IWASAWA'S CONSTANT $\mu$ VANISHES IN CYCLOTOMIC $\mathbb{Z}_p$-EXTENSIONS OF CM FIELDS

PREDA MIHĂILESCU

Abstract. Let $K$ be a galois CM extension of $\mathbb{Q}$ and $K_\infty$ its cyclotomic $\mathbb{Z}_p$-extension. Let $A_n$ be the $p$-parts of the class groups in the intermediate subfields $K_n \subset K_\infty$ and $A = \lim_{\leftarrow} A_n$. We show that the $p$-rank of $A$ is finite, which is equivalent to the vanishing of Iwasawa's constant $\mu$ for $A$.

1. Introduction

Let $p$ be an odd prime and $K \supset \mathbb{Q}[\zeta]$ be a CM galois extension containing the $p$-th roots of unity, while $(K_n)_{n \in \mathbb{N}}$ are the intermediate fields of its cyclotomic $\mathbb{Z}_p$-extension $K_\infty$. Let $A_n = (\mathcal{C}(K_n))_p$ be the $p$-parts of the ideal class groups of $K_n$ and $A = \lim_{\leftarrow} A_n$ be their projective limit. We denote as usual the galois group $\Gamma = \text{Gal}(K_\infty/K)$ and $\Lambda = \mathbb{Z}_p[[\tau]] \cong \mathbb{Z}_p[[T]]$, where $\tau \in \Gamma$ is a topological generator and $T = \tau - 1$; we let

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

Iwasawa proved in [3] that there are three constants $\lambda, \mu, \nu \in \mathbb{Z}$ which depend only on $K$, such that for sufficiently large $n$,

$$v_p(|A_n|) = \mu p^n + \lambda n + \nu.$$ 

Ferrero and Washington proved in 1980 [1] that $\mu = 0$ for abelian fields $K$ (see also [3], Theorem 7.15). In this paper we prove

Theorem 1. Let $K$ be a CM field and $A = \lim_{\leftarrow} A_n$ be the limit of the $p$-parts of the ideal class groups of the intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension $K_\infty/K$. Then $\mu(A) = 0$. 

Date: Version 1.00 January 20, 2013.
1.1. Notations and plan. The field \( K \) is assumed to be a CM galois extension of \( \mathbb{Q} \) with group \( \Delta \), containing a \( p \)-th root of unity \( \zeta \), and \( K \) contains \( \mathbb{Q} \). We let \( (\zeta_p^n)_{n \in \mathbb{N}} \) be a norm coherent sequence of \( p^n \)-th roots of unity, so \( K_n = \mathbb{K} \). Thus we shall number the intermediate extensions of \( K_\infty \) by \( K_1 = K, K_\infty = \mathbb{K} \). We have uniformly, for sufficiently large \( n \), that \( K_n \) contains the \( p \)-th but not the \( p^{n+1} \)-th roots of unity. In our numbering, \( \omega_n \) annihilates \( K_n^\times \) and all the groups related to \( K_n \), such as \( \mathcal{O}(K_n), \mathcal{O}^\times(K_n) \), etc.

Let \( A = \mathcal{C}(\mathbb{K})_p \), the \( p \)-Sylow subgroup of the class group \( \mathcal{C}(\mathbb{K}) \). The \( p \)-parts of the class groups of \( K_n \) are denoted by \( A_n \) and they form a projective sequence with respect to the norms \( N_{m,n} := N_{K_m/K_n}, m > n > 0 \), which are assumed to be surjective. The projective limit is denoted by \( A = \lim_{\leftarrow n} A_n \).

If \( X \) is a \( \Lambda \)-module, then \( X^\circ \subset X \) denotes its \( \mathbb{Z}_p \)-torsion. If \( X \) has no finite \( \mathbb{Z}_p \)-torsion, then \( X^\circ \) is the \( \mu \) - part of \( X \). For instance, if \( X = A^- \), then \( X^\circ \) is the \( \mu \) - part of this module, thus the maximal \( \Lambda \)-submodule of finite order and the sum of all cyclic submodules with this property. We shall write for simplicity \( M \subset A \) for the infinite part of the \( \mathbb{Z}_p \)-torsion; this is a canonical module on the minus part, but not necessarily on the plus part. The purpose will be to show that \( M = \{1\} \).

For finite abelian \( p \)-groups \( X \), the exponent of \( X \) is the smallest power of \( p \) that annihilates \( X \); the subexponent

\[
\text{sexp}(X_p) = \min \{ \text{ord}(x) : x \in X \setminus X_p \}.
\]

We shall give here first a proof of the fact that \( \mu^- = \mu(A^-) = 0 \) for CM galois extensions which contain the \( p \)-th roots of unity. This is the main step of the proof. The fact that \( \mu^+ = 0 \) then follows quite easily by reflection. For our proof we need the following consequence Theorem 6 of Iwasawa, [3] (see also [6], Lemma 13.15):

**Lemma 1.** Let \( x = (x_n)_{n \in \mathbb{N}} \in M \) with \( x_m = 1 \). Then \( T x \in \omega_m M \).

**Proof.** Lemma 13.15 in [6] directly implies that \( T x \in \omega_m A^- \), so let \( b \in A^- \) with \( T x = \omega_m b \). Then \((\omega_m b)^{\text{ord}(x)} = 1 \), so \( b \) is a torsion element and thus \( b \in M \), which confirms the claim. \( \square \)

We let \( a = (a_n)_{n \in \mathbb{N}} \in M^- \) and show that \( p - \text{rk}(\Lambda a_n / \langle \Lambda a_n \rangle) = \deg(\nu_{a,n}) \) for sufficiently large \( n \). For such \( n \), we choose a totally split prime \( \Omega_n \in a_n \) and construct, using an idea of Thaine, the lateral field \( \mathbb{F}_n = K_n[t^{1/p}] \), which is the compositum with the extension of degree \( p \) contained in the \( q \)-th cyclotomic extension, where \( q \) is the rational prime above \( \Omega_n \); the radical \( t = g(\chi)^p \) is the power of a Gauss sum. The sequence \( a \) lifts to a sequence \( b \in A^-(\mathbb{F}_\infty) \), where \( \mathbb{F}_\infty = K_\infty[t^{1/p}] = \)
\[ \mathbb{K}_\infty[g(\chi)]. \] The construction is summarized in Proposition \[ \square \] in Chapter 2. In the same Chapter we give a description of the kernels of norm and augmentation of the ideal class groups in the cyclic extension \( F_m/\mathbb{K}_m \) defined above.

Based on these auxiliary results deduced in Chapter 2, we complete the proof of the main theorem in Chapter 3. We use Kummer theory and properties of \( \Lambda \)-modules in order to show that \( b \) has contradictory properties: if \( \nu \) generates \( \text{Gal}(F_n/\mathbb{K}_n) \), then \( b^{\nu-1} = 1 \) and \( b^{\nu-1} \neq 1 \). This is proved in the crucial Lemmata \[ \Box \] and \[ \mathfrak{B} \] of Chapter 3. The contradiction implies that \( a \) cannot exist and \( M^- = \{1\} \). The proof of Theorem \[ \square \] follows by reflection.

If \( L \) is a CM extension which does not have the properties used in this proof, then there is a finite extension \( \mathbb{K} \supset L \) which is both galois and contains the \( p \)-th roots of unity. Then \( \mu = 0 \) for \( \mathbb{K} \), and since \( \mathbb{K} \) is CM, complex conjugation is an automorphism of \( L \) and we may define \( \mathbf{A}^- \) although the extension is not galois. Assuming that \( M = (\mathbf{A}^-)(L)) \neq \{1\} \), the lift \( \iota_{\mathbb{K}/L}(M(L)) \subset \mathbf{A}^- (\mathbb{K}) \) cannot be trivial, because primes in classes of \( \mathbf{A}^- (L) \) do not capitulate in \( \mathbb{K}_\infty/L_\infty \). One verifies that this lift contains non trivial elements in \( (\mathbf{A}^-)^{\circ} \), which contradicts the result previously obtained. Therefore the restriction to the fields \( \mathbb{K} \) as defined above is not a loss of generality.

2. Auxiliary results

We assume that \( M^- \neq \{1\} \) and show first:

**Lemma 2.** For each \( a \in M^- \) there is an \( n(a) \) such that for all \( n \geq n(a) \),

1. \[ \text{ord}(a_n) = \text{ord}(a), \] and \[ p^{-\text{rk}(\Lambda a_n)} > p^{n-1} - p^{n(a)-1}. \]

*Proof.* The module \( M^- \) is finitely generated so \( M^-/(p,T)M^- \) is a finite dimensional \( \mathbb{F}_p \)-vector space. Consequently, there is an \( a \in M^- \setminus (p,T)M^- \) with maximal order among all elements with non trivial image in \( M^-/(p,T)M^- \). Let \( q = \text{ord}(a) \) and \( \mathcal{A} = \Lambda a, \mathcal{A}_n = \Lambda a_n \). We show that if \( n(a) = \min\{m : \text{ord}(a_m) = q\} \), then the claim of the Lemma is fulfilled. We prove this by induction on \( n \geq n(a) \); the claim is true for \( n = n(a) \), since \( p^{-\text{rk}(\Lambda a_n(a))} > 0 \). Suppose that the claim holds for all \( m < n \).

Recall that \( \omega_n = (T+1)^{p^{n-1}} - 1 \equiv T^{p^{n-1}} \mod p \) for all \( n \). We have by definition \( \text{ord}(a_n) \leq \text{ord}(a) = q \) and from \( \text{ord}(a_{n-1}) = \text{ord}(N_{n,n-1}(a_n)) \), it also follows that \( \text{ord}(a_n) \geq q \), so \( \text{ord}(a_n) = q \). We use additive notation for typographic simplicity. The group ring relation \( N_{n,n-1} = \)
\( p \omega_n u + \omega_n^{p-1}, u \in \Lambda^x \) can be verified from the definition of the norm \( N = ((\omega_n + 1)^p - 1)/(\omega_n) \); this yields

\[ \iota(a_{n-1}) = \nu_{n,n-1}(a_n) = (p \omega_n u + \omega_n^{p-1}) a_n, \]

and by comparing orders, it follows that \( \text{ord}(\omega_n^{p-1} a_n) = q \). Thus

\[ q = \text{ord}(a_n) \geq \text{ord}(T^j a_n) \geq \text{ord}(T^{(p-1)p^{n-1}} a_n) = q, \quad 0 \leq j < (p-1)p^{n-1}, \]

and thus \( \text{ord}(T^j a_n) = q \) for all \( 0 \leq j < (p-1)p^{n-1} \). By applying the same argument to the pairs \( T^k a_n, \iota(T^k a_{n-1}), k < p^{n-1} - p^{n(a)-1} \), we find that \( p - \text{rk}(A_n) > p^{n-1} - p^{n(a)-1} \) and \( \text{ord}(T^j a_n) = q \) for all \( j \leq p^{n-1} - p^{n(a)-1} \), which completes the proof. \( \square \)

The next lemma investigates the growth of orders of classes in a cyclic extension of degree \( p \).

**Lemma 3.** Let \( L/K \) be a cyclic galois extension of degree \( p \) and \( b \in \mathcal{A}(L) \) be a class with norm \( a = N(b) \) and assume that the ideal lift map \( \iota : \mathcal{A}(K) \to \mathcal{A}(L) \) is injective. Then \( \text{ord}(b) \leq \text{ord}(a) \).

**Proof.** Let \( \nu \in \text{Gal}(L/K) \) be a generator and \( s = \nu - 1, N = N_{L/K} \).

Then

\[ N = \frac{(s + 1)^p - 1}{s} = s^{p-1} + p\left(1 + s\left(\frac{p}{2}\right)/p + \ldots\right) = pu(s) + s^{p-1}, \quad u \in (\mathbb{Z}_p[s])^x. \]

Let \( \iota : \mathcal{A}(K) \to \mathcal{A}(L) \) be the ideal lift map and \( q = \text{ord}(a) \). Then

\[ \iota(a) = b^{\text{ord}(a)} b^{s^{p-1}}, \]

and thus

\[ q \geq \min \left(\text{ord}(b)/p, \text{ord}(b^{s^{p-1}})\right). \]

If \( \text{ord}(b) \leq pq \), the claim of the lemma is true. Assume thus that \( \text{ord}(b) \geq p^2q \). The above inequality implies then that \( \text{ord}(b^{s^{p-1}}) \leq q \).

Let \( y = b^q \in B \). Then \( y^{s^{p-1}} = 1 \) and

\[ N(y) = \iota(a)^q = 1 = y^{\text{ord}(a)} y^{s^{p-1}} = y^{\text{ord}(a)}. \]

Since \( u \in (\mathbb{Z}_p[s])^x \) it follows that \( \text{ord}(y) \leq p \) and thus \( \text{ord}(b) \leq pq \). This completes the proof of the lemma; note that the result is a fortiori true in the case in which \( \iota : \mathbb{Z}_p a \to B \) is not injective, a fact which is not required in our subsequent proofs. \( \square \)

In order to prove that \( \mu^\perp = 0 \), we shall use the type of auxiliary construction introduced by Thaine in [5]. Applied to our context, this yields:
Lemma 4. Let $K$ be like above and $a = (a_n)_{n \in \mathbb{N}} \in M^− \setminus (p,T)M^−$ have maximal order among all $a \in M^−$; let $n > n(a)$, with $n(a)$ defined in Lemma 2. Then there is a prime $Q \in a_n$ which is totally split above $Q$, unramified in $K$ and such that $p^{(q-1)/p} \not\equiv 1 \mod q$, where $q$ is the rational prime below $Q$.

Let $t' = g(\chi) \in Q[\zeta_p, \zeta_q]$ be the Gauss sum of an irreducible character of conductor $q$ and order $p$ and $t = (t')^p \in Q[\zeta_p] \subset K$. For all $m > 0$, we let $F_m = K_m[t^{1/p}] = K_n[t']$ and $F_0 = Q[g(\chi)]$ and $A(F) = \lim_{m \to \infty} A(F_m)$, $M^−(F) = (A^−(F))^\circ$. The extensions $F_m/K_m$ are unramified outside $q$ for all $m > 0$ and $Q$ is totally ramified in $F_n/K_n$. If $R \subset F_n$ is a ramified prime above $Q$ and $b_n = [R] \in A_n^−(F_n)$ is its class, then $b_n$ lifts to a norm coherent sequence $b = (b_m)_{m \in \mathbb{N}} \in M^−(F)$.

The ideal class lift map $\iota_m : A^−(K_m) \to A^−(F_m)$ is injective and $N : A(F_m) \to A(K_m)$ is surjective.

Proof. We first show that one can choose a prime $Q$ as claimed in the lemma. The primes which are totally split in $K_n$ and unramified have density 1. If $Q$ is such a prime and $q \in \mathbb{Z}$ is the rational prime below it, the condition $p^{(q-1)/p} \not\equiv 1 \mod q$ is equivalent to $q$ being inert in $K_n[p^{1/p}]$, while $Q \in a_n$ translates into the fact that the Artin symbols $\varphi(Q) = \varphi(a_n)$ in the Hilbert class field $H_n/K_n$. Since $H_n, K_n[p^{1/p}]$ are linearly disjoint over $K_n$—one field being unramified, the other ramified at $p$—we may apply Tchebotarew, which implies that the primes $Q$ with the desired properties have positive density in $K_n$. Let thus $Q$ be one of these primes and $q \in \mathbb{N}$ be the rational prime below it.

Let $t'$ be the Gauss sum defined in the hypothesis. Since $\zeta_p \in K$, it follows that $t = (t')^p \in K$. Moreover, $F_0, K$ are linearly disjoint over $Q$, since $q$ is the only ramified prime in the first extension; by choice of $Q$, it is unramified in $K$. Therefore $\text{Gal} (F_n/Q) = \text{Gal} (K_n/Q) \times \text{Gal} (F_0/Q)$ and in particular, $F_n$ is also a CM galois extension. Let $\nu \in \text{Gal} (F_0/Q)$ be a generator and $s = \nu - 1$; since $F_0$ and $K$ are linearly disjoint over $Q$, the first field being ramified only at $q$, while $K$ is unramified at $Q$, it follows that $F_m = K_m[g(\chi)]$ and $F_\infty = K_\infty[g(chi)] = \cup_m F_m$ are well defined and $\text{Gal} (F_m/Q) = \text{Gal} (K_m/Q) \times < \nu >$. We write

\[(2) \quad N = N_{F_0/Q} = N_{F_n/K_n} = p + sN'(s) = pu(s) + s^{p-1},\]

according to the decomposition of the norm in $p$-cyclic extensions that follows from $N = \frac{(s+1)^{p-1}}{s}$. Since $F_n/K_n$ is cyclic ramified at $q$, all the primes above $q$ ramify in this extension. Let $R \subset F_n$ be a ramified prime above $Q$ and $b_n = [R]$ be its class and $B_n = \Lambda b_n$. Let $\iota :
$A(\mathbb{K}_n) \to A(\mathbb{F}_n)$ be the ideal lift map; since $\mathbb{F}_n$ is CM and $a_n \in A^-_n$, the lift is injective on $A_n$.

For $m > n$ we may choose by Tchebotarew a prime $\mathfrak{A}_m \subset \mathbb{F}_m$ such that $N_{\mathbb{F}_m/\mathbb{K}_m}(\mathfrak{A}_m) \in a_m$ and $N_{\mathbb{F}_m/\mathbb{F}_n}(\mathfrak{A}_m) \in b_m$, the two extensions $\mathbb{F}_m/\mathbb{K}_m, \mathbb{F}_m/\mathbb{F}_n$ being linearly disjoint over $\mathbb{K}_m$. Letting $b_m = [\mathfrak{A}_m]$ be may define this way a norm coherent sequence that lifts $a$ to $A(\mathbb{F})$ and $N_{\mathbb{F}_\infty/\mathbb{K}_\infty}(b) = a$. The sequence is defined modulo $\ker (N_{\mathbb{F}_\infty/\mathbb{K}_\infty} : A(\mathbb{F}) \to A(\mathbb{K}))$. By construction, we may assume that $b_m \in A(\mathbb{F}_m)^-$ and $\ord(b_m) \leq \ord(a_m)$, by Lemma 3. Therefore $b \in M^-$. The ideal lift map $\iota_m$ is injective, since $\mathbb{F}_m$ is CM and there is no capitulation of ideals in the minus part of class groups in CM extensions. For the surjectivity of the norm, we invoke again Tchebotarew’s Density Theorem. Let $H_m/\mathbb{K}_m$ be the maximal $p$ abelian unramified extension of $\mathbb{K}_m$ and $M_m = H_m[g(\chi)]$. The extensions $\mathbb{F}_m, H_m$ are linearly disjoint, the first being totally ramified. Therefore the galois group $\Gal(M_m/\mathbb{K}_m)$ is a direct product. Let $a \in K_m$ be any ideal class and $x = \varphi(a) = (H_m/\mathbb{K}_m) \in \Gal(H_m/\mathbb{K}_m)$, while $x' = (x, 1) \in (H_m/\mathbb{K}_m) \times \Gal(\mathbb{F}_m/\mathbb{K}_m)$. By Tchebotarew’s Theorem, there are infinitely many primes $p \subset K_m$ which are totally split above $\mathbb{Q}$ and whose Frobenius conjugacy class (in this case: Artin symbol) in $H_m/K_m$ is $x'$. These primes belong by construction to the class $a$ and they are totally split in $\mathbb{F}_m/\mathbb{K}_m$. Let $\mathfrak{P} \subset \mathbb{F}_m$ be any prime above $p$ and $b = [\mathfrak{P}]$. By construction, we have $N(b) = a$, which confirms the claim.

We now show that there are unramified extensions of $\mathbb{F}_m$ with galois group isomorphic to $\Lambda b_m$:

**Lemma 5.** Let $\mathbb{K}_m, \mathbb{F}_m$ be like above and $\mathcal{A}_m = \Lambda a_m, \mathcal{B}_m = \Lambda b_m$. Then there are unramified extensions $\mathbb{K}_{m,a}/\mathbb{K}_m, \mathbb{F}_{m,b}/\mathbb{F}_m$ with $\Gal(\mathbb{K}_{m,a}/\mathbb{K}_m) \cong \mathcal{A}_m$ and $\Gal(\mathbb{F}_{m,b}/\mathbb{F}_m) \cong \mathcal{B}_m$. Moreover, $\mathbb{K}_{m,a}[g(\chi)] \subset \mathbb{F}_{m,b}$ and there is an abelian extension $\mathbb{L}_m/\mathbb{K}_m$ with $\mathbb{L}_m[g(\chi)] = \mathbb{F}_{m,b}$ and $\mathbb{K}_{m,a} \subset \mathbb{L}_m$, while $\exp(\Gal(\mathbb{L}_m/\mathbb{K}_{m,a})) = p$.

**Proof.** Since $a \in M^-$ has maximal order, it follows that the sequence

$$\{1\} \to \Lambda a \to M^-(\mathbb{K}) \to C' \to \{1\}$$

is split and the same holds for

$$\{1\} \to \Lambda b \to M^{-}(\mathbb{F}) \to C \to \{1\}.$$ 

Indeed, for the second, if $b^{T_j} \in (M^-(\mathbb{F}))^p$, then taking norms, we would have $a^{T_j} \in (M^-(\mathbb{K}))^p$, which contradicts the fact that $\ord(a)$
is maximal and so is ord($a^{T^j}$) = ord($a$). There is thus a $\mathbb{Z}_p$-module $C$ with $M^-(\mathbb{F}) = (\Lambda b) \oplus C$. Let $C' = N_{\mathbb{F}/\mathbb{K}}(C)$. Then we also have $(\Lambda a) \oplus C' = M^-(\mathbb{K})$ as a consequence of the surjectivity of the norm.

At finite levels, we have $M^m_\mathbb{K} = \mathcal{A}_m \oplus C'_m$ and $M^m_\mathbb{F} = \mathcal{B}_m \oplus C_m$. Moreover, $M^- \subset \mathcal{A}^-$ also has a complement as a $\mathbb{Z}_p$-module, so there are unramified extensions $\mathbb{F}_\infty \subset \mathbb{M}(\mathbb{F}) \subset \mathbb{H}^-(\mathbb{F})$ with $\text{Gal} (\mathbb{M}(\mathbb{F})/\mathbb{F}_\infty) \cong M^-(\mathbb{F})$ and similar for $\mathbb{K}$. By taking the fixed fields of $\varphi(C)|_{\mathbb{M}(\mathbb{F})}$ and $\varphi(C)|_{\mathbb{M}(\mathbb{K})}$, respectively, we obtain unramified extensions $\mathbb{F}_\infty \subset \mathbb{M}(\mathbb{F}) \subset \mathbb{H}^-(\mathbb{F})$ with $\text{Gal} (\mathbb{F}_\infty/\mathbb{F}_\infty) = \varphi(\Lambda b)$ and $\text{Gal} (\mathbb{K}_\infty/\mathbb{K}_\infty) = \varphi(\Lambda a)$. Since $\iota_{\mathbb{K},\mathbb{F}}(C) \subset C'$ by construction, we have $\mathbb{K}_\infty \subset \mathbb{F}_\infty$. At finite levels, we let $\mathbb{F}_m, b = \mathbb{F}_\infty \cap \mathbb{H}(\mathbb{F})$ and $\mathbb{K}_m, a = \mathbb{K}_\infty \cap \mathbb{H}(\mathbb{K})$. The isomorphisms of galois groups are then $\text{Gal} (\mathbb{F}_m/\mathbb{F}_\infty) = \varphi(\Lambda b_m)$ and $\text{Gal} (\mathbb{K}_m/\mathbb{K}_\infty) = \varphi(\Lambda a_m)$, while $\mathbb{K}_m, a[g(\chi)] \subset \mathbb{F}_m, b$. The existence of the abelian extension $\mathbb{L}_m$ follows by Kummer theory. This completes the proof. □

The following is an overview of the properties of the Thaine shifts constructed above:

**Proposition 1.** Notations being like above, we assume that $M^- = (\mathcal{A}^-)^0 \neq \{1\}$ and let $a = (a_m)_{m \in \mathbb{N}} \subset M^- \setminus (p,T)M^-$ be a non trivial element of $M^-$ which has maximal order in this torsion module, and let $\mathcal{A} = \Lambda a$.

We choose a prime $q \in \mathbb{N}$ together with the Thaine shift of $\mathbb{Z}_p$-extensions defined above and $b \in \mathcal{A}^-(\mathbb{F}_\infty)$ such that

1. The prime $Q \subset a_n \subset M_n$ lying above $q$ is totally split in $\mathbb{K}_n/Q$, unramified in $\mathbb{K}$ and inert in $\mathbb{K}_\infty/\mathbb{K}_n$.
2. The Gauss sum $t = g(\chi) \in \mathbb{F}_0$ uniquely defines the Thaine shift $\mathbb{F}_m = \mathbb{K}_m[t], \mathbb{F}_\infty/\mathbb{K}_\infty$.
3. The ramified prime $\mathfrak{R} \subset \mathbb{F}_n$ defines a class $b_n = [\mathfrak{R}] \in (\mathcal{A}(\mathbb{F}_n))^-$ and this class can be lifted using Tchebotarew to a norm coherent sequence $b = (b_m)_{m \in \mathbb{N}} \in \mathcal{A}^-(\mathbb{F}_\infty)$ such that $N_{\mathbb{F}/\mathbb{Q}}(b_m) = a_m$ for all $m$ and $[\mathfrak{R}] = b_n$.
4. The ideal class lift maps $\iota_m : A^- (\mathbb{K}_m) \to A^- (\mathbb{F}_m)$ are injective and the norms $N : A(\mathbb{F}_m) \to A(\mathbb{K}_m)$ are surjective.
5. We have $b \in M^-(\mathbb{F}_\infty) \setminus (p,T)M^-(\mathbb{F}_\infty)$ and $b$ can be chosen among all possible lifts of $b_n$ with norm $a$, such $\Lambda b$ has minimal exponent.
6. For each $m > n$ there are unramified extensions $\mathbb{F}_m, b \subset \mathbb{F}_m$ and $\mathbb{K}_m, a \subset \mathbb{K}_m$ with

\[ \text{Gal} (\mathbb{F}_m, b/\mathbb{F}_m) \cong \Lambda b_m \quad \text{Gal} (\mathbb{K}_m, a/\mathbb{K}_m) \cong \Lambda a_m, \quad \text{and} \]

\[ \mathbb{K}_m, a[g(\chi)] \subset \mathbb{F}_m, b. \]
Moreover, there is an extension $L_m \supset K_{m,a}$ which is abelian over $K_m$ and \( \exp(\Gal(L_m/K_{m,a})) = p \) while $L_m[g(\chi)] = \mathbb{F}_{m,b}$.

The following lemmata investigate some kernels related to the extension of groups $\iota(A(K_m)) \subset A(\mathbb{F}_m)$.

**Lemma 6.** Let $L/K$ be a cyclic extension of CM fields, of degree $p$ and group $< \nu >$ and suppose that $L/K$ is ramified at the primes above $q$ and unramified outside $q$. Let $D \subset A(L)$ be the subgroup generated by the classes of primes which ramify in $L/K$. Let $s = \nu - 1$ and $\zeta = \zeta_{p,s}$ be a root of unity of largest $p$ power order contained in $L$ and $\xi \in K$ with $N(\xi) = \zeta$. There is an $x \in A^{-}(L)$ and $\xi \in x$ with $N(\xi) = \xi^s$ and $x^p \in \iota(A^{-}(K))$. The norm $N : A(L) \to K$ is surjective and the kernel

$$(4) \mathcal{K}_x := \ker \left( s : A^{-}(L) \to A^{-}(L) \right) = D^{-} \cdot \iota(A^{-}(R)) \cdot < x >.$$  

**Proof.** Since $L/K$ is unramified at $p$, it follows that $\zeta^{1/p} \not\in L$ and the extension being CM, it follows from the Kronecker unit theorem, that $\zeta / N(E(L)) \subset E(K)$. The Hasse Norm Principle ([4], Chapter 5, Theorem 4.5, see also [2] for an early version in cyclic $p$-extensions) implies that $\zeta = N(\xi)$ for some $\mu \in L$ and $\langle \xi \rangle = \xi^s$ for some ideal of $L$, since the Hilbert 90 Theorem holds for ideals in cyclic extensions. Letting $x = [y]$, it is a simple verification that for all $\mathfrak{a} \in x$ there is an $\alpha \in L$ with $\mathfrak{a}^s = (\alpha)$ and $N(\alpha) = \zeta$. We may thus write $N(x^s) = \zeta$ in this sense. We have $N(\overline{\xi}/\zeta) = 1$ and by Hilbert 90, $\overline{\xi}^p = \zeta w^s, w \in L^x$. As ideals, we have $\overline{\xi}^{ps} = (w^s)$ and $N(\overline{\xi}/x)^s = 1$, so $x^p \in \iota(A^{-}(K))$, as claimed. The surjectivity of the norm can be proved by Tchebotarew like in the proof of the Lemma [4] which is a special case.

We obviously have $D^{-} \cdot \iota(A^{-}(R)) \cdot < m > \subset \ker(s)$. For ramified ideals $\mathfrak{Q} \in D^-$, note that $N(\mathfrak{Q}) = \mathfrak{Q}^p$ and thus $[\mathfrak{Q}] \in \ker(N)$ iff the class has order $p$ – this settles also the fact that the exactly the $p$-torsion of $D$ is included in the kernel of the norm. Let now $C_1 = \ker(s)/(D \cdot \iota(A(R)))$. There is an isomorphism of $\mathbb{F}_p$-modules

$$\psi : C_1 \to H^0(E, L/K),$$

which was investigated by Furtwängler in the case of unramified extensions. Let $\delta \in E(K) \setminus N(E(L))$; the Hasse Norm Principle implies that there is an $x \in L^x \setminus E(L)$ with $\delta = N(x)$. The prime ideal decomposition of $x$ shows there is an ideal $\mathfrak{a} \subset L$ such that $x = \mathfrak{a}^s$ and one verifies that $\mathfrak{a}$ cannot be principle, otherwise $\delta \in N(E(L))$. We let $\psi([\mathfrak{a}]) = \delta \mod N(E(L))$, and it is a straightforward verification that this definition extends to an isomorphism of $\mathbb{F}_p$-vector spaces. Complex conjugation acts naturally on $C_1$ and $H^0(E, L/K)$ and from the
definition of \( m \) we see that \( < \psi(m) >_{E} = H^0(E, L/K)^- \). This implies the claim \( \square \).

The next result concerns the kernel of the norm:

**Lemma 7.** Notations being like above, let \( \mathbb{F}_\infty = \mathbb{K}_\infty [g(\chi)] \) and \( A(\mathbb{F}) = \lim \limits_{\rightarrow} A(\mathbb{F}_m) \). Then

\[
(5) \quad \text{Ker} \left( N : A^-(\mathbb{F}) \to A^-(\mathbb{K}) \right) = (A^- (\mathbb{F}))^s, \\
\text{Ker} \left( N : A^- (\mathbb{F}_m) \to A^-(\mathbb{K}_m) \right) = (A^- (\mathbb{F}_m))^s,
\]

*Proof.* Let \( m > n \) be a fixed large integer and \( y \in \text{Ker} (N : A(\mathbb{F}_m) \to A(\mathbb{K}_m)) \). Let \( \mathfrak{Z} \subseteq y \) be a prime that is totally split in \( \mathbb{F}_m/\mathbb{Q} \) and \( \eta = \mathfrak{Z} \cap \mathbb{K}_m \). The choice of \( y \) implies that \( \eta = (\gamma) \) is a principal ideal. We show that \( \gamma \) is a divisor of \( \mathfrak{Z} \) in \( \mathbb{F}_m/\mathbb{Z} \). For any prime \( \mathfrak{A} \subseteq \mathbb{F}_m \) with \( \mathfrak{A} \cap \mathbb{Z} = q \), we have \( \gamma \in N(\mathbb{F}_m, q) \) (e.g. [3], Chapter 4). If \( \mathfrak{Z}' \subseteq \mathbb{F}_m \) is a prime above \( q \) and \( q' = q' \cap \mathbb{K}_m \), then \( \mathbb{K}_m, q'/\mathbb{Q}_q \) is an unramified extension and \( \mathbb{F}_m, q'/\mathbb{K}_m, q' \) is the cyclotomic ramified extension of degree \( p \). Since \( \mathfrak{A} \) is totally split, it follows that \( \gamma \in (\mathbb{K}_m, q)^p \) and by local class field theory, it must be a norm: \( \gamma \in N_{\mathbb{F}_m, q'/\mathbb{K}_m, q'}(\mathbb{O}(\mathbb{F}_m, q')) \). We may thus apply the Hasse Norm Principle to the cyclic extension \( \mathbb{F}_m/\mathbb{K}_m \); since \( \gamma \) is a norm at all primes, it must be a global norm. Let \( y = N_{\mathbb{F}_m, \mathbb{K}_m}(w) \). Then

\[ N(\mathfrak{Z}) = (N(w)) \Rightarrow N(\mathfrak{Z}/(w)) = (1). \]

Denoting with \( \mathcal{I} \) the fractional ideals of \( \mathbb{F}_m \) and using \( H^1(\mathcal{I}, \text{Gal} (\mathbb{F}_m/\mathbb{K}_m)) = \{1\} \), we see that there is an ideal \( \mathfrak{Z} \subseteq \mathbb{F}_m \) with \( \mathfrak{Z} = (w)\mathfrak{Z}^s \). In terms of ideal classes we obtain

\[ y = (\mathfrak{Z}) = [(w)\mathfrak{Z}^s] = [\mathfrak{Z}^s] = [\mathfrak{Z}]^s = z^s, \]

for the class \( z = [\mathfrak{Z}] \). Therefore \( y \in A(\mathbb{F}_m)^s \). Passing to projective limits, we obtain the claim.

We have seen in the previous lemma that the norm is surjective, so we may choose a set of elements \( b_1, b_2, \ldots, b_r \in A(\mathbb{F}_m) \) with norms \( a_i = N(b_i), i = 1, 2, \ldots, r \) that form a base for \( A(\mathbb{K}_m) \). Let \( r' = p - \text{rk}(A(\mathbb{F}_m)/A(\mathbb{F}_m)^s) \geq r \) and let the previously chosen elements be extended to a family \( b_1, b_2, \ldots, b_r' \) which forms a \( (\mathbb{Z}_p) \) base for this quotient. It follows from the Nakayama Lemma that they also generate \( A(\mathbb{F}_m) \) as a \( \mathbb{Z}_p[s] \)-module. Suppose now that \( x \in \ker (N) \) and let

\[ x = \prod_i x_i b_i \cdot y(s), \text{ hence } N(x) = 1 = \prod_i x_i a_i, \]

and by definition of the \( a_i \), we must have \( x_i \equiv 0 \mod \text{ord}(a_i) \). We have shown in Lemma that if \( N(b) = a \), then \( \text{ord}(b) \leq p \text{ord}(a) \), we must have \( \prod_{i=1}^r x_i b_i \in A(\mathbb{F}_m)[p] \). \( \square \)
3. Proof of Theorem 1

The results above contain the technical detail which we need for proving the Theorem 1. As mentioned before, the crux of the proof consists in showing that $\mu^- = 0$.

The steps for this proof are the following: assuming the contrary is true, then there is an $a \in M^- \setminus (p,T)M^-$ and we use the construction of Thaine described in Proposition 1. The construction of $b$ is stiffly connected to $a$ and the proof will follow when we show that this connection requires that $b^* = 1$ on the one hand but also makes this condition impossible, so $b^* \neq 1$.

We now prove $\mu^-(\mathbb{K}) = 0$ following the steps described above:

**Lemma 8.** Notations being like above, $b^* = 1$.

**Proof.** Assume that $b^* \neq 1$. By Lemma 3 we know that $\text{ord}(b) \leq \text{pord}(a) < \infty$. On the other hand, for sufficiently large $n$, we have $N_{\mathbb{F}/\mathbb{K}}(T^3b_n) = T^3a_n \neq 0$ for all $0 \leq j < p^{n-1} - p^{n_0(a)-1}$ and $p - \text{rk}(Ab_n) > p^{n-1} - p^{n_0(a)-1}$. Therefore $b \in M^-(\mathbb{F})$. Since $b^* = 1$, it follows from Lemma 1 that $Tb^* \in \omega_nM^-(\mathbb{F}_1)$. There is thus a $c \in M^-(\mathbb{F}_1) \setminus (p,T)M^-(\mathbb{F}_1)$ such that $Tb = \omega_n g(T)c$. Let $C = (\Lambda c)/(\Lambda b^*)$, a $\Lambda$-module of finite exponent. There is an $N > 0$ such that the ring $\mathbb{Z}/(p^N \cdot \mathbb{Z})[T]$ acts on $C$. Let $C^\perp \subset \mathbb{Z}/(p^M \cdot \mathbb{Z})[T]$ be the annihilator and let $j \geq 0$ be the largest integer such that $C^\perp \equiv 0 \mod p^j$. Then $p^j\mathbb{Z}_p[T]/C^\perp$ is a finite dimensional $\mathbb{F}_p[T]$-module, so there is also a minimal $k$ such that $p^jT^k c \in \Lambda b$, thus $p^jT^k c = b^* \cdot v$, $v \in (\mathbb{Z}_p[T])^\times$. Note that $Tb = \omega_n g(T)c$ implies $k > 0$.

Then $N_{\mathbb{F}/\mathbb{K}}(p^jT^k c) = N_{\mathbb{F}/\mathbb{K}}(v(T)b^*) = 1$ and since $c$ has infinite rank, it follows that $N_{\mathbb{F}/\mathbb{K}}(p^j c) = 1$ we assumed $b^* \neq 1$, so a fortiori $p^j c \neq 0$. We can then apply Lemma 7. Then (5) implies that $c = \lim_{m \rightarrow \infty} c_m \in A^-(\mathbb{F})$. Moreover $c^{\text{ord}(b)} = 1$, so $c \in M^-(\mathbb{F})$ and $c = d^s$ for some $d \in A^-(\mathbb{F})$. Hence $d^{\text{sp}(T^k)} = (T^{v^*(T)}/b^s)^s = 1$.

The identity holds a fortiori at all finite levels, where we can apply (4), finding that $b_m = d_m^{v^{-1}(T)\text{sp}(T^k)} \cdot y_m$ with $y_m \in D_m^- \cdot M_m^-(\mathbb{K}_m). A x_m$, where $D_m \subset A^-(\mathbb{F}_m)$ is the submodule generated by ramified primes and $N(x_m') = \zeta_{p^m}$ in the notation of Lemma 3. In our case the preimage of $\zeta_m$ must be an element $\xi_m \in \mathbb{K}_m := \mathbb{F}_0 \cdot \mathbb{Q}[\zeta_{p^m}]$, and thus $x_m \in A(\mathbb{K}_m)$. In particular $x = \lim_{m \rightarrow \infty} x_m$ cannot have bounded order as a consequence of the Theorem of Ferrero and Washington. Therefore

$$b_m = d_m^{v^{-1}(T)\text{sp}(T^k)} \cdot y_m, \quad y_m \in D_m^- \cdot M_m^-(\mathbb{K}_m).$$
The only ramified primed in $\mathbb{F}_m/K_m$ lie above $q$ and since $\mathcal{Q}_n$ is inert in $K_\infty/K_n$, we have $D_m = \iota_{n,m}(D_n)$. The norm coherence of $b_m, c_m$ implies that $y_m \in M_m^*(K_m)$ and thus $b_m/x_m^{-1}(T)^p^{r/T^k} \in M_m^*(K_m)$ and in the limit there is a $z \in t_{K_\infty,F_\infty}M^-(\mathbb{K})$ such that
\[ b = z \cdot x^{-1}(T)^p^{r/T^k}. \]
It follows that $x$ has finite order too and $x \in M^-(\mathbb{F})$. Taking the norm to $K_\infty$, we obtain
\[ a = z^p : N(x)^{r-1}(T)^{p^{r/T^k}}. \]
Since $k > 0$, this is a contradiction to $a \notin (p,T)M^-(\mathbb{K})$. This completes the proof of the Lemma.

The next lemma now proves that the converse of the claim of Lemma \ref{lem:main1} must also hold:

\textbf{Lemma 9.} Notations being like above, $b^{\ast} \neq 1$.

\textit{Proof.} Assume that $b^{\ast} = 1$ and let $\mathbb{F}_{m,b}, K_{m,a}, L_m$ be defined like in Proposition \ref{trans} so $K_{m,a} \subset L_m$ and $L_m[g(\chi)] = \mathbb{F}_{m,b}$. Let $\lambda^- = p - \text{rk}(A^-/M^-)$. Then $p - \text{rk}(\text{Gal}((L_m \cap H_m(\mathbb{K}))/K_{m,a})) \leq \lambda^-$ and thus $L_m/K_{m,a}$ is almost totally ramified. Since $p - \text{rk}(\text{Gal}(L_m/K_{m,a})) \geq p^{n-1} - p^{n(a-1)} \rightarrow \infty$, there is a totally ramified subextension $L_m \supset M_m \supset K_{m,a}$ with
\[ p - \text{rk}(\text{Gal}(M_m/K_{m,a})) > p^{n-2}. \]
The extension $\mathbb{F}_m/K_m$ is unramified outside $q$, so $M_m/K_{m,a}$ can only be ramified at primes above $q$: only ramification at these primes may be absorbed by the adjunction of $g(\chi)$. However, the primes above $q$ are inert in $K_\infty/K_n$, so there are at most $N = [K_n : \mathbb{Q}]$ such primes in $K_m$. The index $m$ can be chosen large enough and since
\[ p^j := \text{ord}(b) = \text{ord}(\alpha) = \exp(\text{Gal}(L_m/K_m)) \]
is independent on $m$, we can assume that $L_m/K_m$ is a Kummer extension. There are thus $R > p^{n-1} - p^{n-1} - \lambda^- > p^{n-2}$ linearly disjoint cyclic extensions
\[ M_m(i) = K_m[\rho_1] \subset M_m \subset L_m, i = 1, 2, \ldots, R, \]
with $[M_m(i) : K_m] = p^j$ and such that $M_m(i)/(M_m(i) \cap K_{m,a})$ has degree $p$ and is ramified at some prime above $q$. Therefore $(\rho_1) = \mathfrak{A}^{p^j} \cdot q^{p^j-1}$ for some ideal $\mathfrak{A} \in A_m^*$, which may also be the trivial ideal, and some ideal $q$ that decomposes in primes above $q$. If $M_m' = \prod_{i=1}^R M_m(i)$ and $M_m' = M_m' \cap K_{m,a}$, then $M_m'/M_m'$ is a $p$-elementary abelian extension with group of rank $R$, totally ramified at primes above $q$. But we have seen that there are at most $N < p^{n-2} < R$ independent primes above
Proof. The assumption that $c$ is a sequence neither can be contradictory, so cannot be fulfilled – therefore $b$ should satisfy simultaneously Lemma 8 and 9. But these conditions are the Thaine-shifted $\mathbb{Z}$-class group of which we constructed a norm coherent sequence $\mu$. Since $\exists d \in \mathbb{P}$ for all $n$ large enough, such that $p - \text{rk}(A_n^-) \leq \lambda^-$ for all $n$. On the other hand, $p - \text{rk}(\Delta c_n) = \infty$ so we may choose $n$ large enough, such that $p - \text{rk}(\Delta c_n) > 2\lambda^-$, say. If $c \in (p, T)\mathbb{A}^+(\mathbb{K})$, there exists a $d \in (p, T)\mathbb{A}^+(\mathbb{K}) \setminus (p, T)\mathbb{A}^+(\mathbb{K})$ such that $c \in \Lambda d$ and a fortiori, $p - \text{rk}(\Lambda d_n) > \lambda^-$. The group $\Lambda d_n$ allows a direct complement $\mathcal{D}_n \subset A^+_{\mathbb{K}}$ as a $\mathbb{Z}_p$-module; by taking the field $\mathbb{K}_{n, d} \subset \mathbb{H}^+_n$ which is fixed under the Artin image $\varphi(\mathcal{D}_n)$, it is granted that $\text{Gal}((\mathbb{K}_{n, d}/\mathbb{K}_n) \cong \Lambda d_n$. If this field is not a Kummer extension, which may happen if $\text{ord}(d)$ is infinite, we may choose a minimal $n' > n$ such that $\mathbb{K}_{n'} \cdot \mathbb{K}_{n,d}$ is a Kummer extension of $\mathbb{K}_{n'}$. Since $\mathbb{K}_{n'}^+ \cdot \mathbb{K}_{n,d}$ is a totally real extension, reflection shows that $j$ commutes with $\text{Gal}((\mathbb{K}_{n'} \cdot \mathbb{K}_{n,d})/\mathbb{K}_{n'})$. Let $\mathbb{K}_{n,d}' = \mathbb{K}_{n'} \cdot \mathbb{K}_{n,d}$ and $R_n := \text{rad}(\mathbb{K}_{n,d}'/\mathbb{K}_{n,d}') \subset \mathbb{K}_{n'}^*$ be the Kummer radical. Since the extension $\mathbb{K}_{n,d}'/\mathbb{K}_{n,d}$ is unramified, there is a map of $\Lambda$-modules $\psi_n : A_n^- \to \text{rad}(\mathbb{K}_{n,d}'/\mathbb{K}_{n,d}') \subset \mathbb{K}_{n'}^*$: this follows from the fact that $R_n \subset (\mathbb{K}_{n'})^{1-j}$ by reflection, together with the classical description of unramified Kummer extensions. A Kummer extension $\mathbb{L} = \mathbb{K}_n[\rho^{1/q}]$ is unramified over a ground field $\mathbb{K}_n$ which contains the $q$-th roots of unity, iff $(\rho) = \mathfrak{R}^q$ is the $q$-th power of an ideal $\mathfrak{R} \subset \mathbb{K}_n$. This may also be a trivial ideal, but since the intersection of the units with $\mathbb{K}_n^{1-j}$ reduces to the roots of unity, and since these generate only ramified extensions, the existence of the claimed map follows. But then $p - \text{rk}(\Lambda d_n) = p - \text{rk}(\psi_n(A_n^-)) \leq \lambda^-$, which is a contradiction with the choice of $n$. Such a map cannot exist, thus $\mu^+ = 0$, which completes the proof of the Theorem. \qed
References

[1] B. Ferrero and L. Washington. The Iwasawa invariant $\mu_p$ vanishes for abelian fields. *Ann. of Math.*, 109:377–395, 1979.

[2] P. Furtwängler. Über das Reziprozitätsgesetz der $\ell$-ten Potenzreste in algebraischen Zahlkörpern, wenn $\ell$ eine ungerade Primzahl bedeutet. *Abhandlungen der Gesellschaft der Wissenschaften in Göttingen*, 1902.

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

[4] G. Janusz. *Algebraic Number Fields*, volume 55 of *Pure and Applied Mathematics*. Academic Press, 1973.

[5] F. Thaine. On the ideal class groups of real abelian number fields. *Ann. of Math. Series 2*, 128(1):1–18, 1988.

[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