ACTA ARITHMETICA
174.4 (2016)

Relative extensions of number fields and Greenberg's Generalised Conjecture

by

Sören Kleine (München)

1. Introduction. Let p be a fixed rational prime, and let K be a number field. A $\mathbb{Z}_p$-*extension* of K is a field extension L of K such that L/K is Galois with Galois group topologically isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers. More generally, for a natural number $k \in \mathbb{N}$, a $\mathbb{Z}_p^k$-*extension* of K is a Galois extension $\mathbb{L}$ of K such that $\mathrm{Gal}(\mathbb{L}/K)$ is topologically isomorphic to $\mathbb{Z}_p^k$. Each $\mathbb{Z}_p^k$-extension of K arises as the composite of k independent $\mathbb{Z}_p$-extensions.

In this article, we will be mainly concerned with the composite $\mathbb{K}$ of *all* $\mathbb{Z}_p$-extensions of K. Using class field theory, one can show that

$$\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$$

for some integer $d = d(K)$ such that

$$r_2(K) + 1 \leq d \leq [K : \mathbb{Q}].$$

Here $r_2(K)$ denotes the number of pairs of complex conjugate embeddings of K into a fixed algebraic closure.

Leopoldt's Conjecture predicts that in fact $d(K) = r_2(K) + 1$. In particular, if K is a totally real number field, then there should exist exactly one $\mathbb{Z}_p$-extension of K (the so-called *cyclotomic* $\mathbb{Z}_p$-*extension* of K).

Let $\mathbb{L}$ be a $\mathbb{Z}_p^k$-extension of K, and let $\Gamma := \mathrm{Gal}(\mathbb{L}/K) \cong \mathbb{Z}_p^k$. For each integer $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, we consider the intermediate field $\mathbb{L}_n := \mathbb{L}^{\Gamma^{p^n}}$, which is the subfield of $\mathbb{L}$ fixed by Γ^{p^n}. Then each $\mathbb{L}_n$ is abelian over K with Galois group isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^k$. We let A_n denote the p-Sylow subgroup of the ideal class group of the number field $\mathbb{L}_n$.

2010 *Mathematics Subject Classification*: Primary 11R23; Secondary 11R37.
Key words and phrases: class field theory, Greenberg's Conjecture, relative extensions.
Received 25 January 2016; revised 19 May 2016.
Published online 3 August 2016.

DOI: 10.4064/aa8423-5-2016

Let $m, n \in \mathbb{N}$, $m \geq n$. The norm map

$$N_{\mathbb{L}_m|\mathbb{L}_n} : \mathbb{L}_m \to \mathbb{L}_n$$

induces a map $N_{m,n} : A_m \to A_n$. Let $A^{(\mathbb{L})} := \varprojlim A_n$ denote the projective limit of the A_n with respect to these maps. Then $A^{(\mathbb{L})}$ is called the *Greenberg module* attached to the $\mathbb{Z}_p^k$-extension $\mathbb{L}/K$.

We note that $A^{(\mathbb{L})}$ bears in a natural way the structure of a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module. Moreover, one can show that the group ring $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$ is algebraically and topologically isomorphic to the ring $\Lambda_k := \mathbb{Z}_p[[T_1, \ldots, T_k]]$ of formal power series in k variables over $\mathbb{Z}_p$. Here the isomorphism is induced by mapping a set of topological generators $\gamma_1, \ldots, \gamma_k$ of $\mathrm{Gal}(\mathbb{L}/K) \cong \mathbb{Z}_p^k$ to the elements $T_1 + 1, \ldots, T_k + 1$, respectively. R. Greenberg [Gr73] has shown that $A^{(\mathbb{L})}$ is a finitely generated torsion Λ_k-module.

A finitely generated Λ_k-module M is called *pseudo-null* if M is annihilated by two relatively prime elements g, h of the unique factorisation domain Λ_k. If $k = 1$, then this condition is equivalent to saying that M is finite.

Now we are ready to state the main problem to be investigated in this article.

CONJECTURE 1.1 (Greenberg's Generalised Conjecture (GGC); cf. [Gr01, Conjecture 3.5]). *Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of the number field K. Then $A^{(\mathbb{K})}$ is pseudo-null as a Λ_d-module, where we let $d = \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(\mathbb{K}/K))$.*

If, for example, K denotes a totally real number field such that Leopoldt's Conjecture holds for K, then $d(K) = 1$, and (GGC) reduces to the claim that the p-Sylow subgroups A_n of the ideal class groups of the intermediate fields in the cyclotomic $\mathbb{Z}_p$-extension of K remain bounded as $n \to \infty$. In this form, the above conjecture has already been formulated in [Gr76].

Let us stress here that (GGC) only concerns the composite of *all* $\mathbb{Z}_p$-extensions of K; it does not make predictions about the Greenberg modules $A^{(\mathbb{L})}$ of $\mathbb{Z}_p^k$-extensions of K for $k < d$ (in fact, it is known that Greenberg modules of such smaller composites are not necessarily pseudo-null).

The conjecture has been verified numerically for many fields (most of them being real quadratic extensions of $\mathbb{Q}$). Moreover, J. Minardi has proved in his Ph.D. thesis [Mi86] that (GGC) holds for imaginary quadratic fields whose class number is coprime to p, and also for some special sets of imaginary quadratic fields having class number divisible by p. Besides these two classes of examples, the conjecture has been verified in several further special cases (cf., for example, [MS03] and [Ba03]; in the latter reference, (GGC) is proved for certain normal extensions of $\mathbb{Q}$ having two-elementary Galois groups).

In this article, we will first be concerned with two main problems, both of which are motivated by the wish to transfer the property of being pseudo-null from one given module to certain other modules. Throughout the paper, we will assume that K is a number field such that there exist at least two (and thus infinitely many) different $\mathbb{Z}_p$-extensions of K.

We will distinguish two kinds of transfer, namely 'lifting' and 'shifting'. Here 'lifting' means that we are given a number field K and a $\mathbb{Z}_p^k$-extension $\mathbb{L}$ of K, $k \in \mathbb{N}$, such that $A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_k$, and we want to show that for some $\mathbb{Z}_p^d$-extension $\mathbb{K}$ of K containing $\mathbb{L}$, $d > k$, the Greenberg module $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_d$.

Our main result concerning 'lifting' implies that in the study of pseudo-null Greenberg modules of $\mathbb{Z}_p^k$-extensions, it is sufficient to restrict to the case $k = 2$:

THEOREM 2.8. *Let K be a number field. We assume that there exist at least two independent $\mathbb{Z}_p$-extensions of K. Then* (GGC) *holds for K if and only if there exists a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that*

- *$A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_2$, and*
- *only finitely many primes of $\mathbb{L}$ ramify in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K.*

Note that the 'if' part of Theorem 2.8 goes back to [Mi86]. We can go one step further: it is sometimes even sufficient to consider $\mathbb{Z}_p$-extensions of K ($k = 1$):

THEOREM (see Corollary 2.5 below). *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^k$-extension, and suppose that $\mathbb{K}$ contains a $\mathbb{Z}_p$-extension L of K such that*

- *$A^{(L)}$ is finite, and*
- *only one prime of L ramifies in $\mathbb{K}$.*

Then $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_k$.

This last result is particularly useful for proving (GGC) via numerical computations.

On the other hand, 'shifting' pseudo-nullity shall mean that we want to transfer the pseudo-nullity of some $\mathbb{Z}_p^k$-extension $\mathbb{L}/K$ to the $\mathbb{Z}_p^k$-extension $\mathbb{L}'/K'$, where K'/K is a suitable finite p-extension and $\mathbb{L}' = \mathbb{L} \cdot K'$.

One of our main results in this context is based on the following

THEOREM 3.1. *Let K be a number field, let $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension. Suppose that K'/K denotes a finite extension. Let $\mathbb{L}' := \mathbb{L} \cdot K'$.*

(i) *If $A^{(\mathbb{L}')}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]] \cong \Lambda_k$-module, then $A^{(\mathbb{L})}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module.*

(ii) *Suppose now that K'/K is a finite normal p-extension which is unramified outside p, let $k = 2$, and suppose that each prime of K ramifying in K' is only finitely decomposed in $\mathbb{L}$. Then $A^{(\mathbb{L})}/(pA^{(\mathbb{L})})$ is finite if and only if $A^{(\mathbb{L}')}/(pA^{(\mathbb{L}')})$ is finite. In particular, in this case $A^{(\mathbb{L}')}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]]$.*

We will study the above questions in Sections 2 and 3, respectively.

Our method shows its full strength if we combine 'lifting' with 'shifting'. This enables us to prove the following result.

THEOREM. *Suppose that K denotes a number field for which a statement slightly stronger than* (GGC) *holds* (*details to be explained in Sections* 3 *and* 4). *Then* (GGC) *holds for every finite normal p-extension of K which is unramified outside p over K.*

In the last section, we will give several applications of the results obtained, including for example the following theorem.

THEOREM 4.6. *Let K be a number field containing exactly one prime above p. If the p-Sylow subgroup $A^{(K)}$ of the ideal class group of K is cyclic, generated by the prime of K dividing p, then* (GGC) *holds for K.*

Moreover, if $\tilde{K}$ denotes any finite extension of K contained in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K, and if K' denotes any finite normal p-extension of $\tilde{K}$ such that $K'/\tilde{K}$ is unramified outside p, then (GGC) *holds for K', and in fact*

$$|A^{(\mathbb{K}')}| \leq |A^{(\tilde{K})}| < \infty.$$

It is easy to find number fields satisfying the conditions of Theorem 4.6; let us just mention one concrete example here (some more are given at the end of Section 4). Suppose that K is the non-normal cubic field defined by the polynomial $x^3 - 9x^2 + 9x + 141$. Then Theorem 4.6 may be applied to K ($p = 3$), and the Greenberg module $A^{(\mathbb{K})}$ of the $\mathbb{Z}_3^2$-extension $\mathbb{K}/K$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

NOTATION. For every algebraic extension (finite or infinite) F of $\mathbb{Q}$ we denote by $H(F)$ the maximal abelian unramified pro-p-extension of F. If F is a $\mathbb{Z}_p^k$-extension of some number field K, then we write $A^{(F)}$ for the Greenberg module of F/K, i.e., the projective limit of the p-Sylow subgroups of the ideal class groups of the finite extensions of K contained in F. Note that $\mathrm{Gal}(H(F)/F)$ is isomorphic to $A^{(F)}$, by class field theory.

2. Lifting pseudo-nullity. In this section, we will deal with the problem of 'lifting' pseudo-nullity, as described in the Introduction. Let K be a fixed number field, and suppose that $\mathbb{L}/K$ denotes a $\mathbb{Z}_p^l$-extension such that $A^{(\mathbb{L})}$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module. Let moreover $\mathbb{K}$ be a

$\mathbb{Z}_p^k$-extension of K, $k > l$, containing $\mathbb{L}$. We would like to conclude that $A^{(\mathbb{K})}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$-module. Obviously it is enough to handle the case $k = l + 1$.

We start with the following simple observation:

LEMMA 2.1. *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^k$-extension, $k \geq 2$. We assume that $\mathbb{L} \subseteq \mathbb{K}$ is a $\mathbb{Z}_p^{k-1}$-extension of K such that*

- *$A^{(\mathbb{L})}$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module, and*
- *the $\mathbb{Z}_p$-extension $\mathbb{K}/\mathbb{L}$ is unramified.*

Then $A^{(\mathbb{K})}$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_k$-module.

Proof. We lift any fixed topological generator $\gamma \in \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \cong \mathbb{Z}_p$ to an element $\overline{\gamma} \in \mathrm{Gal}(H(\mathbb{K})/\mathbb{L})$ (which is uniquely determined by γ since $H(\mathbb{K})/\mathbb{K}$ is abelian), and we define $T := \gamma - 1 \in \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$. Then the field $H(\mathbb{K})^{\langle\overline{\gamma}\rangle}$ fixed by $\overline{\gamma}$ is the maximal subextension of $H(\mathbb{K})$ which is abelian over $\mathbb{L}$, i.e., $H(\mathbb{K})^{\langle\overline{\gamma}\rangle} = H(\mathbb{L})$.

We therefore obtain an injective $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_{k-1}$-module homomorphism

$$\mathrm{Gal}(H(\mathbb{K})^{\langle\overline{\gamma}\rangle}/\mathbb{K}) \hookrightarrow \mathrm{Gal}(H(\mathbb{K})^{\langle\overline{\gamma}\rangle}/\mathbb{L}) = \mathrm{Gal}(H(\mathbb{L})/\mathbb{L}).$$

Now $\mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \cong A^{(\mathbb{L})}$ is pseudo-null as a Λ_{k-1}-module, and

$$\mathrm{Gal}(H(\mathbb{K})^{\langle\overline{\gamma}\rangle}/\mathbb{K}) \cong A^{(\mathbb{K})}/(T \cdot A^{(\mathbb{K})}).$$

This shows that $A^{(\mathbb{K})}/(T \cdot A^{(\mathbb{K})})$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$. It follows by a standard argument (cf. [PR94, Lemme 2]) that $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong (\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]])[[T]]$. ∎

Secondly, we mention the following result.

LEMMA 2.2 (Minardi [Mi86, Proposition 4.B]). *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^k$-extension, $k \geq 3$. We assume that $\mathbb{L} \subseteq \mathbb{K}$ is a $\mathbb{Z}_p^{k-1}$-extension of K such that*

- *$A^{(\mathbb{L})}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module, and*
- *for every prime $\mathfrak{p}$ of K that divides a prime of $\mathbb{L}$ which ramifies in $\mathbb{K}/\mathbb{L}$, the decomposition group $D_\mathfrak{p} \subseteq \mathrm{Gal}(\mathbb{L}/K)$ of $\mathfrak{p}$ has $\mathbb{Z}_p$-rank at least two.*

Then $A^{(\mathbb{K})}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$-module.

REMARKS 2.3. (1) The second condition of Lemma 2.2 is satisfied, for example, if $\mathbb{K}$ contains a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that only finitely many primes of $\mathbb{L}$ lie above p.

(2) Another important example is the case of a ground field K containing exactly one prime dividing p. Then this prime is only finitely decomposed in $\mathbb{K}$, i.e., the $\mathbb{Z}_p$-rank of the corresponding decomposition group equals $k \geq 3$.

In general, the above condition is quite restrictive for primes $\mathfrak{p}$ of K having small ramification indices $e_{\mathfrak{p}}$ and inertia degrees $f_{\mathfrak{p}}$ over $\mathbb{Q}$, because in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K, we have $\mathrm{rank}_{\mathbb{Z}_p}(D_{\mathfrak{p}}) \le e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$.

(3) In some situations (see the applications in Section 4), the module $A^{(\mathbb{L})}$ is not only pseudo-null, but in fact the trivial module. Whereas this immediately implies that $A^{(\mathbb{K})}$ is pseudo-null if $\mathbb{K}/\mathbb{L}$ is unramified (compare the proof of Lemma 2.1), an analogous conclusion does not seem obvious in the setting of Lemma 2.2 (exception: exactly one prime $\mathfrak{p}$ of $\mathbb{L}$ ramifies in the extension $\mathbb{K}/\mathbb{L}$).

We will now deduce two important special cases.

Corollary 2.4. *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^k$-extension. Suppose that $\mathbb{K}$ contains a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that*

- *$A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_2$, and*
- *only finitely many primes of $\mathbb{L}$ ramify in $\mathbb{K}/\mathbb{L}$.*

Then $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_k$.

Proof. This follows inductively by repeatedly using Lemma 2.2. We may assume that $k \ge 3$. Let $\mathbb{L}^{(l)} \subseteq \mathbb{K}$, $2 \le l < k$, be any $\mathbb{Z}_p^l$-extension of K containing $\mathbb{L}$ such that $A^{(\mathbb{L}^{(l)})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}^{(l)}/K)]]$. Choose any $\mathbb{Z}_p^{l+1}$-extension $\mathbb{L}^{(l+1)} \subseteq \mathbb{K}$ of K containing $\mathbb{L}^{(l)}$.

Let $\overline{\mathfrak{p}}$ denote a prime of $\mathbb{L}^{(l)}$ ramifying in $\mathbb{L}^{(l+1)}$. Then $\overline{\mathfrak{p}} \cap \mathbb{L}$ ramifies in $\mathbb{L}^{(l+1)}/\mathbb{L}$ and therefore also in $\mathbb{K}/\mathbb{L}$, implying that $\overline{\mathfrak{p}} \cap K$ is only finitely decomposed in $\mathbb{L}/K$. Therefore the rank of the corresponding decomposition group in $\mathbb{L}^{(l)}/K$ is at least two, so that we may apply Lemma 2.2 and conclude that $A^{(\mathbb{L}^{(l+1)})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}^{(l+1)}/K)]]$. ■

Corollary 2.5. *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^k$-extension, and suppose that $\mathbb{K}$ contains a $\mathbb{Z}_p$-extension L of K such that*

- *$A^{(L)}$ is finite, and*
- *only one prime $\overline{\mathfrak{p}}$ of L ramifies in $\mathbb{K}$.*

Then $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_k$.

The ramification condition is satisfied, for example, if L contains only one prime dividing p. Note that this can only happen if the ground field K itself contains only one prime dividing p, and if this unique prime does not split in L/K.

Proof of Corillary 2.5. We may assume that $k \ge 2$. Note that since $A^{(K)}$ is finite, the prime $\overline{\mathfrak{p}}$ of L which ramifies in $\mathbb{K}$ has to be almost totally ramified. Let $\mathbb{L} \subseteq \mathbb{K}$ be a $\mathbb{Z}_p^2$-extension of K containing L. Then $\overline{\mathfrak{p}}$ ramifies already in $\mathbb{L}/L$.

We will show now that $A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_2$. The statement will then follow from the previous corollary.

Since $\overline{\mathfrak{p}}$ ramifies in the $\mathbb{Z}_p$-extension $\mathbb{L}/L$, there exists a minimal integer $e \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ such that the extension $\mathbb{L}_e/L$ is totally ramified, where $\mathbb{L}_e$ denotes the unique intermediate field of the extension $\mathbb{L}/L$ which is cyclic of degree p^e over L.

We have a surjection

$$\mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \twoheadrightarrow \mathrm{Gal}\big((\mathbb{L} \cdot H(L))/\mathbb{L}\big) \cong \mathrm{Gal}(H(L)/\mathbb{L}_e)$$

with kernel $\mathrm{Gal}(H(\mathbb{L})/(\mathbb{L} \cdot H(L)))$, since $H(L) \cap \mathbb{L} = \mathbb{L}_e$.

This induces a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/L)]]$-module homomorphism

$$\Phi : A^{(\mathbb{L})} \to A^{(L)} \cong \mathrm{Gal}(H(L)/L).$$

It is easy to see that $T \cdot A^{(\mathbb{L})}$ is contained in the kernel of Φ, where we let $T := \gamma - 1$ for some topological generator γ of $\mathrm{Gal}(\mathbb{L}/L) \cong \mathbb{Z}_p$. Since $A^{(L)}$ is finite by assumption, there exists some power p^x of p which annihilates the image of Φ. Furthermore, one can show that the kernel of the induced map

$$\overline{\Phi} : A^{(\mathbb{L})}/(T \cdot A^{(\mathbb{L})}) \to A^{(L)}$$

is annihilated by p^e (cf. Lemma 2.6 below). Therefore

$$p^{x+e} \cdot (A^{(\mathbb{L})}/(T \cdot A^{(\mathbb{L})})) = \{0\}.$$

Let $M = H(\mathbb{L})^{\langle\gamma\rangle}$. Then M is the maximal subextension of $H(\mathbb{L})$ which is abelian over L.

If $\mathfrak{P}$ denotes a prime of M dividing $\overline{\mathfrak{p}}$, then the decomposition group

$$D \subseteq \mathrm{Gal}(L/K)$$

of $\mathfrak{p} := \overline{\mathfrak{p}} \cap K$ acts trivially on the inertia subgroup $I \subseteq \mathrm{Gal}(M/L)$ of $\mathfrak{P}$. Indeed, since $I \cap \mathrm{Gal}(M/\mathbb{L}) = \{0\}$, we may identify I with the inertia subgroup $I_{\overline{\mathfrak{p}}}$ of $\overline{\mathfrak{p}}$ in $\mathrm{Gal}(\mathbb{L}/L)$. The group D acts on $I_{\overline{\mathfrak{p}}}$ (and I) via conjugation, since each element of D fixes $\overline{\mathfrak{p}}$. But $\mathrm{Gal}(\mathbb{L}/K) \cong \mathbb{Z}_p^2$ is abelian, and therefore D acts trivially on $I_{\overline{\mathfrak{p}}}$.

Note that $\overline{\mathfrak{p}}$ is the unique prime of L dividing $\mathfrak{p}$, since $\mathbb{L}/K$ is normal and so every conjugate of $\overline{\mathfrak{p}}$ in L would have to ramify in $\mathbb{L}/L$.

Therefore $D = \mathrm{Gal}(L/K)$. If $\gamma_2 \in \mathrm{Gal}(L/K)$ denotes a topological generator, and if $T_2 := \gamma_2 - 1$, then this means that $T_2 \cdot I = \{0\}$.

Since $T \cdot \mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \cong T \cdot A^{(\mathbb{L})}$ is the closure of the commutator subgroup of $\mathrm{Gal}(H(\mathbb{L})/L)$ (cf. the proof of [Gr73, Proposition 2]), the kernel of $\overline{\Phi}$ is generated by the inertia subgroup $I \subseteq \mathrm{Gal}(M/L)$ of $\mathfrak{P}$. The above observation therefore shows that the kernel of $\overline{\Phi}$ is annihilated by p^e, T and T_2, and hence is finite.

It follows that $A^{(\mathbb{L})}/(T\cdot A^{(\mathbb{L})})$ is a finite, i.e., pseudo-null, $\mathbb{Z}_p[[T_2]]$-module, by the assumption that $A^{(L)}$ is finite. But this means that $A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \mathbb{Z}_p[[T, T_2]]$. ■

The following lemma has been used in the proof of Corollary 2.5.

LEMMA 2.6. *Let $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension, $k \geq 2$. Suppose that $\mathbb{L}$ contains a $\mathbb{Z}_p^{k-1}$-extension L of K such that exactly one prime $\mathfrak{p}$ ramifies in $\mathbb{L}/L$. Let p^e be the index of the inertia subgroup $I_{\mathfrak{p}} \subseteq \mathrm{Gal}(\mathbb{L}/L)$ of $\mathfrak{p}$ in $\mathrm{Gal}(\mathbb{L}/L)$. Let $T := \gamma - 1$, where γ denotes a topological generator of $\mathrm{Gal}(\mathbb{L}/L) \cong \mathbb{Z}_p$. Then there exists a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/L)]]$-module homomorphism*

$$A^{(\mathbb{L})}/(T \cdot A^{(\mathbb{L})}) \to A^{(L)}$$

whose kernel and cokernel are annihilated by p^e.

Proof. This is part of [Kl14, Lemma 5.98]. For convenience, we include a proof.

Let $\mathfrak{P}$ be any prime of $H(\mathbb{L})$ dividing the unique prime $\mathfrak{p}$ of L which ramifies in $\mathbb{L}/L$, and let $I \subseteq G := \mathrm{Gal}(H(\mathbb{L})/L)$ denote the inertia subgroup of $\mathfrak{P}$.

Let $X := \mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \cong A^{(\mathbb{L})}$. The exact sequence

$$0 \to X \to G \to G/X \to 0,$$

together with the fact that $G/X \cong \mathrm{Gal}(\mathbb{L}/L)$ is $\mathbb{Z}_p$-free, implies that G is isomorphic to the semidirect product $X \rtimes G/X$. Note that I may be identified with $p^e \cdot (G/X)$, since $I \cap X = \{0\}$ and thus $I \cong I_{\mathfrak{p}} \subseteq \mathrm{Gal}(\mathbb{L}/L)$.

Since $T\cdot X$ equals the commutator subgroup of G, $G/(T\cdot X)$ is isomorphic to the *direct* product

$$(X/(T \cdot X)) \times (G/X),$$

and

$$G/(T \cdot X + I) \cong (X/TX) \times ((G/X)/I) \cong (X/TX) \times (\mathbb{Z}/p^e\mathbb{Z}).$$

Therefore

$$p^e \cdot (X/(T \cdot X)) \cong (G/(T \cdot X + I))^{p^e} \cong \mathrm{Gal}(H(L)/L)^{p^e}.$$

We have thus shown that

$$p^e \cdot (A^{(\mathbb{L})}/TA^{(\mathbb{L})}) \cong p^e \cdot A^{(L)}.$$

Note that this formula nicely generalises the well-known isomorphism in the case of $e = 0$.

Now we consider the composite map

$$\varphi : A^{(\mathbb{L})}/TA^{(\mathbb{L})} \twoheadrightarrow p^e \cdot (A^{(\mathbb{L})}/TA^{(\mathbb{L})}) \cong p^e \cdot A^{(L)} \hookrightarrow A^{(L)},$$

where the first map is simply multiplication by p^e. Then the cokernel $A^{(L)}/(p^e \cdot A^{(L)})$ of φ is annihilated by p^e, and the first map is the only one which might have a kernel. The lemma follows. ∎

REMARK 2.7. Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^k$-extension containing a $\mathbb{Z}_p$-extension L of K such that at most one prime of L ramifies in $\mathbb{K}$. Let $n \in \mathbb{N}$, and let $\tilde{L} \subseteq \mathbb{K}$ be a $\mathbb{Z}_p$-extension of K such that $[(\tilde{L} \cap L) : K] \geq p^n$. Then at most one prime ramifies in $\mathbb{K}/\tilde{L}$, provided that n is large enough.

Therefore we can reformulate Corollary 2.5 as follows: suppose that $A^{(\mathbb{K})}$ is *not* pseudo-null. If $L \subseteq \mathbb{K}$ is a $\mathbb{Z}_p$-extension of K such that at most one prime of L ramifies in $\mathbb{K}$, then there exists some $n \in \mathbb{N}$ such that $\mu(\tilde{L}/K) > 0$ or $\lambda(\tilde{L}/K) > 0$ for each $\mathbb{Z}_p$-extension $\tilde{L}/K$ satisfying $[(\tilde{L} \cap L) : K] \geq p^n$ (here $\mu(\tilde{L}/K)$ and $\lambda(\tilde{L}/K)$ denote the Iwasawa invariants of the $\mathbb{Z}_p$-extension $\tilde{L}/K$; note that $A^{(\tilde{L})}$ is finite if and only if $\mu(\tilde{L}/K) = \lambda(\tilde{L}/K) = 0$).

We will finally develop a converse of Corollary 2.4 and apply it to proving pseudo-nullity; in fact, this result shows that it is sufficient to be able to handle the case of $\mathbb{Z}_p^2$-extensions.

THEOREM 2.8. *Let K be a number field. We assume that there exist at least two independent $\mathbb{Z}_p$-extensions of K. Then* (GGC) *holds for K if and only if there exists a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that*

- *$A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]] \cong \Lambda_2$, and*
- *only finitely many primes of $\mathbb{L}$ ramify in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K.*

Proof. If $d(K) = 2$, i.e., the composite of all $\mathbb{Z}_p$-extensions of K is a $\mathbb{Z}_p^2$-extension, then we can simply take $\mathbb{L} = \mathbb{K}$. From now on, we will assume that $d(K) \geq 3$.

The 'if' statement immediately follows from Corollary 2.4. We will thus assume that K satisfies (GGC). Let $\mathcal{I} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be the set of primes of K dividing p. Since each of these primes ramifies in the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^{\mathrm{cyc}} \subseteq \mathbb{K}$ of K, the inertia subgroups

$$I_{\mathfrak{p}_i}(\mathbb{K}/K) \subseteq D_{\mathfrak{p}_i}(\mathbb{K}/K) \subseteq \mathrm{Gal}(\mathbb{K}/K)$$

must have $\mathbb{Z}_p$-rank at least one for $1 \leq i \leq t$.

We will construct a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K containing K_∞^{cyc} which satisfies the desired conditions. Each prime $\mathfrak{p}_j$ whose inertia subgroup has $\mathbb{Z}_p$-rank equal to one will be unramified in $\mathbb{K}/\mathbb{L}$, since it is in fact unramified in $\mathbb{K}/K_\infty^{\mathrm{cyc}}$.

Therefore such primes may be ignored. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ denote the remaining primes. The inertia subfields $T_{\mathfrak{p}_i} := \mathbb{K}^{I_{\mathfrak{p}_i}}$ are contained in $\mathbb{Z}_p^{d(K)-2}$-extensions of K for $1 \leq i \leq s$.

Let $d := d(K)$. For each $\mathfrak{p}_i$, we define a $\mathbb{Z}_p^{d-1}$-extension $L_{\mathfrak{p}_i}$ of K by letting

(a) $L_{\mathfrak{p}_i} := K_\infty^{\mathrm{cyc}} \cdot T_{\mathfrak{p}_i}$ if $T_{\mathfrak{p}_i}$ is a $\mathbb{Z}_p^{d-2}$-extension of K (i.e., $\mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}) = 2$), or

(b) $L_{\mathfrak{p}_i} := K_\infty^{\mathrm{cyc}} \cdot T_{\mathfrak{p}_i} \cdot \tilde{T}_{\mathfrak{p}_i}$ if $r := \mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}) > 2$, where $\tilde{T}_{\mathfrak{p}_i}$ is any $\mathbb{Z}_p^{r-2}$-extension of K such that the composite $L_{\mathfrak{p}_i}$ is a $\mathbb{Z}_p^{d-1}$-extension of K.

Now we choose a $\mathbb{Z}_p^{d-1}$-extension $\mathbb{L}^{(d-1)}$ of K containing K_∞^{cyc} such that for every $1 \le i \le s$, $\mathbb{L}^{(d-1)} \cap L_{\mathfrak{p}_i}$ is contained in a $\mathbb{Z}_p^{d-2}$-extension of K. Then the primes of $\mathbb{L}^{(d-1)}$ dividing some prime $\mathfrak{p}_i$ of case (a) are unramified in $\mathbb{K}/\mathbb{L}^{(d-1)}$. Indeed, there exists a $\mathbb{Z}_p$-extension $L \subseteq T_{\mathfrak{p}_i}$ which is not contained in $\mathbb{L}^{(d-1)}$. Then $\mathbb{L}^{(d-1)} \cdot L$ is of finite index in $\mathbb{K}$, and unramified over $\mathbb{L}^{(d-1)}$ at the primes dividing $\mathfrak{p}_i$.

The primes of $\mathbb{L}^{(d-1)}$ dividing some $\mathfrak{p}_i$ of case (b) may ramify in $\mathbb{K}/\mathbb{L}^{(d-1)}$; however, for such $\mathfrak{p}_i$,

$$\mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}(\mathbb{L}^{(d-1)}/K)) \ge \mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}(\mathbb{K}/K)) - 1 \ge 3 - 1 = 2.$$

In both cases, $\mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}(\mathbb{L}^{(d-1)}/K)) \ge 2$.

Inductively, we obtain a $\mathbb{Z}_p^2$-extension $\mathbb{L} = \mathbb{L}^{(2)}$ of K containing K_∞^{cyc} such that $\mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}(\mathbb{L}/K)) = 2$ for every prime $\mathfrak{p}_i$ of K which is divisible by primes ramifying in $\mathbb{K}/\mathbb{L}$. In particular, each of these primes splits into finitely many primes of $\mathbb{L}$, i.e., only finitely many primes of $\mathbb{L}$ ramify in $\mathbb{K}$.

Note that we constructed $\mathbb{L} = \mathbb{L}^{(2)}$ by an inductive procedure, excluding in every step finitely many possible $\mathbb{Z}_p^j$-extensions. We will now see that it is possible to choose $\mathbb{L}$ such that moreover $A^{(\mathbb{L})}$ is pseudo-null as a Λ_2-module.

Since (GGC) holds for K, $A^{(\mathbb{K})}$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \cong \Lambda_d$-module. But then $A^{(\mathbb{L}^{(d-1)})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}^{(d-1)}/K)]] \cong \Lambda_{d-1}$ for all but finitely many possible choices of $\mathbb{L}^{(d-1)}$. This follows from [Mi86, Corollary 1 of Proposition 4.D]. In order to be allowed to apply Minardi's result, we have to check that $\mathbb{K}$ contains a $\mathbb{Z}_p$-extension M of K such that no prime of K dividing p is totally split in M, and such that $\mu(M/K) = 0$. Now K_∞^{cyc} is contained in $\mathbb{K}$, and therefore the set of $\mathbb{Z}_p$-extensions of K in which all the primes of K dividing p ramify is dense in the set of all $\mathbb{Z}_p$-extensions of K. Moreover, since $A^{(\mathbb{K})}$ is pseudo-null, $\mu(M/K) = 0$ for all $\mathbb{Z}_p$-extensions M of K which are not contained in a finite number of certain $\mathbb{Z}_p^{d-1}$-extensions (this has been proved by P. Monsky [Mo81, Theorem I]; note that $m_0(\mathbb{K}/K) = 0$ in Monsky's notation, since $A^{(\mathbb{K})}$ is pseudo-null).

We may therefore choose $\mathbb{L}^{(d-1)}$ as described above, with the additional restriction of avoiding the finitely many $\mathbb{Z}_p^{d-1}$-extensions that do not share the pseudo-nullity property.

Inductively, we may construct a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K as claimed in the statement of the theorem. ∎

REMARK 2.9. The $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K constructed in the proof of Theorem 2.8 always contains the cyclotomic $\mathbb{Z}_p$-extension of K. Therefore the fact that $A^{(\mathbb{L})}$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module implies that the direct limit $\varinjlim A_n$ of the ideal class groups of the intermediate fields of $\mathbb{L}/K$ is trivial (this follows from [LN00, Proposition 3.6]).

More briefly: if (GGC) holds for K, then there exists a $\mathbb{Z}_p^2$-extension of K in which all the ideals of K of p-power order capitulate.

Lannuzel and Nguyen Quang Do proved in [LN00] that (GGC) for K implies that one can expect capitulation in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K; we have just proved that it is in fact possible to obtain capitulation already at a lower dimension (cf. also [Ba07]).

3. Shifting pseudo-nullity.

We will now deal with the second of the two problems stated in the Introduction, i.e., we want to transfer the pseudo-nullity of a $\mathbb{Z}_p^k$-extension $\mathbb{L}/K$ to the pseudo-nullity of the $\mathbb{Z}_p^k$-extension $(\mathbb{L}\cdot K')/K'$ where K' is a suitable finite extension of K.

In view of Theorem 2.8, we will most of the time restrict to the case of a $\mathbb{Z}_p^2$-extension $\mathbb{L}/K$.

THEOREM 3.1. *Let K be a number field, let $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension. Suppose that K'/K denotes a finite extension. Let $\mathbb{L}' := \mathbb{L}\cdot K'$. In what follows, we will identify $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]] \cong \Lambda_k \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$.*

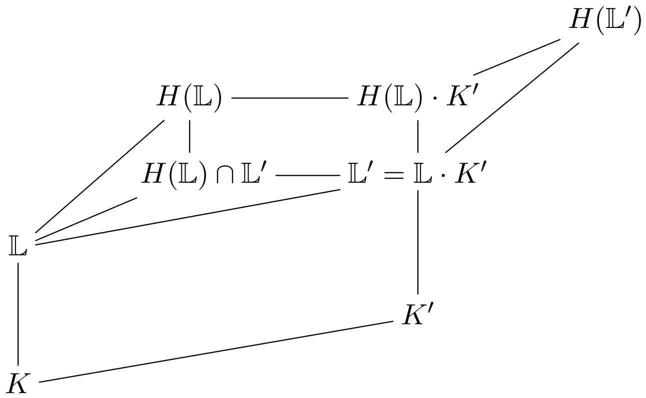
- (i) *If $A^{(\mathbb{L}')}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]]$-module, then $A^{(\mathbb{L})}$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$-module.*
- (ii) *Suppose now that K'/K is a finite normal p-extension which is unramified outside p, let $k = 2$, and suppose that each prime of K ramifying in K' is only finitely decomposed in $\mathbb{L}$. Then $A^{(\mathbb{L})}/(pA^{(\mathbb{L})})$ is finite if and only if $A^{(\mathbb{L}')}/(pA^{(\mathbb{L}')})$ is finite. In particular, in this case $A^{(\mathbb{L}')}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]]$.*

Proof. Class field theory implies that

$$A^{(\mathbb{L})} \cong \mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \quad \text{and} \quad A^{(\mathbb{L}')} \cong \mathrm{Gal}(H(\mathbb{L}')/\mathbb{L}').$$

Since $H(\mathbb{L})$ is normal over $\mathbb{L}$, we may conclude that $H(\mathbb{L})\cdot K' = H(\mathbb{L})\cdot \mathbb{L}'$ is a normal extension of $\mathbb{L}\cdot\mathbb{L}' = \mathbb{L}'$ and that $\mathrm{Gal}((H(\mathbb{L})\cdot K')/\mathbb{L}')$ is isomorphic to a subgroup of the abelian group $\mathrm{Gal}(H(\mathbb{L})/\mathbb{L})$. Hence $H(\mathbb{L})\cdot K' \subseteq H(\mathbb{L}')$.

We summarise the relations between the fields in the following diagram.



There exists a surjective Λ_k-module homomorphism

$$\mathrm{Gal}(H(\mathbb{L}')/\mathbb{L}') \twoheadrightarrow \mathrm{Gal}((H(\mathbb{L}) \cdot K')/\mathbb{L}') \cong \mathrm{Gal}\big(H(\mathbb{L})/(\mathbb{L}' \cap H(\mathbb{L}))\big).$$

Our assumption about $A^{(\mathbb{L}')}$ therefore implies that the Galois group

$$\Delta := \mathrm{Gal}\big(H(\mathbb{L})/(\mathbb{L}' \cap H(\mathbb{L}))\big)$$

is pseudo-null as a Λ_k-module.

Now we look at the exact sequence

$$0 \to \Delta \to \mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \to \mathrm{Gal}\big((\mathbb{L}' \cap H(\mathbb{L}))/\mathbb{L}\big) \to 0.$$

Since $H(\mathbb{L}) \cap \mathbb{L}'$ is a finite extension of $\mathbb{L}$, it follows that $\mathrm{Gal}((\mathbb{L}' \cap H(\mathbb{L}))/\mathbb{L})$ is pseudo-null as a Λ_k-module, proving that also $\mathrm{Gal}(H(\mathbb{L})/\mathbb{L}) \cong A^{(\mathbb{L})}$ is pseudo-null. This shows (i).

Turning to the proof of (ii), we will write $A := A^{(\mathbb{L})}$ and $A' := A^{(\mathbb{L}')}$.

We may in fact assume that $\mathbb{L} \cap K' = K$. Indeed, letting $\tilde{K} := \mathbb{L} \cap K'$, we have $\mathbb{L} \cdot \tilde{K} = \mathbb{L}$ and $\mathbb{L}' \cdot \tilde{K} = \mathbb{L}'$. Therefore we may replace K by $\tilde{K}$ (note that K' is a normal p-extension of $\tilde{K}$, unramified outside p).

Moreover, since every finite p-group is solvable, we may assume that K'/K is cyclic of degree p (the conclusion then follows by induction).

Let σ denote a generator of $G := \mathrm{Gal}(K'/K)$, and write $S := \sigma - 1$. We may thus identify the group ring $\mathbb{Z}_p[G]$ with a suitable quotient of the ring $\mathbb{Z}_p[S]$ of polynomials over $\mathbb{Z}_p$ in the variable S, dividing out the ideal generated by the element $(S+1)^p - 1$.

Now, $\mathbb{L}'$ is normal (and in fact abelian) over K, and G may be lifted to a subgroup of $\mathrm{Gal}(\mathbb{L}'/K)$, corresponding to $\mathrm{Gal}(\mathbb{L}'/\mathbb{L})$. In particular, G acts on $A' = A^{(\mathbb{L}')}$ in a natural way. Moreover,

$$S^p = (\sigma - 1)^p \equiv \sigma^p - 1 \bmod p$$

annihilates the quotient $A'/(p \cdot A')$.

We note that

$$\operatorname{rank}_p(A') = \dim_{\mathbb{F}_p}(A'/(p \cdot A')) = \operatorname{rank}_p(A'/(S^p \cdot A'))$$

(here $\mathbb{F}_p$ denotes the field with p elements). This means that

$$\begin{aligned} \operatorname{rank}_p(A') \le\ & \operatorname{rank}_p(A'/(S \cdot A')) + \operatorname{rank}_p((S \cdot A')/(S^2 \cdot A')) + \cdots \\ & + \operatorname{rank}_p((S^{p-1} \cdot A')/(S^p \cdot A')) \\ \le\ & p \cdot \operatorname{rank}_p(A'/(S \cdot A')), \end{aligned} \tag{3.1}$$

where we have used the fact that for every integer $j \in \mathbb{N}$ the map

$$S^j : A'/(S \cdot A') \to (S^j \cdot A')/(S^{j+1} \cdot A')$$

given by the action of S^j on A' is a well-defined and surjective homomorphism.

Now we translate the inequality (3.1) into a Galois-theoretic statement. Recall that $A' \cong \operatorname{Gal}(H(\mathbb{L}')/\mathbb{L}')$. We describe the quotient $A'/(S \cdot A')$. If $M' \subseteq H(\mathbb{L}')$ denotes the maximal subextension which is abelian over $\mathbb{L}$, then $\mathbb{L}' \subseteq M'$, and

$$\operatorname{Gal}(M'/\mathbb{L}') \cong A'/(S \cdot A').$$

We consider the abelian extension $M'/\mathbb{L}$. If K'/K is unramified, then actually

$$M' = H(\mathbb{L}).$$

In the general situation of Theorem 3.1 (i.e., K'/K unramified outside p), the field $H(\mathbb{L}) \subseteq M'$ corresponds to the maximal unramified subextension. In particular, since $M'/\mathbb{L}$ is abelian, $\operatorname{Gal}(M'/H(\mathbb{L}))$ is generated by the inertia subgroups of the primes of $\mathbb{L}$ ramifying in M'. Since $M'/\mathbb{L}'$ is unramified, each of the corresponding inertia subgroups has order $p = [\mathbb{L}' : \mathbb{L}]$. Since $\operatorname{rank}_p(\operatorname{Gal}(M'/\mathbb{L}'))$ is finite if and only if $\operatorname{rank}_p(\operatorname{Gal}(M'/\mathbb{L}))$ is finite, and since our assumptions concerning K' imply that only finitely many primes ramify in $\mathbb{L}'/\mathbb{L}$, it follows that

$$\operatorname{rank}_p(A'/(S \cdot A')) = \operatorname{rank}_p(\operatorname{Gal}(M'/\mathbb{L}'))$$

is finite if and only if

$$\operatorname{rank}_p(H(\mathbb{L})/\mathbb{L})) = \operatorname{rank}_p(A)$$

is finite.

Now suppose that $\operatorname{rank}_p(A)$ is finite. Since

$$\operatorname{rank}_p(A') \le p \cdot \operatorname{rank}_p(A'/(S \cdot A'))$$

by inequality (3.1), it follows that $\operatorname{rank}_p(A')$ is finite. If, on the other hand, $\operatorname{rank}_p(A')$ and therefore also $\operatorname{rank}_p(A'/(S \cdot A')) \le \operatorname{rank}_p(A')$ is finite, then the above shows that $\operatorname{rank}_p(A) < \infty$. ■

REMARKS 3.2. (1) If $A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$ and moreover torsion-free as a $\mathbb{Z}_p$-module, then $A^{(\mathbb{L})}/(pA^{(\mathbb{L})})$ is finite and thus the theorem applies (cf. [Gr78, Lemma 3]).

(2) There do of course exist pseudo-null Λ_2-modules A having infinite p-rank, e.g. $A = \Lambda_2/(p, T_1)$.

(3) We can prove an analogue of Theorem 3.1(ii) for $\mathbb{Z}_p^k$-extensions $\mathbb{K}/K$, $k > 2$: we assume that there exists a $\mathbb{Z}_p^2$-extension $\mathbb{L} \subseteq \mathbb{K}$ of K such that

- $A^{(\mathbb{L})}/(pA^{(\mathbb{L})})$ is finite, and
- only finitely many primes of $\mathbb{L}$ ramify in $\mathbb{K}$.

This property is more restrictive than just assuming that $A^{(\mathbb{K})}$ is pseudo-null (compare Theorem 2.8!). One can show that it is equivalent to the following: for a suitable choice of variables $T_1, \ldots, T_k$ of $\Lambda_k = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$, the quotient

$$A^{(\mathbb{K})}/((p, T_1, \ldots, T_{k-2}) \cdot A^{(\mathbb{K})})$$

is finite (idea: if $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is generated topologically by suitable elements $\gamma_1, \ldots, \gamma_{k-2}$, then we let $T_i := \gamma_i + 1$, $1 \leq i \leq k-2$). The proof of Theorem 3.1 then goes through with minor changes (for example, M' is now defined to be the maximal subextension of $H(\mathbb{L}')$ which is abelian over $\mathbb{L} = \mathbb{K}^{\langle T_1+1, \ldots, T_{k-2}+1\rangle}$; here we identify $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}'/K')]] \cong \Lambda_k$ with $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$).

Suppose now that $\mathbb{L}/K$ is a $\mathbb{Z}_p^2$-extension such that $A^{(\mathbb{L})}$ is pseudo-null over the group ring $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$. We would like to say something about the Greenberg module $A^{(\mathbb{L}')}$ of a shift $\mathbb{L}' = \mathbb{L} \cdot K'$ if $A^{(\mathbb{L})}$ is not finitely generated over $\mathbb{Z}_p$. We start with the following observation.

Recall that for each torsion Λ_2-module N, there is an associated *characteristic power series* $f_N \in \Lambda_2$, uniquely determined up to multiplication by units. Note that N is pseudo-null if and only if f_N is a unit.

LEMMA 3.3. *Suppose that* $\mathbb{L}/K$ *is a* $\mathbb{Z}_p^2$*-extension such that* $A := A^{(\mathbb{L})}$ *is pseudo-null over* $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$. *Let* K'/K *be a finite normal* p*-extension unramified outside* p, *let* $\mathbb{L}' := \mathbb{L} \cdot K'$, *and suppose that each prime of* K *ramifying in* K' *is finitely decomposed in* $\mathbb{L}/K$. *In what follows, we will identify* $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]] \cong \Lambda_2 \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$.

(i) *The characteristic power series* $f_{A'} \in \Lambda_2$ *of* $A' := A^{(\mathbb{L}')}$ *is prime with* p.

(ii) *For every* $\gamma \in \Gamma := \mathrm{Gal}(\mathbb{L}'/K') \cong \mathrm{Gal}(\mathbb{L}/K)$ *with* $\gamma \notin \Gamma^p$, *and* $T := \gamma - 1$, *if there exists some annihilator of* A *which is not contained in* $(p, T) \subseteq \Lambda_2 \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}/K)]]$, *then also* $f_{A'} \notin (p, T)$.

Proof. Since A is pseudo-null, there exists an annihilator $\Phi \in \Lambda_2$ of A which is prime with p. By [Gr78, Lemma 2] we may choose the variables

T_1, T_2 of Λ_2 (corresponding to a suitable choice of topological generators of $\mathrm{Gal}(\mathbb{L}/K) \cong \mathbb{Z}_p^2$) such that $A/((p, T_1) \cdot A)$ is finite.

Let us first assume that $G := \mathrm{Gal}(K'/K)$ is cyclic of degree p, as in the proof of Theorem 3.1. We write $G = \langle \sigma \rangle$ and define $S := \sigma - 1$.

As in the proof of Theorem 3.1, we may conclude that

$$A'/((S, p, T_1) \cdot A')$$

is finite. An analogue of inequality (3.1) for the module $A'/(T_1 \cdot A')$ instead of A' shows that also $A'/((p, T_1) \cdot A')$ is finite (note that the module $A'/(T_1 \cdot A')$ has a Galois-theoretic meaning: $A'/(T_1 \cdot A') \cong \mathrm{Gal}(X/\mathbb{L}')$, where $X \subseteq H(\mathbb{L}')$ denotes the maximal subextension which is abelian over the $\mathbb{Z}_p$-extension $\mathbb{L}'^{\langle T_1 + 1 \rangle}$ of K').

Inductively, we can prove that $A'/((p, T_1) \cdot A')$ is finite for every p-extension K' of K as in the lemma.

But if $A'/((p, T_1) \cdot A')$ is finite, then so is $\Lambda_2/(f_{A'}, p, T_1)$ (cf. [Kl14, Corollary 5.62]). This shows that $f_{A'} \notin (p, T_1)$, so in particular p does not divide $f_{A'}$, proving (i).

Now suppose that $f_{A'} \in (p, T)$ for some $T = \gamma - 1$. Then the above shows that $A/((p, T) \cdot A)$ has to be infinite. However, if there exists some annihilator $g \in \Lambda_2$ of A such that $g \notin (p, T)$, then $\Lambda_2/(p, T, g)$ is finite.

Indeed, $\Lambda_2/(p, T) \cong \mathbb{F}_p[[T_2]]$, where $T_2 = \gamma_2 - 1$ has been chosen so that $\Gamma = \langle \gamma, \gamma_2 \rangle$. Now $R := \mathbb{F}_p[[T_2]]$ is a regular local ring of Krull dimension one, and the maximal ideal of R is generated by T_2. Since $g \notin (p, T)$, the coset of g is a non-trivial element of R. Assuming that $g \in \Lambda_2$ is a non-unit (otherwise $A/((p, T) \cdot A) = \{0\}$, and thus $A = \{0\}$ by Nakayama's Lemma), we may conclude that the coset of g in R contains a power of T_2.

Therefore $R/(g)$ and thus also $A/((p, T) \cdot A) = A/((p, T, g) \cdot A)$ are finite. ∎

Remarks 3.4. (1) In [Mo81], P. Monsky described the growth of class numbers of the intermediate fields of multiple $\mathbb{Z}_p$-extensions in terms of so-called m_0- and l_0-invariants, which generalise Iwasawa's classical μ- and λ-invariants. Using this language, Lemma 3.3 shows that $m_0(\mathbb{L}'/K') = 0$, and that

$$l_0(\mathbb{L}'/K') \leq \min\{l_0(g) \mid g \in \mathrm{Ann}(A)\},$$

where $\mathrm{Ann}(A) \subseteq \Lambda_2$ denotes the annihilator ideal of A.

(2) Lemma 3.3(i) generalises a well-known result of K. Iwasawa about μ-invariants (cf. [Iw73, Theorem 2]). Note that a prime of K which does not lie above p cannot be finitely decomposed in a $\mathbb{Z}_p^2$-extension of K; this is what makes it necessary to restrict to shifts K'/K which are unramified outside p.

The fact that a Λ_k-module A is pseudo-null can be expressed by saying that the Krull dimension of the quotient ring $\Lambda_k/\mathrm{Ann}(A)$ is at most

$$k-1=(k+1)-2,$$

i.e., the *codimension* of A is at least two. We will now prove that the stronger assumption that $\mathrm{codim}(A)\geq 3$ implies that shifting works very well.

LEMMA 3.5. *Suppose that $\mathbb{L}/K$ denotes a $\mathbb{Z}_p^k$-extension, $k\geq 2$, such that $A:=A^{(\mathbb{L})}$ satisfies* $\mathrm{codim}(A)\geq 3$. *Let K'/K be a finite normal p-extension unramified outside p, and suppose that each prime of K which ramifies in K' is finitely decomposed in $\mathbb{L}/K$. Then $A':=A^{(\mathbb{L}')}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}'/K')]]\cong\Lambda_k$, where we let $\mathbb{L}':=\mathbb{L}\cdot K'$.*

Proof. Since the Krull dimension of the local ring $\Lambda_k/\mathrm{Ann}(A)$ is at most $(k+1)-3=k-2$, there exist elements $g_1,\ldots,g_{k-2}\in\Lambda_k$ such that $\Lambda_k/(\mathrm{Ann}(A)+(g_1,\ldots,g_{k-2}))$ and therefore also $A/((g_1,\ldots,g_{k-2})\cdot A)$ are finite. Then also $A/((p,g_1,\ldots,g_{k-2})\cdot A)$ is finite.

Let us first assume that K'/K is cyclic of degree p. Using the notation from the proof of Theorem 3.1, we may conclude that

$$A'/((S,p,g_1,\ldots,g_{k-2})\cdot A')$$

is finite: indeed, we have shown in that proof that due to our ramification constraints there exist exact sequences

$$0\to A'/(S\cdot A')\to M\to N_1\to 0$$

and

$$0\to N_2\to M\to A\to 0$$

with N_1 and N_2 finite and M a finitely generated Λ_k-module.

But this means that also

$$A'/((p,g_1,\ldots,g_{k-2})\cdot A')$$

is finite, by an analogue of inequality (3.1) from the proof of Theorem 3.1(ii). Therefore the Krull dimension of the quotient ring $\Lambda_k/\mathrm{Ann}(A')$ is bounded by

$$1+(k-2)=k-1=(k+1)-2,$$

i.e., A' is pseudo-null over Λ_k.

The case of a general finite normal p-ramified p-extension (which has a solvable Galois group) now follows by induction, using the fact that in each step the finiteness of

$$A/((p,g_1,\ldots,g_{k-2})\cdot A)$$

directly transfers, as we have just proved, to the finiteness of

$$A'/((p,g_1,\ldots,g_{k-2})\cdot A').\ \blacksquare$$

REMARKS 3.6. (1) If $k = 2$, then the module $A = A^{(\mathbb{L})}$ has $\operatorname{codim}(A) \geq 3$ if and only if A is finite. In particular, the statement of the previous lemma then is a special case of Theorem 3.1(ii).

(2) If $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^k$-extension, $k \geq 2$, then we can summarise the main results of the current section as follows. Suppose that K'/K is a finite normal p-extension unramified outside p, and that each prime of K ramifying in K' is finitely decomposed in $\mathbb{K}/K$. Then $A^{(\mathbb{K}')}$, $\mathbb{K}' = \mathbb{K} \cdot K'$, is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}'/K')]]$ in the following two situations (which of course are not disjoint):

(a) $A^{(\mathbb{L})}/(p \cdot A^{(\mathbb{L})})$ is finite for some $\mathbb{Z}_p^2$-extension $\mathbb{L} \subseteq \mathbb{K}$ of K such that only finitely many primes of $\mathbb{L}$ ramify in $\mathbb{K}$,

(b) $\operatorname{codim}(A^{(\mathbb{K})}) \geq 3$.

In the situation of (a), it is in fact sufficient that the primes of K ramifying in K' are finitely decomposed in the $\mathbb{Z}_p^2$-extension $\mathbb{L}/K$ (apply first Theorem 3.1 to the extension $\mathbb{L}'/\mathbb{L}$, $\mathbb{L}' = \mathbb{L} \cdot K'$, and then Corollary 2.4 to $\mathbb{K}'/\mathbb{L}'$).

4. Applications. In this section, we will discuss several applications of the results obtained in the preceding sections.

THEOREM 4.1. *Let K be a number field, let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of K. Let K' be a finite normal p-ramified p-extension of K. Suppose that one of the conditions mentioned in Remark* 3.6(2) *holds for $\mathbb{K}/K$. Assume that for every prime $\mathfrak{p}$ of K dividing p, the decomposition group $D_{\mathfrak{p}}(\mathbb{K}/K)$ has $\mathbb{Z}_p$-rank at least two. Then* (GGC) *holds for K'.*

Proof. In both cases, $A^{(\mathbb{K})}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$, i.e., (GGC) holds for K (in case (a), this follows from Corollary 2.4).

We define $\tilde{\mathbb{K}}' := \mathbb{K} \cdot K'$. Then Theorem 3.1 (or Remark 3.2(3)) and Lemma 3.5 imply that $A^{(\tilde{\mathbb{K}}')}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\tilde{\mathbb{K}}'/K')]]$.

Let $\mathfrak{p}'$ denote any prime of K' dividing p, and write $\mathfrak{p} := \mathfrak{p}' \cap K$. Then

$$\operatorname{rank}_{\mathbb{Z}_p}(D_{\mathfrak{p}'}(\tilde{\mathbb{K}}'/K')) = \operatorname{rank}_{\mathbb{Z}_p}(D_{\mathfrak{p}}(\mathbb{K}/K)) \geq 2$$

by assumption. This shows that we may apply Lemma 2.2 to (a chain of multiple $\mathbb{Z}_p$-extensions spanning) the extension $\mathbb{K}'/\tilde{\mathbb{K}}'$, proving that $A^{(\mathbb{K}')}$ is pseudo-null over $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}'/K')]]$. ∎

REMARKS 4.2. (1) The decomposition constraint in Theorem 4.1 holds for $\mathbb{K}/K$ if K contains a primitive p-th root of unity, or if K contains a normal extension k of $\mathbb{Q}$ which is imaginary (i.e., $r_2(k) \neq 0$), and it is conjectured to hold for every imaginary number field K (cf. [LN00, Théorème 3.2 and Remarque 3.3]). Moreover, the constraint holds if K contains exactly one prime above p. This will be the case in most of our examples.

(2) The above condition is needed in order to ensure that Lemma 2.2 can be applied to the extension $\mathbb{K}'/(\mathbb{K}\cdot K')$. If the primes of $\mathbb{K}\cdot K'$ dividing some $\mathfrak{p}'$ of K' are unramified in $\mathbb{K}'$, i.e., if the $\mathbb{Z}_p$-ranks of the inertia groups $I_{\mathfrak{p}'}((\mathbb{K}\cdot K')/K')$ and $I_{\mathfrak{p}'}(\mathbb{K}'/K')$ are equal, then the conclusion of Theorem 4.1 remains true also if the $\mathbb{Z}_p$-rank of $D_{\mathfrak{p}}(\mathbb{K}/K)$, $\mathfrak{p}=\mathfrak{p}'\cap K$, is equal to one ($\mathfrak{p}'$ does not affect the applicability of Lemma 2.2).

The following observation significantly enlarges the set of shifts K'/K to which we can apply Theorem 4.1; namely, instead of considering shifts of K itself, we look at suitable extensions of intermediate number fields in $\mathbb{K}/K$. Since usually the ideal class groups of these fields grow when the degree over K increases, there do even exist many *unramified* shifts arising this way.

Corollary 4.3. *Let K be a number field. Suppose that there exists a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that*

- $A^{(\mathbb{L})}/(p\cdot A^{(\mathbb{L})})$ *is finite, and*
- *only finitely many primes of $\mathbb{L}$ divide p.*

Then (GGC) *holds for every number field K' arising as a finite normal p-ramified p-extension of any finite intermediate field of the extension $\mathbb{L}/K$.*

Proof. For every finite extension $\tilde{K}$ of K contained in $\mathbb{L}$, $\mathbb{L}/\tilde{K}$ is a $\mathbb{Z}_p^2$-extension, and case (a) of Remark 3.6(2) is valid for $\tilde{K}$. Moreover, we may apply Theorem 4.1 to any finite p-ramified p-extension K' of $\tilde{K}$, since all the primes of $\tilde{K}$ dividing p are finitely decomposed in $\mathbb{L}/\tilde{K}$. ∎

We will now mention an important special case; in what follows, an *admissible shift* K' of a number field K is any finite normal p-ramified p-extension of any finite extension $\tilde{K}$ of K contained in the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K.

Corollary 4.4. *Let K be an imaginary quadratic field. Assume that $A^{(\mathbb{K})}/(p\cdot A^{(\mathbb{K})})$ is finite. Then* (GGC) *is valid for every admissible shift K' of K.*

Proof. Since $K/\mathbb{Q}$ is imaginary quadratic, $\mathbb{K}/K$ is a $\mathbb{Z}_p^2$-extension. Moreover, it is well-known that $\mathbb{K}$ contains only finitely many primes dividing p (cf. [Mi86, Lemma 3.1]). The statement thus follows from the previous corollary. ∎

Another class of examples arises from the number fields K containing exactly one prime dividing p. If the class number of such a field K is not divisible by p, then it is well-known that $A^{(\mathbb{K})}=\{0\}$. In particular, conditions (a) and (b) of Remark 3.6(2) are fulfilled, so that we immediately obtain the following result.

COROLLARY 4.5. *Let K be a number field containing exactly one prime above p. Suppose that the class number of K is coprime to p. Let K' denote an admissible shift of K. Then* (GGC) *holds for K'.*

We will now describe a more general situation, proving results analogous to Corollary 4.5.

THEOREM 4.6. *Let K be a number field containing exactly one prime $\mathfrak{p}$ above p. If this prime generates the group $A^{(K)}$, then* (GGC) *holds for K, and also for every admissible shift K' of K.*

Actually we will prove that

$$|A^{(\mathbb{K}')}| \leq |A^{(\tilde{K})}| < \infty,$$

where $\tilde{K} = \mathbb{K} \cap K'$ is the intermediate field corresponding to K' (i.e., $K'/\tilde{K}$ is a normal p-ramified p-extension).

To prove Theorem 4.6 we make use of the following two results.

THEOREM 4.7 (Chevalley's Theorem). *Let L/K be a cyclic extension of number fields, let $G := \mathrm{Gal}(L/K)$. Then*

$$|(A^{(L)})^G| = \frac{|A^{(K)}| \cdot e(L/K)}{[L:K] \cdot [\mathcal{O}_K^* : (N(L^*) \cap \mathcal{O}_K^*)]}.$$

Here $e(L/K)$ denotes the product of the ramification indices of all the primes ramifying in L/K, $N : L^* \to K^*$ is the norm map, and $\mathcal{O}_K^*$ denotes the group of units of K.

Proof. See [La90, §13.4]. ∎

LEMMA 4.8. *Let L/K be an abelian unramified extension of number fields of degree p^r, and suppose that $A^{(K)}$ is cyclic* (*this implies that L/K has to be cyclic*). *Then:*

(a) $|A^{(L)}| = |A^{(K)}|/p^r$, *and $A^{(L)}$ is again cyclic.*
(b) $A^{(L)} = i(A^{(K)})$, *where i denotes the map induced by the lifting of ideals of K to ideals of L.*

Proof. L is one of the intermediate fields of the extension $H(K)/K$. Since $A^{(K)}$ is cyclic, these intermediate fields are uniquely determined by their degrees over K:

$$K =: K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s := H(K),$$

where each extension K_{i+1}/K_i is cyclic and unramified of degree p. In particular, this means that $|A^{(K_i)}| \leq p \cdot |A^{(K_{i+1})}|$ for every i.

Moreover, $A^{(H(K))} = \{0\}$, since $A^{(K)}$ is cyclic (cf. [Be12, Proposition 2.5.1]). Therefore the above chain of field extensions implies that in fact $|A^{(K_i)}| = |A^{(K)}|/p^i$ for every $i \in \{0, \ldots, s\}$ (in other words, $H(K_i) = H(K)$ for every i). This proves (i).

For (ii), we note that Chevalley's Theorem 4.7 implies the equality $|(A^{(L)})^G| = |A^{(K)}|/p^r$, where $G := \mathrm{Gal}(L/K)$. Therefore $(A^{(L)})^G = A^{(L)}$, by (i). But L/K is unramified and cyclic, and so $(A^{(L)})^G = i(A^{(K)})$. ∎

Proof of Theorem 4.6. Recall that $A^{(K)}$ is cyclic generated by the prime ideal $\mathfrak{p}$ dividing p. Let $\tilde{K} := \mathbb{K} \cap K'$. Then $A^{(\tilde{K})}$ is again cyclic, generated by the unique prime of $\tilde{K}$ dividing $\mathfrak{p}$.

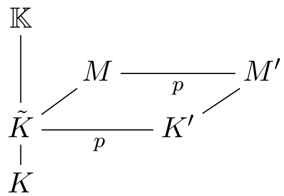
Indeed, if $\tilde{K}/K$ is unramified, then this follows from Lemma 4.8. We may therefore assume that $\tilde{K}/K$ is totally ramified at $\mathfrak{p}$. For any number field F containing K, we define the quotient $(A')^{(F)} := A^{(F)}/B^{(F)}$, where $B^{(F)}$ denotes the subgroup generated by the primes of F dividing $\mathfrak{p}$. Then $(A')^{(K)} = \{0\}$, by construction.

Moreover, one can show that

$$(A')^{(\tilde{K})}/((T_1, \ldots, T_r) \cdot (A')^{(\tilde{K})}) \cong (A')^{(K)} = \{0\},$$

where $T_1 = \gamma_1 - 1, \ldots, T_r = \gamma_r - 1$ for fixed generators $\gamma_1, \ldots, \gamma_r$ of $\mathrm{Gal}(\tilde{K}/K)$. Therefore $(A')^{(\tilde{K})} = \{0\}$ by Nakayama's Lemma.

Now we let $M := H(\tilde{K})$, $M' := M \cdot K'$. We may assume that $K'/\tilde{K}$ and M'/M are cyclic extensions of degree p (the theorem then follows by induction, since each finite p-group is solvable).



Since $A^{(\tilde{K})}$ is cyclic, $A^{(M)} = \{0\}$. Moreover, M contains exactly one prime $\mathfrak{P}$ dividing p. Since M'/M is unramified outside this unique prime $\mathfrak{P}$, we see that $\mathfrak{P}$ is actually (totally) ramified in M'/M.

Therefore

$$A^{(M')}/(S \cdot A^{(M')}) \cong A^{(M)} = \{0\},$$

where now $S = \sigma - 1$ for some generator σ of $\mathrm{Gal}(M'/M)$. This implies that $A^{(M')} = \{0\}$.

Since M' contains exactly one prime above p, it follows that $A^{(\mathbb{M}')} = \{0\}$, where $\mathbb{M}'$ denotes the composite of all $\mathbb{Z}_p$-extensions of M'.

Theorem 3.1(i) implies that $A^{(\mathbb{K}')}$ is pseudo-null, i.e., (GGC) holds for K'. Looking at the proof of Theorem 3.1(i), we can actually say more:

$$\mathrm{Gal}(H(\mathbb{K}')/(M' \cdot \mathbb{K}' \cap H(\mathbb{K}')) = \{0\},$$

i.e., $M' \cdot \mathbb{K}' \supseteq H(\mathbb{K}')$ and thus

$$|A^{(\mathbb{K}')}| \leq |\mathrm{Gal}(M'/K')| \leq |A^{(\tilde{K})}|. \;\blacksquare$$

EXAMPLE 4.9. We will finally mention some non-trivial examples. Suppose that $p = 3$. Let K be a cubic number field such that $r_1(K) = r_2(K) = 1$, where $r_1(K)$ and $r_2(K)$ denote the numbers of real embeddings and pairs of complex embeddings of K into a fixed algebraic closure. In particular, K is not normal over $\mathbb{Q}$. There exist $r_2(K) + 1 = 2$ independent $\mathbb{Z}_p$-extensions of K (since $r_1(K) + r_2(K) - 1 = 1$, the group of units of K is an infinite $\mathbb{Z}$-module of rank 1, and therefore Leopoldt's Conjecture holds for K).

Suppose that $p = 3$ ramifies in $K/\mathbb{Q}$, $(3) \cdot \mathcal{O}_K = \mathfrak{p}^3$, and that the prime $\mathfrak{p}$ of K dividing 3 generates the (p-primary part of the) ideal class group of K. Then (GGC) holds for K, and in fact $|A^{(\mathbb{K})}| \leq 3$ by Theorem 4.6. It is easy to find examples of cubic fields satisfying the above conditions. For example, consider the fields generated by some root of one of the polynomials

$$\begin{aligned} f_1(x) &:= x^3 - 9x^2 + 90x + 141, \\ f_2(x) &:= x^3 - 9x^2 + 9x + 141, \\ f_3(x) &:= x^3 + 18x + 18. \end{aligned}$$

One might wonder whether the Greenberg modules in the above examples are non-trivial. In fact, it is easy to see that $A^{(\mathbb{K})}$ will be non-trivial (and therefore cyclic of order 3) if and only if the maximal unramified p-abelian extension $H(K)$ of K is not contained in $\mathbb{K}$ (use the fact that $|A^{(H(K))}| = 1$, and that both K and $H(K)$ contain exactly one prime dividing $p = 3$).

Therefore the number field K defined by the polynomial f_3 has trivial $A^{(\mathbb{K})}$, since one can check that the first step of the cyclotomic $\mathbb{Z}_3$-extension of K is unramified. It is more difficult to show that the fields defined by the first two polynomials actually satisfy $H(K) \cap \mathbb{K} = K$. One way is to use the following approach suggested to us by C. Greither.

Class field theory yields an exact sequence

$$0 \to \mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*} \to J_{\mathfrak{p}} \xrightarrow{\text{cont}} \mathrm{Cl}(K) \to 0,$$

where $\mathcal{O}_K^*$ denotes the group of units of K, which can be embedded into the group $\mathcal{O}_{\mathfrak{p}}^*$ of units of the local field $K_{\mathfrak{p}}$ completed at $\mathfrak{p}$. We write $\overline{\mathcal{O}_K^*}$ for the corresponding closure, and $J_{\mathfrak{p}} := (\prod'_{v\nmid 3} K_v^*/\mathcal{O}_v^* \times K_{\mathfrak{p}}^*)/K^*$ (here K^* is embedded diagonally, and $\prod'$ denotes the restricted product, i.e., we consider only the elements in $\prod_{v\nmid 3} K_v^*/\mathcal{O}_v^*$ which have finitely many non-trivial components).

The above sequence induces an exact sequence

$$(\star) \qquad 0 \to (\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3) \to J_{\mathfrak{p}}(3) \xrightarrow{\text{cont}} A^{(K)} \to 0$$

of the corresponding (pro-)3-parts.

Claim 1. *If the sequence* $(\star)$ *splits, then* $H(K) \cap \mathbb{K} = K$.

Proof. If $\mathcal{M}(K)$ denotes the maximal pro-3-abelian extension of K which is unramified outside $\mathfrak{p}$, then

$$J_{\mathfrak{p}}(3) \cong \mathrm{Gal}(\mathcal{M}(K)/K)$$

by class field theory. If $(\star)$ splits, then this group contains $\mathrm{Gal}(H(K)/K)$ as a direct summand. Therefore $\mathbb{K} \cap H(K) = K$, because $H(K)$ cannot be contained in some $\mathbb{Z}_3$-extension L of K. Indeed, if $H(K) \subseteq L$, then the subgroup $\mathrm{Fix}(L)$ of $\mathrm{Gal}(\mathcal{M}(K)/K)$ fixing L would be a non-trivial subgroup of

$$(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3) \times \{0\} \hookrightarrow \mathrm{Gal}(\mathcal{M}(K)/K).$$

But then $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathcal{M}(K)/K)/\mathrm{Fix}(L)$ could not be pro-cyclic. ∎

Now we choose a generator θ of K, i.e., $K = \mathbb{Q}(\theta)$, $f(\theta) = 0$ for the corresponding polynomial f. One can check that in the above examples (i.e., $f \in \{f_1, f_2\}$), $\mathcal{O}_K = \mathbb{Z}[\theta]$, and $\mathfrak{p} = (3, \theta)$. In other words, θ is a uniformiser of the maximal ideal of the local field $K_{\mathfrak{p}}$.

Moreover, using the equations $f_i(\theta) = 0$, $i = 1, 2$, one sees that in both cases $u := \theta^3/3$ is a 1-unit, in fact $u \equiv 1 \mod 3$, and therefore $u \in \mathcal{O}_{\mathfrak{p}}^*(3)$.

Claim 2. *If* $A^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$ *is generated by the prime* $\mathfrak{p}$ *of* K *dividing* 3, *then the sequence* $(\star)$ *splits if and only if the class* $[u] \in \left(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*}\right)(3)$ *is a cube.*

Proof. Since $A^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$, the sequence $(\star)$ splits if and only if there exists an element $m \in J_{\mathfrak{p}}(3)$ such that $\mathrm{cont}(m) = [\mathfrak{p}]$ generates $A^{(K)}$ and $m^3 = 1$ in $J_{\mathfrak{p}}(3)$.

Indeed, if such an element m exists, then we can define a split

$$s : A^{(K)} \to J_{\mathfrak{p}}(3)$$

via $s([\mathfrak{p}]) := m$. On the other hand, if a split s exists, then $m := s([\mathfrak{p}])$ has the desired properties.

Now suppose that $[u]$ is a cube in $(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3)$. Writing $[u] = [\alpha]^3$, we may conclude that the class

$$[(\ldots, 1, (\theta/\alpha)^3, 1, \ldots)] = [(\ldots, 1/3, (\theta/\alpha)^3 1/3, 1/3, \ldots)]$$

of $(\theta/\alpha)^3$ in $J_{\mathfrak{p}}(3)$ equals $[1]$, and

$$\mathrm{cont}([(\ldots, 1, \theta/\alpha, 1, \ldots)]) = \mathrm{cont}([(\ldots, 1, \theta, 1, \ldots)]) = [\mathfrak{p}].$$

This means that $m := [(\ldots, 1, \theta/\alpha, 1, \ldots)] \in J_{\mathfrak{p}}(3)$ does the job.

If, on the other hand,

$$\mathrm{cont}(m) = [\mathfrak{p}] = \mathrm{cont}([(\ldots, 1, \theta, 1, \ldots)])$$

for some $m \in J_{\mathfrak{p}}(3)$ satisfying $m^3 = 1$, then $[(\ldots, 1, \theta, 1, \ldots)]/m$ lies in the kernel of cont and so may be identified with some $[\alpha] \in (\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3)$.

Moreover,

$$\begin{aligned}[(\ldots,1,\theta,1,\ldots)^3/m^3] &= [(\ldots,1,\theta,1,\ldots)^3] = [(\ldots,1,\theta,1,\ldots)^3/3] \\ &= [(\ldots,1/3,\theta^3/3,1/3,\ldots)] = [(\ldots,1/3,u,1/3,\ldots)]\end{aligned}$$

equals the image of $[u]$ in $J_{\mathfrak{p}}(3)$, and therefore $[u] = [\alpha]^3$ is a cube in $(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3)$. ∎

Claim 3. *If $f(x) = x^3 + 3ix^2 + 3jx + 3k$ for integers*

$$i \equiv 6 \bmod 9, \qquad j \equiv 3 \bmod 9, \qquad k \equiv 20 \bmod 27,$$

then the sequence ($\star$) splits for the field K defined by f. Since $f_1(x)$ and $f_2(x)$ are of the shape described in Claim 3, this shows that the corresponding Greenberg modules $A^{(\mathbb{K})}$ are isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Proof. We will build on Claim 2. It is sufficient to prove that u is a cube modulo 9θ. Indeed, in this case we can apply Hensel's Lemma (cf. [Ei95, Theorem 7.3]) to the polynomial $g(x) := x^3 - u \in (\mathbb{Z}_3[\theta])[x]$; the approximate root a of g to be found below will satisfy $g'(a) \sim 3$, so that we need to show that

$$g(a) \equiv 0 \bmod (3^2 \cdot (\theta)).$$

Now the conditions on i, j and k imply that

$$u = \theta^3/3 = -i\theta^2 - j\theta - k \equiv 3\theta^2 + 6\theta + 7 \bmod (9\theta).$$

On the other hand, we compute the third power of the element $a := 1 + 2\theta$ in $\mathcal{O}_{\mathfrak{p}}^*$:

$$\begin{aligned}(1+2\theta)^3 &\equiv 1 + 6\theta + 3\theta^2 - \theta^3 = 1 + 6\theta + 3\theta^2 + 3i\theta^2 + 3j\theta + 3k \\ &= 1 + 3k + (6+3j)\theta + (3+3i)\theta^2 \equiv 7 + 6\theta + 3\theta^2 \bmod (9\theta). \ ∎\end{aligned}$$

In the previous examples, the Greenberg modules $A^{(\mathbb{K})}$ have in fact been finite. We will conclude our exposition with an example in which (GGC) holds, but $A^{(\mathbb{K})}$ is not finite.

Example 4.10. We will again consider $p = 3$. Let K be the cubic field defined by the polynomial

$$f(x) = x^3 - 6x^2 + 18x + 30.$$

Then $|A^{(K)}| = 3$, $r_1(K) = r_2(K) = 1$, and 3 is ramified in K, and K contains exactly one prime $\mathfrak{p}$ dividing 3.

We will first prove that (GGC) holds for K, using our Corollary 2.5. If L denotes the *cyclotomic $\mathbb{Z}_3$-extension* of K, generated by 3-power roots of unity, then one can see (e.g., using PARI) that L/K is totally ramified at $\mathfrak{p}$, and that the ideal class groups of the first two layers L_1 and L_2 of L (cyclic of degrees 3 and 9 over K) both are isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We will now use the following result due to T. Fukuda.

THEOREM 4.11 (Fukuda, [Fu94, Theorem 1]). *Let L/K be a $\mathbb{Z}_p$-extension with intermediate fields L_n, $n \in \mathbb{N}$, $L_0 := K$. Let $e \geq 0$ be the smallest integer such that every prime of K which ramifies in L/K is totally ramified in L/L_e. Then:*

(i) *If there exists some $n \geq e$ such that*
$$|A^{(L_{n+1})}| = |A^{(L_n)}|,$$
then $|A^{(L_m)}| = |A^{(L_n)}|$ for all $m \geq n$ (in particular, we then have $|A^{(L)}| = |A^{(L_n)}| < \infty$).

(ii) *If there exists an integer $n \geq e$ such that*
$$\mathrm{rank}_p(A^{(L_n)}) = \mathrm{rank}_p(A^{(L_{n+1})}),$$
then $\mathrm{rank}_p(A^{(L_m)}) = \mathrm{rank}_p(A^{(L_n)})$ *for all $m \geq n$.*

This theorem implies that $|A^{(L)}| = 27$ is finite. Since the prime $\mathfrak{p}$ of K dividing 3 is totally ramified in L, Corollary 2.5 implies that (GGC) holds for K.

On the other hand, we will now prove that $A^{(\mathbb{K})}$ is infinite. We will make use of the following fact.

LEMMA 4.12. *Let p be any prime. Let K be a cubic number field such that $r_1(K) = r_2(K) = 1$. Suppose that $H(K)$ is contained in $\mathbb{K}$, and that $A^{(K)}$ is* not *generated by primes dividing p. Then $A^{(\mathbb{K})}$ is infinite.*

Proof. J. Minardi has proved a stronger version of this lemma for imaginary quadratic ground fields K (see [Mi86, Proposition 3.C]).

Let $M \subseteq H(K)$ denote the maximal subextension in which all the primes of K dividing p are totally decomposed. Our assumption concerning $A^{(K)}$ implies that $M \neq K$. If $\mathbb{M}$ denotes the composite of all $\mathbb{Z}_p$-extensions of M, then $\mathbb{M}/\mathbb{K}$ will be unramified, since for every prime $\mathfrak{p}_i$ of K dividing p, and any prime $\mathfrak{P}_i$ of M dividing $\mathfrak{p}_i$, the $\mathbb{Z}_p$-rank of the inertia subgroup $I_{\mathfrak{P}_i}(\mathbb{M}/M) \subseteq \mathrm{Gal}(\mathbb{M}/M)$ of $\mathfrak{P}_i$ is equal to $\mathrm{rank}_{\mathbb{Z}_p}(I_{\mathfrak{p}_i}(\mathbb{K}/K))$.

Since $M \subseteq H(K) \subseteq \mathbb{K}$ by assumption, we may conclude that $\mathbb{M} \subseteq H(\mathbb{K})$. Moreover, $d(K) = r_2(K) + 1 = 1 + 1 = 2$, whereas
$$d(M) \geq r_2(M) + 1 \geq p \cdot r_2(K) + 1 = p + 1,$$
and therefore the extension $\mathbb{M}/\mathbb{K}$ and the group $A^{(\mathbb{K})}$ are infinite. ∎

Returning to our example, one can easily (e.g., with PARI) check that the prime $\mathfrak{p}$ of K dividing 3 is principal. It therefore remains to show that $H(K) \subseteq \mathbb{K}$. This can be done by using the approach from the previous Example 4.9: write $K = \mathbb{Q}(\theta)$. Using the notation from that example, we have to show that there does not exist an element $m \in J_{\mathfrak{p}}(3)$ such that cont(m) generates $A^{(K)}$ and $m^3 = 1$. It turns out that the prime 2 also ramifies in K, and $(2) \cdot \mathcal{O}_K = \mathfrak{q}^3$ for a generator $\mathfrak{q}$ of $A^{(K)}$. Moreover, θ is a uniformiser of the maximal ideal of $\mathcal{O}_{\mathfrak{q}}$.

If there exists an element $m \in J_{\mathfrak{p}}(3)$ with the above properties, then m has, modulo some element $\alpha \in \ker(\mathrm{cont}) = (\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3)$, a representative of the form

$$t = (\ldots, 1, \underline{1}, \overline{\theta}, 1, \ldots),$$

where we write $\overline{\theta}$ for the uniformiser θ in the $\mathfrak{q}$-component and $\underline{1}$ for the element 1 in the $\mathfrak{p}$-component.

We consider the unit $u := 1/2 \in \mathcal{O}_{\mathfrak{p}}^*(3)$. Note that

$$\theta^3 = 6 \cdot (\theta^2 - 3\theta - 5) = 2 \cdot w$$

for some unit $w \in \mathcal{O}_{\mathfrak{q}}^*$, and therefore

$$[t^3] = [(\ldots, 1, \underline{1}, \overline{2w}, 1, \ldots)] = [(\ldots, 1, \underline{1}, \overline{2}, 1, \ldots)] = [(\ldots, 1/2, \underline{u}, \overline{1}, 1/2, \ldots)].$$

This last element equals the image of u in $J_{\mathfrak{p}}(3)$, since

$$[(\ldots, 1/2, \underline{1}, \overline{1}, 1/2, \ldots)] = [1]$$

in $J_{\mathfrak{p}}(3)$, because $1/2$ is a v-adic unit for every $v \notin \{\mathfrak{p}, \mathfrak{q}\}$.

Since $m^3 = 1$, we may conclude that

$$[(\ldots, 1, \underline{u}, 1, \ldots)] = [t^3] = [(t/m)^3] = [(\ldots, 1, \underline{\alpha^3}, 1, \ldots)]$$

in $J_{\mathfrak{p}}(3)$, and therefore $u = \alpha^3$ is a cube in $(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*})(3)$. However, computing modulo 9, it is easy to see that neither $\pm u$ nor $\pm u\eta$ nor $\pm u\eta^2$, where η denotes the fundamental unit of K, is congruent to one of the finitely many representatives of the cubes of $\left(\mathcal{O}_{\mathfrak{p}}^*/\overline{\mathcal{O}_K^*}\right)(3)$ modulo 9.

Now Claim 2 of Example 4.9 implies that the exact sequence $(\star)$ does not split for K. Since $A^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$, one can show that this means that $J_{\mathfrak{p}}(3)$ has no finite 3-torsion, i.e., $H(K)$ has to be contained in $\mathbb{K}$.

Remark 4.13. It remains an interesting open question whether our ‘shifting’ procedure, i.e., Theorem 4.1, can be applied to the field K from Example 4.10. This amounts to showing that $\mathrm{rank}_p(A^{(\mathbb{K})})$ is finite.

Acknowledgements. I would like to thank C. Greither for carefully reading preliminary versions of this article, and pointing out a gap in one of the proofs. The exposition of the paper has considerably profited from his suggestions. Moreover, I am grateful to the anonymous referee for suggesting numerous improvements.

References

[Ba03] A. Bandini, *Greenberg's conjecture for $\mathbb{Z}_p^d$-extensions*, Acta Arith. 108 (2003), 357–368.

[Ba07] A. Bandini, *Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions*, J. Number Theory 122 (2007), 121–134.
[Be12] T. Bembom, *The capitulation problem in class field theory*, Ph.D. thesis, Univ. of Göttingen, 2012.
[Ei95] D. Eisenbud, *Commutative Algebra. With a View toward Algebraic Geometry*, Springer, New York, 1995.
[Fu94] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), 264–266.
[Gr73] R. Greenberg, *The Iwasawa invariants of Γ-extensions of a fixed number field*, Amer. J. Math. 95 (1973), 204–214.
[Gr76] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.
[Gr78] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. 47 (1978), 85–99.
[Gr01] R. Greenberg, *Iwasawa theory—past and present*, in: Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001, 335–385.
[Iw73] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_l$-extensions*, in: Number Theory, Algebraic Geometry and Commutative Algebra, in Honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1–11.
[Kl14] S. Kleine, *A new approach to the investigation of Iwasawa invariants*, Ph.D. thesis, Univ. of Göttingen, 2014.
[La90] S. Lang, *Cyclotomic Fields I and II*, 2nd ed., Springer, New York, 1990.
[LN00] A. Lannuzel et T. Nguyen Quang Do, *Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres*, Manuscripta Math. 102 (2000), 187–209.
[MS03] W. G. McCallum and R. T. Sharifi, *A cup product in the Galois cohomology of number fields*, Duke Math. J. 120 (2003), 269–310.
[Mi86] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D. thesis, Univ. of Washington, 1986.
[Mo81] P. Monsky, *Some invariants of $\mathbb{Z}_p^d$-extensions*, Math. Ann. 255 (1981), 229–233.
[PR94] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) 17 (1984).

Sören Kleine
Institut für Theoretische Informatik, Mathematik und Operations Research
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
D-85577 Neubiberg, Germany
E-mail: soeren.kleine@unibw.de