

THE GROSS-KUZ'MIN CONJECTURE FOR CM FIELDS

PREDA MIHĂILESCU

ABSTRACT. Let $A' = \varprojlim_n$ be the projective limit of the p -parts of the ideal class groups of the p integers in the \mathbb{Z}_p -cyclotomic extension $\mathbb{K}_\infty/\mathbb{K}$ of a CM number field \mathbb{K} . We prove in this paper that the T part $(A')^-(T) = 0$. This fact has been explicitly conjectured by Kuz'min in 1972 and was proved by Greenberg in 1973, for abelian extensions \mathbb{K}/\mathbb{Q} . Federer and Gross had shown in 1981 that $(A')^-(T) = 0$ is equivalent to the non-vanishing of the p -adic regulator of the p -units of \mathbb{K} .

1. INTRODUCTION

Let p be an odd prime and \mathbb{K} be a galois CM extension, while $(\mathbb{K}_n)_{n \in \mathbb{N}}$ are the intermediate fields of its cyclotomic \mathbb{Z}_p -extension \mathbb{K}_∞ . Thus $\mathbb{K}_\infty = \mathbb{K} \cdot \mathbb{B}$, where \mathbb{B}/\mathbb{Q} is the \mathbb{Z}_p -extension of \mathbb{Q} . Let $A_n = (\mathcal{C}(\mathbb{K}_n))_p$ be the p -parts of the ideal class groups of \mathbb{K}_n and $A = \varprojlim_n A_n$ be their projective limit. The subgroups $B_n \subset A_n$ are generated by the classes containing ramified primes above p and we let

$$(1) \quad \begin{aligned} A'_n &= A_n/B_n, \\ B &= \varprojlim_n B_n, \quad A' = A/B. \end{aligned}$$

The quotients A'_n arise also as ideal class groups of the ring of p -integers $\mathcal{O}(\mathbb{K})[1/p]$, [7], §4. We let $E_n = (\mathcal{O}(\mathbb{K}_n))^\times$ be the global units of \mathbb{K}_n and $E'_n = (\mathcal{O}(\mathbb{K}_n)[1/p])^\times$ be the p -units.

We denote as usual the galois group $\Gamma = \text{Gal}(\mathbb{K}_\infty/\mathbb{K})$ and $\Lambda = \mathbb{Z}_p[\Gamma] \cong \mathbb{Z}_p[[\tau]] \cong \mathbb{Z}_p[[T]]$, where $\tau \in \Gamma$ is a topological generator and $T = \tau - 1$. With this, the module \mathbf{A} is a finitely generated Λ -torsion module. We let

$$\omega_n = (T + 1)^{p^{n-1}} - 1 \in \Lambda, \quad \nu_{n+1,n} = \omega_{n+1}/\omega_n \in \Lambda.$$

The groups A, A', B are natural multiplicative groups endowed with an action of Λ . We therefore write this action multiplicatively, so $a^T = \tau(a)/a$, etc. It may be useful at places to skip for simplicity

of notation to additive written groups, and this shall be indicated in the text; moreover, generic, abstract Λ -modules will be always written additively, for the same reasons.

If M is a Noetherian Λ -torsion module and $f \in \mathbb{Z}_p[T]$ is a distinguished polynomial, we define the f -part and the f -torsion of M by

$$(2) \quad \begin{aligned} M(f) &= \{x \in M : \exists n > 0 : f^n x = 0\}, \\ M[f] &= \{x \in M : fx = 0\} \subset M(f). \end{aligned}$$

Since M is finitely generated, there is a minimal n such that $f^n M(f) = 0$, and we denote this by $\text{ord}_f(M)$, the f -order. Moreover, there is an exact sequence of pseudoisomorphisms

$$(3) \quad 0 \rightarrow M[f] \rightarrow M(f) \rightarrow M(f) \rightarrow M(f)/(fM(f)) \rightarrow 0,$$

in which the middle arrow is induced by the map $x \mapsto fx$. We define herewith, in analogy to the p -rank of finite abelian p -groups, the f -rank of M as the common number of elements of a minimal set of generators of $M[f]$ and $M/(fM(f))$, as Λ -modules.

Leopoldt emitted in 1962 the hypothesis that p -adic regulator of the units $E(\mathbb{K})$ should be non-vanishing. His initial conjecture referred to abelian fields \mathbb{K} but it was soon accepted that one should expect that the same happens in general for arbitrary number fields \mathbb{K} . The statement for abelian fields could be proved in 1967 by Brumer [2], using a p -adic variant of Baker's fundamental result on linear forms in logarithms and an earlier argument of Ax [1]. The argument of Ax had been formulated several years before Baker's achievement and it reduced the conjecture of Leopoldt to the exact p -adic variant of Baker's theorem on linear forms. Greenberg showed in 1973 [5] how to define the p -adic regulator $R(E'(\mathbb{K}))$ of the p -units, and could prove, using the same argument of Ax and the Baker-Brumer result on linear forms in p -adic logarithms, that the regulator $R(E'(\mathbb{K}))$ does not vanish for abelian extension \mathbb{K}/\mathbb{Q} . Several years later, in 1981, Federer and Gross [4] considered the question of the vanishing of the $R(E'(\mathbb{K}))$ for arbitrary CM extensions \mathbb{K}/\mathbb{Q} . Unlike Greenberg, they cannot yield a proof for this assumption; in exchange, they prove that $R(E'(\mathbb{K})) \neq 0$ is equivalent to $B^- = A^-(T)$. This yields a useful translation of the Diophantine statement about the regulator into a class field theoretical statement about the vanishing of $(A')^-(T)$. Quite at the same time as Greenberg, and just around the Curtain, L. Kuz'min had formulated in a lengthy paper [9] on Iwasawa theory the *Hypothesis H*, which contains the statement $|A'(T)| < \infty$ for all number fields \mathbb{K} . The connection to regulators is not considered in Kuz'min's paper, but we have here an adequate generalization of Gross's conjecture to arbitrary number

fields \mathbb{K} . In the case of CM fields, the Hypothesis H contains also a statement $|(A^+)'(T)| < \infty$. This is a consequence of Leopoldt's conjecture, but not equivalent to it. In fact, we prove in [12] that Leopoldt's conjecture for CM fields is equivalent to $|A^+(T)| < \infty$, requiring thus also the finiteness of B^+ , which is not object of Hypothesis H. Recently, some authors – e.g. [10] – refer to the (generalized) Gross conjecture, meaning the general class field theoretic assumption that $A'(T) = 0$ for all number fields. This we denote by Gross-Kuz'min conjecture and restrict here to the initial formulation of Gross, which claims that $(A')^-(T)$ for CM fields.

The conjecture of Leopoldt also has a simple class field theoretical equivalent, which was proved by Iwasawa already in 1973, in his seminal paper [7]: for CM fields \mathbb{K} , this amounts to the fact that the maximal p -abelian p -ramified extension $\Omega(\mathbb{K}^+)$ is a finite extension of \mathbb{K}_∞^+ .

We shall stress here the dual Diophantine and class field theoretical aspects of the conjectures of Gross-Kuz'min and Leopoldt by using the common term of *regulator conjectures of classical Iwasawa theory*. In 1986, L.J.Federer undertook the task of generalizing the classical results of Iwasawa theory – which can be considered as results on then asymptotic behavior of A_n, A'_n , to generalized class groups. She thus considers the structure of the galois groups of the maximal abelian p -extensions $\mathbb{L}_n/\mathbb{K}_n$ which are ray-class field to some fixed ray, and in addition split the primes contained in a separate fixed set of places of \mathbb{K} . The paper is algebraic in nature with little reference to the field theoretic background, but it confirms the general nature of Iwasawa theory. In this flavor, one may ask in what way the regulator conjectures of classical Iwasawa theory generalize of Federer's ray class fields, and whether these generalization also afford equivalent formulations, in Diophantine and in class field theoretical forms. It is likely that one may encounter a proper embedding of Jaulent's conjecture – which is a purely Diophantine generalization of the Leopoldt conjecture, see [8] – in a systematic context of class field theory.

The purpose of this breve remarks was to situate the questions and methods that we shall deploy below in their broad context. One can find in Seo's recent paper [14] a good overview of further conjectures related to the ones discussed above. In this paper we prove the initial Gross conjecture:

Theorem 1. *Let p be an odd prime and \mathbb{K} a CM extension of \mathbb{Q} . Let $\mathbb{K}_\infty = \cup_n \mathbb{K}_n$ be the \mathbb{Z}_p -cyclotomic extension of \mathbb{K} and let A_n, A'_n be the p -parts of the ideal class groups of the integers, resp. the p -integers of*

\mathbb{K}_n ; let $A' = \varprojlim_n A'_n$. Then

$$(A')^-(T) = \{1\}.$$

1.1. Additional notations. In this paper \mathbb{K} is a galois CM extension of \mathbb{Q} with group $\Delta = \text{Gal}(\mathbb{K}/\mathbb{Q})$. We also assume that the primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$ and the norms $N_{m,n}A_m \rightarrow A_n$ are surjective for all $m > n \geq 1$. We let $\mathbb{H}_n \supset \mathbb{K}_n$ be the maximal p -abelian unramified extensions of \mathbb{K}_n – the p -Hilbert class fields of \mathbb{K}_n – and $X_n := \text{Gal}(\mathbb{H}_n/\mathbb{K}_n) \cong A_n$, via the Artin Symbol, which we shall denote by φ . The composita with \mathbb{K}_∞ are $\overline{\mathbb{H}}_n = \mathbb{H}_n \cdot \mathbb{K}_\infty$. Let $\mathbb{H} = \cup_n \mathbb{H}_n$ be the maximal unramified p -extension of \mathbb{K}_∞ and $X = \text{Gal}(\mathbb{H}/\mathbb{K}_\infty)$. The isomorphisms $\varphi : A_n \rightarrow X_n$ are norm compatible and yield an isomorphism in the projective limit, which we shall also denote by φ :

$$(4) \quad \varphi(A) = \varphi(\varprojlim_n A_n) = \varprojlim_n (\varphi(A_n)) = \varprojlim_n (X_n) = X.$$

The maximal subextension of \mathbb{H}_n which splits all the primes above p is denoted by $\mathbb{H}'_n \subset \mathbb{H}_n$ and we have

$$\text{Gal}(\mathbb{H}'_n/\mathbb{K}_n) \cong A'_n \quad \text{Gal}(\mathbb{H}_n/\mathbb{H}'_n) = \varphi(B_n).$$

The injective limit is $\mathbb{H}' \subset \mathbb{H}$, with $\text{Gal}(\mathbb{H}/\mathbb{H}') = \varphi(B)$. (e.g. [7], §3. - 4.)

Let $\wp \subset \mathbb{K}$ be a prime above p and $D(\wp) \subset \Delta$ denote its decomposition group; we let $C \subset \Delta$ be a set of coset representatives for $\Delta/D(\wp)$ and $2s = |C|$. If $\wp^+ \subset \mathbb{K}^+$, the prime above \wp , is unsplit, then $B^- = \{1\}$ and it follows from Lemma 1 below, that $A^-(T) = \{1\}$, so the Gross conjecture is trivially true. We assume therefore that the primes of \mathbb{K}^+ above p are split in \mathbb{K}/\mathbb{K}^+ , so there are s pairs of conjugate primes above p in \mathbb{K} .

The local units of \mathbb{K}_n are

$$U_n = U(\mathbb{K}_n) = \mathcal{O}(\mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \prod_{\nu \in C} U(\mathbb{K}_{n,\nu\wp}).$$

where $U(\mathbb{K}_{n,\nu\wp})$ are the units in the completion of \mathbb{K}_n at the ramified prime above $\nu\wp$. We write $U_n^{(1)} = \prod_{\nu \in C} U^{(1)}(\mathbb{K}_{n,\nu\wp})$ and $\overline{E}_n \subset U_n^{(1)}$ is the intersection of the p -adic completion of the diagonal embedding $E_n \hookrightarrow U_n$ with $U_n^{(1)}$.

The maximal p -abelian p -ramified extension of \mathbb{K}_n is denoted by $\Omega(\mathbb{K}_n)$ and $\Omega = \cup_n \Omega(\mathbb{K}_n)$. By class field theory, we have ([13], Chapter 5, Theorem 4.1):

$$\text{Gal}(\Omega_n/\mathbb{H}_n) \cong U_n^{(1)}/\overline{E}_n.$$

1.2. List of symbols. We give here a list of the notations introduced below in connection with Iwasawa theory

p	An odd rational prime,
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 CM extension of \mathbb{Q} ,
$\mathbb{K}_\infty, \mathbb{K}_n$	The cyclotomic \mathbb{Z}_p -extension of \mathbb{K} , and intermediate fields,
Δ	$\text{Gal}(\mathbb{K}/\mathbb{Q})$,
$A(\mathbf{K})$	$=$ p -part of the ideal class group of the field \mathbf{K} ,
Γ	$\text{Gal}(\mathbb{K}_\infty/\mathbb{K}) = \mathbb{Z}_p\tau$, τ a topological generator of Γ ,
J	$=$ The image of complex conjugation in $\text{Gal}(\mathbb{K}_\infty/\mathbb{Q})$,
T	$=$ $\tau - 1$,
$*$	Iwasawa's involution on Λ induced by $T^* = (p - T)/(T + 1)$,
s	$=$ The number of primes above p in \mathbb{K}^+ ,
C	$=$ Coset representatives, for $\Delta/D(\wp)$,
$A'_n = A'(\mathbb{K}_n)$	The p -part of the ideal class group of the p -integers of \mathbb{K}_n ,
A'	$=$ $\varprojlim A'_n$,
B	$=$ $\langle \{b = (b_n)_{n \in \mathbb{N}} \in A : b_n = [\wp_n], \wp_n \supset (p)\} \rangle_{\mathbb{Z}_p}$,
\mathbb{B}	The (cyclotomic) \mathbb{Z}_p -extension of \mathbb{Q} ,
\mathbb{H}	The maximal p -abelian unramified extension of \mathbb{K}_∞ ,
$\mathbb{H}' \subset \mathbb{H}_\infty$	The maximal subextension that splits the primes above p ,
$\Omega(\mathbb{K})$	$=$ The maximal p -abelian p -ramified extension of \mathbb{K} ,
$\overline{\mathbb{H}}_1$	$=$ $\mathbb{H}_1 \cdot \mathbb{K}_\infty$,
Φ	$=$ $\Omega^-(\mathbb{K}) \cap \mathbb{H}$,
$\mathbb{M}_\wp \subset \Omega^-(\mathbb{K})$,	The maximal subextension in which all the primes above p , except for $(\wp, \overline{\wp})$, are totally split,
$\mathbb{U}_\wp \subset \mathbb{M}_\wp$,	The unique unramified \mathbb{Z}_p -subextension of \mathbb{M}_\wp ,
\wp	$=$ The Artin symbol, see also (4) ,
E_n	$=$ $\mathcal{O}(\mathbb{K}_n)^\times$,
E'_n	$=$ $(\mathcal{O}(\mathbb{K}_n)[1/p])^\times$,
U_n	$=$ $U(\mathbb{K}_n) = \mathcal{O}(\mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \prod_{\nu \in C} U(\mathbb{K}_{n, \nu\wp})$,
$U_n^{(1)}$	$=$ $\prod_{\nu \in C} U^{(1)}(\mathbb{K}_{n, \nu\wp})$
\overline{E}_n	$=$ $\left(\bigcap_N E_n \cdot U_n^{p^N} \right) \cap U_n^{(1)}$.

1.3. Plan of the paper. The core of the proof relays on the following:

Proposition 1. *Let $\Omega(\mathbb{K})$ be the maximal p -abelian p -ramified extension of \mathbb{K} , let $\mathbb{K}_\infty/\mathbb{K}$ be the \mathbb{Z}_p -cyclotomic extension and $\mathbb{H}/\mathbb{K}_\infty$ its maximal p -abelian unramified extension. Then*

$$(5) \quad \text{Gal}((\Omega(\mathbb{K}) \cap \mathbb{H}^-)/\mathbb{K}_\infty) \sim B^-.$$

The Gross conjecture follows from (5) by a sequence of elementary auxiliary arguments, which shall be exposed in the introduction of Chapter 2. We then consider the example of the case when \mathbb{K} is an imaginary quadratic extension. This is also a special case of Greenberg's theorem, but our proof uses class field theory and can therefore be generalized to the non commutative case. After having introduced in this way the central observation for our approach, we give in Chapter three the proof of Proposition 1 by means of class field theory and the global Artin symbol for the group $\text{Gal}(\Omega^-(\mathbb{K})/\mathbb{H}^-(\mathbb{K}))$.

2. REDUCTION TO PROPOSITION 1

We begin by proving that the main result follows from Proposition 1. First, notice that if $(A')^-(T) = \{1\}$ holds for galois CM extension of \mathbb{Q} , then it holds a fortiori for arbitrary CM fields \mathbb{L}/\mathbb{Q} . Indeed, let \mathbb{L} be a arbitrary and $\mathbb{K} = \mathbb{L}[\theta]$ be the normal closure. We consider the cyclotomic \mathbb{Z}_p -extensions of both \mathbb{L} and \mathbb{K} and define $A'(\mathbb{K}), A'(\mathbb{L})$ in the obvious way. Assuming that the Gross conjecture does not hold for \mathbb{L} , then $((A'(\mathbb{L}))^-(T))$ is infinite. Since $\text{Ker}(\iota : A(\mathbb{L}) \rightarrow A(\mathbb{K}))$ is finite and the ideal lift map commutes with the action of Λ , it follows that $((A'(\mathbb{K}))^-(T))$ must also be infinite, in contradiction with the assumption. Therefore it suffices to prove the conjecture for galois CM extensions.

2.1. Auxiliary results. The following simple result implies that, if $a \in A^-(T)$ represents the class $a' \in (A')^-(T)$, then $a = a' \cdot b$ for some non trivial $b \in B^-$.

Lemma 1. *Let \mathbb{K} be a CM galois extension of \mathbb{Q} and suppose that $(A')^-(T) \neq \{1\}$. Then $\text{ord}_T(A^-(T)) > 1$ and*

$$T - \text{rk}(A^-) = T - \text{rk}(B^-).$$

Proof. Assuming that $(A')^-(T) \neq \{1\}$, there is some $a = (a_n)_{n \in \mathbb{N}} \in A^-$ with non trivial image $a' \in (A')^-[T]$. We show that $\text{ord}_T(a) = 2$. Let $\mathfrak{Q}_n \in a_n$ be a prime, let n be sufficiently large and $\text{ord}(a_n) = p^{n+z}$. Let $(\alpha_0) = \mathfrak{Q}^{p^{n+z}}$ and $\alpha = \alpha_0/\overline{\alpha_0}$; since $a' \in (A')^-[T]$ it also follows that $a_n^T \in B^-$ and thus $\mathfrak{Q}^T = \mathfrak{R}_n$ with $b_n := [\mathfrak{R}_n] \in B_n$. If $b_n \neq 1$, then $\text{ord}_T(a) = 1 + \text{ord}_T(a') = 2$, and we are done.

We thus assume that $b_n = 1$ and derive a contradiction. In this case $\mathfrak{R}_n^{1-j} = (\rho_n)$ is a p -unit and $(\alpha^T) = (\rho_n^{p^{n+z}})$, so

$$\alpha^T = \delta \rho_n^{p^{n+z}}, \quad \delta \in \mu_{p^n}.$$

Taking the norm $N = N_{\mathbb{K}_n/\mathbb{K}}$ we obtain $1 = N(\delta)N(\rho_n)^{p^{n+z}}$. The unit $N(\delta) \in E(\mathbb{K})^{1-j} = \mu(\mathbb{K}) = \langle \zeta_{p^k} \rangle$ - we must allow here, in general,

that $\mathbb{K} \cap \mathbb{B} = \mathbb{B}_k$, for some maximal $k > 0$. It follows that $\rho_1 := N(\rho_n)$ verifies $\rho_1^{p^{n+z}} = \delta_1$, and since $\delta_1 \notin E(\mathbb{K})^{p^{k+1}}$, it follows that $\rho_1^{p^k} = \pm 1$ and by Hilbert 90 we deduce that $\rho_n^{p^k} = \pm x^T, x \in \mathbb{K}_n^\times$. In terms of ideals, we have then

$$\begin{aligned} \mathfrak{Q}^{(1-j)Tp^{n+z}} &= (\alpha^T) = (x^{Tp^{n+z-k}}), \quad \text{hence} \\ \left(\mathfrak{Q}^{(1-j)p^k} / (x) \right)^{Tp^{n+z-k}} &= (1) \quad \Rightarrow \quad (\mathfrak{Q}^{(1-j)p^k} / (x))^T = (1). \end{aligned}$$

But \mathfrak{Q} is by definition not a ramified prime, so the above implies that a_n has order bounded by p^k , which is impossible since $a_n \in A_n^-$, and thus $\text{ord}(a_n)$ is unbounded. This contradiction confirms the claim $\text{ord}_T(A^-(T)) > 1$ and implies that $A^-[T] = B^-$. From (3) and the definition of the T -rank, we conclude that B^- and $A^-(T)$ have the same T -rank. \square

As mentioned in the introduction, if the primes above p are not split in \mathbb{K}/\mathbb{K}^+ , then $B^- = \{1\}$ the the lemma implies that $T\text{-rk}(A^-(T)) = T\text{-rk}(B^-) = 0$. If the primes above p are split in \mathbb{K}/\mathbb{K}^+ , we shall prove in Chapter 3 that $T\text{-rk}(B^-) = s$.

2.2. Field tailoring. Since we follow an explicite field-theoretic approach, and since the galois correspondence is order reversing for lattices of subfields, it will be useful to provide an auxiliary construction, in which the interesting groups $(A')^-(T), A^-(T)$ appear as direct galois groups of some adequate subextensions of \mathbb{H}^- . This is done in the following:

Lemma 2. *Let the notations be like above and let $F(T)$ be the minimal annihilator polynomial of $p^m A$, where p^m is an annihilator of the \mathbb{Z}_p -torsion of A . Let $f|F$ be an irreducible divisor of F ; then there is a positive constant $M > 0$ and a subgroup $C \subset A$ with the following property. Let $\overline{\mathbb{K}}_\infty = \mathbb{H}^{p^M \text{Gal}(\mathbb{H}/\mathbb{K}_\infty)}$ and $\mathbb{H}_f = \mathbb{H}^C$. Then*

$$\begin{aligned} \text{Gal}(\mathbb{H}_f/\overline{\mathbb{H}}) &\sim A(f) \quad \text{and} \quad \exists a^{(i)} \in A(f), \quad i = 1, 2, \dots, s \text{ with:} \\ (6) \quad \text{Gal}(\mathbb{H}_f/\overline{\mathbb{H}}) &= \bigoplus_{i=1}^s \Lambda\varphi(a^{(i)}), \end{aligned}$$

where the Artin map $\varphi : A \rightarrow \text{Gal}(\mathbb{H}/\mathbb{K}_\infty)$ acts by restriction on \mathbb{H}_f .

Proof. Let p^m be the exponent of the \mathbb{Z}_p -torsion submodule $A^\circ \subset A$ and let $F(T) \in \mathbb{Z}_p[T]$ be the minimal annihilator polynomial of $p^m A$, while $\mathcal{F} = \{f_1(T), f_2(T), \dots, f_t(T)\} \subset \mathbb{Z}_p[T]$ are the irreducible distinguished polynomials dividing $F(T)$. By the theory of elementary

Λ -modules [7], there is an elementary Λ -module

$$\mathfrak{E} = \bigoplus \Lambda/(g_i^{e_i}), \quad \text{such that } \mathfrak{E} \sim A.$$

The primes g_i above are either p or one of the polynomials f_i , the exponents are positive and a prime may occur repeatedly in the sum. The above pseudoisomorphism is, in additive notation, explicitly

$$0 \rightarrow K_1 \rightarrow A \rightarrow \mathfrak{E} \rightarrow K_2 \rightarrow 0,$$

with finite p -abelian kernel and cokernel. We may choose $M \geq m$ such that p^M annihilates K_1 and K_2 . Then $\mathcal{A} := p^M A$ is a \mathbb{Z}_p -free finitely generated Λ -torsion module and in view of the above we have

$$\mathcal{A} = \bigoplus_{i=1}^t \mathcal{A}(f_i).$$

Let $f \in \mathcal{F}$ be a fixed distinguished polynomial. The f -part $\mathcal{A}(f)$ is a finitely generated Λ -module, so there is a minimal set

$$\{c^{(1)}, c^{(2)}, \dots, c^{(r(f))}\} \subset A \setminus A^{(p,T)} \quad \text{such that } \mathcal{A}(f) \sim p^M \bigoplus_{j=1}^{r(f)} \Lambda c^{(j)}.$$

By taking M sufficiently large, we may argue like before and assume that the implicit kernels and cokernels in the above pseudoisomorphism are trivial. We obtain a representation of \mathcal{A} as a direct sum of cyclic Λ -modules, which are all annihilated by some power of an irreducible distinguished polynomial.

With this choice of M we let $\overline{\mathbb{K}} = \mathbb{H}^{p^M \varphi(A)} = \mathbb{H}^{\varphi(A)}$. By definition, $\text{Gal}(\mathbb{H}/\overline{\mathbb{K}}) \cong \varphi(\mathcal{A})$ is a direct sum of cyclic, \mathbb{Z}_p -torsion free Λ -modules. Let now $C = \bigoplus_{g \in \mathcal{F} \setminus \{f\}} \varphi(\mathcal{A}(g)) \subset \text{Gal}(\mathbb{H}/\overline{\mathbb{K}})$ and $\mathbb{H}_f = \mathbb{H}^C$. By construction, we have $\text{Gal}(\mathbb{H}_f/(\overline{\mathbb{K}} \cap \mathbb{H}_f)) \cong \mathcal{A}(f)$ and the group is a direct sum of finitely many cyclic Λ -modules annihilated by powers of f . This completes the proof of the lemma. \square

The complex conjugation induces canonical decompositions of the class groups and also of the extensions, so $\mathbb{H} = \mathbb{H}^+ \cdot \mathbb{H}^-$, the first factor being fixed by $\varphi(A^-)$ and the second by $\varphi(A^+)$. We can thus apply the above Lemma to the subfield \mathbb{H}^- and the corresponding galois group $\varphi(A^-)$. As a consequence, we have

Corollary 1. *Let $\overline{\mathbb{K}}$ and M be defined like in the previous lemma and assume that (5) holds. Then there is a subfield $\mathbb{H}_T^- \subset \mathbb{H}^-$ such that*

$$\text{Gal}(\mathbb{H}_T^-/(\mathbb{H}_T^- \cap \overline{\mathbb{K}})) = p^M \varphi(A^-(T))$$

is a direct sum of cyclic Λ -modules and

$$(7) \quad \text{Gal}((\Omega(\mathbb{K}) \cap \mathbb{H}_T^-)/(\overline{\mathbb{K}} \cap \mathbb{H}_T^-)) \cong B^-.$$

Proof. The module $\mathcal{A} = p^M A$ defined in the proof of the previous lemma allows a decomposition $\mathcal{A} = \mathcal{A}^- \oplus \mathcal{A}^+$ and the extension \mathbb{H}_T may be chosen like in the lemma. Let then $\mathbb{H}_T^- = \mathbb{H}_T \cap \mathbb{H}^-$; it follows from the definition that $\text{Gal}(\mathbb{H}_T^-/(\mathbb{H}_T^- \cap \overline{\mathbb{K}})) = \mathcal{A}^-(T) = p^M \varphi(A^-(T))$, which confirms the first claim. For (7), we may assume that p^M is sufficiently large to annihilate the cokernel in the pseudoisomorphism (5). The relation (7) then follows from (5) and the definition of \mathbb{H}_T^- and $\overline{\mathbb{K}}$. \square

2.3. The main reduction. We are now able to prove that Proposition 1 implies Theorem 1. This follows from the equivalence of the following statements:

Lemma 3. *Let \mathbb{K} be a CM extension of \mathbb{Q} and $\Phi = \Omega(\mathbb{K}) \cap \mathbb{H}^-$. The following statements are equivalent:*

- A. $A^-(T) = B^-$.
- B. $\text{Gal}(\Phi/\mathbb{K}_\infty) \sim B^-$.
- C. $[\Phi \cap \mathbb{H}' : \mathbb{K}_\infty] < \infty$.

Proof. We shall prove that $B \Rightarrow A \Rightarrow C \Rightarrow B$. Assume that (5) holds (which is the same as point B). By definition of A, A' and \mathbb{H}, \mathbb{H}' , we have $\mathbb{K}_\infty \subset (\mathbb{H}')^- \subset \mathbb{H}^-$ and $\text{Gal}(\mathbb{H}^-/(\mathbb{H}')^-) \cong B^-$. Let now $\Phi = \Omega(\mathbb{K}) \cap \mathbb{H}^-$; the Proposition 1 implies that $[\Phi \cap (\mathbb{H}')^- : \mathbb{K}_\infty] < \infty$. The galois correspondence yields an exact sequence

$$0 \rightarrow \text{Gal}(\Phi/(\overline{\mathbb{K}} \cap \mathbb{H}_T^-)) \rightarrow \text{Gal}(\mathbb{H}_T^-/(\overline{\mathbb{K}} \cap \mathbb{H}_T^-)) \rightarrow \text{Gal}(\mathbb{H}_T^-/\Phi) \rightarrow 0;$$

from the equality of T -ranks

$$(8) T\text{-rk}(B^-) = T\text{-rk}(\text{Gal}(\mathbb{H}^-/\Phi)) = T\text{-rk}(\mathcal{A}^-(T)/(T\mathcal{A}^-(T))),$$

we see that for every \mathbb{Z}_p -extension $\mathbb{K}_\infty \subset \mathbb{L} \subset \Phi$, the group $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ contains the nontrivial decomposition group of some prime above p . Moreover, if $a \in A^-(T)$ is such that $\varphi(a)$ generates by restriction

$\text{Gal}(\Phi/(\Phi \cap \overline{\mathbb{K}}))$, then the image $\bar{a} \in \mathcal{A}^-(T)/(T\mathcal{A}^-(T))$ is non trivial. From (8) and (7) we deduce that $\text{Gal}(\Phi/(\Phi \cap \overline{\mathbb{K}}))$ is generated by $\mathbb{Z}_p \varphi(b)$ for some $b \in B^-$ and thus $1 \neq \bar{b} \in \mathcal{A}^-(T)/(T\mathcal{A}^-(T))$, so $b \notin T\mathcal{A}^-(T)$. the rank equality (8) indicates that this holds for all $b \in B^-$, and consequently $\text{ord}_T(A^-(T)) = 1$ and $A^-(T) = B^-$, which is point A, so $B \Rightarrow A$.

The implication $A \Rightarrow C$ is simple: let $\mathbb{L} \subset \Phi$ be any \mathbb{Z}_p -extension. Since $(A')^-(T) = \{1\}$ by assumption and $\text{Gal}(\Phi/\mathbb{K}_\infty)^T = \{1\}$, it

follows that all the primes above p cannot be split in \mathbb{L} , since otherwise, there must exist an $a \in A'(T)$ with $\varphi(a)|_{\mathbb{L}} \neq 1$, which contradicts the premise $(A')^-(T) = \{1\}$, and thus $A \Rightarrow C$. Moreover, if $[\Phi \cap \mathbb{H}' : \mathbb{K}_\infty] < \infty$, then $\text{Gal}(\Phi/\mathbb{K}_\infty) \sim \text{Gal}(\Phi/(KP \cap \mathbb{H}')) \subseteq \varphi(B^-)$. By comparing ranks, we conclude that $\text{Gal}(\Phi/\mathbb{K}_\infty) \sim B^-$ and thus C implies B, which completes the proof. \square

In view of this reduction, it will suffice to prove any of the statements A, B or C in order to confirm the Gross conjecture. We next do this for the case of an imaginary quadratic extension of \mathbb{Q} , thus providing a simple illustration of one of the core ideas of the proof in the next chapter.

2.4. The case of imaginary quadratic extensions. Let \mathbb{K}/\mathbb{Q} be an imaginary quadratic extension of \mathbb{Q} in which p is split. Then $U^{(1)}(\mathbb{K}) = (\mathbb{Z}_p^{(1)})^2$ and $\Omega = \mathbb{K}_\infty \cdot \mathbb{H}_1 \cdot \Omega^-$ is the product of two \mathbb{Z}_p -cyclotomic extensions of \mathbb{H}_1 ; we have $\text{Gal}(\Omega/\mathbb{H}_1) = \varphi(U^{(1)}(\mathbb{K}))$. One may take the second \mathbb{Z}_p -extension in Ω also as being the anticyclotomic extension. In analyzing a similar example, Greenberg makes in [6] the following simple observation: since \mathbb{Q}_p has only two \mathbb{Z}_p -extensions and \mathbb{K}_∞ contains the cyclotomic ramified one, it remains that, locally $\Omega^-/(\mathbb{K}_\infty \cdot \mathbb{H}_1)$ is either trivial or an unramified \mathbb{Z}_p -extension. In both cases, $\Omega^- \subset \mathbb{H}$ is a global, totally unramified \mathbb{Z}_p -extension of $\mathbb{K}_\infty \cdot \mathbb{H}_1$. The remark settles the question of ramification, but does not address the question of concern, namely splitting. However, in this case we know more, from Greenberg's proof of the non-vanishing of the p -adic regulator for the p -units in an abelian extension of \mathbb{Q} . Using the result of Federer and Gross, this is equivalent to the fact that $(A')^-(T) = \{1\}$ in the present case. Therefore in this example, Ω^- cannot possibly split the primes above p .

We give a proof of this fact by means of class field theory, a proof which can therefore be extended to arbitrary CM extensions \mathbb{K}/\mathbb{Q} .

Lemma 4. *For imaginary quadratic \mathbb{K}/\mathbb{Q} we have $A^-(T) = B^-$.*

Proof. We have seen above that $\Omega(\mathbb{K})/\overline{\mathbb{H}}_1$ must be an unramified \mathbb{Z}_p -extension. Since we assumed that p is split in \mathbb{K} , there are two primes $\wp, \bar{\wp} \subset \mathbb{K}$ above p . Let $\mathfrak{P} \in \Omega$ be a prime above \wp , let $\tilde{j} \in \text{Gal}(\Omega/\mathbb{H}_1)$ be a lift of complex conjugation. Since $\Omega_{\mathfrak{P}}/\mathbb{K}_\wp$ is a product of \mathbb{Z}_p -extensions of \mathbb{Q}_p , and since \mathbb{Q}_p does not have two independent ramified \mathbb{Z}_p -extensions, it follows that the inertia group $I(\mathfrak{P}) \cong \mathbb{Z}_p$ is cyclic. The prime \wp is totally ramified in $\mathbb{K}_\infty/\mathbb{K}$, so it also follows that $\tau|_{\mathbb{K}_\infty}$ is a topological generator of Γ . We may in this way fix a lift of Γ to $\tilde{\Gamma} \subset \text{Gal}(\Omega/\mathbb{K})$. Then $\tau^j = j \cdot \tau \cdot j$ generates $I(\mathfrak{P}^j) \cong \mathbb{Z}_p$ and

since $\tau^j|_{\mathbb{K}_\infty} = \tau|_{\mathbb{K}_\infty}$, it follows that $x := \tau^j \cdot \tau^{-1} \in \text{Gal}(\Omega/\mathbb{K})$ fixes \mathbb{K}_∞ . Moreover, x cannot have finite order: indeed, if $x^q = 1$, then $I^q(\wp) = I^q(\overline{\wp})$ and the fixed field $\Omega(\mathbb{K})^{I^q(\wp)}$ is an infinite extension of \mathbb{K} in which the only ramified primes $\wp, \overline{\wp}$ have finite inertia. This would imply the existence of an infinite unramified extension of \mathbb{K} , which is absurd.

We conclude that the primes above \wp are not totally split in $\Omega_1/(\mathbb{H}_1 \cdot \mathbb{K}_\infty)$: otherwise, the primes above $\overline{\wp}$ are also totally split and x must have finite order. In the present case $T\text{-rk}(B^-) = 1$. It follows that Proposition 1 holds for \mathbb{K} and by Lemma 3, this is equivalent to $A^-(T) = B^-$, which completes the proof. \square

3. THE GENERAL CASE

We let $\Omega_1 = \Omega(\mathbb{K})$, so Ω_1/\mathbb{K} is the maximal p -abelian p -ramified extension of \mathbb{K} . It contains in particular \mathbb{K}_∞ and $\mathbb{Z}_p\text{-rk}(\Omega_1/\mathbb{H}_1) = r_2 + 1 + \mathcal{D}(\mathbb{K})$, where $\mathcal{D}(\mathbb{K})$ is the Leopoldt defect. Since \mathbb{K} is CM, complex multiplication acts naturally on $\text{Gal}(\Omega_1/\mathbb{K}_\infty)$ and induces a decomposition

$$\text{Gal}(\Omega_1/\mathbb{K}_\infty) = \text{Gal}(\Omega_1/\mathbb{K}_\infty)^+ \oplus \text{Gal}(\Omega_1/\mathbb{K}_\infty)^-;$$

this allows us to define

$$(9) \quad \begin{aligned} \Omega_1^- &= \Omega_1^{\text{Gal}(\Omega_1/\mathbb{K}_\infty)^+} \\ \Omega_1^+ &= \Omega_1^{\text{Gal}(\Omega_1/\mathbb{K}_\infty)^-}, \end{aligned}$$

two extensions of \mathbb{K}_∞ .

3.1. The contribution of class field theory. We shall prove below that $[\Phi \cap \mathbb{H}' : \mathbb{K}_\infty] < \infty$. Since this is one of the three equivalent formulations of the Gross conjecture, proved in Lemma 3, the Theorem 1 then follows. For the proof of the above fact, we use a decomposition of $\Omega_1^-/\overline{\mathbb{H}}_1$ in a product of s subextensions with groups of equal \mathbb{Z}_p -rank, and such that in each extension there is exactly one pair of complex conjugate primes from \mathbb{K} which are not completely split: it will turn out by using the arguments in the proof of Lemma 4, that these primes only split in finitely many factors in the given extension.

The extension Ω_1/\mathbb{K} is an infinite extension with $\overline{\mathbb{H}}_1 \subset \Omega_1$ and $\mathbb{Z}_p\text{-rk}(\text{Gal}(\Omega_1/\mathbb{H}_1)) = \mathcal{D}(\mathbb{K}) + r_2(\mathbb{K}) + 1$ (see. [13], p. 144). Here $r_2(\mathbb{K})$ is the number of pairs of conjugate complex embedding and the 1 stands for the extension $\mathbb{K}_\infty/\mathbb{K}$, while $\mathcal{D}(\mathbb{K})$ is the *Leopoldt defect*, which is expected to vanish. We write $\mathcal{X} = \text{Gal}(\Omega_1/\mathbb{H}_1)$ and $\mathcal{X}_0 = \text{Gal}(\Omega_1/\overline{\mathbb{H}}_1)$.

Recall that $\mathfrak{K} := \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a galois algebra and Δ lifts by continuity to a subgroup of $\text{Gal}(\mathfrak{K}/\mathbb{Q}_p)$. In particular Δ and j act on U_1 and we have a canonic splitting $U_1 = U_1^+ \oplus U_1^-$. Since we assumed that the primes above p in \mathbb{K}^+ split in \mathbb{K}/\mathbb{K}^+ , if $u \in U_1$ has $\iota_{\wp}(u) = x$, $\iota_{\bar{\wp}}(u) = y$, then ju verifies

$$\iota_{\wp}(ju) = \bar{y}, \quad \iota_{\bar{\wp}}(ju) = \bar{x}.$$

Moreover, $u \in U_1^-$ iff $u = v^{1-j}$, $v \in U$; we also have then $\mathbf{N}_{\mathfrak{K}/\mathbb{Q}_p}(u) = 1$. Thus, if $\iota_{\wp}(v) = v_1$ and $\iota_{\bar{\wp}}(v) = v_2$, then

$$(10) \quad \iota_{\wp}(u) = v_1/\bar{v}_2, \quad \iota_{\bar{\wp}}(u) = v_2/\bar{v}_1 = 1/\overline{\iota_{\wp}(u)}.$$

One can analyze U_1^+ in a similar way. The group $\text{Gal}(\overline{\mathbb{H}}_1/\mathbb{H}_1) = \mathcal{X}/\mathcal{X}_0$ is an invariant factor of $\mathcal{X} = \varphi(U_1^{(1)}/\overline{E}_1)$ under the action of Δ by conjugation on \mathcal{X} . Let

$$\mathfrak{A}(\Delta) = \left\{ x \in \mathbb{Z}_p[\Delta] : x = \sum_{\sigma \in \Delta} x_{\sigma} \sigma, \text{ with } \sum_{\sigma} x_{\sigma} = 0 \right\}$$

be the augmentation ideal of $\mathbb{Z}_p[\Delta]$. Then \mathfrak{A} annihilates $\mathcal{X}/\mathcal{X}_0$ and $U^{(1)}(\mathbb{Q}_p)$. By choosing $\tilde{\Gamma} := \varphi^{-1}(U^{(1)}(\mathbb{Q}_p)) \subset \text{Gal}(\Omega_1/\mathbb{H}_1)$ we obtain a natural lift of $\text{Gal}(\overline{\mathbb{H}}_1/\mathbb{H}_1)$. Having assumed that the norms are surjective in $\mathbb{K}_{\infty}/\mathbb{K}$ we also have $\mathbb{H}_1 \cap \mathbb{K}_{\infty} = \mathbb{K}$ and thus $\text{Gal}(\overline{\mathbb{H}}_1/\mathbb{K}) = \Gamma \times \text{Gal}(\mathbb{H}_1/\mathbb{K})$. The group $\tilde{\Gamma}$ is a lift of Γ , since it restricts to a subgroup of Γ and $U^{(1)}(\mathbb{Q}_p) \subset U_1^{(1)}$ is not contained in any strictly larger cyclic subgroup of $U_1^{(1)}$. We fix furthermore a lift $\tilde{j} \subset \mathcal{X}$ of j .

Let us write for simplicity $U = (U_1^{(1)})^-$. The Artin map is galois covariant, so

$$(11) \quad \text{Gal}(\Omega_1^-/\overline{\mathbb{H}}_1) \cong U/\overline{E}^- \sim U.$$

There exists for each pair of conjugate primes $\wp, \bar{\wp} \subset \mathbb{K}$ above p a subalgebra

$$(12) \quad V_{\wp} = \{u \in U^{(1)} : \iota_{\wp}(u) = 1/\overline{\iota_{\bar{\wp}}(u)}; \iota_{\nu\wp} = 1, \forall \nu \in C \setminus \{1, j\}\},$$

$$U = \prod_{\nu \in C^+} V_{\wp},$$

where the second relation follows from (10) and the definition of U . Since ν acts by conjugation on V_{\wp} we deduce from the above that

$$\mathbb{Z}_p\text{-rk}(U) = s \cdot \mathbb{Z}_p\text{-rk}(V_{\wp}) = \mathbb{Z}_p\text{-rk}(\mathcal{X}_0) = r_2 = s \cdot |D(\wp)|,$$

and thus $\mathbb{Z}_p\text{-rk}(V_{\nu\wp}) = |D(\wp)|$ for all $\nu \in C^+$. There exist extensions $\mathbb{M}_{\nu\wp} \subset \Omega^-$, which are fixed by

$$F_{\nu\wp} = \varphi \left(\prod_{\nu' \in C^+; \nu' \neq \nu} V_{\nu'\wp} \right) \subset \varphi(U)$$

and verify

$$\text{Gal}(\mathbb{M}_{\nu\wp}/(\overline{\mathbb{H}}_1 \cap \mathbb{M}_{\nu\wp})) = \varphi(V_{\nu\wp})|_{\mathbb{M}_{\nu\wp}}.$$

By construction, all the primes above p except for $\wp, \overline{\wp}$, are totally split in $\mathbb{M}_{\wp}/\overline{\mathbb{H}}_1$, while there are only finitely many primes above \wp and $\overline{\wp}$ in \mathbb{M}_{\wp} . We have indeed $\text{Gal}(\mathbb{M}_{\wp}/\overline{\mathbb{H}}_1) \cong V_{\wp}$, since the local Artin symbol vanishes for all conjugate primes, while the \mathbb{Z}_p -ranks of local and global extensions coincide. Therefore $(\wp, \overline{\wp})$ can only split in \mathbb{H}_1/\mathbb{K} . The extension $\Omega^-(\mathbb{K})\overline{\mathbb{H}}_1$ decomposes in

$$(13) \quad \Omega_1^- = \prod_{\nu \in C^+} \mathbb{M}_{\nu\wp}.$$

Suppose that $\mathbb{L} \subset \mathbb{M}_{\wp} \cap \Phi$ is an unramified \mathbb{Z}_p -extension of $\overline{\mathbb{H}}_1$ and let $\mathfrak{P} \subset \mathbb{L}, \mathfrak{p}' \subset \mathbb{K}_{\infty}$ be primes above \wp . Then $\mathbb{L}_{\mathfrak{P}} \supseteq \overline{\mathbb{K}}_{\infty, \wp'} \supset \mathbb{K}_{\wp}$ is a tower of local, abelian extensions. The extension $\mathbb{K}_{\infty, \wp'} = \mathbb{K}_{\wp}[\mu_{p^{\infty}}]$ is the cyclotomic ramified extension of \mathbb{K}_{\wp} . Since $\mathbb{L}_{\mathfrak{P}}/\mathbb{K}_{\infty, \wp'}$ is unramified, it is either the trivial extension, or the \mathbb{Z}_p -unramified extension of \mathbb{K}_{\wp} . Letting $\mathbb{Q}_p^{(ab)}$ be the compositum of the two \mathbb{Z}_p -extensions of \mathbb{Q}_p , we see that $\mathbb{L}_{\mathfrak{P}} \subset \mathbb{K}_{\wp} \cdot \mathbb{Q}_p^{(ab)}$. The group $U_{\wp} \sim \mathbb{Z}_p[D(\wp)]$ (e.g. [13], p. 141) and thus

$$\mathbb{Z}_p\text{-rk}(\varphi(V_{\wp})) = |D(\wp)| = \mathbb{Z}_p\text{-rk}(\mathbb{Z}_p[D(\wp)]) = \mathbb{Z}_p\text{-rk}(U_{\wp}).$$

In particular, there is exactly one \mathbb{Z}_p -subextension $\mathbb{L} \subset \mathbb{M}_{\wp}$ which is fixed under the action of $D(\wp)$ by conjugation, and herewith verifies $\mathbb{L}_{\mathfrak{P}} \subset \mathbb{K}_{\wp} \cdot \mathbb{Q}_p^{(ab)}$. Since \mathbb{Q}_p has only one unramified \mathbb{Z}_p -extension, it follows that there exists exactly one unramified \mathbb{Z}_p -subextension $\overline{\mathbb{H}}_1 \subset \mathbb{L} \subset \mathbb{M}_{\wp}$, which is also a \mathbb{Z}_p -extension of \mathbb{K}_{∞} . The prime \wp' may split in $\overline{\mathbb{H}}_1/\mathbb{K}_{\infty}$ and also in some finite subfield of \mathbb{L} . We denote this unique unramified subextension by

$$\mathbb{U}_{\wp} = \mathbb{M}_{\wp} \cap \Phi.$$

From $\Omega^-(\mathbb{K}) = \prod_{\nu} \mathbb{M}_{\nu\wp}$ and $\mathbb{M}_{\nu\wp} \cap \Phi = \mathbb{U}_{\nu\wp}$, we deduce

$$(14) \quad \overline{\mathbb{H}}_1 \cdot \Phi = \overline{\mathbb{H}}_1 \cdot \prod_{\nu \in C^+} \mathbb{U}_{\nu\wp}.$$

Since $\overline{\mathbb{H}}_1 \subset \Phi$ by definition, and not all cyclic subextensions in $\overline{\mathbb{H}}_1/\mathbb{K}_\infty$ need be \mathbb{Z}_p -extendable, the factor $\overline{\mathbb{H}}_1$ appearing in the above identity cannot be removed. Whether or not the inclusion $\mathbb{U}_\wp \cap \overline{\mathbb{H}}_1 \supseteq \mathbb{K}_\infty$ is an equality, is a question related to *floating elements*: i.e. $a = (a_n)_{n \in \mathbb{N}} \in A$ with $a_1 = 1$. The intersection is trivial iff $\text{Gal}(\mathbb{U}_\wp/\mathbb{K}_\infty) = \mathbb{Z}_p\varphi(b)$ for some $b \in B^-$ and b is floating. This question is interesting in itself, but will not be of further relevance for our present purpose. We have thus proved:

Lemma 5. *Let \mathbb{K} be a galois CM extension and assume that the primes $\wp^+ \subset \mathbb{K}^+$ split in \mathbb{K}/\mathbb{K}^+ . For each prime $\wp \subset \mathbb{K}$ there is a canonic (up to finite subextensions) \mathbb{Z}_p -extension $\mathbb{U}_\wp \subset \Omega^-(\mathbb{K}) \cap \mathbb{H}$ in which all the primes above p are split, except possibly for $(\wp, \overline{\wp})$. In particular, Ω^- contains exactly $s = |C|/2$ unramified \mathbb{Z}_p -extensions of \mathbb{K}_∞ .*

3.2. Proof of Theorem 1. We shall now use the same arguments like in the proof of Lemma 4 and show that for all $\nu \in C^+$ the extensions $\mathbb{U}_{\nu\wp}$ do not split the primes $(\nu\wp, \nu\overline{\wp})$. Since for each ν , different primes are inert in $\mathbb{U}_{\nu\wp}$ and the compositum of all these extensions is Φ , this implies that $[\Phi \cap \mathbb{H}' : \mathbb{K}_\infty] < \infty$. We are thus left to prove:

Lemma 6. *Let $\wp \subset \mathbb{K}$ be any prime above p and let \mathbb{U}_\wp, Φ be defined like above. Then $\wp, \overline{\wp}$ are not totally split in \mathbb{U}_\wp .*

Proof. Let \wp be fixed and $\mathbb{U} = \mathbb{U}_\wp$. Since Ω/\mathbb{H}_1 is abelian, the extension \mathbb{U}/\mathbb{H}_1 is also galois and abelian.

Let $\mathfrak{P} \subset \mathbb{U}$ be a fixed prime above \wp and $\tilde{j} \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ be a lift of complex conjugation. Let $I(\mathfrak{P}), I(\mathfrak{P}^{\tilde{j}}) \subset \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ be the inertia groups of the two conjugate primes. Like in Lemma 4, $\text{Gal}(\mathbb{U}/\mathbb{H}_1) \cong \mathbb{Z}_p^2$ and $\mathbb{U}_{\mathfrak{P}}/\mathbb{K}_\wp$ is a product of at most two \mathbb{Z}_p -extensions of \mathbb{Q}_p . It follows that the inertia groups are isomorphic to \mathbb{Z}_p and distinct: otherwise, their common fixed field in \mathbb{U} would be an unramified \mathbb{Z}_p -extension of \mathbb{H}_1 , which is absurd.

For $\nu \in C \setminus \{1, j\}$, the primes above $\nu\wp$ are totally split in $\mathbb{U}/\mathbb{K}_\infty$. Let $\tilde{\tau} \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ generate the inertia group $I(\mathfrak{P})$, so that a generator of $I(\mathfrak{P}^{\tilde{j}})$ is $\tilde{\tau}^{\tilde{j}} \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$. The primes $\wp, \overline{\wp}$ are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$ so $\tilde{\tau}, \tilde{\tau}^{\tilde{j}}$ restrict to the same topological generator of Γ , while $\tilde{\tau}^{1-\tilde{j}} \in \text{Gal}(\mathbb{U}/\mathbb{K}_\infty)$ has infinite order, – as a consequence of $I(\mathfrak{P}) \cap I(\mathfrak{P}^{\tilde{j}})$ being finite. It follows that the prime $\wp' \subset \overline{\mathbb{H}}_1$ above \wp and below \mathfrak{P} cannot be totally split in $\mathbb{U}/\overline{\mathbb{H}}_1$, so $[\mathbb{U} \cap \mathbb{H}' : \mathbb{K}_\infty] < \infty$. This completes the proof of the lemma and, in view of the remarks preceding it, the proof of Theorem 1. \square

We have shown in Lemma 3 that $[\mathbb{H}' \cap \Phi : \mathbb{K}_\infty] < \infty$ is equivalent to the Gross conjecture, so the proof is complete.

Remark 1. *The above proof is intimately related to the case when \mathbb{K} is CM and \mathbb{K}_∞ is the \mathbb{Z}_p -cyclotomic extension of \mathbb{K} . The methods can be extended to non CM fields, with the use of some additional ingredients. These have been sketched in [11] and will be exposed in depth in an ulterior paper. Carroll and Kisilevsky¹ have given in [3] examples of \mathbb{Z}_p -extensions other than the cyclotomic, in which $A'(T) \neq \{1\}$.*

Acknowledgment: I thank Vicențiu Pașol for helpful discussions and comments during the writing of preliminary versions of this paper.

REFERENCES

- [1] J. Ax. On the units of an algebraic number field. *Illinois Journal of Mathematics*, 9:584–589, 1965.
- [2] A. Brumer. On the Units of Algebraic Number Fields. *Mathematika*, 14:121–124, 1967.
- [3] J. Carroll and H. Kisilevsky. On the Iwasawa invariants of certain \mathbb{Z}_p -extensions. *Compositio Mathematica*, 49(2):217–229, 1983.
- [4] L. Federer and B. Gross. Regulators and Iwasawa modules. *Invent. Math.*, 62(3):443–457, 1981.
- [5] R. Greenberg. On a certain ℓ -adic representation. *Invent. Math.*, 21:117–124, 1973.
- [6] R. Greenberg. On the Iwasawa invariants of totally real fields. *American Journal of Mathematics*, 98:263–284, 1973.
- [7] K. Iwasawa. On \mathbb{Z}_ℓ - extensions of number fields. *Ann. Math. Second Series*, 98:247 – 326, 1973.
- [8] J. Jaulent. Sur les conjectures de Leopoldt et Gross. In *Journées Arithmétiques de Besançon (1985)*, volume 147-48 of *Astérisque*, pages 107–120, 1987.
- [9] L. Kuz'min. The Tate module for algebraic number fields. *Math. USSR Izvestija*, 6(2):263–321, 1972.
- [10] M. Le Floch, A. Movahhedi, and T. Nguyen-Quang-Do. On capitulation cokernels in Iwasawa theory. *American Journal of Mathematics*, 127(4):851–877, 2005.
- [11] P. Mihăilescu. The T and T^* components of Λ - modules and Leopoldt's conjecture. Math. Arxiv, Sept. 2010. <http://front.math.ucdavis.edu/0905.1274>.
- [12] P. Mihăilescu. The Leopoldt Conjecture for CM fields. Math. Arxiv, May 2011. <http://front.math.ucdavis.edu/1105.4544>.
- [13] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined Second Edition edition, 1990.
- [14] S. Seo. On the Tate module of a number field. Downloadable preprint, ASARC, Korea, July 2011. http://mathsci.kaist.ac.kr/asarc/bbs/view.php?board_id=preprint&no=93.

(P. Mihăilescu) MATHEMATISCHES INSTITUT DER UNIVERSITÄT GÖTTINGEN
E-mail address, P. Mihăilescu: preda@uni-math.gwdg.de

¹I am grateful to Hershy Kisilevsky for having pointed me out this result.