mathbb{M}/(\mathbb{M} \cap \widetilde{\mathbb{H}}))$ and the group fixing $\mathbb{M}$ is $Z_0' = Z_0 \cap M$, so there is an exact sequence

$$1 \to \tilde{Z}_0 \to Z \to Z_0' \to 1.$$

We assume $M \cap A[T]$ is maximal in the sense that if $a \in A(T)$ and $p^m a \in M \cap A[T]$ for an $m \geq 0$, then $a \in M \cap A[T]$, a property to which we shall refer here as $p - T$ - *maximal*; then $Z_0 = \tilde{Z}_0 \cdot Z_0'$ as a direct product. Indeed, it follows from $p-T$ - maximality, that for each maximal cyclic submodule $Z \subset Z_0$, finite or infinite, if $Z \cap Z_0' \neq \{1\}$, then $Z \subset Z_0'$, which implies the claim. We have seen that $\Gamma \cong I(\wp)$ so $Z_0 \cong \mathrm{Gal}(\Omega(\mathbb{K})^{I(\wp)}/\mathbb{K}_0)$, while $\tilde{Z}_0' \cong \mathrm{Gal}((\Omega(\mathbb{K}) \cap \mathbb{M})^{I(\wp)}/\mathbb{K}_0)$. The maximality property of $M^\dagger \cap A[T]$ implies that Z_0' is a direct term in Z_0, which confirms the claim.

Let $Y_0' = TM \cdot Z_0'$. Since $1 \to TQ \to TX \to TM \to 1$ is exact, combining with the previous sequence, we find an exact sequence

$$1 \to \nu_{n,0}\tilde{Y_0} \to \nu_{n,0}Y_0 \to \nu_{n,0}Y_0' \to 1.$$

But we know already that $\tilde{Y_n} = \nu_{n,0}\tilde{Y_0}$ and $Y_n = \nu_{n,0}Y_0$ by Lemma 8, so by comparing the last sequence with (24), we find $Y_n(M) = \nu_{n,0}Y_0' = \nu_{n,0}(TM) \cdot Z_0'$. This completes the proof for the $p - T$ maximal case.

For the general case we see that we only need a local modification in the intersection $M \cap A[T]$. We let the $p - T$ - hull $\overline{M} \supset M$ be defined as the smallest $p - T$ - maximal submodule $A \supset \overline{M} \supset M$, so

$$a \in \overline{M} \Leftrightarrow a \in M \text{ or } a^{p^m} \in M \cap A[T].$$

The previous proof implies that $\overline{M}$ verifies (22). Let $Z_0(\overline{M}) = \oplus_i \mathbb{Z}_p b_i$ and $q_i = p^{e_i}$ be the principal divisor factors for the decomposition of $Z_0(M)$ as a submodule:

$$Z_0(M) = \oplus_i \mathbb{Z}_p b_i^{q_i}.$$

Then $b_i^{r_i} \in Z_n(\overline{M})$ iff $b_i^{q_i r_i} \in Z_n(M)$, and since $Z_n(\overline{M}) = \nu_{n,0} Z_0(\overline{M})$ we conclude that $Z_n(M) = \nu_{n,0}(M)$ too, which completes the proof. □

We can apply this Proposition to various canonic submodules such as $A^\dagger, A^\circ, A^+, A-$, etc.

References

[1] T. Fukuda. Remarks on $\mathbb{Z}_p$-extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8):264–266, 1994.

[2] K. Iwasawa. On Γ - extensions of algebraic number fields. *Bull. Amer. Math. Society*, 65:183 – 226, 1959.

[3] K. Iwasawa. On $\mathbb{Z}_\ell$ - extensions of number fields. *Ann. Math. Second Series*, 98:247 – 326, 1973.

[4] S. MacLane. *Homology*. Springer, 1994.

[5] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined second edition edition, 1990.

[6] L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1996.

(P. Mihăilescu) Mathematisches Institut der Universität Göttingen
E-mail address, P. Mihăilescu: preda@uni-math.gwdg.de

Contents

SNOQIT II: UNITS AND KUMMER THEORY IN IWASAWA EXTENSIONS

Date: Version 1.00 September 21, 2010.

Key words and phrases. 11R23 Iwasawa Theory, 11R27 Units.

Abstract. This is the second part of Snoqit, a series of papers that draw upon discussions and "Seminar Notes on Open Questions in Iwasawa Theory", held in 2007/2008 together with Samuel J. Patterson. The paper is concerned with Kummer pairings and units. Using the information on growth of IW modules from Snoqit I we develop projective-projective pairings for general base fields. The central results of the paper are related to the Iwasawa linear space. We give an explicite construction of this space and, based of its properties prove three major conjectures, of Greenberg, Leopoldt and Gross-Kuz'min. All the three conjectures are proved in the context of CM extensions, but the methods extend to arbitrary fields, using arguments from [8].

1. Introduction

The Λ - modules of this second part of Snoqit[1] are directly related to the Iwasawa theory of cyclotomic $\mathbb{Z}_p$ - extensions. We shall always consider finite galois extensions $\mathbb{K}/\mathbb{Q}$ as base fields, and these will contain the p-th roots of unity. The purpose of this section is to base the Kummer theory on a projective - projective pairing and to derive some usual properties of this pairing. A parallel object of the paper are systems of global and local units. This requires an alternative definition of Kummer radicals, which is used by algebrists in other contexts, and which leads in a natural way to projective systems of radicals.

1.1. **Notation and Facts from Snoqit I.** Some usual notations have been already introduced in Snoqit I. We shall deal with more fields and extensions in this section, and mention that the notation chosen is closer to the one of Lang in [9], and thus in many points different from the one used by Iwasawa in [5]. As a rule, $\mathbb{K}_n \supset \mathbb{K}$ are the intermediate fields of the cyclotomic $\mathbb{Z}_p$-tower of $\mathbb{K}$ and $\mathbb{K}_\infty = \cup_n \mathbb{K}_n$. For n sufficiently large, $\mathbb{K}_n$ contains the p^n-th but not the p^{n+1}-th roots of unity. More precisely, there is a $k > 0$ such that $\mathbb{K}$ contains the p^k-th but not the p^{k+1}-th roots of unity, and we shall write $\mathbb{K} = \mathbb{K}_0 = \mathbb{K}_1 = \ldots = \mathbb{K}_k$. Since the extensions $\mathbb{K}/\mathbb{Q}$ are in general not

[1] Snoqit stands for *Seminar Notes on Open Questions in Iwasawa Theory.* The papers cover a series of results the emerged from the discussions in a series of seminars held together with Samuel J. Patterson and V. Vuletescu in 2007/2008 and will appear as a self contained contribution in the Proceedings of the Jubilaeum Conference in honor of Paddy's 60-th anniversary

abelian, they may be non trivial extensions of the p^k-th cyclotomic extension of $\mathbb{Q}$, so we cannot require $\mathbb{K} = \mathbb{K}_1 \neq \mathbb{K}_2$.

The p-parts of the class groups of $\mathcal{O}(\mathbb{K}_n)$ respectively the ideal class groups of the p-integers of $\mathbb{K}_n$ are A_n, A'_n and $\mathbf{B}_n \subset A_n$ is the subgroup generated by all classes of A_n which contain a product of ramified primes above p. These primes are by definition totally ramified above $\mathbb{K}$ and the norms $N_{m,n} := \mathbb{N}_{\mathbb{K}_m,\mathbb{K}_n}$ are all surjective.

Let $\mathfrak{K}_n = \mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and the *local units* $U_n = (\mathcal{O}(\mathfrak{K}_n))^\times$; then $\mathbb{K}_n$ is dense in $\mathfrak{K}_n$ in the product topology and $\mathfrak{K}_n/\mathbb{Q}_p$ is a galois algebra with group containing $\Delta_n = \mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$. The diagonal embedding $\mathbb{K}_n \hookrightarrow \mathfrak{K}$ will be denoted by $\iota_{\mathbb{K}}$ or even ι, where it can be distinguished in the context from the ideal lift maps $\iota_{n,m} : A_n \to A_m$.

We let $\wp \subset \mathbb{K}$ be a prime above p, $\Delta = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and $C = \Delta/D(\wp)$ a set of coset representatives of the decomposition group $D(\wp) \subset \Delta$ of $\wp$. The primes above p in $\mathbb{K}$ are then $P = \{\nu\wp : \nu \in C\}$ and we assume that they are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. We denote by $\wp_n$ the prime of $\mathbb{K}_n$ above $\wp$ and $P_n = \{\nu\wp_n : \nu \in C\}$. Then

$$U_n = \prod_{\nu \in C} U(\mathbb{K}_{n,\nu\wp_n}),$$

is the product of the units in the completions of $\mathbb{K}_n$ at the primes in P_n. The completion of the diagonal embedding $E_n \hookrightarrow U_n$ is denoted by $\overline{E}_n$. The subgroups $U^{(1)}(\mathbb{K}_{n,\nu\wp_n}) \subset U(\mathbb{K}_{n,\nu\wp_n})$ have the usual meaning and we let

$$\begin{aligned} U_n^{(1)} &= \prod_{\nu \in C} U^{(1)}(\mathbb{K}_{n,\nu\wp_n}), \\ U'_n &= \{u \in (U_n^{(1)})^+ \ : \ \mathbf{N}_{\mathbb{K}_n/\mathbb{Q}}(u) = 1; \end{aligned}$$

the second definition holds only for CM extensions $\mathbb{K}$.

The Leopoldt defect of $\mathbb{K}_n$ is

$$\mathcal{D}(\mathbb{K}_n) = \mathbb{Z}\text{-rk}(E_n) - \mathbb{Z}_p\text{-rk}(\overline{E}_n),$$

and the sequence $\mathcal{D}(\mathbb{K}_n)$ is increasing and has a constant upper bound [12], Lemma 13.22. We may thus assume that $\mathcal{D}(\mathbb{K}_n) = \mathcal{D}(\mathbb{K})$ for all $n \geq k$.

As a general rule, we use multiplicative notation for Λ-modules which arise from a multiplicative context, such as galois groups and class groups. The additive notation is kept for abstract Λ-modules. If X a is $\mathbb{Z}_p$-module, we write $\widetilde{X} = X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$; the embedding $X \hookrightarrow \widetilde{X}$ is given by $x \to x \otimes 1$.

Ad-hoc extensions of $\mathbb{K}_\infty$, with groups which are Λ-torsion modules (or smaller) will be denoted by $\mathbb{F}, \mathbb{L}, \mathbb{M}$, while $\mathbb{H}/\mathbb{K}_\infty$ is the maximal unramified p - abelian extension of $\mathbb{K}_\infty$. We use Lang's notation Ω with various indices for *large* extensions of $\mathbb{K}_\infty$, with groups that contain non trivial free Λ-submodules. In particular Ω is the maximal p - abelian p - ramified extension of $\mathbb{K}_\infty$; its most important subfields are $\Omega_E = \cup_n \mathbb{K}_n[E_n^{1/p^n}]$ and $\Omega_{E'} = \cup_n \mathbb{K}_\infty[(E'_n)^{1/p^n}]$, with $E'_n \supset E_n$ the p - units of $\mathbb{K}_n$. The maximal p - ramified p - abelian extension of $\mathbb{K}_n$ is $\Omega_n \subset \Omega$; it contains $\mathbb{K}_\infty$. If $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ is an extension with $\mathbb{F}/\mathbb{K}$ galois, then $\mathbb{F}_n = \mathbb{F} \cap \Omega_n$, so $\mathbb{K}_\infty \subset \mathbb{F}_n$. Also, the λ-part of $\mathbb{F}$ is defined by

$$\mathbb{F}_\lambda = \mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)^\dagger},$$

the fixed field of the $\mathbb{Z}_p$-torsion $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)^\dagger$ of the galois field. If $X = \mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ is a Λ-torsion module, then $\mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{K}_\infty)$ is a finitely generated $\mathbb{Z}_p$- free Λ-module. If we also have $\mathbb{F} \subset \mathbb{H}$, we let $\mathbb{F}_n = \mathbb{H}_n \cap \mathbb{F}$: in this case ramification allows to define $\mathbb{F}_n/\mathbb{K}_n$ as an extension such that $\mathbb{K}_{n+1} \not\subset \mathbb{F}_n$. Suppose that $X' \subset \mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty)$ is the fixing group of $\mathbb{F}$, and $\mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty)/X'$ is p-coalescence closed, in the sense of Snoqit I. Then X has property F, so it is a Weierstrass module.

It will be useful in some cases to consider subextensions of $\mathbb{K}_n$ which are Kummer. If $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ is galois over $\mathbb{K}$, we write $\underline{\mathbb{F}}_n \subset \mathbb{F}_n$ for the maximal abelian Kummer extension of $\mathbb{K}_n$ contained in $\mathbb{F}_n$: it contains $\zeta_{p^{2n}}$ but not $\mathbb{K}_\infty$. In particular, $\underline{\Omega}_{E,n} = \mathbb{K}_n[E_n^{1/p^n}], \underline{\Omega}_{E',n} = \mathbb{K}_n[(E'_n)^{1/p^n}]$. We write $\mathbb{H}_E = \mathbb{H} \cap \Omega_E$ and $\mathbb{H}' \subset \mathbb{H}$ is the maximal subextension of $\mathbb{H}$ which splits all the primes above p; the notations $\mathbb{H}_n, \mathbb{H}'_n, \mathbb{H}_{E,n}$ are the natural.

We recall from Snoqit I, that IW modules, which model the properties of the Λ-modules encountered in Iwasawa theory, have the property F. All IW modules M are projective limits of norm coherent sequences M_n of finite or infinite abelian p-groups; we do not consider injective limits. The Weierstrass modules are Λ-torsion, $\mathbb{Z}_p$-torsion free modules with property F. If M is an additively written Λ-torsion module and f a distinguished polynomial dividing the minimal polynomial $f_M(T)$, we defined in Snoqit I the f-part and the f-socle by

$$\begin{aligned} M(f) &= \{x \in M : \exists n > 0 \text{ such that } f^n x = 0\} \\ M[f] &= \{x \in M : fx = 0\}. \end{aligned}$$

These are p-coalescence closed submodule of M. An important property of Weierstrass modules M, which was proved in Snoqit I, is

Fact 1.

$$M(T) = M[T], \quad Y_1(M) = TM \oplus M[T], \tag{1}$$

where $Y_1(M) = \ Ker\ (N_{\infty,1} : M \to M_1) \subset M$ *is the kernel of the norm from infinity. Moreover, there is a canonic complement* $M' \subset M$ *with* $M = M' \oplus M[T]$*.*

Iwasawa proved that $A = \text{proj}\lim_n A_n$ has property F - it is to date the only relevant maximal IW module that we know. It follows from a lemma proved in Snoqit I, that all submodules $M' \subset M$ which are p-coalescence closed, i.e. $x \in M, p^n x \in M' \Rightarrow x \in M'$, also have property F.

A further property of Weierstrass modules $M = \varprojlim_n M_n$ is that for n sufficiently large and $m > n$, the lift maps $\iota_{n,m} : M_n \to M_m$ (see also Snoqit I) are all injective and if $a = (a_l)_{l \in \mathbb{N}} \in M$, then $a_m^{p^{m-n}} = \iota_{n,m}(a_n)$. As a consequence, if all the M_n are finite, then there is a constant $z = z(M)$ such that $\text{ord}(a_m) \leq p^{m+z}$ for $a_m \in M_m$. In general, if M i s simply an IW module – so it may contain $\mathbb{Z}_p$-torsion submodules. There is a constant $n_0 = n_0(\mathbb{K})$ such that various useful facts occur, such as

1. For all Weierstrass submodules $M' \subset M$, the p-ranks of M'_n are stable for $n \geq n_0$ and for all $a \in A \setminus \mathfrak{M}A$ we have $a_0 \neq 1$ (there are no *floating* classes).
2. For all finite submodules $M'' \subset M$, the exponents of M_n are stable for $n \geq n_0$ and $M''_n \cong M''_{n_0}$ as finite abelian p-groups, for $n \geq n_0$.
3. For all $a = (a_n)_{n \in \mathbb{N}} \in M$ such that Λa is a pure μ-module[2], the maps $\iota_{n,m} : \Lambda a_n \to \Lambda a_m$ are injective and $\exp(\Lambda a_n) = \exp(\Lambda a)$ for all $m > n \geq n_0$.
4. The Leopoldt defect $\mathcal{D}(\mathbb{K})$ is stable for all $n \geq 0$.

We shall choose $\mathbb{K}$ such that $n = n_0$ and let $k \geq 1$ be the largest integer such that $\zeta_{p^k} \in \mathbb{K}$. Thus $\mathbb{K}_0 = \mathbb{K}_1 = \ldots = \mathbb{K}_k \neq \mathbb{K}_{k+1}$. These reviews the most important results from Snoqit I, that we shall use in this paper.

1.2. **Plan of the paper.** The results of this paper can be shown to hold for arbitrary galois extensions of $\mathbb{Q}$, which contain the p-th roots of unity. The base extensions $\mathbb{K}$ will thus be galois extensions of $\mathbb{Q}$ which contain the p-th roots of unity, and k is the least integer such that $\zeta_{p^k} \in \mathbb{K}$, so $\mathbb{K}_1 = \mathbb{K}_2 = \ldots = \mathbb{K}_k$. We assume that $\mathbb{K}$ enjoys the properties 1.-4. listed above.

For proving the deeper theorems in this general setting, we need an apparatus based on Leopoldt involutions and $\Lambda[\Delta]$-modules, which replaces the action of complex conjugation in ordinary CM fields. This

[2] We defined Λ-cyclic μ-modules as modules $\Lambda a \cong \Lambda/(p^s)$ for $s \geq 1$.

is developed in [8] and will be integrated in a subsequent paper. Here we chose to develop the general results for arbitrary galois extensions, but restrict for the proof of the main conjectures, to CM fields.

The Chapter 2 is a brief introduction containing for future reference some results in arbitrary galois extensions $\mathbb{K}$ as above, and which do not explicitly require complex conjugation. In this section we develop the Kummer theory of cogalois radicals and projective-projective pairings. A short section is related to the extension $\Omega_{E'}/\Omega_E$.

The Chapter 3 is dedicated to the construction of the Iwasawa linear space. The methods and most of the results are inspired from Iwasawa's seminal work [5] and in particular from his construction of the skew symmetric pairing on the *Iwasawa linear space*, which turned out to be the obstruction space to Greenberg's conjecture. In §3.1 we review elements of Takagi theory which play an important role in the sequel, and in §3.2 we show that the module $\mathrm{Gal}(\Omega/\Omega_{E'})$ has property F and contains an important factor X which is a Weierstrass module: this factor is the starting point for the construction of Iwasawa's linear space. As a consequence of property F we have a simple structure for the T and T^* parts of A, namely: $A(T^*) = A[T^*], A(T) = A[T]$ and, moreover, $A[T] \sim \mathbf{B} \oplus A'[T]$, so $A'[T] \cap \mathbf{B}$ is at most finite. The original Conjecture of Gross is then consequence of the elementary Lemma 7. We consider here however the generalized Conjecture of Kuz'min and Gross, which states that $A'[T]$ is finite. In section §3.3 we introduce a simplification of the construction of Iwasawa, which consists in shifting the canonical subextensions of $\Omega/\Omega_{E'}$ to non canonical extensions of $\mathbb{K}_\infty$, by means of their radicals. This method allows to recover the same results in a more transparent way, in small extensions of $\mathbb{K}_\infty$ or $\mathbb{H}_{E'} = \mathbb{H} \cap \Omega_{E'}$.

The Section §3.4 is dedicated to the T and T^* parts of $\mathrm{Gal}(\Omega/\Omega_{E'})$. The fundamental Lemma 5 implies that the Conjectures of Leopoldt and of Gross-Kuz'min are in fact equivalent and indicates the way for a proof of both conjectures, which is given at the end of this section. *The proof can be considered as fixing an error in the proof of Proposition 5 of* [8], *by adding the information provided from the new Lemma 5.* The proof of this Lemma uses Takagi Theory and is not explicitly contained in [5], although it may be understood as a consequence of Iwasawa's Lemma 14, which will be commented in more detail in the paper. Finally, in §3.5 we construct that Iwasawa linear space $A^{(S)}$ for the F-part of A, where F is the largest divisor of the minimal polynomial of A, which is coprime to T and T^*. We also prove the following important consequence:

$$A^{(S)} \neq \{1\} \Rightarrow \mathrm{Gal}(\mathbb{H}_{E'}/\mathbb{K}_\infty) = \mathrm{Gal}(\mathbb{H}_E/\mathbb{K}_\infty)^\dagger, \tag{2}$$

thus $\mathbb{H}_{E'}/\mathbb{K}_\infty$ has finite exponent, if $A^{(S)} \neq 1$.

In Chapter 4 we use the ideas introduced by Thaine in the proof of his celebrated theorem [11] and give a proof of Greenberg's conjecture for CM extensions. Starting from a CM extension $\mathbb{K}$ in which $A^{(S)} \neq \{1\}$, we choose $a \in (A^{(S)})^- \setminus A^p$ and a totally split prime $\mathfrak{Q} \in a_n$. Using Thaine's ideas, this gives raises to a cyclotomic extension $\mathbb{F}/\mathbb{K}$ with its own Iwasawa tower $\mathbb{F}_m = \mathbb{F} \cdot \mathbb{K}_m$. We choose $[\mathbb{F}_n : \mathbb{K}_n] = \mathrm{ord}(a_n)$ and let $\mathfrak{R} \subset \mathbb{F}_m$ be the ramified prime above $\mathfrak{Q}$. Since there is no capitulation in minus parts, $\mathrm{ord}(\mathfrak{R}) = (\mathrm{ord}(a_n))^2$. However, locally, if $(\alpha) = \mathfrak{Q}^{(1-\jmath)\mathrm{ord}(a_n)}$ is such that $\alpha \in U_n(\mathbb{K})^{\mathrm{ord}(a_n)}$ – as predicted by Proposition 4 – then $\alpha \mathcal{O}\mathbb{F}_n = \mathfrak{R}^{\mathrm{ord}(a_n)^2}$, but the local order does not grow. We can now choose a lift $b = (b_m)_{m\in\mathbb{N}} \in A^-(\mathbb{F})$ with $b_n = [\mathfrak{R}]$ and $N_{\mathbb{F}/\mathbb{K}}(b) = a$. We show that $b \notin A^{(S)}(\mathbb{F})$, while $A^{(S)}(\mathbb{F}) \neq \{1\}$, which contradicts Theorem 2. An alternative proof raises a contradiction to some additional facts proved in Proposition 4, in Appendix C. Thus, the Thaine shift reveals an instability of the Iwasawa linear space under shifting to ramified cyclotomic extensions, and it follows that this space must be trivial as predicted by the Greenberg conjecture. The same ideas yields an alternative proof for the Conjecture of Leopoldt.

The major results of this paper end here and the reader interested in a quick entry to the understanding of these proofs may concentrate on Chapters 3 and 4 and the references given there. For the sake of completeness, we have left a series of partial results, which had been proved using elementary methods prior to the completion of §3. These are included in the Appendices A-D. In Appendix A we give a self-contained proof of the fact that $\mathbf{B}^+$ is finite in CM extensions, a fact which follows from Leopoldt's conjecture.

In Appendix B we prove a useful result on *order reversal* in Kummer extensions with galois groups which are elementary parts of Λ-modules. Together with elementary consequences of class fields theory, this leads to an independent proof of the classical Conjecture of Gross. In Appendix C we develop a detailed understanding of the radical shifts for minus parts $B \subset A^-$: in this case the shifts can be defined canonically over $\mathbb{K}_\infty$ and the results in §3 and §4 can be followed in a detailed manner. The main Proposition 4 of this appendix is used for an alternative proof of the Greenberg Conjecture in §4. Finally, Appendix D gives some consequences for the Leopoldt conjecture which depend only on the material developed in the previous appendices.

1.3. **List of symbols.** The general notations from Iwasawa theory which we use here are:

p	A rational prime,
$X^\dagger$	The $\mathbb{Z}_p$ - torsion of the abelian group X ,
X°	The maximal finite submodule of the Λ-module X ,
ζ_{p^n}	Primitive p^n-th roots of unity with $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for all $n > 0$.,
μ_{p^n}	$\{\zeta_{p^n}^k, k \in \mathbb{N}\}$,
$\mathbb{K}$	A galois extension of $\mathbb{Q}$ containing the p^k-th roots of unity
$\mathbb{K}_\infty, \mathbb{K}_n \in$	The cyclotomic $\mathbb{Z} - p$ - extension of $\mathbb{K}$, resp. its n-th intermediate field,
Δ	$\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$,
s	The number of primes above p in $\mathbb{K}$,
Γ	$\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) = \mathbb{Z}_p\tau, \quad \tau$ a topological generator of Γ
$\tilde{\Gamma}$	The universal lift of Γ to $\mathrm{Gal}(\Omega/\mathbb{K}_\infty$ (§3.2)
T	$\tau - 1$,
$*$	Iwasawa's involution on Λ induced by $T^* = (p^{k+1} - T)/(T+1)$,
Λ	$\mathbb{Z}_p[[T]], \quad \Lambda_n = \Lambda/(\omega_n \Lambda)$,
ω_n	$(T+1)^{p^{n-(k+1)}} - 1, \quad (\mathbb{K}_n^\times)^{\omega_n} = \{1\}$,
$N_{m,n}$	$\mathbf{N}_{\mathbb{K}_m/\mathbb{K}_n} = \mathbf{N}_{\mathfrak{K}_m/\mathfrak{K}_n}; \quad N_n = N_{\mathbb{K}_n/\mathbb{K}}$,

E_n	$=$	$\mathcal{O}(\mathbb{K}_n)$,
E_n'	$=$	The p-units of $\mathbb{K}_n \supset E_n$,
$\mathfrak{K}_n$	$=$	$\mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p, \quad \iota_{\mathbb{K}} : \mathbb{K}_n \hookrightarrow \mathfrak{K}_n$,
U_n	$=$	$\mathcal{O}(\mathfrak{K}_n)$,
$A_n = A(\mathbb{K}_n)$		The p - part of the ideal class group of $\mathbb{K}_n$,
A		$\varprojlim A_n$,
$\iota_{n,m}$	$:$	$A_n \rightarrow A_m$: The ideal lift map ,
$A_n' = A'(\mathbb{K}_n)$		The p - part of the ideal class group of the p - integers of $\mathbb{K}_n$,
A'	$=$	$\varprojlim A_n'$,
$\mathcal{D}(\mathbb{K})$	$=$	$\mathbb{Z}$-rk$(E_n) - \mathbb{Z}_p$-rk$(\iota_{\mathbb{K}}(E_n)) =$ The Leopoldt defect of the field $\mathbb{K}$,
$\mathbf{B}$	$=$	$\langle \{ b = (b_n)_{n \in \mathbb{N}} \in A : b_n = [\wp_n], \wp_n \supset (p) \} \rangle_{\mathbb{Z}_p}$,
Ω	$=$	The maximal p - abelian p - ramified extension of $\mathbb{K}_\infty$,
Ω_n'	$=$	The fixed subfield of $\tilde{\Gamma}_n \subset \tilde{\Gamma}$,
Ω_E		$\cup_{n=0}^\infty \mathbb{K}_n[E(\mathbb{K}_n)^{1/p^n}] = \mathbb{K}_\infty[E^{1/p^\infty}]$,
$\Omega_{E'}$		$\cup_{n=0}^\infty \mathbb{K}_n[E'(\mathbb{K}_n)^{1/p^n}] = \mathbb{K}_\infty[E'^{1/p^\infty}]$,
$\mathbb{H}$		The maximal p - abelian unramified extension of $\mathbb{K}_\infty$.

The use of ι both for the diagonal embedding and the ideal lift map is redundant, but confusion is avoided not only by using explicite, different indices, but mostly by the scarce use of the embeddings of $\mathbb{K}_n$ in $\mathfrak{K}_n$ or the individual completions at primes above p. If X is a $\mathbb{Z}_p$-free, finitely generated Λ-torsion module and $f \in \mathbb{Z}_p[T]$, we let

$$\begin{aligned} X[f] &= \{x \in X : fx = 0\}, \\ X(f) &= \{x \in X : f^n x = 0, n \geq 1\} \supseteq X[f] \end{aligned}$$

For X a Noetherian Λ-module, we let $X_\lambda = X/X^\dagger$. In terms of extensions, if $\mathbb{K}_\infty \subset \mathbb{L} \subset \mathbb{M} \subset \Omega$ are such that $\mathbb{L}, \mathbb{M}$ are galois over $\mathbb{K}$ and $X = \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ is a Noetherian Λ-module, then

$$\mathbb{M}_\lambda = \mathbb{M}^{\mathrm{Gal}(\mathbb{M}/\mathbb{L})^\dagger} = \mathbb{M}^{X^\dagger}, \quad \mathrm{Gal}(\mathbb{M}_\lambda/\mathbb{L}) \cong X_\lambda.$$

This is a general construction for removing μ-parts without using the assumption that $\mu = 0$ in our modules. Some notations in Takagi theory, used in §3 are:

$$\begin{aligned} \mathbb{T}_n^{(N)} &= \text{The } p \text{ - part of the ray class field of } \mathbb{K}_n \text{ to the ray } (p^N), \\ \mathbb{T}^{(N)} &= \cup_n \mathbb{T}_n^{(N)} \subset \Omega, \\ \mathbb{T}_n &= \cup_N \mathbb{T}_n^{(N)} = \Omega_n, \\ \mathfrak{X}_n^{(N)} &= \mathrm{Gal}(\mathbb{T}_n^{(N)}/\mathbb{K}_n), \\ \mathfrak{X}^{(N)} &= \mathrm{Gal}(\mathbb{T}^{(N)}/\mathbb{K}_\infty), \\ X &= \mathrm{Gal}(\Omega/\Omega_{E'}), \\ X_\lambda &= \mathrm{Gal}(\Omega_\lambda/\Omega_{E'}) \cong X/X^\dagger, \end{aligned}$$

Except for the groups introduced above, we do not use special notations for galois groups. We use intensively auxiliary constructions on infinite extensions, which consist in taking intersections and fixed subfields. These constructions are mainly related to subfields of Ω and $\mathbb{H}$. Accordingly, the letters Ω and $\mathbb{H}$ endowed with various indices of exponents describe p-abelian extensions of $\mathbb{K}_\infty$ which are p-ramified or unramified. The use of this indices and exponents is consistent and made explicite in the context. The symbols $\mathbb{F}, \mathbb{L}, \mathbb{M}$ are used for ad-hoc extensions and their signification is scope - dependent.

Note that the maximal p-abelian extension of $\mathbb{K}_n$ is $\Omega_n \supset \mathbb{K}_\infty$, while $\Omega'_n \subset \Omega_n$ intersects $\mathbb{K}_\infty$ in $\mathbb{K}_n$. For arbitrary $\mathbb{F} \subset \Omega$, we let then $\mathbb{F}_n = \mathbb{F} \cap \Omega_n$ and $\mathbb{F}'_n = \mathbb{F} \cap \Omega'_n$. Since the universal lift is only defined in §3, the convention above is not used in §2. We sometimes write $E(\mathbb{K}), \Omega(\mathbb{K})$ for E_1, Ω_1, stressing the relation of these groups and fields with the ground field $\mathbb{K}$.

2. Kummer theory of extensions with Λ - modules as galois groups

Let $\mathbb{K}$ be as above and $n_0 = n_0(\mathbb{K})$ be defined with respect to the IW module $A = \varprojlim_n A_n$; we assume also that $n_0 \geq \exp(A^{\dagger})$, the $\mathbb{Z}_p$-torsion submodule of A. Let $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ be a galois extension of $\mathbb{K}$, with $\mathbb{F} = \cup_{n=1}^{\infty} \mathbb{F}_n$, with $\mathbb{F}_n, \underline{\mathbb{F}}_n$ defined above; unlike $\mathbb{F}_n$, the extension $\underline{\mathbb{F}}_n/\mathbb{K}_n$ is in general not a galois extension of $\mathbb{K}$. It is usual to define a Kummer radical of $\mathbb{F}_n$ as the maximal multiplicative subgroup with $\mathbb{K}_n^{\times} \supset \mathrm{rad}(\mathbb{F}_n/\mathbb{K}_n) \supset (\mathbb{K}_n^{\times})^{p^n}$ such that $\mathbb{F}_n = \mathbb{K}_n[\mathrm{rad}(\mathbb{F}_n/\mathbb{K}_n)^{1/p^n}]$. By definition, $(\mathbb{F}_n)_{n \in \mathbb{N}}$ and $(\underline{\mathbb{F}}_n)_{n \in \mathbb{N}}$ are injective sequences.

We shall denote Kummer pairings of an abelian extension $\mathbb{M}/\mathbb{L}$ of exponent N, with $\zeta_N \in \mathbb{L}$, by $\langle ., . \rangle_{\mathbb{M}/\mathbb{L}}$, leaving the indication of the extension out, when it is obvious from the context. In an injective sequence of fields, we write $\langle ., . \rangle_n = \langle ., . \rangle_{\mathbb{F}_n/\mathbb{K}_n}$, and $N = p^n$ in this case. The pairing is given by: $\langle \sigma, b \rangle_{\mathbb{M}/\mathbb{L}} = \sigma(b^{1/N})/b^{1/N}$.

We recall that the pairing is non degenerate and it verifies the fundamental *reflection* identity, which is a consequence of the galois covariance of Kummer pairings:

$$\langle \alpha^x, \nu \rangle_{\mathbb{M}/\mathbb{L}} = \langle \alpha, \nu^{\chi(x) x^{-1}} \rangle_{\mathbb{M}/\mathbb{L}}, \quad \forall x \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}), \tag{3}$$

where $\chi : \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \to \mathbb{Z}/(q \cdot \mathbb{Z})$ is the cyclotomic character. The relation extends to the Leopoldt reflection involution $* : \mathbb{Z}_p[\Delta] \to \mathbb{Z}_p[\Delta]$,

$$\theta = \sum_{\sigma \in \Delta} a_\sigma \sigma \quad \mapsto \quad \theta^* = \sum_{\sigma \in \Delta} a_{\sigma^{-1}} \cdot \chi^{-1}(\sigma) \sigma. \tag{4}$$

If M is a $\Lambda[\Delta]$-module, we denote by $M^{\bullet}$ the module on which the action of $\Lambda[\Delta]$ is twisted by the Leopoldt involution, thus,

$$(\lambda, x) \in (\Lambda[\Delta], M) \mapsto \lambda^* x.$$

Classically (e.g. [9], p 151), the Kummer pairings are defined at infinity by taking projective limits on the galois groups, but injective limits on the radicals. This way, useful isomorphisms are lost, as we shall see below when discussing the radicals built from ideal classes. Therefore we shall give a definition of radicals which allows also projective limits.

2.1. **On p-units.** Let $a = (a_n)_{n \in \mathbb{N}} \in A$ be a sequence of finite order p^m. Then for all $n \geq m$ and all $\mathfrak{A} \in a_n$ we have $\mathfrak{A}^{p^m} = (\alpha)$ for an $\alpha \in \mathbb{K}_n^{\times}$. Moreover, for $N > n$ sufficiently large, the ideal $\mathfrak{A}$ is principal in $\mathbb{K}_N$, so $\mathfrak{A}\mathcal{O}(\mathbb{K}_N) = (\beta)$ and comparing principal ideals we find that $\alpha = e\beta^{p^m}$ for an unit $e \in E_N$. The extension $\mathbb{L}_n = \mathbb{K}_n[\alpha^{1/p^m}]$ is p-ramified by construction and $\mathbb{K}_N \cdot \mathbb{L}_n = \mathbb{K}_N[e^{1/p^m}] \subset \Omega_E$.

Let $\mathbb{H}_{E'} = \mathbb{H} \cap \Omega_{E'} \supseteq \mathbb{H}_E$. We let $e' \in E_n$ be a p-unit, so $e' = e \cdot \prod_{\nu \in C} (\nu \pi_n)^{j(\nu)}$, with $e \in E_n$ and $(\pi_n) = \wp_n^{\text{ord}(\wp_n)}$ a generator of the principal ideal $\wp_n^{\text{ord}(\wp_n)}$; recall that there are s primes above p in $\mathbb{K}$ and they are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. We denoted by C a set of coset representatives of $\Delta/D(\wp)$, for $\wp$ one of these primes; the prime $\wp_n \subset \mathbb{K}_n$ is the ramified prime above $\wp$. Let $s' < s = ess.\ p\text{-rk}(\mathbf{B})$, $\mathbf{b} = (b_n)_{n\in\mathbb{N}} \in \mathbf{B}$ with $b_n = [\wp_n]$ and $C' \subset C$ a subset of cardinality s' such that

$$\mathbf{B}' = \langle \{ \nu \mathbf{b} : \nu \in C' \} \rangle_{\mathbb{Z}_p} \subset \mathbf{B}$$

is a maximal subset of independent classes of infinite order, so $ess.\ p\text{-rk}(\mathbf{B}') = ess.\ p\text{-rk}(\mathbf{B})$. If $s' = 0$, then $C' = \emptyset$ and we are done. Otherwise, for sufficiently large $m > n > 0$ it follows from the property F of the ramified IW module $\mathbf{B}$ that $\text{ord}(\mathbf{b}_m) = p^{m-n}\text{ord}(\mathbf{b}_n)$. Let $\pi_0 \in \mathbb{K}$ with $(\pi_0) = \wp^{\text{ord}(\wp)}$, where $\wp$ can be also a principal ideal: in this case, the sequence $\mathbf{b} \in \mathcal{F}(A)$ is *floating*, in the terminology of Snoqit I. We claim that

$$\Omega_{E'} = \prod_{\nu \in C'} \Omega_E[(\nu\pi_0)^{1/p^\infty}], \tag{5}$$

where $\Omega_E[(\nu\pi_0)^{1/p^\infty}] := \cup_n \Omega_E[(\nu\pi_0)^{1/p^n}]$.

The inclusion $\prod_{\nu \in C'} \Omega_E[(\nu\pi_0)^{1/p^\infty}] \subset \Omega_{E'}$ is obvious from the definition of $\Omega_{E'}$. Conversely, if $\mathbb{L} \subset \Omega_{E'}$ is a non trivial $\mathbb{Z}_p$-extension of Ω_E with $\mathbb{L} = \cup_n \Omega_E[(e'_n)^{1/p^n}]$, the definition of C' implies, for sufficiently large n, that $e'_n = e_n \cdot \pi_n \cdot (\pi'_n)^k$, where $\pi_n \in \langle \nu\pi_0, \nu \in C' \rangle_{\mathbb{Z}}$ and $\pi'_n = \mathfrak{p}_n^{\text{ord}(\mathfrak{p}_n)}$ with $b'_n = [\mathfrak{p}_n] \in \mathbf{B}^\dagger$. But then $\Omega_E[(\pi'_n)^{1/p^n}] = \Omega_E$ by the previous remark on classes of finite order, and it remains that $\mathbb{L} \subset \prod_{\nu \in C'} \Omega_E[(\nu\pi_0)^{1/p^\infty}]$, which confirms the claim.

It can be shown by class field theory that $[\Omega_{E'} \cap (\Omega_E \cdot \mathbb{H}) : \Omega_E] < \infty$, so $\Omega_{E'}/\Omega_E$ is almost completely ramified, and so is

$$\prod_{\nu \in C'} \mathbb{H}_E[(\nu\pi_0)^{1/p^\infty}]/\mathbb{H}_E = \mathbb{H}_{E'}/\mathbb{H}.$$

2.2. **Co-galois radicals and their projective limits.** In this section we consider an alternative definition of Kummer radicals. As a prerequisite, we chose a norm coherent sequence of p^n-th roots of unity $\zeta_{p^n} \in \mathbb{K}_n$ and let $T(W) = \varprojlim_n \langle \zeta_{p^n} \rangle_{\mathbb{Z}}$ be the Tate module associated to the groups of p^n-th roots of unity. We have $Z = (\zeta_{p^n})_{n\in\mathbb{N}} \in T(W)$ as topological generator.

Let $r \geq n_0$ and $\mathbb{L} \subseteq \mathbb{K}_r$ be a finite or infinite extension which is galois over $\mathbb{Q}$ and $\mathbb{M}/\mathbb{L}$ be a (finite) Kummer extension of exponent $q = p^r$ which is galois over $\mathbb{K}$.

We let the **cogalois radical** of $\mathbb{M}/\mathbb{L}$ be

$$\mathcal{R}(\mathbb{M}/\mathbb{L}) = \left(\mathbb{L}^\times\langle(\mathrm{rad}(\mathbb{M}/\mathbb{L}))^{1/q}\rangle\right)/\mathbb{L}^\times \subset \mathbb{L}^\times.$$

This alternative definition of radicals is commonly used in cogalois theory - see also Albu's monograph [1]. We retrieve the Kummer radical via $\mathrm{rad}(\mathbb{M}/\mathbb{L}) = (\mathbb{L}^\times)^q \cdot (\mathcal{R}(\mathbb{M}/\mathbb{L}))^q$. For $x \in \mathcal{R}(\mathbb{M}/\mathbb{L})$ with order $s = \mathrm{ord}(x)$, we find representatives $\overline{x} \in \mathbb{K}^\times$ such that $\overline{x}^{1/s} \equiv x \bmod K^\times$. Note also that the symbol $\overline{x}^{1/s}$ is well defined in $\mathcal{R}(\mathbb{M}\mathbb{L})$, when $s|r$, since $\mu_r \subset \mathbb{L}^\times$.

The Kummer pairing is defined in terms of cogalois radicals by

$$\begin{aligned} \langle .,. \rangle_{\mathbb{M}/\mathbb{L}} \quad &: \quad \mathrm{Gal}(\mathbb{M}/\mathbb{L}) \times \mathcal{R}(\mathbb{M}/\mathbb{L}) \to \mu_{p^r}, \\ (\sigma, x) \quad &\mapsto \quad \sigma(\overline{x}^{1/s})/\overline{x}^{1/s}. \end{aligned}$$

The simplest properties of cogalois radicals are:

Lemma 1. *Let $\mathbb{M}/\mathbb{L}$ be a finite abelian Kummer p - extension with galois group $G = Gal(\mathbb{M}/\mathbb{L})$ and $R = \mathcal{R}(\mathbb{M}/\mathbb{L})$; suppose moreover that there is a subfield $\mathbf{k} \subseteq \mathbb{L}$ such that $\mathbb{M}/\mathbf{k}, \mathbb{L}/\mathbf{k}$ are galois and let $\Delta = Gal(\mathbb{L}/\mathbf{k})$. Then $G \cong R^\bullet$ as $\mathbb{Z}_p[\Delta]$ - modules, where $\bullet$ denotes the action of $\mathbb{Z}_p[\Delta]$ via Leopoldt reflection. Moreover, there is an order reversing map on the lattices of subgroups $l : I(G) \to I(R)$ induced by Kummer duality.*

Proof. The twisted isomorphism of $\mathbb{Z}_p[\Delta]$ modules is a common consequence of Kummer duality - the pairing is not modified by the alternative definition of radicals. The isomorphism of the lattices of subgroups is an expression of the Galois correspondence - see [1], .

If $\mathcal{A} = \{a_1, a_2, \ldots, a_r\} \subset \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ is a p - base (in the sense that $\prod_i a_i^{e_i} = 1$ iff $e_i \equiv 0 \bmod \mathrm{ord}(a_i)$), then there is a *dual base* $\mathcal{B} = \mathcal{A}^\bullet = \{\beta_1, \beta_2, \ldots, \beta_r\} \subset \mathcal{R}(\mathbb{M}/\mathbb{L})$ which is defined as follows: for each i, let $C_i = \langle \mathcal{A} \setminus \{a_i\}\rangle_{\mathbb{Z}}$ be the subgroup generated by all base elements except a_i and $\mathbb{M}_i = \mathbb{M}^{C_i}$, which is a cyclic extension with group $\mathbb{Z}_p a_i$. Let $\beta_i \in \mathcal{R}(\mathbb{M}/\mathbb{L})$ be such that $\mathbb{M}_i = \mathbb{L}[\beta_i]$ and $\langle \beta_i, a_i\rangle_{\mathbb{M}/\mathbb{L}} = \zeta_s$, where $s = \mathrm{ord}(a_i)|q$; by construction we have

$$\langle \beta_i, a_j \rangle = \zeta_q^{e(i,j)}, \quad e(i,j) = \delta_{i,j} \cdot \frac{q}{\mathrm{ord}(a_i)}. \tag{6}$$

□

We let $\mathbb{K}_\infty \subseteq \mathbb{F} \subset \Omega$ be an extension tower with $\mathbb{F}$ galois over $\mathbb{K}$ and $\mathbb{F}/\mathbb{K}_\infty$ an infinite extension, $X = \mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ and $X_n = \mathrm{Gal}(\mathbb{F}_n/\mathbb{K}_n)$. The sequence $(X_n)_{n\in\mathbb{N}}$ forms by definition a norm coherent system, both when X_n are finite and infinite. We define the duals $R_m = \mathcal{R}(\mathbb{F}_m/\mathbb{K}_m)$ as follows.

Suppose first that X_n are finite, $\mathbb{F}_n \cap \mathbb{K}_{n+1} = \mathbb{K}_n$ and there is a $z(X) \in \mathbb{N}$ with $\exp(X_n) \leq p^{n+z}$ for all $n \geq 0$. Then $\mathbb{F}_n \cdot \mathbb{K}_{n+z}$ is a Kummer abelian extension and the radical $\mathcal{R}((\mathbb{F}_n \cdot \mathbb{K}_{n+m})/\mathbb{K}_{n+m})$ is a well defined cogalois radical for all $m \geq z$. In the limit, $\mathcal{R}((\mathbb{F}_n \cdot \mathbb{K}_\infty)/\mathbb{K}_\infty)$ is well defined.

If $\mathbb{K}_\infty \subset \mathbb{F}_n$, the previous definition holds over $\mathbb{K}_\infty$. If in addition X_n are not finite, then we consider the sequence of extensions $\mathbb{L}_m = \mathbb{F}_n \cdot \mathbb{K}_m \cap \underline{\Omega}_m$, which are the maximal Kummer abelian extensions of $\mathbb{K}_m$ contained in the shift $\mathbb{F}_n \cdot \mathbb{K}_m$ for $m > n$. Then

$$R_{n,m} = \mathcal{R}((\mathbb{L}_m \cdot \mathbb{K}_\infty)/\mathbb{K}_\infty) \tag{7}$$

is a well defined sequence of cogalois radicals with $R_{n,m} \subset R_{n,m'}$ for $m' > m$. Thus, we may define $\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n) = \cup_{m \geq n} R_{n,m}$ with $R_{n,m}$ given by (7) and

$$R_n := \cup_{m \geq n} R_{n,m} = \mathcal{R}((\mathbb{F}_n \cdot \mathbb{K}_\infty)/\mathbb{K}_\infty).$$

There is an alternative definition, starting from $\mathbb{F}_n \cdot \mathbb{K}_\infty$: let

$$B_n = \{x \in \mathbb{K}_\infty \cdot \mathbb{F}_n \ : \exists m > 0 : x^{p^m} \in \mathbb{K}_\infty\}. \tag{8}$$

Then B_n is a group and we claim that $\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n) = B_n/(\mathbb{K}_\infty^\times)$. Indeed, if $y \in \mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)$, then there is an $x \in \mathbb{K}_\infty$ and an $m > 0$ such that $y = x^{1/p^m} \cdot (\mathbb{K}_\infty)^\times$, so $x \in B_n$. The converse is also a simple verification. Since $\mathbb{F}/\mathbb{K}$ is galois, for $x \in B_n, y \in \mathbb{K}_\infty$ with $x^{p^m} = y$, we also have $(\tau y)^{1/p^m} \in B_n$ for all the roots τy. Recall that the image $\overline{x} \in \mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)$ does not depend on the choice of a particular root y^{1/p^m}, so the action of τ on $\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)$ is well defined. This makes $\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)$ into a Λ-module.

With this definitions we have both for the finite and infinite case of X_n the same radical definition:

Definition 1 (Cogalois radicals). *Let $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ be an intermediate extension with $\mathbb{F}/\mathbb{K}$ galois and $X = Gal(\mathbb{F}/\mathbb{K}_\infty)$; let $\mathbb{F}_n = \Omega_n \cap \mathbb{F}$ and $X_n = Gal(\mathbb{F}_n/\mathbb{K}_n)$ with $X = \varprojlim_n X_n$. Then we define*

$$\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n) = \mathcal{R}((\mathbb{F}_n \cdot \mathbb{K}_\infty)/\mathbb{K}_\infty) = B_n/(\mathbb{K}_\infty^\times), \tag{9}$$

where the radical in the middle is defined above, using (7) and B_n is given by 8.

If $\mathbb{K}_\infty \subset \mathbb{L} \subset \mathbb{F} \subset \Omega$ is a tower in which both $\mathbb{L}$ and $\mathbb{F}$ are galois over $\mathbb{K}$ and $X = Gal(\mathbb{F}/\mathbb{L})$, we define $\mathcal{R}(\mathbb{F}_n/\mathbb{L}_n)$ in analogy with $\mathcal{R}(\mathbb{F}/\mathbb{K}_\infty)$, replacing $\mathbb{K}_n$ with $\mathbb{L}_n$. If additionally, $\mathbb{L}$ and $\mathbb{F}$ are galois over $\mathbb{Q}$, the radicals are unchanged, but X is a $\Lambda[\Delta]$-module.

The duals $R_m = \mathcal{R}(\mathbb{F}_m/\mathbb{K}_m) \cong X_m^\bullet$ are also Λ-modules, endowed with the Leopoldt-twisted action of Λ. We may thus define a natural projective limit with respect to the twisted norms $N_{m,n}^*$. This can be seen directly as a consequence of duality; also, if $x = R_m^{N^*_{m,n}}$, then $x^{\omega^*_n} = 1$ and by duality, $(\mathrm{Gal}(\mathbb{K}_m[x]/\mathbb{K}_m)^{\omega_n} = 1$, so $\mathbb{K}_m[x]$ is the lift of an extension of $\mathbb{K}_n$. With this, we define $\mathcal{R}(\mathbb{F}/\mathbb{K}_\infty) = \varprojlim_n R_n$. We also need the injective limit $\mathcal{R}_i(\mathbb{F}/\mathbb{K}_\infty) = \varinjlim_n \mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)$: we have in a natural way

$$\mathbb{F} = \cup_n \mathbb{K}_\infty[\mathcal{R}(\mathbb{F}_n/\mathbb{K}_n)] = \mathbb{K}_\infty[\mathcal{R}_i(\mathbb{F}/\mathbb{K}_\infty)],$$

but $\mathbb{K}_\infty[\mathcal{R}(\mathbb{F}/\mathbb{K}_\infty)]$ makes no sense.

We constructed a natural dual R of the group X, which is a projective limit with respect to the twisted norms $N^*_{m,n}$. We have $R_n = N^*_{\infty,n} R = \{x \in \mathcal{R}_i(\mathbb{F}/\mathbb{K}_\infty) \ : \ \omega^*_n x = 1\}$.

Remark 1. *The cogalois radicals are closely related to the definition of Tate and Iwasawa of radicals as submodules of $\mathfrak{K} = \mathbb{K}^\times \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$, [5], § 7. The radicals of subextensions $\mathbb{F} \subset \mathbb{K}_{ab}$, the maximal abelian p-extension of $\mathbb{K}_\infty$ arise there as annihilators, via Kummer pairing, of the subgroup $H \subset Gal(\mathbb{K}_{ab}/\mathbb{K}_\infty)$, fixing $\mathbb{F}$.*

Proposition 1. *Let $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ be a galois extension of $\mathbb{K}$ with $X = Gal(\mathbb{F}/\mathbb{K}_\infty)$ a Weierstrass module and $X_n = Gal((\mathbb{F} \cap \Omega_n)/\mathbb{K}_n)$ finite. Let $R_n = \mathcal{R}(\mathbb{F}_m/\mathbb{K}_m)$ be defined like above; then $(R_n)_{n \in \mathbb{N}}$ form a projective system with respect to the twisted norms $N^*_{m,n}$ and we let $R = \varprojlim_n R_n$. Moreover, the lifts $\iota'_{n,m} : R_n \to R_m$ are also injective.*

$$\langle .,. \rangle_n : Gal((\mathbb{F}_n \cdot \mathbb{K}_{n+z})/\mathbb{K}_{n+z}) \times R_n \to \mu_{p^{n+z}}$$

be the natural Kummer pairings of the abelian Kummer extensions $(\mathbb{K}_{n+z}\mathbb{F}_n)/\mathbb{K}_{n+z}$. Then the system of pairings is compatible with the pairs of maps $(N_{m,n}, N^*_{m+z,n+z})$ and there is a projective projective pairing $\langle .,. \rangle_\infty : X \times R \to T(W)$. The pairing is bilinear, non degenerate and Λ (or even $\Lambda[\Delta]$, if $\mathbb{F}/\mathbb{Q}$ is galois) covariant.

Proof. We have already proved the existence of R. The compatibility follows from the following computation, for $x = (x_n) \in X, r = (r_n) \in R$:

$$\begin{aligned} \langle \iota_{n,m}(x_n), r_m \rangle_m &= \langle \nu_{m,n}(x_m), r_m \rangle_m \\ &= \langle x_m^{p^{m-n}}, r_m \rangle_m \\ &= \left(\langle x_m, r_m \rangle_m\right)^{p^{m-n}} . \end{aligned}$$

The finite level pairings are Kummer and they induce by compatibility a projective - projective pairing in the limit. We shall denote this pairing by $\langle .,. \rangle_{\mathbb{F}} : \mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty) \times \mathcal{R}(\mathbb{F}/\mathbb{K}_\infty) \to T(W)$ □

3. Ray class fields, shifted radicals and Iwasawa's linear space

This paper is strongly inspired by Iwasawa's construction of a skew symmetric pairing on $\mathrm{Gal}(\Omega/\Omega_{E'}) \times \mathrm{Gal}(\Omega/\Omega_{E'})$, [5] §9-11. In this paper we only need the fact that the space on which the pairing is defined, *Iwasawa's linear space* is selfdual. We shall derive this fact in detail in this chapter, together with two fundamental lemmata, which are used in the proofs of the conjectures of Leopoldt and Greenberg.

3.1. **Ray class fields.** Takagi's theory of ray class fields plays a crucial role in Iwasawa's proofs and in our construction.

Let $N > 0$ and consider the p - parts $\mathbb{T}_m^{(N)}$ of the ray class fields of $\mathbb{K}_m$ to the modulus (p^N). Then $\mathbb{H}_m \subset \mathbb{T}_m^{(N)}$. We have injective sequences with to m and N:

$$\mathbb{T}_m^{(N)} \subset T_{m+1}^{(N)} \quad \forall\, m \geq 0 \quad \text{ and } \quad \mathbb{T}_m^{(N)} \subset \mathbb{T}_m^{N+1} \quad \forall N \geq 0.$$

We let $\mathbb{T}_m = \cup_N \mathbb{T}_m^N$; this is by definition the maximal p-ramified p-abelian extension of $\mathbb{K}_m$, so we have $\Omega_m = \mathbb{T}_m$. The galois groups are

$$\mathfrak{X}_m^N = \mathrm{Gal}(\mathbb{T}_m^{(N)}/\mathbb{K}_m), \quad \mathfrak{X}_m = \mathrm{Gal}(\mathbb{T}_m/\mathbb{K}_m) = \mathrm{Gal}(\Omega_m/\mathbb{K}_m).$$

For fixed N we let $\mathbb{T}^N = \cup_m \mathbb{T}_m^{(N)}$ and $\mathfrak{X}^{(N)} = \mathrm{Gal}(\mathbb{T}^{(N)}/\mathbb{K}_\infty)$. Finally,

$$\Omega = \cup_N \mathbb{T}^{(N)} = \cup_m \mathbb{T}_m = \cup_m \Omega_m, \quad \mathfrak{X} = \mathrm{Gal}(\Omega/\mathbb{K}_\infty).$$

We have the projective limits

$$\mathfrak{X}^{(N)} = \varprojlim_m \mathfrak{X}_m^{(N)}, \quad \mathfrak{X}_m = \varprojlim_N \mathfrak{X}_m^{(N)}, \quad \mathfrak{X} = \varprojlim_N \mathfrak{X}^{(N)} = \varprojlim_m \mathfrak{X}_m.$$

We may lift Γ canonically to $\mathrm{Gal}(\Omega_m/\mathbb{K})$ as follows: for fixed N, m, the groups $\mathfrak{Y}_m^{(N)} = \mathrm{Gal}(\mathbb{T}_m^{(N)}/\mathbb{K})$ are finite metabelian groups. Moreover, $\Delta_m = \mathrm{Gal}(\mathbb{K}_m/\mathbb{Q})$ acts on $\mathfrak{Y}_m^{(N)}$ by conjugation, making it into a $\mathbb{Z}_p[\Delta_m]$ - module. We define $\tilde{\Gamma}_m^{(N)} \subset \mathfrak{Y}_m^{(N)}$ as the subgroup annihlated by the augmentation $\mathfrak{A} = \{t \in \mathbb{Z}_p[\Delta_m] : \mathbf{N}_{\mathbb{K}_n,\mathbb{Q}} t = 0\}$. This is a well defined subgroup of p-rank one, and we have the restriction properties

$$\tilde{\Gamma}_m^{(N+1)}|_{\mathbb{T}_m^{(N)}} = \tilde{\Gamma}_m^{(N)}.$$

Therefore, in the projective limit there is subgroup $\tilde{\Gamma}_m \subset \mathfrak{Y}_m$ which lifts Γ canonically to $\mathrm{Gal}(\Omega_m/\mathbb{K})$. It is a priori possible, that the restriction $\tilde{\Gamma}_m|_{\mathbb{K}_\infty} \subsetneq \Gamma_m$. The following argument shows that this is not the case: by Tschebotarew, we may find a prime $\mathfrak{q} \subset \mathbb{K}_m$ such that

$x_{\mathfrak{q}} := \left(\frac{\mathbb{T}_m^{(N)}/\mathbb{K}_m}{\mathfrak{q}}\right) \subset \tilde{\Gamma}_m$ is a generator. But then $x_{\mathfrak{q}}|_{\mathbb{K}_\infty}$ fixed $\mathbb{K}_m$, which confirms the claim.

With this we may define for all m the field $\Omega'_m = \Omega_m^{(\tilde{\Gamma})_m^{p^{m-k}}}$; here k is the largest integer with $\zeta_{p^k} \in \mathbb{K}$, so $\Gamma^{p^{m-k}}$ fixes $\mathbb{K}_m$ and, of course, we assume $m \geq k$. Then Ω'_m is a canonical abelian subextension of $\Omega_m/\mathbb{K}_m$ which does not contain $\mathbb{K}_{m+1}$ and $\mathrm{Gal}(\Omega'_m/\mathbb{K})$ is fixed by Γ_m and ω_m in $\mathrm{Gal}(\Omega/\mathbb{K})$.

We also have upwards compatibility:

$$\tilde{\Gamma}_{m+1}|_{\Omega_m} = \tilde{\Gamma}_m,$$

and thus we may define a universal lift $\tilde{\Gamma} = \varprojlim_m \tilde{\Gamma}_m \in \mathrm{Gal}(\Omega/\mathbb{K})$. From now on, any lift of Γ to a subextension of $\mathbb{K}_\infty \subset \mathbb{F} \subset \Omega$ will be understood as a restriction $\tilde{\Gamma}|_{\mathbb{F}}$.

We shall use the following expression for the "principal ideal theorem" of Takagi theory:

Lemma 2. *Let $I \subset \mathbb{K}_m$ be an ideal and*

$$x_N = \left(\frac{\mathbb{T}_m^{(N)}/\mathbb{K}_m}{I}\right) \in \mathfrak{X}_m^{(N)}, \quad x = \varprojlim_N x_N \in \mathfrak{X}_m.$$

Then

$$x_N = 1 \Leftrightarrow I = (\gamma) \quad \textit{and there is a } e_N \in E_n \textit{ such that} \quad e_N\gamma \equiv 1 \bmod p^N\mathcal{O}(\mathbb{K}_m), \tag{10}$$

$$x = 1 \Leftrightarrow I = (\gamma) \quad \textit{and} \quad 1 \in \gamma \cdot \overline{E}_n. \tag{11}$$

Proof. The statement (10) is the usual formulation of the Principal Ideal Theorem of ray class fields. For (11), consider the diagonal embeddings $\gamma e_N \hookrightarrow \mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Then $\lim_{N\to\infty} \gamma e_N = 1$ and since $e := \lim_{N\to\infty} e_N \in \overline{E}_n$, it follows that $1 = \gamma e \in \gamma\overline{E}_n$, as claimed. □

3.2. **Property F.** Let $X = \mathrm{Gal}(\Omega/\Omega_{E'})$ and $\Omega_\lambda = \Omega^{X^{circ}}$, $X_\lambda = X/X^\dagger = \mathrm{Gal}(\Omega_\lambda/\Omega_{E'})$. Iwasawa constructs a skew symmetric pairing on X_λ and shows that this space is selfdual with respect to this pairing. Our construction will be simplified by *shifting* the base field from Ω'_E to $\mathbb{K}_\infty$, by means of radicals. Unlike the classical, this construction is not canonical; however it is precisely the fact of being non canonical, while preserving canonical subparts, that will bring an important new insight: when $X_\lambda \cap \mathrm{Gal}((\mathbb{H} \cdot \Omega_{E'})/\Omega_{E'}) \neq \{1\}$, then $\mathbb{H}_{E'}/\mathbb{K}_\infty$ has finite exponent. We shall define the Iwasawa linear space as a submodule of A' rather then a galois group. The following fact about X will be useful below:

Lemma 3. *The galois group $X = Gal(\Omega/\Omega_{E'})$ has property F. Letting $X_\lambda = X/X^\dagger$, for $X \in \{A, A', \mathbf{B}\}$, there is a direct sum decomposition*

$$X_\lambda = X_\lambda[T] \oplus X_\lambda(F'), \tag{12}$$

where F' is the maximal divisor of the minimal polynomial $G_X(T)$, which is coprime to T. This induces $\Omega_\lambda = \Omega_T \cdot \Omega_{F'}, \Omega_T \cap \Omega_{F'} = \Omega_{E'}$. Moreover, $A'/(A')^\circ$ has property F with respect to the twisted action of Λ and in particular $A(T^*) = A[T^*]$. For A we have:

$$A_\lambda[T] = \mathbf{B}_\lambda[T] \oplus A'_\lambda[T],$$

and

$$A'_\lambda = A'[T] \oplus A[T^*] \oplus A(F), \tag{13}$$

where $F|F'$ is the maximal factor which is coprime to T^*.

Proof. It is known (e.g. [5], §9) that $\mathrm{Gal}(\Omega/\Omega_{E'})$ is a Λ-torsion module without finite $\mathbb{Z}_p$-torsion and $\mathcal{R}(\Omega/\Omega_{E'}) \hookrightarrow A'$. Moreover $X[T] = \mathrm{Gal}((\Omega_1 \cdot \Omega_{E'})/\Omega_{E'})$. It is a known fact, which we shall prove for completeness in the Appendix below, that

$$\mathbb{Z}_p\text{-rk}(\mathrm{Gal}((\Omega_1 \cap \Omega_{E'})/\mathbb{K}_\infty)) = r_2,$$

and $X[T] \neq \{1\}$ iff the Leopoldt conjecture is false for $\mathbb{K}$.

Having defined a lifts $\tilde{\Gamma}$ of Γ above, the proof of Property F for X follows the same steps as Iwasawa's for the fact that $\mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty)$ has property F. See for instance the Appendix of Snoqit 1 or the proofs of Iwasawa's theorem to which we referred there.

The fact 1 has now important consequences for X_λ, which is a p-maximal submodule of X, and thus inherits the property F: thus X_λ is a Weierstrass module. The decomposition (12) follows from this fact, and letting $\Omega_T = \Omega_\lambda^{X_\lambda(F')}$ and $\Omega_{F'} = \Omega_\lambda^{X_\lambda[T]}$ we obtain the disjoint decomposition of Ω_λ over $\Omega_{E'}$.

Moreover, the radicals inherit by duality the property F with respect to the twisted action of Λ. Since $A(T^*) = A'(T^*)$ it follows from the same fact, that $A(T^*) = A[T^*]$. Finally, both A and A' have property F, so A_λ, A'_λ are Weierstrass modules. In particular, it follows that for $a \in A'[T]$ we have $a^T = 1$; from the definition we might also have $a^T = b \in \mathbf{B}$, but this would imply $A(T) \supsetneq A[T]$ in contradiction with Fact 1. This implies the decomposition of $A_\lambda[T]$. Since A' has both $A[T^*]$ and $A'[T]$ as direct terms, and $A(T^*) = A[T^*]$, the decomposition 13 follows. □

Note that $\mathfrak{X} = \mathrm{Gal}(\Omega/\mathbb{K}_\infty)$ is too large for having property F: it contains a free Λ-submodule of rank r_2, so in particular $\mathfrak{X}(T)$ has infinite height, an incompatibility with property F.

3.3. **Radical shifts.** There is a map $\rho_1 : A'_n \to \mathcal{R}((\Omega_n \cdot \Omega_{E'})/\Omega_{E'})$ which is constructed as follows: let $\mathfrak{A} \in a_n \in A'_n, \alpha \in \mathbb{K}_n^\times$ be such that

$$\begin{aligned} \mathfrak{A} &\in a_n \in A'_n, \alpha \in \mathbb{K}_\infty^\times : \quad (\alpha) = \mathfrak{A}^{\mathrm{ord}(a_n)}, \\ \rho_1(a_n) &= \Omega_{E'} \cdot \alpha^{1/\mathrm{ord}(a_n)}. \end{aligned} \tag{14}$$

Then one verifies that $\rho_1 : A'_n \to \mathcal{R}(\Omega_n/\Omega_{E'})$ is an injective map and passing to projective limits we obtain a map $\rho_1 : A' \hookrightarrow \mathcal{R}(\Omega/\Omega_{E'})$. The kernel consists of the maximal finite submodule $\mathrm{Ker}\ (\rho_1) = (A')^\circ$. We see already from the previous steps, that one has to take composita of all relevant base fields with $\Omega_{E'}$ in order to follow the canonical construction. It would be therefore be helpful to perform the same construction over the base fields $\mathbb{K}_n$ or $\mathbb{K}_\infty$.

Observe that the roots $\alpha^{1/\mathrm{ord}(a_n)}$ define the radical canonically over $\Omega_{E'}$, yet they are meaningful expressions over $\mathbb{K}_\infty$ too. This leads to idea of *shifting radicals* down to $\mathbb{K}_\infty$. When doing this, canonicity is lost and one has to find a definition which conserves the norm coherence of radicals and is compatible with ramification properties[3]. Since $\mathrm{Ker}\ (\rho_1) = (A')^\circ$, it suffices to define a map $\rho_0 : A'/(A')^\circ \to \mathcal{R}(\Omega/\mathbb{K}_\infty)$ which is injective. Consider $a = (a_n)_{n\in\mathbb{N}} \in A'$ with non trivial image in $A'/(A')^\circ$, so $\iota_{n,n+1}\Lambda a_n \to \Lambda a_{n+1}$ is injective for $n > 0$.

We shall define a radical map $\rho_0 : A'_m \to \mathcal{R}(\Omega_m/\mathbb{K}_\infty)$ for all $m > 0$. For any $a_n \in A_n$ we let $\alpha(a_n) \in \mathbb{K}_\infty^\times$ be chosen by the procedure in (14); as additional condition, we assume that the degree

$$\left[\mathbb{K}_\infty[\alpha(a_n)^{1/\mathrm{ord}(a_n)}] \cap \mathbb{H} \ : \ \mathbb{K}_\infty\right] \tag{15}$$

is maximal among all possible choice for α. This describes a procedure which associates to $a_n \in A_n$ an $\alpha(a_n) \in \mathbb{K}_n^\times$ such that the degree in (15) is maximal. We still have to make some choices for obtaining a norm coherent map $\rho_0 : A' \hookrightarrow \mathcal{R}(\Omega/\mathbb{K}_\infty)$. The map will be defined first on A'_n so the different levels are norm compatible for sufficiently large n. We let first $\rho_0(A^\circ) = 1$, so the kernel is conserved from ρ_1. In particular for all $a = (a_n)_{n\in\mathbb{N}} \in A^\circ$ and all n we have $\rho_0(a_n) = 1$.

Consider now the μ-part. The extension Ω/Ω_λ has a pure μ-module as galois group. There is thus a maximal μ-module $R_\mu \subset \mathcal{R}(\Omega/\Omega_{E'})$; we let

$$A'_\mu = \rho_1^{-1}(R_\mu) \cdot (A')^\circ \subset A'.$$

Let $a \in A'_\mu$ be an element of a minimal set of generators of A'_μ as a Λ-module and $q = p^r = \mathrm{ord}(a)$. For $n > \max(r, n_0)$, we may choose $\alpha(a_n)$ as above and define $\rho_0(a_n) = \alpha(a_n) \cdot \mathbb{K}_\infty$. The choice of $\alpha(a_n)$ is

[3] In CM fields there is canonic shift of $\mathrm{Gal}(\Omega^-/\Omega_{E'})$ down to $\mathbb{K}_\infty$. This is developed in the Appendix

up to p - units, so the extension is not unique. However, if $\mathfrak{B} \in a_n$ is an other ideal, then $\mathfrak{B} = \mathfrak{A} \cdot (\nu)$ and thus $\mathfrak{B}^{\mathrm{ord}(a_n)} = (\alpha_n) \cdot (\nu^{\mathrm{ord}(a_n)})$, so $\alpha(a_n) \cdot \nu^{\mathrm{ord}(a_n)}$ is a valid representative for the ideal $\mathfrak{B}$, which generates the same extension as $\alpha(a_n)$. The choice thus depends only on p - units but not on the particular ideal $\mathfrak{A} \in a_n$. The map is then extended by multiplicativity and galois covariance to $(A'_{mu})_n$. We have the following "onto" property: $\Omega_{E'}[\rho_0((A'_{mu})_n)] = \Omega_{m,\mu} \cdot \Omega_{E'}$.

Let now $A'_\lambda \subset A'$ be a set of representatives for $A'/(A')^\dagger \cong \mathcal{R}(\Omega_\lambda/\Omega_{E'})^\bullet$. Starting from a minimal set of generators for $A'/(A')^\dagger$, we define like in the μ-case, the map ρ_0 on $(A'_\lambda)_n$. We need to be more careful in this case with numeration. The extension $\Omega_{F,n}/\Omega_{E'}$ is finite and its exponent is at most $p^{n+z'(A)}$, where z' is a constant of the dual module $X_\lambda^\bullet$ in Lemma 3. Therefore, we have for all $n \geq 0$:

$$\Omega_{E'}[\rho_0((A'_\lambda)_{n+z'})] \supseteq \Omega_{n,F} \cdot \Omega_{E'}.$$

The extension $\Omega_T/\Omega_{E'}$ is infinite and cannot be generated by final radicals. Instead, the maximal Kummer subextension $\Omega_{T,n}/\Omega_{E'}$ of exponent $p^{n+z'}$ contained in the radical extension above.

We now show that for any $m > n$ we may choose $\alpha(a_m) \in \mathbb{K}_\infty^\times$ to represent a_m in such a way that

$$\mathbb{K}_\infty[\alpha(a_n)^{1/\mathrm{ord}(a_n)}] \subset (\mathbb{K}_\infty[\alpha(a_m)^{1/\mathrm{ord}(a_m)}])^{(n)}, \tag{16}$$

the last being the normal closure of $\mathbb{K}_\infty[\alpha_m^{1/\mathrm{ord}(a_m)}]$ over $\mathbb{K}_0$. We assume first that a has infinite order. In this case, the last condition is equivalent to $\alpha(a_m) = \alpha(a_n)^c \cdot x^{\mathrm{ord}(a_n)}, (c,p) = 1$. Let $\mathfrak{Q} \in a_m$ be a totally split prime and $\mathfrak{R} = N_{m,n}\mathfrak{Q} \in a_n$. From property F we have $[\nu_{m,n}\mathfrak{Q}] = a_m^{p^{m-n}}$; let $\mathfrak{A} = \mathfrak{R} \cdot (\nu)$ and $\alpha(a_m) \in \mathbb{K}_\infty^\times$ with $(\alpha(a_m) = \mathfrak{Q}^{\mathrm{ord}(a_m)}$ have the local maximality property required above. Then

$$(\alpha(a_m) = \left(\mathfrak{Q}^{p^{m-n}}\right)^{\mathrm{ord}(a_n)} = (\mathcal{O}(\mathbb{K}_{m+z}) \cdot \mathfrak{R})^{\mathrm{ord}(a_n)} \, (\alpha(a_n)\nu^{\mathrm{ord}(a_n)}).$$

It follows that the condition $\alpha(a_m) = \alpha(a_n)x^{\mathrm{ord}(a_n)}$ can be fulfilled for an adequate choice of $\alpha(a_m)$ modulo p - units in $E'_{m+z} \cap U_{n+z}^{\mathrm{ord}(a_n)}$, so (16) holds. We may choose $\rho_0(a_m) = \mathbb{K}_\infty^\times \cdot \alpha_m^{1/\mathrm{ord}(a_m)}$ and $\rho_0(a_k) = \mathbb{K}_\infty^\times \cdot N_{m,k}(\alpha_m)^{1/\mathrm{ord}(a_m)} = \mathbb{K}_\infty^\times \cdot \alpha_k^{1/\mathrm{ord}(a_k)}$ for $0 \leq k < m$. By continuing the procedure iteratively, we obtain a map $\rho_0(a) \in \mathcal{R}(\Omega/\mathbb{K}_\infty)$. We shall also need the injective limit for a describing infinite extensions, so we let $\rho'(a) = \cup_m \rho_0(\Lambda a_m)$.

Suppose now that a has finite order p^s and $\exp(\Lambda a_m) = p^s$ for all $m \geq 0$. Choosing $\mathfrak{Q} \in a_m$ like before, we have $\mathrm{ord}(\mathfrak{Q}) = \mathrm{ord}(\mathfrak{R}) = p^s$.

One can prove like above that there is a choice of $\alpha(a_m) \in \mathbb{K}_m^\times$ such that $(\alpha(a_m) = \mathfrak{Q}^{p^s}$ and (16) holds.

Let $\Omega_A = \mathbb{K}_\infty[\rho_0'(A')] \subset \Omega$, a non canonic extension of $\mathbb{K}_\infty$ with $\Omega_A \cap \Omega_{E'} = \mathbb{K}_\infty$ and $\Omega = \Omega_A \cdot \Omega_{E'} = \Omega_{E'}[\rho_0'(A')]$. Indeed, by construction, both conditions $\Omega_A \cap \Omega_{E'} = \mathbb{K}_\infty$ and $\Omega_A \cdot \Omega_{E'} = \Omega$ are fulfilled. Let $\mathbb{H}_A = \mathbb{H} \cap \Omega_A, \mathbb{H}_{A,\lambda} = \mathbb{H}_A \cap \mathbb{H}_\lambda$. We also have an induced definition for $\Omega_{A,F}, \Omega_{A,T}$ and the unramified subextensions $\mathbb{H}_{A,F}, \mathbb{H}_{A,T}$. Moreover, $\Omega_{A,\mu} = \mathbb{K}_\infty[\rho_0((A')^\dagger)]$ and $\mathbb{H}_{A,\mu} = \Omega_{A,\mu} \cap \mathbb{H}$. We consider canonical submodules of A':

Lemma/Definition 1. *The subgroup $A_G \subset A_\lambda$ fixing $\mathbb{H}_{E',\lambda}$ in $\mathbb{H}_\lambda$ is a canonical Λ-submodule. The module*

$$A_L := \{a \in A'_\lambda \ : \ \mathbb{H}_E[\rho_0'(a)] \subset \mathbb{H}\} \subset A'_\lambda = A'/(A')^\dagger$$

does not depend on the choice of the lift ρ_0.

We define a function $\ell : A' \to \mathbb{N}$ as follows: for $a \in A'$, $\ell(a) = \infty$ if $a \in A_L$ and $\ell(a) = [\mathbb{H}_{E'}[\rho_0'(a)] \cap \mathbb{H} : \mathbb{H}_{E'}]$ otherwise: this map is well defined and for $\ell(a)+\ell(b) = \infty$ we have $\ell(ab) = \infty$ iff $\ell(a) = \ell(b) = \infty$. For $a_n \in A'_n$ we also let $\ell(a_n) = [\mathbb{K}_\infty[\rho_0(a_n)] \cap \mathbb{H} : \mathbb{K}_\infty]$.

Proof. We explain here the facts from the definition that require a proof. Since $\mathbb{H}_{E'} \subset \mathbb{H}$ is a canonical subfield, its fixing group is a canonical Λ-submodule. We shall prove later that $A_G \subset A'$. Since

$$\mathbb{H}_\lambda = \Omega_\lambda \cap \mathbb{H} = \Omega_{E'}[\rho_0(A'_\lambda] \cap \mathbb{H} = \mathbb{H}_{E'}[\rho_0(A'_\lambda)] \cap \mathbb{H}$$

for all choices of ρ_0 and since the maximality of the degree (15) holds for all these choices, it follows that there is a maximal $A_L \subset A'$ such that $\mathbb{H} = \mathbb{H}_{E'}[\rho_0(A_L)]$ for all ρ_0. Thus A_L is well defined. The multiplicativity rule for ℓ follows from the fact that $\mathbb{H}_{E'}[\rho_0'(ab)]$ is totally unramified iff both $\mathbb{H}_{E'}[\rho'(a)]$ and $\mathbb{H}_{E'}[\rho_0'(b)]$ are totally unramified. □

From the previous construction we have the following result on shifted radicals:

Lemma 4. *Notations being like above, there is a non canonical map $\rho_0 : A' \to \mathcal{R}(\Omega/\mathbb{K}_\infty)$ such that*

1. *For any choice of ρ_0 we have $\Omega = \Omega_{E'}[\rho_0'(A')]$ and $\mathbb{H} = \mathbb{H}_{E'}[\rho_0'(A_L)]$.*
2. *The extension $\Omega_A := \mathbb{K}_\infty[\rho_0(A')]$ verifies $\Omega_A \cdot \Omega_{E'} = \Omega$ while $\Omega_A \cap \Omega_{E'} = \mathbb{K}_\infty$. However Ω_A depends on the choice of ρ_0.*

If $a \in A'$ has infinite order, we may write $\mathbb{K}_\infty[a^{1/p^\infty}] = \mathbb{K}_\infty[\rho_0'(a)]$ for a fixed shift and $\mathbb{H}_{E'}[a^{1/p^\infty}] = \mathbb{H}_{E'}[\rho_0'(a)]$ canonically.

We shall consider in more detail the extension $\Omega_{A,\lambda} = \Omega_{A,F} \cdot \Omega_{A,T}$. The purpose of this section is to prove that there is a canonical module

$A^{(S)} \subset A'$ such that $A_G = A_L = A^{(S)} \cdot A^{\dagger}$. This is the Iwasawa linear space.

3.4. **The T and T^* parts and their conjectures.** According to the distinction in property F, the case of the T and T^* parts, which are dual as radicals and galois groups, require a separate treatment. The first result on the T-part is crucial both for the construction of the Iwasawa space and for the proof of Leopoldt's conjecture.

Lemma 5. *Let $\mathcal{D}(\mathbb{K}) = \mathbb{Z}\text{-}rk(E(\mathbb{K})) - \mathbb{Z}_p\text{-}rk(\overline{E}(\mathbb{K}))$ be the Leopoldt defect of $\mathbb{K}$. Then*

$$\mathbb{Z}_p\text{-}rk(\mathcal{R}(\Omega_{A,T}/\mathbb{K}_\infty)) = \mathcal{D}(\mathbb{K}) = ess.\ p\text{-}rk(A(T^*)).$$

Moreover $\mathbb{K}_\infty[\rho_0'(A[T^*])] \subset \mathbb{H}$ for all ρ_0.

Proof. Since $\mathbb{Z}_p$-rk$(\mathrm{Gal}(\Omega_E \cap \Omega(\mathbb{K}))/\mathbb{K}_\infty) = r_2$ and, by class field theory (e.g. [9], p. 144), $\mathbb{Z}_p$-rk$(\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)) = r_2 + \mathcal{D}(\mathbb{K})$ (recall that $\mathbb{K}$ is galois and contains ζ_p, so $r_1 = 0$ and $r = 2r_2$), it follows that

$$\mathbb{Z}_p\text{-rk}(X[T]) = \mathbb{Z}_p\text{-rk}(A[T^*]) = \mathbb{Z}_p\text{-rk}(\mathrm{Gal}((\Omega_1 \cap \mathbb{H})/\mathbb{K}_\infty)) = \mathcal{D}(\mathbb{K}).$$

Suppose that there is a $\mathbb{Z}_p$-extension $\mathbb{L}/\mathbb{K}_\infty$ with $\mathbb{L} \subset \Omega(\mathbb{K}) = \Omega_1$ but $[\mathbb{L} \cap \mathbb{H} : \mathbb{K}_\infty] = p^s < \infty$; in this case we have $\mathbb{L} \subset \mathbb{K}_\infty[\rho_0'(A[T^*])]$ for a radical lift ρ_0'. Let $\mathbb{M} = \mathbb{H} \cap \mathbb{L}$ and $\mathbb{M}_n, \mathbb{L}_n \subset \Omega_n'$ be the extensions of $\mathbb{K}_n$ which are the fixed fields of $\mathbb{M}, \mathbb{L}$ under the universal lift $\tilde{\Gamma}_n$. Then $\mathbb{M}_n \subset \mathbb{L}_n$ and $[\mathbb{M}_n : \mathbb{K}_n] = p^s$ for sufficiently large n; by adequate choice of the ground field, we may assume that this holds already for $n = 1$.

Let now $\mathbb{T}_n^{(N)}$ be the ray class field defined above and assume that N is such that $\mathbb{M}_n \subsetneq \mathbb{L}_n \cap \mathbb{T}_n^{(N)}$. We choose $x_N \in \mathfrak{X}_n^{(N)}[T] = \mathrm{Gal}(\mathbb{T}_n^{(N)}/\mathbb{K}_n)[T]$ which fixes $\mathbb{H}_n$ and generates $\mathrm{Gal}(\mathbb{L}_n \cap \mathbb{M}_n)$; we can choose $x_{N+1} \in \mathfrak{X}_n^{(N+1)}$ such that $x_{N+1}|_{\mathbb{T}_n^{(N)}} = x_N$ and obtain a projective sequence with $x = \varprojlim_N x_N \in \mathfrak{X}_n$. The choice of x_N is possible, since $\mathrm{Gal}(\mathbb{H}_n/\mathbb{K}_n)$ is finite, while $\mathfrak{X}_n^{(N)}$ becomes arbitrarily large with increasing N. By Tchebotarew's Theorem, there is a prime $\mathfrak{q} \subset \mathcal{O}(\mathbb{K}_n)$ which is totally split in $\mathbb{K}_n/\mathbb{Q}$ and coprime to p, such that $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}}\right) = x_N$. Let $\mathfrak{q}_1 = N_{n,1}(\mathfrak{q})$ be the prime of $\mathbb{K}$ below $\mathfrak{q}$. Then the action of x_N by restriction to $\mathbb{L}_1$ implies for all N that

$$\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}}\right)\Bigg|_{\mathbb{L}_1} = \left(\frac{(\mathbb{L}_1 \cap \mathbb{T}_1^{(N)})/\mathbb{M}_1}{\mathfrak{q}_1}\right),$$

and in the limit with respect to N, it follows that $\mathfrak{q}_1$ is inert in $\mathbb{L}_1/\mathbb{M}_1$. We shall raise below a contradiction to this fact, which shows that $\mathbb{L} \subset \mathbb{H}$.

By choice of x_N, the prime $\mathfrak{q}$ fixes $\mathbb{H}$, so it must be principal: $\mathfrak{q} = (\gamma), \gamma \in \mathcal{O}(\mathbb{K})$. We have chosen $x_N \in \mathfrak{X}_n^{(N)}[T]$; thus $x_N^T = 1$ and consequently $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}^T}\right) = 1$. The Lemma 2 implies that $1 \in \gamma^T \cdot \overline{E}_n$, so $\gamma^T \in \overline{E}_n$. It follows that $\gamma = c \cdot e$ with $c \in U(\mathbb{K}), e \in \overline{E}_n$. But then $\gamma_1 = N_{n,1}(\gamma) = c^{p^{n-k}} \cdot N_{n,1}(e)$. We can choose n arbitrarily large, so we may find a generator $\gamma_1' = \gamma_1 e_1$ of the ideal $\mathfrak{q}_1$ with $e_1 \in E$ and such that $\gamma_1' \equiv 1 \bmod p^N$, for $N > M + 1$, where M is the largest integer such that $\mathbb{T}_1^{(M)} \subset \mathbb{H}_1$. Then $y_1 = \left(\frac{\mathbb{L}_1/\mathbb{K}}{\mathfrak{q}_1}\right)$ fixes $\mathbb{L}_1 \cap \mathbb{T}_1^{(N)} \supsetneq \mathbb{M}_1$. Since $\mathbb{L}_1 \cap \mathbb{T}_1^{(N)} \supsetneq \mathbb{M}_1$, this contradicts the fact that $\mathfrak{q}_1$ is inert in $\mathbb{L}_1/\mathbb{M}_1$ established above. The contradiction implies that $\mathbb{L} \subset \mathbb{H}$, as claimed.

We still have to show that for n sufficiently large, $c^{p^{n-k}} \equiv 1 \bmod p^N$ for a fixed N. We prove this fact locally for every completion. Let thus $c' \in \mathbb{K}_\wp$ be the image of c in the completion at a prime of $\mathbb{K}$ above p and let $\pi \in \mathbb{K}_\wp$ be a uniformizor and $e(\mathbb{K})$ be the ramification index of p in $\mathbb{K}$ and thus in $\mathbb{K}_\wp$. We may assume that $v_p(c' - 1) > 0$ – otherwise one can raise γ to a power coprime to p. Then $c' = 1 + d\pi, d \in \mathbb{K}_\wp$ and for $m > 0$,

$$(c')^{p^m} = (1 + d\pi)^{p^m} = 1 + \sum_{i=1}^{p^m} \binom{p^m}{i} \pi^i.$$

From the divisibility of the binomial coefficients by powers of p, we see that for $e(\mathbb{K}) > 1$ we have $\min v_p \left(\binom{p^m}{i} \pi^i\right) = v_p(\pi^{p^m}) = p^m/e(\mathbb{K})$. For $e(\mathbb{K}) = 1$, the minimum is p^m; in both cases it diverges with $m \to \infty$ and thus, for sufficiently large n we may achieve that $(\gamma' - 1) \in p^N U(\mathbb{K}_\wp$ for all primes $\mathbb{K} \supset \wp \supset (p)$. We have chosen $\gamma' = \gamma_1 \cdot e, e \in \overline{E}(\mathbb{K})$, so $e = \lim_{m\to\infty} e_m, e_m \in E(\mathbb{K})$. The sequence converges, so for m sufficiently large, $e_m \gamma_1 \equiv 1 \bmod p^N$ in all completions; therefore, the same holds globally. Thus $\mathbb{L} \subset \mathbb{H}$, and this completes the proof. □

The result above calls for an investigation of the classes in $A[T]$ which build the galois group $\mathrm{Gal}(\mathbb{K}_\infty[\rho'(A[T^*])]/\mathbb{K}_\infty)$. We show that these classes do not generate unramified extensions:

Lemma 6. *Let $a = (a_n)_{n\in\mathbb{N}} \in A[T]$ be such that $\varphi(a)|_{\mathbb{H}_{E'}} = 1$. Then $\ell(a) < \infty$ and $\ell(a_n) = c$ for all n sufficiently large.*

Proof. Let $A_\lambda = A/A^\dagger = A[T^*] \oplus A(F^*) = A[T] \oplus A(F)$ by Lemma 3. There is a canonic field $\mathbb{H}_{E'} \subseteq \mathbb{H}_T \subset \mathbb{H}_\lambda$ which is fixed by the restriction of $A(F)$ to $\mathbb{H}_\lambda$. Then $\mathrm{Gal}(\mathbb{H}_T/\mathbb{H}_{E'}) \hookrightarrow A[T])$ and $\mathcal{R}(\mathbb{H}_T/\mathbb{H}_{E'}) =$

$\rho'_0(A[T^*]) \cdot \mathbb{H}_{E'}^{\times}$. From Lemma 5, it follows that

$$\begin{aligned} \mathbb{Z}_p\text{-rk}(\mathrm{Gal}(\mathbb{H}_T/\mathbb{H}_{E'})) &= \mathbb{Z}_p\text{-rk}(\mathcal{R}(\mathbb{H}_T/\mathbb{H}_{E'})) \\ &= \mathbb{Z}_p\text{-rk}(A[T^*]) = \mathcal{D}(\mathbb{K}). \end{aligned} \tag{17}$$

Let $a \in A[T]$ with $\varphi(a)|_{\mathrm{Gal}(\mathbb{H}_T/\mathbb{H}_{E'})} \neq 1$ and fix $n > 0$. By the choice of the base field given in the introduction, the class lift map $\iota_{n,n+1}$ is injective on $\Lambda a = \mathbb{Z}_p a$ for all $n \geq 0$. Note the identity in the group ring: $N_{n,1} = p^{n-k} + Tw, w \in \mathbb{Z}[T]$.

Let $\mathfrak{Q} \in a_n$ be a totally split prime above $\mathbb{Q}$ which is coprime to p. Then $\mathfrak{Q}^T = (\nu)$ is principal and $N_{n,1}(\nu) \in E(\mathbb{K})$. Let

$$\mathfrak{q} = N_{n,1}(\mathfrak{Q}) = \mathfrak{Q}^{p^{n-k}} \cdot (\nu^w).$$

Raising this identity to the power $q := \mathrm{ord}(a_n)/p^{n-k} = \mathrm{ord}(a_1)$, an equality which follows from the stability of the transitions in Λa, we find

$$(\alpha_1) = \mathfrak{q}^{\mathrm{ord}(a_1)} = \mathfrak{Q}^{\mathrm{ord}(a_n)} \cdot (\nu^{qw}).$$

If $(\alpha_n) = \mathfrak{Q}^{\mathrm{ord}(a_n)}$, the previous identity yields

$$\delta\alpha_n = \alpha_1 \cdot \nu^{-qw}, \quad \delta \in E_n. \tag{18}$$

Let now $N > 0$ be fixed and $x = (x_n)_{n\in\mathbb{N}} \in \mathfrak{X}^{(N)}[T]$ be a lift of $\varphi(a)$ and assume additionally that $\mathfrak{Q}$ was chosen by Tchebotarew's Theorem, so that $x_n = \left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{Q}}\right)$. Then $x_n^T = 1 = \left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{(\nu)}\right)$, and Lemma 2 implies that there is a unit $e_N \in E_n$ with $\nu e_N \equiv 1 \bmod p^N$, for each $N > 0$. It follows that, modulo units, ν is locally arbitrarily small. Then $1 \in \nu\overline{E}_n$ and $\alpha_n^T \in \overline{E}_n^q$, so $\alpha_n \in c_1 \cdot \overline{E}_n^q, c_1 \in U(\mathbb{K})$. The equation (18) implies

$$\alpha_1 \in c_1 \cdot \overline{E(\mathbb{K})}. \tag{19}$$

Let $\mathbb{H}_{E'} \subset \overline{\mathbb{L}} \subset \mathbb{H}_T$ be a $\mathbb{Z}_p$-extension with group generated by $\varphi(a)$ and let $\mathbb{L}/\mathbb{K}$ be the fixed field under $\tilde{\Gamma}$. Since $\mathrm{ord}(a_1) > 1$, it follows by restriction of $\varphi(a)$ to $\mathbb{L}$ that $\mathfrak{q}$ is inert in $\mathbb{L} \cap \mathbb{H}_1$; since $\mathbb{L}/\mathbb{K}$ is a $\mathbb{Z}_p$-extension, it is inert in $\mathbb{L}$ and $x_1 = \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{q}}\right) \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ generates this group. But then

$$\mathbb{Z}_p \left(\frac{\mathbb{L}/\mathbb{K}}{(\alpha_1)}\right) = \mathbb{Z}_p x_1^{\mathrm{ord}(a_1)} = (\mathrm{Gal}(\mathbb{L}/\mathbb{K}))^{\mathrm{ord}(a_1)} = \mathrm{Gal}(\mathbb{L}/(\mathbb{L} \cap \mathbb{H}_1).$$

Let $l \geq 0$ be minimal such that $\mathbb{T}_1^{(l)} \cap \mathbb{L} \supsetneq \mathbb{H}_1 \cap \mathbb{L}$. Then $\left(\frac{\mathbb{T}^{(N)}/\mathbb{H}}{(\alpha_1)}\right) \neq 1$ for $N \geq l$. In particular, there is a maximal $l' \geq 0$ with $\alpha_1\overline{E(\mathbb{K})} \cap U(\mathbb{K})^{p^{l'}} \neq \emptyset$. In view of (19), it follows that $c_1 \notin \overline{E(\mathbb{K})}U(\mathbb{K})^{p^{l'+1}}$. Since

$c_1 \in \alpha_n \cdot \overline{E}_n^q$, we conclude that $\ell(a_n) \leq l'$ and thus $\ell(a) < \infty$, which completes the proof. □

Remark 2. *We note that the above results are in accordance with Iwasawa,* [5], *§9.2, 9.3. We chose to derive them explicitly, due to their major impact for the proof of the outstanding conjectures for T and T^* – since we shall show that it follows from the two lemmata above, that $A[T^*]$ and $A'[T]$ are finite: thus the Leopoldt and the generalized Gross conjectures are true.*

Iwasawa's argument is the following: he considers the map $f = f_a : X_\lambda \rightarrow A_L$ given by $c(x,a)^{p^a} = x^{\omega_n}$, for $y = c(x,a) \in X_\lambda$ and n maximal for fixed a, such that y exists. Then $f_a(x)$ is the preimage of the restriction of $c(x,a)$ to Gal$((\Omega_{E'} \cdot \mathbb{H}'_\lambda)/\Omega_{E'}$ under Artin. Iwasawa makes no attempt to find a precise relation between n and a, but see also the first lemma in the next section. The map f_a is the building map for the skew symmetric pairing, and in §9.2 its kernel is determined. Defining $Y = Gal(\Omega_\lambda/(\Omega_{E'} \cdot \mathbb{H}'_\lambda))$ and $\omega^{-1}(Y) = \cup_n \omega_n^{-1}(Y)$ – which is, with our choice of the base field $\mathbb{K}$, simply $\omega_1^{-1}(Y) = Y[T]$ – Iwasawa proves in Lemma 14, that Ker $(f_a) = Y[T]$. Since $\omega_n = p^{n-k} \cdot u \bmod T^*$, with $u \in \Lambda^*$, this result readily implies our Lemma 5. The result of Lemma 6 is somewhat obscured by the definition of $c(x,a)$, which is singular for $x \in X[T]$; but the explicite computation confirms the expectation raised by Iwasawa's result, namely that the extension $\Omega_{E'}[(A'[T])^{1/p^\infty}]$ is almost completely ramified.

The Lemma 14 of [5] *has an additional striking consequence: if $A' = A'[T] \oplus A'(F')$ is the decomposition given in Lemma 3, it follows from Iwasawa's kernel computation that $\Omega_{E'}[(A'(F'))^{1/p^\infty}] \subset \mathbb{H}' \cdot \Omega_{E'}$. We shall prove in the next section that this is indeed the case, when Iwasawa's linear space is non trivial – or, say, in order to use definitions already known, if $A_L \neq \{1\}$. However, if Greenberg's conjecture is true and $A_L = \{1\}$ – which is in fact always the case for CM extensions $\mathbb{K}$, as we prove below – then $[\Omega_{E'} \cdot \mathbb{H}' : \Omega_{E'}] < \infty$ and since $A(F') \neq \{1\}$ in general, the Lemma 14 appears not to hold in this case. There might be an error in our understanding of Iwasawa's conditions on ℓ'-modules, or even a hidden assumption that indeed $A_L \neq \{1\}$: we do not pursue this issue here and derive directly all the results needed for our proofs – while giving all the tribute to Iwasawa for the direction and methods of investigation.*

The two lemmata above readily imply that $A'[T]$ and $A[T^*]$ are finite. We give here for simplicity the argument only for CM extensions[4] but it generalizes quite strait forwardly to arbitrary base fields $\mathbb{K}$.

Theorem 1. *Let $\mathbb{K}$ be a CM extension of $\mathbb{Q}$. Then Leopoldt's conjecture holds for $\mathbb{K}$ and $A'[T]$ is finite.*

Proof. We may assume that $\mathbb{K}$ is galois and contains the p-th roots of unity, fulfilling in addition all the usual conditions for the base fields, which we established in the introduction. Every CM number field has a finite extension of this kind, and since the $\mathbb{Z}_p$-extensions of the base fields do not vanish under finite extensions, if $\mathcal{D}(\mathbb{K}_{-1}) > 0$ for some CM subfield $\mathbb{K}_{-1} \subset \mathbb{K}$, then $\mathcal{D}(\mathbb{K}) > 0$, so it suffices to prove Leopoldt's conjecture for $\mathbb{K}$.

Assume thus that $\mathbb{K}$ is like above and $\mathcal{D}(\mathbb{K}) > 0$. From Lemma 5 we deduce that *ess.* $p\text{-rk}(A[T^*]) = \mathcal{D}(\mathbb{K})$ and from Lemma 6 we see that there is a submodule $B \subset A'[T]$ with $B \sim (A[T^*])^\bullet$ and $[\mathbb{H}_{E'}[B^{1/p^\infty}] \cap \mathbb{H} : \mathbb{H}_{E'}] < \infty]$.

Let $\mathfrak{G} = \mathrm{Gal}(\Omega^-/\mathbb{H}^-) \sim U^-_\infty/\overline{E}_\infty$, by class field theory – e.g. [9], Chapter 5.6. For $f \in \mathbb{Z}_p[T]$ we let $\Omega_f = (\Omega^-)^{f\mathfrak{G}} \subset \mathfrak{G}$ be the maximal subfield with galois group $\mathfrak{G}_f := \mathrm{Gal}(\Omega_f/\mathbb{H}^-)$ annihilated by f. From the above $B^\bullet \hookrightarrow \mathfrak{G}_{T^*}$ and since $A(T) = A[T]$, it follows that the radicals for $\Omega_{(T^*)^2}/\Omega_{T^*}$ stem from E_∞. Since $R_{(T^*)^2} = \mathcal{R}(\Omega_{(T^*)^2/\mathbb{H}^-})$ is a Λ-module and $\mathcal{R}(\Omega_{(T^*)^2}/\Omega_{T^*}) \subset (E_\infty)^{1/p^\infty}$ while $B^{1/p^\infty} \subset \mathcal{R}(\Omega_{T^*}/\mathbb{H}^-)$, we obtain a contradiction. Indeed, $R_{(T^*)^2}$ has $\mathbb{Z}_p$-rank $2r_2$ and since it is a Λ-module, it has a minimal set of r_2 generators in E^{1/p^∞}. This is incompatible with $B \subset R_{T^*}$. Consequently $B = \{1\}$ and $\mathcal{D}(\mathbb{K}) = 0$.

For completing the proof, we still need to show that $B = A'[T]$. By construction, $A[T^*] \cong \mathrm{Gal}((\mathbb{H}^- \cap \mathbb{K}_\infty[(E(\mathbb{K}))^{1/p^\infty}])/\mathbb{K}_\infty)$ and thus reflection requires $B \sim (A'[T])^+$: indeed, if $\mathbb{L} \subset \Omega(\mathbb{K}) \cap \mathbb{H}$ is any $\mathbb{Z}_p$-extension with galois group generated by $a \in (A'[T])^+$, then by reflection, $\mathcal{R}(\mathbb{L}/\mathbb{K}_\infty) \hookrightarrow A^-(T^*) = A^-[T^*]$, which confirms the claim. On the other hand, we have seen in Lemma 3 that $A[T] = A'[T] \oplus \mathbf{B}$. Thus, $A'[T] \not\sim B$ iff $(A'[T])^- \neq \{1\}$. This is a conjecture of Gross [3], which follows from the elementary lemma below and the decomposition $A^-[T] = (A')^-[T] \oplus \mathbf{B}^-$. □

Lemma 7. *If $a = (a_n)_{n\in\mathbb{N}} \in A^-$ is such that $a^T = 1$. Then $a \in \mathbf{B}$. In particular, if $a \in (A')^-[T]$, then $a^t = \mathbf{b} \in \mathbf{B}^-$.*

[4] The proof of Leopoldt's conjecture which we give here can be understood also as a bug fix for [8]: indeed, the final argument is similar, but it uses the much stronger fact proved in Lemma 5, which implies that the radicals of $\tilde{\Omega}_{T^*}$, in the notation of [8], stem in the critical component not from units but from $(A[T])^+$.

Proof. Let $\mathfrak{A} \in a_n$, so that $\mathfrak{A}^{1-\jmath} \in a_n^2$; it follows that $\mathfrak{A}_n^T = (\nu)$ for a $\nu \in \mathbb{K}_n$, and $\mathbf{N}_{\mathbb{K}_n/\mathbb{K}}(\nu) \in E(\mathbb{K})$. Dividing by the complex conjugate, the Dedekind unit Theorem implies that $\mathbf{N}_{\mathbb{K}_n/\mathbb{K}}(\nu) \in \mu_{p^k}$. Therefore $\nu^{p^k(1-\jmath)} = x^T$ for an $x \in \mathbb{K}_n$, by Hilbert 90 – here k is the largest integer, such that $\zeta_{p^k} \in \mathbb{K}$, thus a constant. Then $\left(\mathfrak{A}^{p^k(1-\jmath)}/(x)\right)^T = (1)$; but this implies that the ideal $\mathfrak{A}^{p^k(1-\jmath)}/(x) \in a_n^{2p^k}$ is ramified. This holds for all n, so $a^{2p^k} \in \mathbf{B}^-$ and since p is odd and by definition of $\mathbf{B}^-$, it follows that $a \in \mathbf{B}^-$ too. □

3.5. **The Iwasawa linear space.** We now consider the F-part of the galois group X_λ. Recall from Lemma 3 that $\Omega_F \subset \Omega_\lambda$ is the fixed field of $X[T] \oplus X[T^*] = \mathrm{Gal}(\Omega_\lambda/\Omega_{E'})[TT^*]$. Let $A_F = \rho_1^{-1}(\Omega_F) \subset A'$ and $\mathbb{H}_F = \mathbb{H}_{E'}[\rho_0'(A_F)] \cap \mathbb{H}_\lambda$.

Before considering the relation between radicals and galois groups, we prove a result on lifts from A to X and cyclic continuations of class fields:

Lemma 8. *Let $a \in A'(F)$. Then there is a lift $x \in X_\lambda = Gal(\Omega_\lambda/\Omega_{E'})$ with $x|_{\Omega_{E'}\cdot\mathbb{H}} = \varphi(a)$ and there is a further $y = c(x,n) \in X_\lambda$ with*

$$x^{\mathrm{ord}(a_n)} = y^{\omega_n}. \tag{20}$$

If $\mathbb{L}/\Omega_{E'}$ is a $\mathbb{Z}_p$-extension and $\mathbb{L}_n = \Omega_n' \cap \mathbb{L}$ intersects $\mathbb{H}_n \cdot \Omega_{E',n}'$ non trivially, then $\mathbb{L}_n \subset \mathbb{H}_n \cdot \Omega_{E',n}'$.

Moreover, if $\mathbb{L}/\mathbb{K}_\infty$ is a $\mathbb{Z}_p$-subextension of $\mathbb{H}$ with $[\mathbb{L}\cdot\mathbb{H}_{E'} : \mathbb{H}_{E'}] = \infty$ and $a \in A$ has $\mathbb{Z}_p(\varphi(a)|_{\mathbb{L}}) = Gal(\mathbb{L}/\mathbb{K}_\infty$, then $\ell(a) = \infty$ and $\ell(a_n) = v_p(\mathrm{ord}(a_n))$ for all n.

Proof. From the definition of Ω_F we know that $\mathrm{Gal}(\Omega_F/\Omega_{E'})$ is an Iwasawa module with annihilator coprime to T. In particular, $\Omega_{F,n}/\Omega_{E',n}$ are finite extensions. If $\mathbb{L}/\Omega_{E'}$ is a $\mathbb{Z}_p$-extension contained in Ω_F and $[\mathbb{L} \cap \Omega_{E'} \cdot \mathbb{H} : \Omega_{E'}] = \infty$, then infinite galois theory implies that $\mathbb{L} \subset \Omega_{E'} \cdot \mathbb{H}$. The lemma states that additionally, $\mathbb{L}_n \subset \Omega_{E',n} \cdot \mathbb{H}_n$ for all n. Let $x \in X_\lambda$ with $x^T \neq 1$ be a generator for $\mathrm{Gal}(\mathbb{L}/\Omega_{E'}$. Since X_λ is a Weierstrass module, for n sufficiently large we have $\mathrm{ord}(x_m) = p^{m-n}\mathrm{ord}(x_n)$ and since $x \notin X_\lambda[T]$, property F implies that $x^{\mathrm{ord}(x_n)} = y^{\mathrm{ord}(x_n)}$ for a $y \in X_\lambda(F)$. Let $a \in A'$ be such that $x|\mathbb{L} = \varphi(a)$: the choice is possible, since $\mathbb{L} \subset \Omega_{E'} \cdot \mathbb{H}$. From property F for A' we deduce that there is a constant $q = p^u$ such that $\mathrm{ord}(x_n) = q\mathrm{ord}(a_n)$ for all n sufficiently large. If $q > 1$, then there is an extension $\mathbb{L}' \supset \mathbb{L}$ of degree q which is a $\mathbb{Z}_p$-extension of $\Omega_{E'}$. But $\mathbb{Z}_p$ has no finite compact subgroups, so we must have $q = 1$ and $\mathbb{L}_n$ has no cyclic extension above $\Omega_{E'}$ which is contained in Ω. The relation (20) also follows from $\mathrm{ord}(a_n) = \mathrm{ord}(x_n)$.

Finally, we shift the radicals to $\mathbb{K}_\infty$. We may consider without restriction of generality that $\mathbb{L} \cap \mathbb{H}_{E'} = \mathbb{K}_\infty$. Then it follows from the facts proved above, that $\mathbb{L}_n/\mathbb{K}_n$ has no cyclic continuation in $\mathbb{T}_n^{(N)}$ above $\mathbb{K}_n$, for any $N > 0$: otherwise, $\mathbb{L}_n \cdot \mathbb{H}_{E',n}$ has a cyclic continuation, which was shown to be impossible. Let $N > 0$ and consider a cycle-decomposition of $\mathrm{Gal}(\mathbb{T}_n^{(N)}/K_n) = \prod_{i=1}^s \mathbb{Z} x_n^{(i)}$, as an abelian p-group. We may assume that $x_n = x_n^{(1)}$ is such that $x_n|_{\mathbb{L}_n} = \varphi(a)$. Then $x_n^{\mathrm{ord}(a_n)} = 1$, and by Tchebotarew's Theorem, there is a prime $\mathfrak{Q}$ which is totally split above $\mathbb{Q}$ and such that $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{Q}}\right) = x_n$. Since $x_n|_{\mathbb{H}} = \varphi(a_n)$, it follows that $\mathfrak{Q} \in a_n$. Let $(\alpha_n) = \mathfrak{Q}^{\mathrm{ord}(a_n)}$; by choice of x_n we have $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{(\alpha_n)}\right) = 1$ and Lemma 2 shows that we may choose α_n – by eventual multiplication by units – such that $\alpha_n \equiv 1 \bmod p^N$. We have shown that $\mathbb{L}_n \subset \mathbb{T}_n^{(N)}$ has no cyclic continuation, and thus N can be chosen arbitrarily large. In particular, we can achieve $\alpha_n \in U_n^{\mathrm{ord}(a_n)}$ and thus $\ell(a_n) = v_p(\mathrm{ord}(a_n))$ for all n, and $\ell(a) = \infty$. This completes the proof. □

The main result of this section defines the Iwasawa selfdual linear space:

Theorem 2 (Iwasawa). *There is a canonical selfdual submodule $A^{(S)} \subset A'/(A')^\circ$ such that*

$$\begin{array}{rcl} \mathbb{H}_\lambda & = & \mathbb{H}_{E',\lambda}[(A^{(S)})^{1/p^\infty}] \quad \textit{and} \\ \textit{Gal}(\mathbb{H}_\lambda/\mathbb{H}_{E',\lambda}) & \cong & A^{(S)}. \end{array} \tag{21}$$

For all $a = (a_n)_{n\in\mathbb{N}} \in A^{(S)}$ we have also at finite levels $n \geq 0$ that $\ell(a_n) = v_p(\mathrm{ord}(a_n))$. If $A^{(S)} \neq \{1\}$, then Gal$(\mathbb{H}_{E',\lambda} \cap \Omega_F) \cong A[T^*]$.

Proof. Let $A_G = \mathrm{Gal}(\mathbb{H}_\lambda/\mathbb{H}_{E',\lambda}) = A_G[T] \oplus A_G(F)$. If $a \in A_G[T]$ then $\ell(a) = \infty$ by Lemma 5, while Lemma 8 implies that the same holds for $a \in A_G(F)$. Thus $\ell(a) = \infty$ for all $a \in A_G$.

On the other hand, the radicals are canonic, since ρ_1 is injective. Therefore the module $A_L \subset A'/(A')^\circ$ with $\mathbb{H}_\lambda = \mathbb{H}_{E',\lambda}[\rho'(A_L)]$ is well defined. However, since $\ell(a) = \infty$ for all $a \in A_G$, it follows also that $A_G \subset A'$: indeed, we have seen that $A[T] = A'[T] \oplus \mathbf{B}[T]$ and $\mathbb{H}_E[(\mathbf{B}[T])^{1/p^\infty}] \cap \mathbb{H} \subseteq \mathbb{H}_{E'}$. This confirms the claim. For any set of representatives $\overline{A}_G$ of A_G mod $(A')^\dagger$ we have $\mathbb{H}_{E',\lambda}[(\overline{A}_G)^{1/p^\infty}] \subseteq \mathbb{H}_\lambda$. By comparing $\mathbb{Z}_p$-ranks, we see that $\overline{A}_G$ has finite index in A_L; however, A_G is p-coalescence closed, so it follows that $A_G \cong A_L$ mod $(A')^\dagger$.

Letting $A^{(S)} = A_L \subset (A')/(A')^{\circ}$, a canonical submodule, we may choose $\overline{A}_G = A_L$, so $A^{(S)} \cong (A^{(S)})^{\bullet}$, so the Iwasawa linear space is selfdual.

Finally, assume that $A^{(S)} \neq \{1\}$. If $\mathbb{H}_{E',\lambda} \cap \Omega_F \neq \mathbb{K}_{\infty}$, Since $A^{(S)}$ fixes $\mathbb{H}_{E'}$, for any $b \in A$ with $\mathrm{ord}(b) = \infty$ and $\varphi(b)|_{\mathbb{H}_{E'}} \neq 1$ we have $\ell(b) < \infty$: otherwise, $b \in A^{(S)}$. Let now $\mathbb{L} \subset \mathbb{H}$ be any $\mathbb{Z}_p$-extension with $\mathbb{L} \cap \mathbb{H}_{E'} = \mathbb{K}_{\infty}$ and $\mathbb{L} \subset \Omega_F$. The last claim of Lemma 8 implies that $b \in A^{(S)}$ for all $b \in A$ with $\mathbb{Z}_p(\varphi(b)|_{\mathbb{L}}) = \mathrm{Gal}(\mathbb{L}/\mathbb{K}_{\infty})$. We may choose a lift ρ_0 and let $\mathbb{H}_F = \mathbb{K}_{\infty}[\rho_0'(A'(F))]$, an extension with group $\mathrm{Gal}(\mathbb{H}_F/\mathbb{K}_{\infty}) = \varphi\left(A^{(S)}\right)\big|_{\mathbb{H}_F}$. Suppose that $\mathbb{L} \not\subset \mathbb{H}_F$, which is possible if $\mathbb{H}_{E',\lambda} \neq \mathbb{K}_{\infty}$. Since $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_{\infty}) \subset \varphi\left(A^{(S)}\right)\big|_{\mathbb{L}}$, it follows that the compositum $\mathbb{H}_F \cdot \mathbb{L}$ has also the restriction of $\varphi\left(A^{(S)}\right)$ as galois group over $\mathbb{K}_{\infty}$. This is however impossible, for since the rank should be larger then $\mathbb{Z}_p\text{-rk}(A^{(S)})$. Therefore we must have $\mathbb{H}_{E',\lambda} \cap \Omega_F = \mathbb{K}_{\infty}$, which completes the proof. Note that we only considered the F parts. For non CM extensions, in which we have not proved the Leopoldt conjecture yet, it is still possible that $\mathrm{Gal}(\mathbb{H}_{E',\lambda}/\mathbb{K}_{\infty}) \cong A[T^*]$. □

Remark 3. *The above results are essentially due to Iwasawa. We have taken from §9 - 11 of his seminal paper* [5] *the fundamental ingredients, which are the use of Takagi theory and the right module to consider. By shifting radicals to $\mathbb{K}_{\infty}$ or $\mathbb{H}_{E'}$ we obtain however a simpler exposition of the facts. Iwasawa's construction of the function f_a described in the previous Remark obscures the case of $A'[T]$ and we have therefore chosen to treat the T and T^* modules separately. However, his results are consistent with ours - modulo the Lemma 14, which might miss the premise $A^{(S)} \neq \{1\}$, since for $A^{(S)} = 1$, the normal case, we may have $\Omega_{E'} = \Omega_{e'} \cdot \mathbb{H}$ and yet $\omega^{-1}(Gal(\Omega_{\lambda}/\Omega_{E'})) \neq 1$.*

Since Lemma 14 implies in particular that $\Omega_{E'}[\rho_1(A[T^*])]/\Omega_{E'}$ is totally unramified, one may argue that Iwasawa's construction of the skew symmetric pairing might have lead to a straight proof of Leopoldt's conjecture, which is close to the one given is this paper.

Iwasawa proceeds in his paper by constructing a skew symmetric pairing on the pair a, b of our proof; for this he uses Hasse's reciprocity in a beautiful way, which is worth reconsidering. We have not done this, since the space $A^{(S)}$ is ephemeral, and we shall prove below that it vanishes, at least for CM base fields.

In fact, since Greenberg's seminal paper [4] *appeared in the same year as the one of Iwasawa, and the conjecture raised in that paper obviously* *implied that $A^{(S)}$ must vanish, this lead, in the opinion of experts*[5] *to a reduced attention for properties and implications of the Iwasawa linear space.*

4. Thaine shifts and the Greenberg Conjecture

Iwasawa asked in [5], the last phrase of §11, the following question: "It would be an important problem, to find out when $\dim(V^+) > 0$"; in the notation of [5], $V = \mathrm{Gal}((\Omega_{E'} \cdot \mathbb{H}')/\Omega_{E'}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The question was considered by his PhD student Ralph Greenberg, who brought in [4], in the same year, evidences for the fact that $\lambda^+ = 0$ should be true for abelian extensions $\mathbb{K}/\mathbb{Q}$. Since then, the term of *Greenberg conjecture* is connected to various statements of finiteness of canonic submodules of A. This may be for instance the statement that $\lambda^+ = 0$ for arbitrary CM fields or the stronger statement that A^+ is finite for arbitrary CM extensions. Starting with Greenberg, much numerical evidence has been gathered for the truth of Greenberg's conjecture. For obvious reasons of complexity, the general computations restrict mostly to quadratic base fields, while some sporadic verifications could be computed in extensions of larger degree. One of the most vast numerical evidence in the literature can be found in [6]; we used it repeatedly for verifying various structure results that lead to the proofs in this paper.

We define here the general Greenberg conjecture as follows:

Conjecture 1. *Let $\mathbb{K}/\mathbb{Q}$ be an arbitrary galois extension containing the p-th roots of unity and $\mathbb{H}/\mathbb{K}_\infty$ the maximal unramified p - abelian extension of its cyclotomic $\mathbb{Z}_p$-extension. Let $\mathbb{H}_{E'} = \mathbb{H} \cap \Omega_E$, with $\Omega_E = \cup_n \mathbb{K}_n[E_n^{1/p^n}]$ and $E_n = \mathcal{O}(\mathbb{K}_n)$. Then*

$$[\mathbb{H} : \mathbb{H}_{E'}] < \infty. \tag{22}$$

The tools for dealing with non CM extensions are more complex and we restricted in this paper the attention to the simpler CM extensions and their radicals. We shall thus prove in this section the

Theorem 3. *If $\mathbb{K}$ is a CM extension, then*

$$\lambda(A^+) = 0, \quad \textit{for} \quad A = \varprojlim_n A_n,$$

and A_n the p parts of the class groups of $\mathbb{K}_n$, the intermediate levels of the $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{K}$.

[5] This was explained by John Coates [2] in a personal discussion concerning the Iwasawa linear space.

The Theorem answers completely the initial question of Iwasawa which was stated only for CM extensions: thus $\dim(V) = 0$, always. We note that it suffices to prove the statement for galois CM extensions containing the p-th roots of unity, that we have considered in this paper. Indeed, if $\mathbb{K}$ is CM, then there is a finite algebraic extension $\mathbb{L} = \mathbb{K}[\theta]$ which is galois, CM and contains the p-th roots of unity. Then $\mathbb{H}^+(\mathbb{K})[\theta] \subset \mathbb{H}^+(\mathbb{L})$, so if $A^+(\mathbb{K})$ is infinite, so is $A^+(\mathbb{L})$.

We shall use the construction introduced by Thaine for the proof of his celebrated Theorem ([11], [12] §15.1). The main facts that we need are gathered in the following:

Lemma 9 (Thaine shift)**.** *Let $\mathbb{K}$ be a CM galois extension of $\mathbb{Q}$ and assume that $\mathbb{K}$ is not a p^k-th cyclotomic extension. Let $a_n \in A_n^- \setminus (A_n^-)^p$ be a class of order $q = p^m$; then there is a cyclic abelian extension $\mathbb{F}_n = \mathbb{K}_n[\eta]$ of degree p^m and a class $b_n \in A_n(\mathbb{F}_n)^-$ with $\mathrm{ord}(b_n) = p^{2m}$ and $b_n^{p^m} \in \iota_{\mathbb{K}_n,\mathbb{F}_n}(a_n)$.*

Proof. We use the Thaine construction. Let $\mathfrak{Q} \in a_n$ be a prime which is totally split $\mathbb{Q}$ and unramified in $\mathbb{K}$, and let $Q \in \mathbb{Z}$ be the rational prime above it. We assume that Q is totally split in $\mathbb{K}_{n+b}$ for a $b \geq m - n$; then $Q \equiv 1 \bmod p^m$ and we let θ be a Q-th root of unity. Let $\mathbb{F} \subset \mathbb{K}[\theta]$ be the subfield of degree p^m and the fields $\mathbb{F}_m = \mathbb{K}_m[\eta] = \mathbb{F}[\zeta_{p^m}]$, for a Gauss period η of θ, build the cyclotomic $\mathbb{Z}_p$ - extension of $\mathbb{F}$. The choice of Q also implies that $\mathbb{F}$ is linearly disjoint from $\mathbb{K}_n$, so $\mathbb{F}_m/\mathbb{Q}$ are galois and $\mathrm{Gal}(\mathbb{F}_m/\mathbb{Q}) = \mathrm{Gal}(\mathbb{K}_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$.

Let $\mathbf{K}_n$ be the p^n-th cyclotomic extension, so by assumption, $\mathbf{K}_n \subsetneq \mathbb{K}_n$. If χ is a Dirichlet character of order p^n and $\beta = (\tau(\chi))^{p^n}$ is its Gauss sum in $\mathbf{K}_n$, then it is a fact of elementary cyclotomy that

$$\mathbb{F}_n = \mathbb{K}_n[\tau(\chi)^{1-\jmath}] = \mathbb{K}_n[\beta^{(1-\jmath)/p^n}].$$

Let $(\alpha') = \mathfrak{Q}^{p^n}$ and $(\alpha) = (\alpha'/\overline{\alpha'})$. Then α is well defined up to roots of unity. From the definition of the Gauss sums we see that $\beta = \mathfrak{q}^{(1-\jmath)\Theta}$, where $\Theta = p^n\vartheta$ is in the Stickelberger Ideal of $\mathbb{Z}/(p^n \cdot \mathbb{Z})[\mathrm{Gal}(\mathbf{K}_n/\mathbb{Q})]$ and $\mathfrak{q} \subset \mathbf{K}$ is a prime above Q. We conclude that $\alpha \notin (\mathbb{F}_n[\eta]^\times)^p$; otherwise, we may assume that $\alpha = \beta x^p$, and since $\mathfrak{Q}$ is totally split in $\mathbb{K}_n/\mathbf{K}_n$, the decomposition in prime ideals modulo p powers yields a contradiction (here we need that $\mathbf{K}_n \neq \mathbb{K}_n$).

Let $\mathfrak{R} \subset \mathbb{F}_n$ be the ramified prime above $\mathfrak{Q}$ and $b_n = [\mathfrak{R}]$. Then $\mathrm{ord}(\mathfrak{R}) = p^m\mathrm{ord}(\mathfrak{Q}) = p^{2m}$. Indeed, let $(\gamma') = \mathfrak{R}^{\mathrm{ord}(\mathfrak{R})}$, while $\gamma = \gamma'/\overline{\gamma}'$; then $\gamma \notin \mathbb{F}_n^p$. Ramification of $\mathfrak{Q}$ implies

$$\begin{aligned} (\gamma) &= \mathfrak{R}^{(1-\jmath)\mathrm{ord}(\mathfrak{R})} = \mathfrak{Q}^{\mathrm{ord}(\mathfrak{R})/p^m} = (\alpha)^{\mathrm{ord}(\mathfrak{R})/p^{2m}}, \quad \text{so} \\ \gamma &= \eta \cdot \alpha^{\mathrm{ord}(\mathfrak{R})/p^{2m}}, \quad \eta \in \mu_{p^n}. \end{aligned}$$

After eventually multiplying γ by $\overline{\eta}$, we see that $\gamma = \alpha^{\mathrm{ord}(\mathfrak{R})/p^{2m}}$ and since $\alpha, \gamma \notin (\mathbb{F}_n[\eta]^{\times})^p$, it follows that $\mathrm{ord}(\mathfrak{R}) = p^{2m}$, which proves the claim. □

As a consequence, we have

Corollary 1. *Let $\mathbb{K}, \mathbb{F}, \mathfrak{Q}$ be like in the Lemma 9 and assume that $\mathbb{K}_{\wp}$ contains the unramified p^M-th extension for M sufficiently large, so p is totally split in $\mathbb{F}/\mathbb{K}$. If $\beta \in \mathcal{O}(\mathbb{K}_n)$ is normalized with $\tilde{\ell}(\beta) = k > 0$, then, $\beta \notin U(\mathbb{F}_n)^{p^{k+1}}$.*

Proof. We prove the claim by induction. Let $\mathbb{K}_n \subset \mathbf{K} \subset \mathbf{L} \subset \mathbb{F}_n$ be a tower with $[\mathbf{L} : \mathbf{K}] = p$ and suppose $\beta \in \mathbf{K}$ has $\tilde{\ell}(\beta) = k$. We shall show that β is not a local p^{k+1}-th power in $\mathbf{L}$ either. Let $\tilde{\wp} \subset \mathbf{K}$ be a prime above p and $\tilde{C} = \mathrm{Gal}(\mathbf{K}/\mathbb{Q})/D(\tilde{\wp}), \tilde{P} = \{\sigma\tilde{\wp} : \sigma \in \tilde{C}\}$, so $U(\mathbf{K}) = \prod_{\sigma \in \tilde{C}} \mathbf{K}_{\sigma\wp}$. Let $\beta = (\beta_\sigma)_{\sigma \in \tilde{C}} \in U(\mathbf{K})$ be the embedding of β in this completion, so $\beta_\sigma = \gamma_\sigma^{p^k}, \gamma_\sigma \in U(\mathbf{K}_{\sigma\wp})$.

The prime p is totally split in $\mathbf{L}/\mathbf{K}$, thus $U(\mathbf{K}_{\sigma\wp})$ splits into a product of the units in p distinct completions, in $\mathbf{L}$. If $G' = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$, then we write under the Chinese Remainder Theorem,

$$U(\mathbf{L}_\sigma) = \prod_{\nu \in G'} \nu U_{\mathbf{K}_\sigma}.$$

Since G' permutes the components of $U(\mathbf{L}_\sigma)$ but fixes β, it follows that the image $\iota_{U(\mathbf{L}_\sigma)}(\beta_\sigma) = (\beta_\sigma, \beta_\sigma, \ldots, \beta_\sigma)$ consists of p copies of β_σ. Therefore, it is a p^k-th power, but not an p^{k+1}-th power in $U(\mathbf{L})$. This holds for all $\sigma \in \tilde{C}$ and also for all subextensions of degree p in the $\mathbb{K}_n \subset \mathbb{F}_n$, therefore β is not a p^{k+1}-th power in $\mathbb{F}_n$ either, as claimed. □

We are now ready to prove Theorem 3:

Proof. If the Greenberg conjecture holds for a field $\mathbb{K}$, we have shown that it holds for its subfields, so we may assume that $\mathbb{K}_{\wp}$ contains the p^M-th unramified extension of $\mathbb{Q}_p$, for sufficiently large M. This can be achieved by a cyclotomic extension of the base field. Therefore the premises of Corollary 1 can be met.

Assume that $\lambda^+(\mathbb{K}) \neq 0$, so $(A^{(S)})^- \neq \{1\}$. Let $a = (a_n)_{n \in \mathbb{N}} \in (A^{(S)}) \setminus A^p$ and $n > n_0$, $q = p^m = \mathrm{ord}(a_n)$. We choose a prime $\mathfrak{Q} \in a_n$ and define $\mathbb{F} = \mathbb{K}[\eta]$ and the cyclotomic $\mathbb{Z}_p$ - extension $\mathbb{F}_n = \mathbb{K}_n[\eta], \mathbb{F}_\infty = \cup_n \mathbb{F}_n$ like in the proof of the Lemma 9, with respect to the rational prime Q below $\mathfrak{Q}$.

From Lemma 9 we see that $\mathfrak{R} \subset \mathbb{F}_n$, the prime above $\mathfrak{Q}$, belongs to a class b_n of order q^2. The Corollary 1 implies that $\ell(b_n) = \ell(a_n) =$

$m < v_p(\mathrm{ord}(b_n))$. We construct a lift of b_n as follows: for $N > n$ we let $\mathfrak{A} \subset \mathbb{F}_N$ be a prime which is totally split over $\mathbb{Q}$ and such that $\mathbf{N}_{N,n}(\mathfrak{A}) \in b_n$ while $\mathbf{N}_{\mathbb{F}/\mathbb{K}}(\mathfrak{A}) \in a_N$; the existence of such primes follows from Tchebotarew's Theorem. We let $b_N = [\mathfrak{A}]$ and repeat the procedure, replacing n by N. Thus we inductively construct a norm coherent sequence $b = (b_n)_{n\in\mathbb{N}} \in A^-(\mathbb{F})$ with $\mathbf{N}_{\mathbb{F}/\mathbb{K}}(b) = a$ and with $b_n = [\mathfrak{R}]$.

If $A^+(\mathbb{K})$ is infinite, then so is $A^+(\mathbb{F})$, thus $A^{(S)}(\mathbb{F}) \neq \{1\}$. From Theorem 2 we see that $\lambda^-(\mathbb{F}) = \mathbb{Z}_p\text{-rk}((A^{(S)})^-(\mathbb{F}))$. In particular $\ell(x) = \infty$ for all $x \in (A')^-(\mathbb{F})$ with $\mathrm{ord}(a) = \infty$. But we have constructed a lift $b \in (A')^-(\mathbb{F})$ for which we have shown that $\ell(b) < \infty$, while $\mathrm{ord}(b) = \infty$. This contradiction yields the proof.

A more elementary proof is based on the explicite properties of the canonical radical shifts for minus parts, derived in Appendix C and Proposition 4. Let $N = n_0(A(\mathbb{F}))$ and $M > N$. From point 2. of Proposition 4 and $\ell(b_n) = v_p(\mathrm{ord}(b_n)) - m < v_p(\mathrm{ord}(b_n))$, we gather that

$$\ell(b_M) \leq \ell(b_n)+v_p(\mathrm{ord}(b_M))-v_p(\mathrm{ord}(b_n)) = v_p(\mathrm{ord}(b_M))-m < v_p(\mathrm{ord}(b_M)).$$

Since $M > n_0(A(\mathbb{F}))$, it follows from point 3. of the same proposition, that $\ell(b) < \infty$. Then point 4. implies that there is an $r > N$ such that for $M > r$, $\beta(b_M) \in \beta(b_r) \cdot U_M(\mathbb{F})^{p^{\ell(b)}\omega_r}$. Since $N_{\mathbb{F}/\mathbb{K}}(\beta(b_M)) = \beta(a_m) \in \rho(a_M)^{\mathrm{ord}(a_M)}$, we conclude that $\beta(a_M) \in \beta(a_r) \cdot U_M(\mathbb{K})^{p^{\ell(b)}\omega_r}$. Since r is fixed, it follows from point 4 of Proposition 4 that $\ell(a) < \infty$, in contradiction with the choice of a. This concludes the proof. □

The point 1. in Proposition 4 plays a central role in the above proof. We have required here $M > n_0(\mathbb{F})$, so the transitions $C_M(\mathbb{F}) = A_{M+1}(\mathbb{F})/\iota_{M,M+1}(A_M(\mathbb{F}))$ are stable; we know though that semistable transitions are a sufficient premise for the claim of point 1 to hold. It can be shown in the Thaine shift, that if Q is split in $\mathbb{K}_n/\mathbb{Q}$ and $b_n = [\mathfrak{R}]$ as in the above proof, then Λb_n contains a submodule $B_n = (\Lambda b_n)^{f_a}$, with f_a the minimal polynomial of a and $B_n \cong \Lambda_n/p^m\Lambda_n$, where $\Lambda_n = \Lambda/(\omega_n\Lambda)$. Therefore none of the transitions $C_k(\Lambda b), k \leq n$ are semistable. This fact shows that our proof is compatible with the existence of modules $\Lambda a \subset (A')^-(\mathbb{K})$ with arbitrarily large, but finite $\ell(a)$.

Remark 4. *The method of Thaine shifts, combined with Proposition 4 offers also an alternative proof of the Leopoldt Conjecture: it suffices to take $a \in A^-[T^*]$, which is an obstruction space to Leopoldt's Conjecture. By Lemma (5) we have $\ell(a) = \infty$ and we may build a Thaine shift like above, lifting a to $b \in A(\mathbb{F})$. We still have* $\mathrm{ord}(b) = \infty$ *and* $\ell(b) < \infty$

and the variant of the proof of Greenberg's conjecture using Proposition 4 then yields a contradiction to $\ell(a) = \infty$.

The methods used for proving $\lambda^+ = 0$, in particular Proposition 2 and the use of Thaine shifts, could also be applied for showing that $\mu^+ = 0$. *This shall be done in a later version of this draft.*

5. Appendix A: Finiteness of $\mathbf{B}^+$

In this section we shall prove:

Theorem 4. *If $\mathbb{K}$ is galois and real, then $\mathbf{B}$ is finite.*

Note that this theorem implies that $\mathbf{B}^+$ is finite for any CM extension: it suffices to take the galois closure and adjoin a p-th root of unity in order to meet the premises of the theorem. If $\mathbf{B}^+$ is infinite in the initial field, it would be infinite also in this finite extension, in contradiction with the theorem.

The field $\mathbb{K}$ is in this section a CM galois extension of $\mathbb{Q}$ containing the p-th roots of unity, so all the notations are consistent with the ones introduced before.

We assume that the field $\mathbb{K} = (\mathbb{K}[\zeta_p])^+$ is the maximal real subfield of a CM extension $\mathbb{K}' = \mathbb{K}[\zeta_p]$ and suppose that $\zeta_{p^k} \in \mathbb{K}'$, but $\zeta_{p^{k+1}} \not\in \mathbb{K}'$. Accordingly, we write $\mathbb{K}_0 = \mathbb{K}_1 = \ldots = \mathbb{K}_k \neq \mathbb{K}_{k+1}$. Then $n' = n-k+1$ in the definition of ω_n.

The central idea of the proof consists in the analysis of $\mathbb{Z}$ - ranks of the *relative* units[6]

$$E_H(\mathbb{K}_n) = \{e \in E(\mathbb{K}_n) : N_{\mathbb{K}_n/\mathbb{K}}(e) = 1\}.$$

Assuming that the Leopoldt defect is stable above $\mathbb{K}$, this module has maximal $\mathbb{Z}_p$ - rank, and so do factors like $E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n)$. On the other hand, we show that the assumption *ess.* p-rk$(\mathbf{B}) =: \mathfrak{B}(\mathbb{K}) > 0$ implies the existence of a defect in the $\mathbb{Z}$ - rank of $E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n)$, equal to $\mathfrak{B}(\mathbb{K})$: this confirms the statement of the Theorem 4.

5.1. **Group rings and units.**

We begin with a general fact on annihilators of Λ - modules. Recall that $\widetilde{X} = X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for $\mathbb{Z}_p$-modules X.

Lemma 10. *Let $\mathbb{K}/\mathbb{Q}$ be a galois extension with group G and $\mathbb{K}_n$ build its cyclotomic $\mathbb{Z}_p$ - extension. Let $b \in A$ be a sequence of classes of infinite order. Then*

[6] These are related, but not identical to Hilbert's relative units in the Theorem Hilbert 91. Unlike Hilbert, we are only interested in $\mathbb{Z}$ - ranks, so the conditions involved are much simpler

1. *There is an ideal* $b^\top = \{x \in \Lambda[G], b^x = 1\} \subset \Lambda[G]$.
2. *Let* $R[G] = \widetilde{\Lambda}[G]$. *There is an idempotent* $\beta_0 \in R[G]$ *such that* $b^\top = \beta_0 R \cap \Lambda[G]$ *and for a fixed power* p^l, *we have* $\beta = p^l \cdot \beta_0 \in \Lambda[G] \setminus p\Lambda[G]$. *In particular*
$$p^l b^\top \subset \beta\Lambda[G] \subset b^\top.$$
3. *At finite levels, let* $\beta_n \in \mathbb{Z}[\omega_n][G]$ *approximate* β *to the order* p^M, *for sufficiently large* $M \geq n$. *Let* $b_n^\top = \{x \in \mathbb{Z}[\omega_n][G] : b_n^x = 1\}$ *and* $\mathrm{ord}(b_n) = p^{n+z}$. *Then*

$$p^l b_n^\top \subset (\beta_n, p^{n+z})\mathbb{Z}[\omega_n][G] \subset b_n^\top. \tag{23}$$

Proof. For 1., one verifies from the definition that $b^\top$ is an ideal in $\Lambda[G]$. It is thus a one sided module; upon tensoring with $\mathbb{Q}_p$, Maschke's Theorem implies that $\tilde{b}^\top = b^\top \otimes \mathbb{Q}_p$ has an orthogonal complement and there is a generating idempotent, that we denote by β_0. The denominator of β only depends on G and thus on $\mathbb{K}$, but not on n; so we denote it with p^l and see that $\beta = p^l\beta_0 \in \Lambda[G] \setminus p\Lambda[G]$. The relation in 2. follows from $\beta_0 R[G] \supset b^\top \supset p^l\beta_0 R[G]$ by multiplying with p^l. The relations at finite levels follow directly from this, by using the order of b_n. □

We assume now that $\mathbb{K}$ has galois group G and is totally real, while $\mathbf{B}$ is infinite. We think of $\mathbb{K}$ as being the maximal real subextension of a CM galois extension which contains the p-th roots of unity; this extension may be denoted at places by $\mathbb{K}'$. The $\Lambda[G]$ - module $\mathbf{B}$ is quasi cyclic, as an indirect consequence of a similar property of the local units U_∞:

Lemma 11. *The group* $\mathbf{B}$ *is* $\Lambda[G]$ *- quasicyclic: there is a* $b = (b_n)_{n\in\mathbb{N}} \in \mathbf{B}$ *with*
$$[\mathbf{B} : \Lambda[G]b] < \infty.$$
If $\beta, b^\top$ *are defined like in the previous lemma with respect to* b, *then*

$$\textit{ess. } p\textit{-rk}(\mathbf{B}) = \mathbb{Q}_p\textit{-rk}(\beta R[G]). \tag{24}$$

Proof. Let $\Omega(\mathbb{K})$ be the product of all the $\mathbb{Z}_p$ - extensions of $\mathbb{K}$; and let $A(T)$ be the T - primary part of A, while $A[T] = \{x \in A(T) : x^T = 1\}$. Then one proves like for abelian p - groups, that
$$A[T] \sim A(T)/(TA(T)).$$
If the Leopoldt defect vanishes, then $\Omega(\mathbb{K})$ is finite and so is $A(T)$. In general, $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{H}_\infty) \hookrightarrow U^-(\mathbb{K}')$ and since the latter module is $\mathbb{Z}_p[G]$ quasicyclic, it follows that so is the galois group. This shows the existence of $b \in \mathbf{B}$ which generates this module under the action of

$\mathbb{Z}_p[G]$, up to pseudoisomorphism. The equality of ranks follows from the definition of annihilators. □

5.2. **Units.** If Leopoldt's conjecture is true for $\mathbb{K}$, then $\mathbf{B}$ is a fortiori finite, so there is nothing to prove. We assume thus that the Leopoldt defect $\mathcal{D}(\mathbb{K}) > 0$ and moreover, it is stationary in the $\mathbb{Z}_p$ extensions, that is $\mathcal{D}(\mathbb{K}_n) = \mathcal{D}(\mathbb{K})$ for all $n \geq 0$.

The norm one units with respect to $\mathbb{K}$ will be denoted by

$$X_H(\mathbb{K}_n) = \{x \in X(\mathbb{K}_n) \ : \ \mathbf{N}_{\mathbb{K}_n/\mathbb{K}}(x) = 1\}, \quad X \in \{E, E', U\}.$$

We let $U'(\mathbb{K}_n) = \{u \in U(\mathbb{K}_n) \ : \ \mathbf{N}_{\mathbb{K}_n/\mathbb{Q}}(u) = 1\}$. Then $\mathcal{D}(\mathbb{K}) = \mathbb{Z}_p\text{-rk}(U'(\mathbb{K}_n)) - \mathbb{Z}_p\text{-rk}(\overline{E}(\mathbb{K}_n))$ for all $n \geq 0$. The units $E_H(\mathbb{K}_n)$ have a family of relative generators:

Lemma 12. *Let r be the number of real embeddings of $\mathbb{K}$; then, for $n > 1$, there is a set $\mathcal{E}_n = \{d_1, d_2, \ldots, d_r\} \subset E_H(\mathbb{K}_n)$ which is $\mathbb{Z}$ - independent and such that*

$$\left[E_H(\mathbb{K}_n) \ : \ \langle \mathcal{E}_n \rangle_{\mathbb{Z}[T]}\right] < \infty.$$

In particular $N_{n,0}(d_i) = 1$ and the norm is also the polynomial of minimal degree in $\mathbb{Z}[T]$ which annihilates d_i. The ranks are

$$\begin{aligned} \mathbb{Z}\text{-}rk(E(\mathbb{K}_n)) &= \mathbb{Z}\text{-}rk(E_H(\mathbb{K}_n)) + \mathbb{Z}\text{-}rk(E(\mathbb{K}); \\ \mathbb{Z}_p\text{-}rk(\overline{E(\mathbb{K}_n)}) &= \mathbb{Z}_p\text{-}rk(\overline{E_H(\mathbb{K}_n)}) + \mathbb{Z}_p\text{-}rk(\overline{E(\mathbb{K})}). \end{aligned} \tag{25}$$

Moreover

$$\mathbb{Z}\text{-}rk\left(E_H(\mathbb{K}_n)/E(\mathbb{K}_n)^T\right) = r. \tag{26}$$

For $\mathbb{Z}_p$ - ranks, we have $\mathbb{Z}\text{-}rk(E_H(\mathbb{K}_n)) = \mathbb{Z}_p\text{-}rk(\overline{E_H(\mathbb{K}_n)})$

Proof. We start with a computation of ranks: if $r = |G|$, then there is a $\mathbb{Z}$-base $\mathcal{E}_0 = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r-1}\}$ for $E(\mathbb{K})$, by Dirichlet's unit Theorem. Suppose that $[\mathbb{K}_n : \mathbb{K}] = p^{n'}, n' = n - k$. Then

$$\mathbb{Z}\text{-rk}(E(\mathbb{K}_n)) = R - 1 = (p^{n'} - 1)r + (r - 1), \quad R = p^{n'}r.$$

This equation reflects already the first claim in (25): one may choose a Minkowski unit in E_n and deduce the relation between $\mathbb{Z}$-ranks. The relation is conserved, when passing to p - adic completions in $U(\mathbb{K}_n)$, and this proves (25). Since $\mathbb{K}_n/\mathbb{K}$ is galois, there is a Minkowski unit $D \in E(\mathbb{K}_n)$ such that $\left[E(\mathbb{K}_n) : D^{\mathbb{Z}[\text{Gal}(\mathbb{K}_n/\mathbb{Q})]}\right] < \infty$. Let $e = N_{n,0}(D)$; then $N_{n,0}(D^{p^{n'}}/e) = 1$ and thus $D' = D^{p^{n'}}/e \in E_H(\mathbb{K}_n)$ and since D is Minkowski, it follows also that $\left[E_H(\mathbb{K}_n) : (D')^{\mathbb{Z}[T]}\right] < \infty$. We may thus even choose $d_i = (D')^{\sigma_i}, \sigma_i \in G$. The ranks occurring in (26) can now be estimated by using the unique D'; thus

$$\begin{aligned}\mathbb{Z}\text{-rk}(E_H(\mathbb{K}_n)/E(\mathbb{K}_n)^T &= \mathbb{Z}\text{-rk}\left((D')^{\mathbb{Z}[T,G]}/D^{T\mathbb{Z}[G,T]}\right)\\ &= \mathbb{Z}\text{-rk}\left(\mathbb{Z}[T,G]/(T\mathbb{Z}[T,G])\right) = |G| = r.\end{aligned}$$

This proves (26). Passing now to $\mathbb{Z}_p$ - ranks, from the fact that the Leopoldt defect was assumed stationary, we deduce in particular that $\mathbb{Z}_p\text{-rk}(\overline{E_H(\mathbb{K}_n)}) = \mathbb{Z}\text{-rk}(E_H(\mathbb{K}_n))$ and this equality applies to all proper submodules of $E_H(\mathbb{K}_n)$ and their completions. □

The proof of the Theorem 4 will follow if we show that the assumption that **B** is not finite, leads to a contradiction with (26): there is a defect in the rank of $E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n)$, which is induced by the primes $\wp_n$ with $\wp_n^{\text{ord}(\wp_n)} = (\pi), \pi \in \mathbb{K}$.

Let $(\alpha) \subset \mathbb{K}_n$ be an ambig ideal which is not ramified. Then there is an ideal $\mathfrak{A} \in a_0 \in A_0$ such that $(\alpha) = \mathfrak{A} \cdot \mathcal{O}(\mathbb{K}_n)$, so the primes in a_0 capitulate completely in $\mathbb{K}_n$. Since A_0 is a finite group, there is a fixed $m > 0$, depending only on $\mathbb{K}$, such that all the primes from classes in A_0 that capitulate completely in $\mathbb{K}_\infty$, already capitulate in $\mathbb{K}_m$. Therefore $\alpha \in E(\mathbb{K}_n) \cdot \mathbb{K}_m$ and in general, if $(\beta) \subset \mathcal{O}(\mathbb{K}_n)$ is any ambig ideal, then

$$\beta \in \mathbb{K}_m^\times \cdot E'(\mathbb{K}_n). \tag{27}$$

The units in $E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n)$ are of particular interest: they are characterized by the following

Lemma 13. *Notations being like above,*

$$E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n) \subset \left(E_H(\mathbb{K}_m) \cdot (E'(\mathbb{K}_n))^T\right)/E^T(\mathbb{K}_n),$$

and

$$E_H(\mathbb{K}_n)^{N_{m,0}}/E(\mathbb{K}_n)^{\omega_m} \subset (E'(\mathbb{K}_n))^{\omega_m}/E(\mathbb{K}_n)^{\omega_m}. \tag{28}$$

Proof. Let $e \in E_H(\mathbb{K}_n) \setminus E(\mathbb{K}_n)^T$. Then by Hilbert 90, $e = \gamma^T$ and (γ) is an ambig ideal, thus the product of a p - unit, by an ideal of $\mathbb{K}$ that capitulates in $\mathbb{K}_m$. Since all the ideals of classes in A_0 which capitulate, do so already in $\mathbb{K}_m$, if follows that $\gamma = c_m \cdot \mathfrak{p}$ with $c_m \in \mathbb{K}_m$ and $\mathfrak{p} \in E'(\mathbb{K}_n)$. Hence, $e = c_m^T \cdot \mathfrak{p}^T \in E_H(\mathbb{K}_m) \cdot (E'(\mathbb{K}_n))^T$, which is the first claim. Applying the norm $N_{m,0} = \mathbf{N}_{\mathbb{K}_m/\mathbb{K}}$ to this equation, c_m^T is annihilated and we obtain $e^{N_{m,0}} = \mathfrak{p}^{\omega_m}$. Therefore, $E_H^{N_{m,0}} \subset (E'(\mathbb{K}_n))^{\omega_m} \cdot E(\mathbb{K}_n)^{\omega_m}$, which implies the claim of (28). □

5.3. **The hypothesis of infinite B.** We now apply the assumption $|\mathbf{B}| = \infty$ for the estimation of the rank $\mathbb{Z}\text{-rk}(E'(\mathbb{K}_n)^T/E(\mathbb{K}_n)^T)$. This will raise a contradiction between (28) and (26).

We let $b = (b_n)_{n\in\mathbb{N}} \in \mathbf{B}$ be a sequence of infinite order, such that $\wp_n \in b_n$ for some primes $\wp_n \subset \mathbb{K}_n$ above p. Let $\beta_0 \in \mathbb{Q}_p[G]$ be a generator of the annihilator $b^\top \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, defined above and p^l such that $\beta = p^l\beta_0 \in \mathbb{Z}_p[G] \setminus p\mathbb{Z}_p[G]$. The orthogonal complement of $\beta_0\mathbb{Q}_p[G]$ in $\mathbb{Q}_p[G]$ is generated by $\alpha_0 = 1 - \beta_0 \in \mathbb{Q}_p[G]$. Let $p^k = \text{ord}(\wp_0)$ and $\pi \in \mathbb{K}$ with $(\pi) = \wp_0^{p^k}$. Since the order of b_n diverge, $\text{ord}(b_n) = p^{z+n'}$ and $\wp_n^{p^{n'+z}} = (\pi)$. Furthermore, for a large fixed M, say $M > n+z+l$, we let $\alpha_M, \beta_M \in \mathbb{Z}[G]$ be rational approximants of α, β to order p^M, so $\beta_M \cdot \alpha_M = p^M r, r \in \mathbb{Z}[G]$. By Lemma (11), β_M annihilates also $\wp_n$ and thus $\wp_n^{\beta_M} = (\nu_n)$ for a p - unit $\nu_n \in E'(\mathbb{K}_n)$. Then $e_n := \nu_n^T \in E_H(\mathbb{K}_n)$: it is a unit, since $\wp_n^T = (1)$ and

$$\mathbf{N}_{\mathbb{K}_n/\mathbb{K}}(e_n) = \left(\mathbf{N}_{\mathbb{K}_n/\mathbb{K}}(\nu_n)\right)^T = 1.$$

Moreover,

$$(\nu_n^{\alpha_M}) = (\wp_n^{p^M r}) = \pi^{r'}.$$

It follows that there is a unit $\varepsilon \in E_n$ with $\nu_n^{\alpha_M} = \varepsilon \cdot \pi^{r'}$ and thus

$$e_n^{\alpha_M} = \varepsilon^T \in E_H(\mathbb{K}_n) \cap E(\mathbb{K}_n)^T. \tag{29}$$

Applying $\nu_{m,0}$, since $\omega_m = T\nu_{m,0}$, we obtain $e_n^{\alpha_M\nu_{m,0}} \subset E(\mathbb{K}_n)^{\omega_m}$. We claim that in general

Lemma 14. *Notations being like above,*

$$\mathbb{Z}\text{-}rk(E_H(\mathbb{K}_n)/E(\mathbb{K}_n)^T) = \mathbb{Z}\text{-}rk\left(e_n^{\mathbb{Z}[G]}/(e_n^{\mathbb{Z}[G]} \cap E(\mathbb{K}_n)^T)\right). \tag{30}$$

Proof. Let $\mathfrak{p} \in E'(\mathbb{K}_n)$ be a p - unit, thus $(\mathfrak{p}) = \wp_n^\theta$ for a $\theta \in \mathbb{Z}[G^+]$. Since $\mathfrak{p}$ is principal, it follows that $\theta \in b_n^\top$ and from point 3. of Lemma 10 we know that $p^l\theta \in (\beta_M, p^{n+k+l})$.

Hence $p^l\theta = \beta_M r_1 + p^{n'+k+l} \cdot r_2; r_1, r_2 \in \mathbb{Z}[G,T]$, and

$$\begin{aligned} (\mathfrak{p}^{p^l}) &= \wp_n^{p^l\theta} = \wp_n^{\beta_M r_1} \cdot \wp_n^{r_2 p^{n'+k+l}} \\ &= \left(\nu_n^{r_1} \cdot \pi^{p^l r_2}\right) \end{aligned}$$

Passing to algebraic numbers, we find a unit ε such that

$$\mathfrak{p}^{p^l} = \varepsilon \cdot \nu_n^{r_1} \cdot \pi^{p^l r_2},$$

and after applying T to this identity and using (29), we obtain

$$e' = \mathfrak{p}^{Tp^l} = \varepsilon^T \cdot e_n^{r_1} \in e_n^{\mathbb{Z}} \cdot E(\mathbb{K})^T.$$

Therefore

$$(31)\qquad \begin{array}{rcl} E'(\mathbb{K}_n)^{p^l T} & \subset & e_n^{\mathbb{Z}} \cdot E(\mathbb{K}_n)^T, \quad \text{and} \\ E_H(\mathbb{K}_n) & \subset & E_H(\mathbb{K}_m) \cdot e_n^{\mathbb{Z}} \cdot E(\mathbb{K}_n)^T. \end{array}$$

Finally, since $\omega_m = T \cdot \nu_{m,0}$, we may apply $\nu_{m,0}$ to the last identity and annihilate $E_H(\mathbb{K}_m)$. Note that $e_n^{\omega_m} = e_n^{p^m + O(T)}$ and thus

$$\begin{array}{rcl} e_n^{\omega_m \mathbb{Z}[G,T]} & \subset & e_n^{\mathbb{Z}[G]} \cdot E(\mathbb{K}_n)^T, \quad \text{and} \\ (D')^{\nu_m} & = & (D')^{p^m} \cdot E^{Th(T)} \in e_n^{\mathbb{Z}[G]} \cdot E(\mathbb{K}_n)^T \end{array}$$

which implies that

$$\mathbb{Z}\text{-rk}(E_H(\mathbb{K}_n)/E(\mathbb{K}_n)^T) \leq \mathbb{Z}\text{-rk}(e_n^{\mathbb{Z}[G]}/(e_n^{\mathbb{Z}[G]} \cap E(\mathbb{K}_n)^T).$$

The inequality $\mathbb{Z}\text{-rk}(E_H(\mathbb{K}_n)/E(\mathbb{K}_n)^T) \geq \mathbb{Z}\text{-rk}\left(e_n^{\mathbb{Z}[G]}/(e_n^{\mathbb{Z}[G]} \cap E(\mathbb{K}_n)^T)\right)$ is trivial, since $e_n \in E_H(\mathbb{K}_n)$. From the two we obtain the rank equality in (30). □

5.4. **Proof of the Theorem 4.** The Theorem 4 follows from the above:

Proof. Let

$$\mathfrak{b}(\mathbb{K}) = ess.\ p\text{-rk}(\mathbf{B}) = r - \mathbb{Z}_p\text{-rk}(\alpha \mathbb{Z}_p[G]) = r - \mathbb{Z}\text{-rk}\left(e_n^{\mathbb{Z}[G]}/(e_n^{\mathbb{Z}[G]} \cap E(\mathbb{K}_n)^T)\right).$$

Then

$$\mathbb{Z}\text{-rk}\left(e_n^{\mathbb{Z}[G]}/(e_n^{\mathbb{Z}[G]} \cap E(\mathbb{K}_n)^T)\right) = r - \mathfrak{B}(\mathbb{K}).$$

From (26), we have $\mathbb{Z}\text{-rk}\left(E_H(\mathbb{K}_n)/E_H(\mathbb{K}_n)^T\right) = r$, while (29) and (30) together with the above yield the value $r - \mathfrak{B}(\mathbb{K})$ for this rank. It follows that $\mathfrak{B}(\mathbb{K}) = 0$, which completes the proof of the Theorem 4. □

Observe that the defect $\mathfrak{B} = ess.\ p\text{-rk}(\mathbf{B})$ in the rank of $E_H(\mathbb{K}_n)/E^T(\mathbb{K}_n)$ is connected to the fact that the p - units are localized in $E'(\mathbb{K}) \cdot (E'(\mathbb{K}_n))^\beta$, which is a consequence of the fact that the ramified ideals do not capitulate. We note that Theorem 4 confirms the Greenberg conjecture for $\mathbf{B} \subset A$.

6. Appendix B: Units in CM fields

The results that we develop in the rest of this paper hold for general galois extensions containing the p-th roots of unity, thus for fields $\mathbb{K}$ as considered above. The apparatus of proof is more involved though. Therefore we assume from now on that $\mathbb{K}$ is a CM galois extension of $\mathbb{Q}$ which contains the p-th roots of unity. Thus, complex conjugation is an element $\jmath \in \Delta = \text{Gal}(\mathbb{K}/\mathbb{Q})$ and it naturally splits groups and

$\Lambda[\Delta]$ - modules related to $\mathbb{K}_\infty/\mathbb{K}$ in their plus and minus parts. We have for instance $A = A^+ \oplus A^-$, where $A^+ = (1+\jmath)A, A^- = (1-\jmath)A$; here we use the fact that p is odd, otherwise one should divide by 2. Also, $\mathbb{H}^+ = \mathbb{H}^{\varphi(A^-)}$ and $\mathbb{H}^- = \mathbb{H}^{\varphi(A^+)}$.

6.1. **Order reversal in Kummer extensions.** It is useful to consider primary parts in more depth. We note the following *phenomenon of order reversal in Kummer pairings.* Let $f \in \Lambda$ be a distinguished polynomial and suppose that $a = (a_n)_{n\in\mathbb{N}} \in A^-\setminus(A^-)^p$ has characteristic polynomial f^k for $k > 1$. Let $\mathbf{A} = (\Lambda a)^{(c)}$ be the p-coalescent hull of Λa; this is a $\mathbb{Z}_p$-complementable module, thus $A^- = \mathbf{A} \oplus \mathbf{A}'$, for a $\mathbb{Z}_p$-module $\mathbf{A}' \subset A^-$. We let $\mathbb{H}_a = (\mathbb{H}^-)^{\mathbf{A}'} \subset \mathbb{H}^-$, a field with $\mathrm{Gal}(\mathbb{H}_a/\mathbb{K}_\infty) \cong \Lambda a$. For $n > 0$ let $\mathbb{L}_n \subset \mathbb{H}_{a_n}$ be a maximal cyclic extension such that $\mathbb{H}_{a_n} = \mathbb{L}^\Lambda$. Let $p^{n+z(a)}$ be the order of a_n and $\mathbb{L}_n = \mathbb{K}_{n'}[\beta^{1/p^{n+z(a)}}], n' = nz(a)$ and $r = p\text{-rk}(\Lambda a_n) = k\cdot\deg(f)$; then $B = \{\beta, \beta^\tau, \ldots, \beta^{\tau^{r-1}}\}$ span a radical of $\mathbb{H}_{a,n}$. Let $\Delta_n = \mathrm{Gal}(\mathbb{H}_{a_n}/\mathbb{K}_{n'}) \cong \mathbf{A}_n$ and $R_n = \mathcal{R}(\mathbb{H}_{a,n}/\mathbb{K}_n)$, so $\beta^{1/p^{n+z(a)}} \in R_n \cdot (\mathbb{K}_{n'})^\times$. By duality, we have $\beta^{f^k(T^*)} \in \mathbb{F}_{n'}^{p^{n+z(a)}}$.

In terms of Kummer pairing, we have the following fact: if

$$\langle \beta^{(f(T^*))^i}, \mu\rangle_{\mathbb{H}_{a_n}} = \zeta_{p^m},$$

for a $\mu \in \Delta$ and $0 \leq i < k$, then $\mu \notin \Delta_n^{(f(T))^{k-i}}$. The reason is simply that for $\mu = \nu^{(f(T))^{k-i}}$ we would have:

$$\begin{aligned}\langle \beta^{(f(T^*))^i}, \mu\rangle_{\mathbb{L}'_m} &= \langle \beta, \mu^{(f(T))^i}\rangle_{\mathbb{L}'_m} = \langle \beta, \nu^{(f(T))^{k-i+i}}\rangle_{\mathbb{L}'_m}\\ &= \langle \beta, 1\rangle_{\mathbb{L}'_m} = 1,\end{aligned}$$

which contradicts the choice of μ.

Therefore we have the following order reversing property

Lemma 15. *Let $f \in \mathbb{Z}_p[T]$ be a distinguished polynomial and $a \in A^- \setminus A^p$ have characteristic polynomial f^k for $k > 1$. Let $\mathbb{H}_{a,n}$ be the subfield of $\mathbb{H}_n$ defined above, with $\Delta_n =$ Gal$(\mathbb{H}_{a,n}/\mathbb{K}_{n'}) \cong \mathbf{A}_n$ and $R_n = \mathcal{R}(\mathbb{H}_{a,n}/\mathbb{K}_n)$ be the radical. Then*

$$\mathbb{H}_{a,n}^{\varphi\left(\mathbf{A}_n^{f(T)^i}\right)} = \mathbb{K}_{n'}[R_n^{f(T^*)^{k-i}}], \quad i = 0, 1, \ldots, k-1. \tag{32}$$

The Lemma 15 completely describes the class field associated to a submodule of the primary part $A^-(f)$. In general, we have:

Proposition 2. *Notations being like above, let $a = (a_n)_{n\in\mathbb{N}} \in A^- \setminus A^p$ have characteristic polynomial $g \in \mathbb{Z}_p[T]$ and $\mathbf{A} = (\Lambda a)^{(c)}$. Then there is a canonic injective sequence of class fields $\mathbb{H}_{a,n} \subset \mathbb{H}_n$ with*

(i) *Gal$(\mathbb{H}_{a,n}/\mathbb{K}_n) \cong \Lambda a_n$;*

(ii) *$\mathbb{H}_{a,n} \subset \mathbb{H}_{a,m}$ for $0 \leq n < m$.*

(iii) *If $g = f^k$, $k > 1$ is the power of a prime polynomial, then (32) holds.*

(iv) *Let $n' = \max(n, n+z(a))$, with $z(a)$ defined above. The radicals $R_n = \mathcal{R}(\mathbb{H}_{a,n}/\mathbb{K}_n$ form a projective sequence. If $\mathbb{H}_a = \cup_n \mathbb{H}_{a,n}$ and $R = \varprojlim_n R_n$, then the projective - projective pairing pairing $\langle ., . \rangle_{\mathbb{H}_a} : \mathbf{A} \times R \to W$ verifies*

$$
\begin{aligned}
(33)\ \mathbb{H}_a{}^{\varphi\left(\mathbf{A}^{f(T)^i}\right)} &= \mathbb{K}_\infty[R^{f(T^*)^{k-i}}], \quad i = 0, 1, \ldots, k-1, \\
\langle a, \rho \rangle_{\mathbb{H}_a} &= 0 \quad \textit{for} \quad a \in \mathbf{A}[f^j], \rho \in R[f^l],\ j + l > k+1.
\end{aligned}
$$

6.2. **Global and local units and related fields.** We recall that $E_n, E'_n \subset \mathbb{K}_n$ are the units, resp. the p - units of $\mathbb{K}_n$ and

$$U_n = \mathcal{O}(\mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \prod_{\wp \supset (p)} \mathcal{O}(\mathbb{K}_{n,\wp})$$

is the product of the units in all the completions of $\mathbb{K}_n$ at primes above p. The algebra $\mathfrak{K}_n = \mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a galois algebra with group containing $\text{Gal}(\mathbb{K}_n/\mathbb{Q})$ and $\mathbb{K}_n \hookrightarrow \mathfrak{K}_n$ is dense in the product topology.

Let $\wp \in \mathbb{K}$ be a prime above p and $C = \Delta/D_\wp$ be a set of coset representatives of the decomposition group of $\wp$ in Δ. Then $P = \{\nu\wp : \nu \in C\}$ is the set of all the primes of $\mathbb{K}$ above p and by assumption, these primes are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. A uniformizor $\pi \in U_n$ is an element whose embeddings $\iota_{\nu\wp}(\pi) \in \mathbb{K}_n n, \nu\wp$ are uniformizors of the respective completions, for all $\nu \in C$. Herewith we let

$$
\begin{aligned}
U_n^{(1)} &= \{u \in U_n : u - 1 \equiv 0 \bmod \pi\}, \\
U'_n &= \{u \in U_n^{(1)} : \mathbf{N}_{\mathbb{K}_n/\mathbb{Q}}(u) = 1\}
\end{aligned}
$$

If $\mathbf{K}/\mathbb{Q}_p$ is a finite local extension, we also write $\mathbf{K}_n = \mathbf{K}[\mu_{p^{n+1}}]$ and $U_n, U_n^{(1)}, U'_n$ are defined like in the "global" case. Then

Lemma 16. *Let $\mathbf{K}/\mathbb{Q}_p$ be a local finite galois extension with $\mathbf{K} \cap \mathbb{Q}_p[\mu_{p^\infty}] = \mathbb{Q}_p[\mu_{p^{k+1}}]$. Then the system $(U'_n)_{n \in \mathbb{N}}$ defined above is norm coherent and the norm is surjective at all levels, that is*

$$\mathbf{N}_{\mathbf{K}_m/\mathbf{K}_n}(U'_m) = U'_n, \quad \forall m > n > 0.$$

Proof. This follows from class field theory: $\text{Gal}(\mathbf{K}/\mathbb{Q}_p)$ acts by conjugation on the groups $\Gamma_{n,m} = \text{Gal}(\mathbf{K}_n/\mathbf{K}_m)$, which are fixed under this action. By class field theory,

$$\Gamma_{n,m} \cong \mathbf{K}_m^\times / \mathbf{N}_{\mathbf{K}_n/\mathbf{K}_m}(\mathbf{K}_n^\times). \tag{34}$$

But $\mathbf{K}_n/\mathbf{K}_m$ is totally ramified, so we have

$$\mathbf{K}_m^\times / \mathbf{N}_{\mathbf{K}_n/\mathbf{K}_m}(\mathbf{K}_n^\times) = U_m^{(1)} / \mathbf{N}_{\mathbf{K}_n/\mathbf{K}_m}(U_n^{(1)}),$$

and (34) implies that the norm residue group is $\mathrm{Gal}(\mathbf{K}/\mathbb{Q}_p)$ - invariant, and it thus is a quotient of $\mathbb{Z}_p$. Since $\mathbf{N}(U'_n) = \{1\}$ by definition, it follows that the restriction of the norm to U'_n is indeed surjective. □

We now show that there are local Minkowski units and describe their relation to the global ones. Serre proves in [10], §1.4, Proposition 3, in the case when $\mathbf{K}/\mathbb{Q}_p$ is a local field, that the group $U^{(1)}(\mathbf{K})$ contains a cyclic $\mathbb{Z}_p[G]$ module of finite index, which is isomorphic to $\mathbb{Z}_p[G]$: thus $U^{(1)}(\mathbf{K})$ is quasi - cyclic.

Using this result one obtains units $\xi \in U$ generating $\mathbb{Z}_p[G]$ - modules of finite index $\underline{U} \subset U$, which we call local Minkowski units for $\mathbf{K}$. Let $\wp \in P$ be fixed and $\upsilon \in \mathbb{K}_{\wp}$ be a local Minkowski unit, according to Serre. Then we define $\xi = \xi(\upsilon) \in U$ and $\tilde{\rho} \in U$ by:

$$\iota_{\tau\wp}(\xi) = \begin{cases} \upsilon & \text{for } \tau = 1, \\ 1 & \text{for } \tau \in G, \tau \neq 1. \end{cases} \tag{35}$$

$$\iota_{\tau\wp}(\tilde{\rho}) = \begin{cases} 1 & \text{for } \tau = 1, \\ 0 & \text{for } \tau \in G, \tau \neq 1. \end{cases} \tag{36}$$

The set C acts on ξ and for $\sigma \in C$, the unit ξ^{σ} satisfies:

$$\iota_{\tau\wp}(\xi) = \begin{cases} \upsilon & \text{for } \tau = \sigma, \\ 1 & \text{for } \tau \in G, \tau \neq \sigma. \end{cases}$$

We denote units the generators $u \in \underline{U}$ for U by *local Minkowski units*. The previous construction shows that such units exist. Since $\mathbf{N}_{\mathbb{K}_n/\mathbb{Q}}(E_n) = \{1\}$, local units of norm one are interesting for the embedding $E_n \hookrightarrow U'_n$. The module $U'_n \subset U_n$ is a quasi - cyclic $\mathbb{Z}_p[\Delta]$ submodule of U_n with $U_n^{(1)}/U'_n = U^{(1)}(\mathbb{Z}_p) \cong \mathbb{Z}_p$. For a $\mathbb{Z}_p$ - module M we denote $\tilde{M} = M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$: thus $\tilde{U}' \cong (1 - \mathbf{N}_{\mathbb{K}/\mathbb{Q}}/|\Delta|)\mathbb{Q}_p[\Delta]$, the last being a two sided module in $\mathbb{Q}_p[\Delta]$. For any $\mathbb{K}$ we have $\overline{E}(\mathbb{K}) \subset U'$ and therefore $U^{(1)}(\mathbb{Z}_p)$ is mapped injectively in Δ by the Artin map. Let $\xi_0 \in U'_0 \setminus U'^p_0$ be a local Minkowski unit for U'_0. From Lemma 16 we conclude that there is a norm coherent system $(\xi_n)_{n\in\mathbb{N}}, \xi_n \in U'_n$ in which ξ_n are local Minkowski units for U'_n.

The global units E_n embed diagonally in U_n and their completion in the product topology is written $\overline{E}_n \subset U_n$. There may be a rank loss in this completion step and the possible difference

$$\mathcal{D}(\mathbb{K}_n) := \mathbb{Z}\text{-rk}(E_n) - \mathbb{Z}_p\text{-rk}(\overline{E}_n)$$

is called the Leopoldt defect, since Leopoldt conjected in 1962 the vanishing of $\mathcal{D}(\mathbb{K}_n)$, at least for abelian extensions of $\mathbb{Q}$. After the proof of this fact in 1967, by Baker and Brumer, the fact that $\mathcal{D}(\mathbb{K}) = 0$ for all number fields remained as an open conjecture, which also caries the name of Leopoldt. It is known ([12], Proposition) that the Leopoldt defect $\mathcal{D}(\mathbb{K}_n)$ is stationary for sufficiently large n; we assume that $\mathbb{K}$ is chosen such that $\mathcal{D}(\mathbb{K}_n) = \mathcal{D}(\mathbb{K})$. As a consequence, we have

$$\mathbb{Z}\text{-rk}(E_n/E_0) = \mathbb{Z}_p\text{-rk}(\overline{E}_n/\overline{E}_0).$$

We define $E_\infty = \cup_n E_n$ and $U_\infty = \cup_n U_n$; this traditional definition as injective limits is in contrast with our approach, but it allows to use in a first step the commonly established results. It is a known fact that

Fact 2. *The module $V = U'_\infty/(U'_\infty \cap \overline{E}_\infty)$ is a finitely generated Λ - torsion module. We let $F_E \in \mathbb{Z}_p[T]$ be its minimal polynomial and p^m be the exponent of the μ - part of V. Note that the radical $R = \mathcal{R}(\mathbb{H}_E/\mathbb{K}_\infty) \sim V$.*

Let $G_E|F_E$ is the largest factor that is not divisible by T. The condition $T^2 \nmid F_E$ is a consequence of Leopoldt's conjecture, so it must be assumed separately. As a consequence of the above, we have $(U'_n)^{p^m F_E(T)} \subset \overline{E}_n$.

The question whether E_n also contain norm coherent sequences of Minkowski units is treated in the following

Proposition 3. *Notations being like above, we assume that $T^2 \neq F_E(T)$. Then there is a norm coherent sequence of Minkowski units $\delta_n \in E_n$.*

Proof. Let $e_n \in E_n \setminus E_n^p$ be a Minkowski unit and $e_0 = N_{n,0}(e_n)$, which is a Minkowski unit for $E(\mathbb{K})$. Let $U''_n = \{x \in U_n : N_{n,0}(x) = 1\} \subset U'_n$; we let ξ_n be a norm coherent system of local Minkowski units for U'_n and ϑ_n be an induced system of generators of U''_n. We may assume that ξ_0 is such that there is an idempotent $\alpha_0 \in \mathbb{Q}_p[\Delta]$ with $\alpha = p^k\alpha_0 \in \mathbb{Z}_p[\Delta]$ and such that $\xi_0^\alpha = e_0$; the idempotent is related to the annihilator ideal of $e_0 \in \overline{E}(\mathbb{K})$.

We have seen that $\mathbb{Z}_p\text{-rk}(U''_n) = \mathbb{Z}_p\text{-rk}(\overline{E}_{H,n})$. The module $\Lambda \supset \mathbb{Z}_p$ acts on the completion of E_n and by choosing $e_n \in E_n \setminus E_n^p$ we have then $e_n^\Lambda \supset \overline{E}_{H,n} \supset (U'')_n^{p^m G_E(T)}$. Therefore, there is thus a $\beta \in (\mathbb{Z}_p[\Delta \times \Gamma])^\times$ such that

$$e_n^{\beta\Lambda} \supset (U'')_n^{p^m G_E(T)} \supset \vartheta_n^{p^m G_E(T)\Lambda}.$$

It follows that $\xi_n^{(\alpha+T\beta)p^m G_E(T)} \in e_n^\Lambda$. Since this holds for all n, the ξ_n are norm coherent local Minkowski units, and $m, G_E(0)$ are p - adic constants that do not depend on n, it follows that

$$[E_0 : N_{n,0}(\overline{E}_n)] < \infty, \quad \forall n \geq 0.$$

This gives the following inductive construction of norm coherent sequences of global Minkowski units: start by $\delta_0 \in \xi_0^{\alpha p^m G_E(0)\mathbb{Z}_p[\Delta]}$ and $\delta_0 \in E(\mathbb{K})$ is Minkowski. Then, for arbitrary $n > 0$, we have seen that there is a $\delta_n \in \overline{E}_n$ with $N_{n,0}\delta_n = \delta_0$. We show that we may choose $\delta_n \in E_n$. But this follows from $\overline{(N_{n,0}E_n)} = N_{n,0}\overline{E}_n$, which is a consequence of the fact that $\Gamma \hookrightarrow \mathrm{Gal}(\mathfrak{K}_n/\mathbb{Q}_p)$. We may thus find for arbitrary large n a unit $\delta_n \in E_n$ which is Minkowski and is sent by the norm to δ_0. Applying the same result to E_n, we find $\delta_{2n} \in E_{2n}$ which is Minkowski and sent by the norm to δ_n, etc. By induction, this yields a norm coherent sequence of units $\delta_m \in E_m$ with $N_{m,n}(\delta_m) = \delta_n$ for all $m > n \geq 0$. □

As a consequence we have

Corollary 2. *Notations being like above, there is an $n_1 > 0$ such that*

$$N_{m,n}(E_m) \cdot E_{n_1} = E_n \quad \text{for all} \quad m > n > n_1.$$

In particular, if $T^2 \nmid F_E(T)$, both U_∞ and $E_\infty, \overline{E}_\infty$ can be defined as projective limits.

Proof. Since $N_{n,0}(E_n)$ has finite index in E_0, it follows that the indices $[E_n : N_{n+1,n}(E_{n+1})]$ must stabilize to 1 beyond some level, which is n_1. Thus $[N_{m,n}(E_m) \cdot E_{n_1} : E_n] = 1$ for all $m > n > n_1$. We obtain a projective system with respect to the norms. □

6.3. **The p - ramified extensions of the minus part.** The extension $\Omega_n/\mathbb{K}_n$ is an infinite extension and $\mathbb{Z}_p$-rk$(\mathrm{Gal}(\Omega_n/\mathbb{K}_n)) = \mathcal{D}(\mathbb{K}) + r_2(\mathbb{K}_n) + 1$. Here $r_2(\mathbb{K}_n)$ is the number of pairs of conjugate complex embedding and the 1 stands for the extension $\mathbb{K}_\infty/\mathbb{K}_n$, thus

$$\mathbb{Z}_p\text{-rk}\left(\mathrm{Gal}((\Omega_n\mathbb{K}_\infty)/\mathbb{K}_\infty)\right) = r_2(\mathbb{K}_n) + \mathcal{D}(\mathbb{K}).$$

It is a folklore fact, which we shall prove for completeness below, that the *regular* part $r_2(\mathbb{K}_n)$ in the above rank stems from $\Omega_n \cap \Omega_E$. The intersection can be described precisely by:

Lemma 17. *Notations being like above, we define for $m > n$: $\mathcal{E}'_m = \{e^{N^*_{m,n}} : e \in E_m\}$ and $\mathcal{E}_m = \mathcal{E}'_m \cdot (E_m)^{p^m}$; here $*$ is the Iwasawa involution* [9], *p. 150. Then*

$$\Omega_n^- \cdot \mathbb{K}_\infty = \mathbb{H}_n \cdot \cup_m \mathbb{K}_m[\mathcal{E}_m^{1/p^m}] \times \mathbb{T}_n, \tag{37}$$

where $\mathbb{T}_n/\mathbb{K}_n$ is an extension with group Gal$(\mathbb{T}_n/\mathbb{K}_n) \cong (\mathbb{Z}/(p^n{\cdot}\mathbb{Z}))^{s-1}$, $s = |C|$, which shall be described in the proof.

Proof. We show that the subgroups $\mathcal{E}_m$ give an explicite construction of $\Omega^- \cap \Omega_1$, as radicals. The proof uses reflection, class field theory and some technical, but strait forward estimations of ranks.

A classical result from class field theory [9], , says that

$$\mathrm{Gal}(\Omega_n/\mathbb{H}_n) \cong U_n^{(1)} / \left(\overline{E}_n \cap U_n^{(1)} \right).$$

Since $(\mathbb{U}_n^{(1)})^- \cap \overline{E}_n = \mu_{p^n}$, it follows that $\mathrm{Gal}(\Omega_n/\mathbb{H}_n) = (U_n^{(1)})^- \times \mathcal{T}(U_n^-)/\mu_{p^n}$, where the torsion part $\mathcal{T}(U_n^-) = \prod_{\nu \in C} \mu_{p^n}$ is the product of the images of the p^n - th roots of unity in the single completions, factored by the diagonal embedding of the global units.

For the proof, we need to verify that ranks are equal on both sides. Let $\pi_\nu \in \mathbb{K}_n$ be a list of integers such that $(\pi_\nu) = \wp^{\nu h}$ for h the order of the class of $\wp^\nu$. Then we identify immediately $\mathbb{T}_n = \prod_{\nu \in \mathbb{C}} \mathbb{K}_n[\pi_\nu^{1/p^n}]$ as a p - ramified extension with group $\mathrm{Gal}(\mathbb{T}_n/\mathbb{K}_n) = \mathcal{T}(U_n^-)/\mu_{p^n} \subset \mathrm{Gal}(\Omega_n/\mathbb{H}_n)$.

A straight forward computation in the group ring yields that $T^* x \equiv 0 \bmod (\omega_n, p^n)\Lambda$ iff $x \in N_{n,0}^* \Lambda$. On the other hand, suppose that $x \in \mathcal{R}((\Omega_n \mathbb{K}_m)/\mathbb{K}_m) \cap E_m$. This observation and Kummer theory imply that $x^{\omega_n^*} \in \mathcal{E}_m$. Therefore $\cup_m \mathbb{K}_m[\mathcal{E}_m^{1/p^m}] = \Omega_n^- \cap \Omega_E$. Comparing ranks, we see that if $\Omega_n^- \cdot \mathbb{K}_\infty \neq \mathbb{T}_n \cdot \mathbb{H}_n \cdot \Omega_n^- \cap \Omega_E$, then there is an extension $\Omega_n^- \supset \Omega_n'' \supsetneq (\Omega_n^- \cap \Omega_E)$, such that

$$\mathbb{Z}_p\text{-rk}(\mathrm{Gal}(\Omega_n''/\mathbb{K}_\infty)) = r_2(\mathbb{K}_n) = \mathbb{Z}_p\text{-rk}(\mathrm{Gal}(\Omega_n^- \cap \Omega_E)).$$

Since $\Omega_E \subset \Omega$ it follows that $\mathrm{Gal}((\Omega_n^- \cap \Omega_E)/\mathbb{K}_\infty)$ is a factor of $\mathrm{Gal}(\Omega_n^-/\mathbb{K}_\infty)$ and also of $\mathrm{Gal}(\Omega_n''/\mathbb{K}_\infty)$.

The index $[\mathrm{Gal}(\Omega_n'' : \mathbb{K}_\infty) : \mathrm{Gal}((\Omega_n^- \cap \Omega_E)/\mathbb{K}_\infty)] < \infty$ and since $\mathrm{Gal}(\Omega_n''/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$ - module and thus has no finite compact subgroups, it follows from infinite galois theory that $\Omega_n'' = \Omega_n^- \cap \Omega_E$, which completes the proof. □

An important consequence is the following:

Corollary 3. *If $\mathbb{L} \subset \mathbb{H}$ is a cyclic subextension in which not all the primes above p are split then either $\mathbb{L}/\mathbb{K}_\infty$ is finite or $\mathbb{L} \subset \mathbb{H}_{E'}$. Moreover, there is a subfield $\mathbb{H}_B^- \subset \mathbb{H}$ such that Gal$(\mathbb{H}_B^-/\mathbb{K}_\infty) \cong \mathbf{B}^-$ and in each $\mathbb{Z}_p$ - subextension of $\mathbb{H}_B$ a prime above p is inert.*

Proof. Since $\mathbf{B}^+$ is finite by Theorem 4, it follows that the only elements of infinite order of $\mathbf{B}$ lay in $\mathbf{B}^-$. If the primes $\wp^+ \in \mathbb{K}^+$ are not split in $\mathbb{K}/\mathbb{K}^+$, then they either are inert, case in which $\mathbf{B} = \mathbf{B}^+$ is finite, or they are ramified, and then $\wp = \overline{\wp}$ as ideals, for all primes $\wp \supset (p), \wp \subset \mathbb{K}$. In both cases $\mathbf{B} = \mathbf{B}^+$ is by assumption finite, so there is nothing to prove.

If $\wp^+$ is split, then complex conjugation induces pairs of primes above p which lay above the same prime of $\mathbb{K}^+$. We let $C = C^+ \cdot \{1, \jmath\}$, with the obvious meaning for C^+ and define $s = |C^+|$, the number of pairs of conjugate primes above p in $\mathbb{K}$. Let $\mathbb{M} \subset \Omega_0$ be the product of all $\mathbb{Z}_p$ - extensions of $\mathbb{K}$, so $\text{Gal}(\mathbb{M}/\mathbb{H}_0) \cong U_0^{(1)}/\overline{E}_0$ by class field theory and $\text{Gal}(\mathbb{M}^-/(\mathbb{H}_0 \cdot \mathbb{T}_0)) \cong (U_0^{(1)})^-/\mathcal{T}(U_0)$. Let φ denote the global Artin symbol and $\varphi_\wp$ the local in the completion at the prime $\wp$. Then $\varphi|_{\text{Gal}(\mathbb{M}^-/\mathbb{K}_\infty)}$ is uniquely determined by the values of $\varphi_{\nu\wp}, \nu \in C^+$, since $\varphi(x\overline{x})|_{\text{Gal}(\mathbb{M}^-/\mathbb{K}_\infty)} = 1$. Thus, omitting the finite extension $\mathbb{H}_0 \cdot \mathbb{T}_0$,

$$\text{Gal}(\mathbb{M}^-/\mathbb{K}_\infty) \sim \prod_{\nu \in C^+} U_{0,\wp}^{(1)}.$$

Now for any $\wp$, the field $\mathbb{K}_\wp$, we let $d = |D_\wp|$. It is known ([5], §12) that $\mathbb{K}_\wp$ has $d+1$ independent $\mathbb{Z}_p$ - extensions and if $\mathbf{M}$ is the product of all these extensions and $\mathbb{K}_\wp^c$ is the ramified cyclotomic $\mathbb{Z}_p$ - extension, then $\text{Gal}(\mathbf{M}/\mathbb{K}_\wp^c) \sim \mathbb{Z}_p[D_\wp]$ is a pseudocyclic $\mathbb{Z}_p[D_\wp]$ - module of maximal rank d, containing the unramified $\mathbb{Z}_p$ -extension as the one with galois group fixed by $D_\wp$. We claim that $\mathbb{H}_B = \mathbb{M}^- \cap \mathbb{H}$ is an extension with $\mathbb{Z}_p$ - free group of rank $\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{H}_B/\mathbb{K}_\infty)) = s$. Consider $\mathbb{M}_\wp^-/\mathbb{K}_\wp^c$; by comparing the rank

$$s \cdot d = r_2(\mathbb{K}) = \mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}^-/\mathbb{K}_\infty))$$

with the product of the ranks of $\text{Gal}(\mathbf{M}_\wp/\mathbb{K}_\wp^c)$ over all $\nu\wp, \nu \in C^+$, we see that $\text{Gal}(\mathbb{M}_\wp^-/\mathbb{K}_\infty) \cong \text{Gal}(\mathbf{M}_\wp/\mathbb{K}_\wp^c)$ and

$$\text{Gal}(\mathbb{M}^-/\mathbb{K}_\infty) \sim \prod_{\nu \in C^+} \text{Gal}(\mathbf{M}_{\nu\wp}/\mathbb{K}_{\nu\wp}^c).$$

In particular, there are s mutually linearly disjoint $\mathbb{Z}_p$ subextensions $\mathbb{L}_\nu \subset \mathbb{M}^-$ with $\text{Gal}(\mathbb{L}_\nu/\mathbb{K}_\infty) \cong \text{Gal}(\mathbf{M}_{\nu\wp}/\mathbb{K}_{\nu\wp}^c)$, which do not split all the primes above p and whose galois groups are equal to the decomposition groups of $\nu\wp$ in the respective extensions. Let $b_n = [\wp_n^{1-\jmath}]$ with $\wp_n$ the ramified prime of $\mathbb{K}_n$ above $\wp$. Then $\nu b = (\nu b_n)_{n \in \mathbb{N}} \in \mathbf{B}^-$ for all $\nu \in C^+$ and $\text{Gal}(\mathbb{L}_\nu/\mathbb{K}_\infty) = \varphi(\nu b)$ by restriction of the Artin symbol. We claim that $\mathbf{B}^- = \langle \nu b : \nu \in C^+ \rangle_{\mathbb{Z}_p}$. Since ι is injective in the finite levels of A^-, it suffices to show that $\mathbb{Z}_p\text{-rk}(\mathbf{B}^-) = s$. The images of the classes $[\nu\wp_n], [\nu\overline{\wp}_n]$ are dependent in $\mathbf{B}^-$ and since for $\nu \in C^+$ they span all the classes of primes above p; the claim follows from the definition of $\mathbf{B}^-$. Finally, since $\mathbb{M}^- \subset \Omega_E$ by Lemma 17, it follows that $\mathbb{H}_{E'} = \mathbb{H} \cap M^- = \prod_{\nu \in C^+} \mathbb{L}_\nu$, which completes the proof. □

6.4. **An alternative approach for the conjecture of Gross.** The corollary 3 is a natural consequence of class field theory. However, from the point of view of galois theory, one is used to consider $\mathbb{H}' \subset \mathbb{H}$, the maximal subextension of $\mathbb{H}$ which splits all the primes above p, as a fixed field of $\mathbf{B}$. Here, it arises basically as a direct complement of $\mathbb{H}_B$. This is a useful fact, indicating already that $(A')^-(T)$ and $\mathbf{B}^-$ should be complementary: indeed, since $\mathbf{B}^-$ fixes $(\mathbb{H}')^-$, A' is a factor. On the other hand $\mathrm{Gal}((\Omega_1 \cap \Omega_E^- \cap \mathbb{H})/\mathbb{K}_\infty)$, let $\mathbf{B}^-$ appear as a factor. We shall consider the consequences of this discrepancy in this section.

The Lemma 7 has the following important consequence:

Theorem 5. *Notations being like above,* $(A')^-[T] = \{1\}$.

Proof. Using Weierstrass modules, the proof is immediate and was given in Theorem 1. We give an alternative proof, which is an application of the order reversal lemma. Suppose that $(A')^-[T] \neq \{1\}$.

A straight forward computation shows that if $a_n' \in (A_n')^-$ verifies $(a_n')^T = 1$ as a class of A', then for all $a_n \in a_n' = a_n \cdot B_n^-$ we have $a_n^T \neq 1$; in particular, fixing a representant $a_n \in A_n^-$ of a_n', there is a $1 \neq b_n \in \mathbf{B}_n^-$ such that $a_n^T = b_n$.

From Lemma 6 it follows that for each $a \in A^-(T)$ of T - order j we have $a^{T^{j-1}} \in \mathbf{B}^-$ and the socle - roof lemma implies that $A(T)$ is $\Lambda[\Delta]$ - cyclic, like $\mathbf{B}^-$. Let $\mathbb{H}_B \subset \mathbb{H}_T \subset \mathbb{H}^-$ be the a subfield with $\mathrm{Gal}(\mathbb{H}_T/\mathbb{K}_\infty) = A^-(T)$ and let $R = \mathcal{R}(\mathbb{H}_T/\mathbb{K}_\infty)$ and $R' = \mathcal{R}(\mathbb{H}_B/\mathbb{K}_\infty) \subset \varprojlim_n \mathcal{E}_n$. The order reversal Lemma 15 implies that $\mathrm{Gal}(\mathbb{H}_B/\mathbb{K}_\infty) \cong A^-(T)/(TA^-(T))$, since $(R')^{T^*} = 1$. However, we know from Corollary 3 that $\mathrm{Gal}(KH_B/\mathbb{K}_\infty) = \mathbf{B}^- = A[T]$. Let $b \in \mathbf{B}^- \cap A(T)^T, b \notin A^p$, so $b = a^T$ for an $a \in A^- \setminus (A^-)^p$. There is a $\mathbb{Z}_p$ - subextension $\mathbb{L} \subset \mathbb{H}_B$ with group generated by $\varphi(b)$: here we need the Corollary and the fact that the primes above p are not totally split in any subfield of $\mathbb{H}_B$. Let $e \in R'$ be a generator of $\mathcal{R}(\mathbb{L}/\mathbb{K}_\infty)$ Then there is a $c \in \mathbb{Z}_p^\times$ such that, in the additive projective - projective Kummer pairing,

$$c = \langle b, e \rangle_{\mathbb{L}/\mathbb{K}_\infty} = \langle b, e \rangle_{\mathbb{H}_T/\mathbb{K}_\infty} = \langle a^T, e \rangle_{\mathbb{H}_T/\mathbb{K}_\infty} = \langle a, e^{T^*} \rangle_{\mathbb{H}_T/\mathbb{K}_\infty} = 0,$$

since $(R')^{T^*} = 1$ and a fortiori $e^{T*} = 1$. We obtain a contradiction to $c \in \mathbb{Z}_p^\times$ and herewith, to the assumption that $b = a^T$. It follows that for all $b \in \mathbf{B}^-$ there exists no $a \in A^-$ with $b = a^T$, so plainly $A^-(T) = A^-[T] = \mathbf{B}^-$, which completes the proof. □

Remark 5. *The above result was conjected by Gross, in connection with the non vanishing of certain* p *- adic regulator of* p *- units, which was proved in* [3] *to be equivalent to the statement of the Theorem.*

The class field theoretic statement that $A'(T)$ is finite, was considered by Kuz'min, and then Tong, as the generalized Gross conjecture.

Since $M[T]$ is a direct term in Weierstrass modules M, we have the

Corollary 4. *Let $A_\lambda = A^-/(A^-)^\dagger \cong Gal(\mathbb{H}_\lambda^-/\mathbb{K}_\infty$ and $A'_\lambda = A'^-/(A'^-)^\dagger$. Then*

$$A_\lambda = A'_\lambda \oplus \mathbf{B}^-,$$

and $f_{A'}(0) \neq 0$.

Proof. The module A_λ is by definition Weierstrass and thus $A_\lambda = A_\lambda[T] \oplus M$, where the complement M has minimal polynomial coprime to T. From Lemma 4 we know that $A_\lambda[T] = \mathbf{B}^-$ and the definition of A' and A'_λ implies that $M = A'_\lambda$. This completes the proof. □

7. Appendix C: Radicals from A^-

We start with a proof of

Lemma 18. *The extension $(\Omega_{E'} \cap \Omega \cdot \mathbb{H})/\Omega_E$ is finite.*

Proof. Let $2s = |C|$ be the number of distinct primes above p in $\mathbb{K}$. If these primes are not split in $\mathbb{K}/\mathbb{K}^+$, then Theorem 4 implies that $\mathbf{B}$ is finite. We assume thus that all the primes of $\mathbb{K}^+$ above p are split in $\mathbb{K}/\mathbb{K}^+$ and let $C' = \mathrm{Gal}(\mathbb{K}^+/D(\wp^+))$ with $|C'| = s$. Then P is a set of s pairs of conjugate primes $(\nu\wp, \overline{\nu\wp})_{\nu \in C'}$ and $\wp_n \cdot \overline{\wp}_n$ have bounded order for all $n \geq 0$, as consequence of the same Theorem. By Corollary 3 we know that $\mathbb{Z}_p\text{-rk}(\mathbf{B}^-) = s$ and $\mathbf{B}^- = \langle [(\nu\wp)^{1-\jmath}] : \nu \in C' \rangle_{\mathbb{Z}_p}$ while $ess.\ p\text{-rk}(\mathbf{B}) = \mathbb{Z}_p\text{-rk}(\mathbf{B}^-)$ as consequence of the finiteness of $\mathbf{B}^+$. Note that the definition of C' is consistent with the one used in the section on p units; we thus deduce from (5) that

$$\Omega_{E'} = \prod_{\nu \in C'} \Omega_E \left[\left(\nu \pi_0^{1-\jmath} \right)^{1/p^\infty} \right].$$

Let $b_n \in \mathbf{B}_n^- = [\wp_n^{1-\jmath}]$; since $\wp$ is totally ramified in $\mathbb{K}_n/\mathbb{K}$, $\mathrm{ord}(b_n) = p^{n-l}\mathrm{ord}(b_l)$ with l the smallest integer such that $[\wp_l] \neq 1$. But then $\wp_n^{(1-\jmath)\mathrm{ord}(b_n)} = (\pi_l^{1-\jmath})$ with $(\pi_l) = \wp_l^{\mathrm{ord}(b_l)}$. Since the generator $\pi_l^{1-\jmath}$ of this principal ideal is uniquely defined up to roots of unity, it follows that $\mathbb{K}_\infty[(\pi_l^{1-\jmath})^{1/p^\infty}] \cap \mathbb{H}$ is finite over $\mathbb{K}_\infty$ and a fortiori $[\Omega_{E'} \cap (\Omega_E \cdot \mathbb{H}) : \Omega_E] < \infty$, as claimed. In particular $\mathbb{H}_{E'}/\mathbb{H}_E$ is at most a finite extension. □

The Theorem 2 gave a general characterization of the Iwasawa linear space $A^{(S)}$, which is canonical, even when the radical shifts ρ_0 are not. In CM fields, the radical shifts ρ_0 can be defined in a canonical way at least on A^-, so we can obtain a simplified proof of the facts of this Proposition. Similar results can be obtained for μ-parts; we shall do this at a later point.

We give below an elementary investigation of the canonical radicals of the minus part, together with some additional properties of the radicals $((A^{(S)})^-)^{1/p^\infty}$.

By Corollary 4, $A^{(S)}[T] = \{1\}$ and $A^{(S)} \subset A'$. Since $E_n^- = \mu_{p^n}$ is a finite module, it follows that for $a \in (A')^-$ the extension $\mathbb{K}_\infty[a^{1/p^\infty}]$ is well defined: indeed, if $\alpha_n' \in \mathbb{K}_n, \mathfrak{A} \in a_n^{1/2}$ are such that $(\alpha_n') = \mathfrak{A}^{\mathrm{ord}(a_n)}$ then $\alpha_n := (\alpha_n')^{1-\jmath} \in \mathbb{K}_n^{1-\jmath}$ is well defined up to roots of units, and

$$\begin{aligned} \beta(a_n) &:= \alpha_n \bmod \mu_{p^n} \cdot (\mathbb{K}_n^\times)^{\mathrm{ord}(a_n)} \\ &\in \mathbb{K}_n^{1-\jmath} / \left(\mu_{p^n} \cdot (\mathbb{K}_n^\times)^{(1-\jmath)\mathrm{ord}(a_n)} \right) \end{aligned} \tag{38}$$

depends only on a_n, while $(\alpha_n) = \mathfrak{A}^{2\mathrm{ord}(a_n)}$ and $\mathfrak{A}^2 \in a_n$, by choice. Therefore the extension $\mathbb{K}_\infty[a_n^{1/\mathrm{ord}(a_n)}] = \mathbb{K}_\infty[\beta(a_n)^{1/\mathrm{ord}(a_n)}]$ is well defined. For each $a = (a_n)_{n\in\mathbb{N}} \in (A')^- \setminus A^p$ we may define a unique $\beta(a_n) \in (\mathbb{K}_n^\times)^{1-\jmath} / \left(\mu_{p^n} \cdot (\mathbb{K}_n^\times)^{(1-\jmath)\mathrm{ord}(a_n)} \right)$, as in (38); we let $\rho_0(a_n) = \mathbb{K}_{2n+z} \cdot < \beta(a_n)^{1/\mathrm{ord}(a_n)} >_{\mathbb{Z}}$ – the index $2n$ allows at this point to circumvent the implicit roots of unity in the definition of the radical: their roots are all in $\mathbb{K}_{2n+z}$. Let $\rho_0(a) = \cup_n \mathbb{K}_\infty \cdot \rho_0(a_n)$; note that the definition of ρ_0 is consistent with the one given in §2.3; however, it is canonical in this case. We also let $\rho_1(a_n) = \Omega_{E',2n+z} \cdot \rho_0(a_n)$, $\rho_1(a) = \Omega_{E'} \cdot \rho_0(a)$ and define $\Omega_\lambda = \Omega^{\mathrm{Gal}(\Omega/\Omega_{E'})^\dagger}$, by analogy with $\mathbb{H}_\lambda$. Then we have by construction of ρ_1 that

$$\mathcal{R}(\Omega_\lambda^+ / \Omega_{E'}) = \rho_1((A')^-)/\Omega_{E'}^\times.$$

We also have an extension $\overline{\mathbb{H}}_A^+ := \mathbb{K}_\infty[\rho_0((A')^-)]$ with

$$\mathcal{R}(\overline{\mathbb{H}}_A^+ / \mathbb{K}_\infty) = \rho_0((A')^-)/(\mathbb{K}_\infty)^\times = \mathcal{R}(\Omega_\lambda^+ / \Omega_{E'}).$$

We recall the construction of $\beta(a_n)$ for reference:

Lemma 19. *Let $a_n \in (A_n')^-$. There is a well defined value*

$$\beta(a_n) \in (\mathbb{K}_n^\times)^{1-\jmath} / \left(\mu_{p^n} \cdot (\mathbb{K}_n^\times)^{(1-\jmath)\mathrm{ord}(a_n)} \right),$$

such that for all $\mathfrak{B} \in a_n^{1/2}, \alpha' \in \mathbb{K}_n$ with $(\alpha') = \mathfrak{B}^{\mathrm{ord}(a_n)}$ we have

$$\alpha := \alpha'/\overline{\alpha'} \equiv \beta(a_n) \bmod \mu_{p^n} \cdot (\mathbb{K}_n^\times)^{\mathrm{ord}(a_n)}.$$

Also, $\alpha^{1/\mathrm{ord}(a_n)} \in \rho_0(a_n)$.

Let $a = (a_n)_{n\in\mathbb{N}} \in (A')^-$; we consider now the local behavior of radicals built from the classes a_n. Since $\mathbb{H}^+ = \overline{\mathbb{H}}_A^+ \cup \mathbb{H}$, there is a well defined function $\ell : (A')^- \to \mathbb{Z}_{\geq 0}$ such that

$$[\mathbb{K}_\infty[\rho] \cap \mathbb{H} \ : \ \mathbb{K}_\infty] = p^{\ell(a)} \forall a \in (A'_n)^-, \quad \forall n. \tag{39}$$

We let $\ell(a) = \lim_n \ell(a_n)$. This definition is consistent with the previous general definition of the map ℓ, and it takes advantage of the simple making of the radicals in the minus part. We deduce more details about the growth of the function $\ell(a_n)$ below. We start with

Definition 2. *We define the functions $\tilde{\ell}_{0,n}, \ \tilde{\ell}_n : (\mathbb{K}_n^\times)^{1-\jmath} \to \mathbb{Z}_{\geq 0}$ for $x \in (\mathbb{K}_n^\times)^{1-\jmath}$ by*

$$\begin{aligned} \tilde{\ell}_{0,n}(x) &= \max\{j \in \mathbb{Z}_{\geq 0} : x \in U_n^{p^j}\}, \\ \tilde{\ell}_n(x) &= \max\{\ell_0(\zeta_{p^n}^k(x) : 0 \leq k < p^n\}. \end{aligned}$$

If $x \in (\mathbb{K}_n^\times)^{(1-\jmath)}$ has $\tilde{\ell}_{0,n}(x) < \tilde{\ell}_n(x)$ and $y = \zeta^j x$ with $\tilde{\ell}_{0,n}(y) = \tilde{\ell}_n(x)$, we say that y is a normed representant for x; the number x is normed if $\tilde{\ell}_{0,n}(x) = \tilde{\ell}_n(x)$. If $\tilde{\ell}_n(x) = m \leq n$ and x is normed, then x has p^{n-m} normed representants, since $\zeta_{p^n}^{p^m} = \zeta_{p^{n-m}} \in U_n^{p^m}$. In particular, normed representants are unique only for $\tilde{\ell}_n(x) \geq n$.

By definition,

$$\widetilde{\ell}_n(x^c) = \widetilde{\ell}_n(x); \tilde{\ell}_{0,n}(x^c) = \tilde{\ell}_{0,n}(x), \quad \textit{for all } c \in \mathbb{Z} \setminus p\mathbb{Z}.$$

For normed $x \in (\mathbb{K}_n^\times)^{1-\jmath}, x \neq 1$, the values $\tilde{\ell}_m(x) = \tilde{\ell}_n(x)$ for all $m \geq n$. Indeed, if this was not the case, there is an $m \geq n$ such that $\tilde{\ell}_{m+1}(x) = \tilde{\ell}_m(x) + 1$, so $x = u_m^{p^k} = u_{m+1}^{p^{k+1}}$ with $k = \tilde{\ell}_m(x), u_j \in U_j \setminus U_j^p$, for $j \in \{m, m+1\}$. Then $u_{m+1}^p = \xi u_m$ for some $\xi \in \mu_{p^{m+1}}$; if $\xi \in \mu_{p^m}$, then $U_{m+1} = U_m[\zeta_{p^m}^{1/p}] = U_m[(\xi u_m)^{1/p}]$; thus, by Kummer theory, $\xi u_m = \xi' \cdot z_m^p, y_m, z_m \in U_m$. But then $\left(\frac{\xi' z_m^p}{\xi}\right)^{p^k} = x$ and $\ell_m(x) = k+1$, which contradicts the assumption. If $\xi \in \mu_{p^{m+1}} \setminus \mu_{p^m}$, then taking the norms $N = N_{\mathbb{U}_{m+1}/U_m}$ we obtain theat $N(\xi) \in U_m^p$, which is impossible. This confirms the claim, showing that there is a well defined function $\tilde{\ell} : (\mathbb{K}_\infty^\times)^{1-\jmath} \to \mathbb{Z}_{\geq 0}$ with $\tilde{\ell}(x) = \tilde{\ell}_m(x)$ for $x \in \mathbb{K}_n$ and all $m \geq n$. The same holds for $\tilde{\ell}_{0,n}$: there is a well defined map $\tilde{\ell}_0 : \mathbb{K}_\infty \to \mathbb{Z}_{\geq 0}$ with $\tilde{\ell}_0(x) = \tilde{\ell}_{0,m}(x)$ for all $x \in \mathbb{K}_n$ and $m \geq n$.

Let $a = (a_n)_{n \in \mathbb{N}} \in (A')^-$ be given and $m > n > 0$. Consider $\mathfrak{R} \in a_m$, a prime which is completely split over $\mathbb{Q}$ and let $\mathfrak{Q} = \mathbf{N}_{m,n}(\mathfrak{R})$ and $\alpha \in (\mathbb{K}_m^\times)^{1-\jmath}$ be related to $\mathfrak{R}$ by the procedure above. We may also choose α to be normed. If $\tilde{\ell}(\alpha) < v_p(\mathrm{ord}(a_m))$, then $\left[\mathbb{K}_\infty[\alpha^{1/\mathrm{ord}(a_m)}] \cap \mathbb{H}\right] = p^{\tilde{\ell}(\alpha)} = p^{\ell(\alpha)}$, so $\tilde{\ell}(\alpha) = \ell(\alpha)$. If $\ell(\alpha) = v_p(\mathrm{ord}(a_m))$, it may be that $\tilde{\ell}(\alpha) > \ell(\alpha)$. In this case, we choose $\gamma \in \mathbb{K}^\times$ with

$$\gamma \notin U_n^p, \quad \text{and} \quad \mathbf{N}_{\mathbb{K}_m/\mathbb{K}}(\gamma) \notin U(\mathbb{K})^p, \tag{40}$$

and consider the ideals $\mathfrak{R}_1 = \mathfrak{R}(\gamma) \in a_m$ and $\mathfrak{Q}_1 = \mathfrak{Q} \cdot (N_{m,n}(\gamma)) = N_{m,n}(\mathfrak{R}_1) \in a_n$. Then $\mathfrak{R}_1$ gives raise to a new value $\alpha_1\alpha\gamma^{(1-\jmath)\mathrm{ord}(a_n)} \in \rho(a_n^2) \cdot \mathbb{K}_m^\times$ and by construction we have $\ell(\alpha_1) = \mathrm{ord}(a_n)$. We retain this construction in:

Definition 3. *Let $a = (a_n)_{n\in\mathbb{N}} \in (A')^-$. Let $m > 0$; a pair $(\mathfrak{A}, \alpha) \in a_n \times (\mathbb{K}_n^\times)^{1-\jmath}$ is called an* instantiation pair *for a_n^2, if $\alpha = \beta^{1-\jmath}, (\beta) = \mathfrak{A}^{\mathrm{ord}(a_n)}$ and $\tilde{\ell}(\alpha) = \ell(a_n)$, while $N_{\mathbb{K}_m/\mathbb{K}}(\beta) \not\in U(\mathbb{K})^p$.*

We have shown above how to construct instantiation pairs. By the choice (40) we deduce for $m > n \geq 0$ that $(N_{m,n}(\mathfrak{A}, N_{m,n}(\alpha)^{1/p^{m-n}})$ is an instantiation pair for a_n^2, where the root $N_{m,n}(\alpha)^{1/p^{m-n}}$ is chosen among all possible values, such that the $\tilde{\ell}_{0,n}$ is maximal. Using instantiations, we investigate the behavior of $\ell(a)$ under the norm map.

Proposition 4. *Let $a = (a_n) \in (A')^-$ have infinite order and n_0 be such that p-rk(A_n) = p-rk(A_{n+1}) for $n \geq n_0$. Then*

1. *For $m > n \geq k$, with k the largest integer with $\mu_{p^k} \subset \mathbb{K}$, we have*
$$\ell(a_m) - \ell(a_n) \leq v_p(\mathrm{ord}(a_m)) - v_p(\mathrm{ord}(a_n)),$$
2. *Suppose that the transition $C_n = (A'_{n+1})^-/\iota_{n,n+1}((A'_n)^-)$ is stable or semistable. If $\ell(a_n) < v_p(\mathrm{ord}(a_n))$, then $\ell(a_m) = \ell(a_n)$ for all $m > n$.*
3. *We have $\ell(a) = \infty$ iff $\ell(a_n) = v_p(a_n)$ for all $n \geq n_0$. For all $a, b \in (A')^-$ with $\ell(a)+\ell(b) = \infty$, we have $\ell(ab) = \min(\ell(a), \ell(b))$ and there is a canonic module*
$$(A^{(S)})^- = \{x \in (A')^- : \ell(x) = \infty\}.$$
4. *We have $\ell(a) = m < \infty$ iff there is an $r \geq n_0$ and a $\alpha_r \in \mathbb{K}_r \cap U_r^{p^m} \setminus U_r^{p^{m+1}}$ such that for all $n > r$ and all $\alpha_n \in \rho(a_n)^{\mathrm{ord}(a_n)}$*

$$\alpha_n \in \alpha_r \cdot U_n^{p^{m\omega_r}} \cdot \mathbb{K}_n^{\mathrm{ord}(a_n)}. \tag{41}$$

Proof. For claim 1., let $(\mathfrak{R}, \alpha_m)$ be an instantiation for a_m and $\mathfrak{Q} = \mathbb{N}_{m,n}(\mathfrak{R})$. Let $\alpha_m = u_m^{p^{\ell(a_m)}}, u_m \in U_m \setminus U_m^p$ with $\alpha_m^{1/\mathrm{ord}(a_m)} \in \rho(a_m)$ and $\beta_n = N_{m,n}(\alpha_m) = N_{m,n}(u_n)^{p^{\ell(a_m)}}$. Then $\tilde{\ell}(\beta_n) \geq \ell(a_m)$, since we may have $N_{m,n}(u_m) \in U_n^p$. On the other hand,

$$(N_{m,n}(\alpha_m)) = \left(\mathfrak{Q}^{\mathrm{ord}(a_n)}\right)^{\mathrm{ord}(a_m)/\mathrm{ord}(a_n)}.$$

From the definition of instantiations, $(\mathfrak{Q}, \alpha_n)$ with $\alpha_n^{\mathrm{ord}(a_m)/\mathrm{ord}(a_n)} = \beta$ is an instantiation of a_n^2, so we obtain

$$\tilde{\ell}(\beta) = \tilde{\ell}(\alpha_n)^{\mathrm{ord}(a_m)/\mathrm{ord}(a_n)} = \ell(a_n) + v_p(\mathrm{ord}(a_m)/\mathrm{ord}(a_n)).$$

Combining with $\tilde{\ell}(\beta_n) \geq \ell(a_m)$, we obtain

$$\tilde{\ell}(\beta) = \ell(a_n) + v_p(\mathrm{ord}(a_m)/\mathrm{ord}(a_n)) \geq \ell(a_m),$$

which is point 1.

We now prove 2. and write for simplicity $N = \mathbf{N}_{n+1,n}$ and $t = \tau_n$. Let $m = n+1$ and $(\mathfrak{R}, \alpha_m)$ like before. For semistable transitions there is an $l < p-1$ such that $a_{n+1}^{t^l} = 1$ and thus $\nu_{n+1,n}(a_{n+1}) = a_{n+1}^{pu}$ for $u \in (\mathbb{Z}_p[t])^\times$. Then $\nu_{n+1,n}(\mathfrak{R}) = \mathfrak{R}^{pu} \cdot (\gamma)$ for a principal ideal $(\gamma) \subset \mathbb{K}_n^\times$. Let $q = \mathrm{ord}(a_n), p \cdot q = \mathrm{ord}(a_{n+1})$; then

$$N_{n+1,n}(\alpha_{n+1}) = \alpha_{n+1}^{pu} \gamma^{(1-\jmath)pq}.$$

But $(N_{n+1,n}(\alpha_{n+1})) = \mathfrak{R}^{(1-\jmath)pq} = \mathfrak{Q}^{(1-\jmath)pq} = (\alpha_n^p)$, for $\alpha_n \in \rho(a_n)^q$. Then, after eventually multiplying by a root of unity,

$$\alpha_n = \alpha_{n+1}^u \cdot \gamma^{(1-\jmath)q}.$$

If $p^{\ell(a_n)} < q$, it follows from the above identity that $\ell(a_{n+1}) = \ell(a_n)$. By induction, we obtain the claim 2. Note that for $n > n_0$, all transitions are stable, so the premises of this statement are always true for sufficiently large n. As a direct consequence, $\ell(a) < \infty$ if there is an $n > n_0$ with $\ell(a_n) < v_p(a_n)$. This is the first part of claim 3.

It follows from claim 2 that $\ell(ab) = \infty$ iff $\ell(a) = \ell(b) = \infty$, which shows that the set $(A^{(S)})^-$ is canonically defined. This is an elementary redefinition of the minus part of the Iwasawa linear space given in (21). Since $\ell(\tau a) = \ell(a)$ for all $a \in (A')^-$, it is a module. If either $\ell(a) = m$ or $\ell(b) = m$ is finite, then $\ell(ab) = m$ by point 2. Note that if both $\ell(a)$ and $\ell(b)$ are finite, then $\ell(ab)$ may be larger than both, it may even be infinite.

For proving (41), let $\ell(a) = \ell(a_{n_1}) = m$, let $n > r > n_1$ and choose $(\mathfrak{R}, \alpha_n)$ an instantiation of a_n. We have thus $\alpha_n = u_n^{p^m}, u_n \in U_n \setminus U_n^p$; moreover, the premises imply that $\alpha_r = u_r^{p^m}, u_r \in U_r \setminus U_r^p$. Then

$$N_{n,r}(\alpha_r) = \alpha_r^{p^{n-r}} = N_{n,r}(u_n)^{p^m} = u_r^{p^n}.$$

It follows that $N_{n,r}(u_n) = \eta u_r^{p^{n-r}}, \eta \in \mu_{p^n}$ and the norming condition on α_n, α_r implies that $\eta = 1$. Thus $N_{n,r}(u_n/u_r) = 1$ and Hilbert 90 applied to U_n yields $u_m = u_r \cdot v_n^{\omega_r}$. The claim follows from the fact that α_n is uniquely defined up to elements from $(\mathbb{K}_n^\times)^{\mathrm{ord}(a_n)}$ and roots of unity, as shown in (38).

8. Appendix D: On Leopoldt's Conjecture

The results proved in the previous Appendix parts, yield an elementary proof of the following

Theorem 6. *If $\mathbb{K}/\mathbb{Q}$ is a totally real extension in which the primes above p are totally split, then Leopoldt's conjecture holds for $\mathbb{K}$.*

Proof. Assume that $\mathbb{K}$ satisfies the premises of the theorem, but the Leopoldt defect is positive. Then there is a $\mathbb{Z}_p$-extension $\mathbb{L}/\mathbb{K}$. The normal closure of $\mathbb{K}$ is a real galois extension $\mathbb{K}[\alpha]$ and $\mathbb{L}[\alpha]$ is a non trivial extension of $\mathbb{K}[\alpha]$: thus Leopoldt's conjecture is also false for the galois closure. We may thus assume without restriction of generality that $\mathbb{K}$ is galois and real.

Let $\wp \subset \mathbb{K}$ be a prime above p which ramifies in $\mathbb{L}$; we may also assume without restriction of generality that $\wp$ does not split in any subextension of $\mathbb{L}$: this can always be achieved by taking a finite extension of $\mathbb{K}$. Since p is totally split in $\mathbb{K}$, the completion $\mathbb{K}_\wp = \mathbb{Q}_p$ has the two $\mathbb{Z}_p$-extensions $\mathbb{L}_\wp, \mathbb{K}_{\infty,\wp}$. On the other hand, the only $\mathbb{Z}_p$-extensions of $\mathbb{Q}_p$ are the unramified one and the cyclotomic ramified $\mathbb{Q}_p[\mu_{p^\infty}]$. Since the latter is absorbed in $\mathbb{K}_\infty$, it follows that $(\mathbb{L}\cdot\mathbb{K}_\infty)/\mathbb{K}_\infty$ is unramified at $\wp$. This holds for all primes that ramify in $\mathbb{L}$, and since $\mathbb{K}$ is galois, it follows that $\mathbb{L} \cdot \mathbb{K}_\infty \subset \mathbb{H}$. Since $\mathbb{K}$ is real, Theorems 4 and 3 imply that $\lambda(A) = 0$ so $\mathbb{H}$ must be finite. Therefore, the Leopoldt defect $\mathcal{D}(\mathbb{K}) = 0$, which completes the proof. □

Remark 6. *The above is a simplified and improved version of the proof given for this fact in* [7]. *The argument was used by Greenberg in* [4] *in order to prove the existence of Λ - modules with arbitrary large λ. The Theorem 4 has the following more general consequence. If $\mathbb{K}/\mathbb{Q}$ is galois with group G and $\wp$ is a prime above p with decomposition group $D \subset G$, then the extension $\Omega(\mathbb{K})_\wp/\mathbb{K}_{\infty,\wp}$ has a galois group $\Delta_\wp$ which is a cyclic $\mathbb{Z}_p[D]$ module with annihilator in the augmentation of this group ring. Indeed, if the norm part was not trivial, we would find a $\mathbb{Z}_p$ - subextension $\mathbb{K}_\infty \subset \mathbb{L} \subset \Omega(\mathbb{K})$ such that $Gal(\mathbb{L}_\wp/\mathbb{K}_{\infty,\wp})$ is fixed by conjugation by $D_\wp$: the local extension $\mathbb{L}_\wp$ must then be a $\mathbb{Z}_p$ - extension of $\mathbb{Q}_p$, and we apply the same argument as before to raise a contradiction. Therefore, the group $\Delta_\wp$ is contained in the augmentation of $\mathbb{Z}_p[D_\wp]$ for all $\wp$.*

One can also prove by elementary means that if $\mathbb{L}/\mathbb{K}$ is a cyclic extension of degree p in which the prime p is not split, and if Leopoldt's conjecture holds for $\mathbb{K}$, then it holds for $\mathbb{L}$. This is also an improvement of a result proved in [7]. *Since we gave a general prove above, we leave this proof out here.*

□

References

[1] T. Albu. *Cogalois theory*. Number 252 in Monographs and textbooks in pure and applied mathematics. Marcel Dekker Inc., 2003.

[2] J. Coates. Personal communication, November 2009.

[3] L. Federer and B. Gross. Regulators and Iwasawa modules. *Invent. Math.*, 62(3):443–457, 1981.

[4] R. Greenberg. On the Iwasawa invariants of totally real fields. *American Journal of Mathematics*, 98:263–284, 1973.

[5] K. Iwasawa. On $\mathbb{Z}_\ell$ - extensions of number fields. *Ann. Math. Second Series*, 98:247 – 326, 1973.

[6] J. Kraft and R. Schoof. Computing Iwasawa modules of real quadratic number fields. *Compositio Mathematica*, 97:135–155, 1995.

[7] P. Mihăilescu. The t and t^* components of λ - modules and Leopoldt's conjecture. http://front.math.ucdavis.edu/0905.1274.

[8] P. Mihăilescu. Leopoldt's conjecture for some galois extensions. In *Proceedings SANT*. Universitätsverlag Göttingen, 2009.

[9] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined second edition edition, 1990.

[10] J. Serre. Local Class Field Theory. In Cassels and Fröhlich, editors, *Algebraic Number Theory*, pages 129–161. Academic Press, 1967.

[11] F. Thaine. On the ideal class groups of real abelian number fields. *Annals of Math.*, 128:1–18, 1988.

[12] L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1996.

(P. Mihăilescu) Mathematisches Institut der Universität Göttingen
E-mail address, P. Mihăilescu: `preda@uni-math.gwdg.de`