ON THE GALOIS STRUCTURE OF ARITHMETIC COHOMOLOGY II: RAY CLASS GROUPS

DAVID BURNS AND ASUKA KUMON

ABSTRACT. We investigate the explicit Galois structure of ray class groups. We then derive consequences of our results concerning both the validity of Leopoldt's Conjecture and the existence of families of explicit congruence relations between the values of Dirichlet L-series at $s = 1$.

1. INTRODUCTION

The primary aim of this article is to investigate aspects of the explicit Galois structure of a natural family of ray class groups of number fields. This subject has a rather long history but aside from any intrinsic interest it may have there are also two ways in which it can have important consequences.

Firstly, such Galois structures are closely linked to the validity, or otherwise, of Leopoldt's Conjecture. In this context they have already been much studied in the literature, both in relatively simple cases (see, for example, Miki and Sato [19]) and in more involved Iwasawa-theoretic contexts (see, for example, Khare and Wintenberger [15]).

Secondly, ray class groups arise in the cohomology of complexes that occur in the formulation of the natural leading term conjectures for both p-adic and complex valued equivariant L-series that have been studied in recent years and, via this interpretation, explicit structural information on ray class groups directly translates into explicit congruence relations between such leading terms.

To study this problem we combine the general approach introduced by the first author in [5] to investigate the explicit Galois structure of compactly supported p-adic cohomology groups together with the approach used by Macias Castillo and the first author in [6] to prove a natural interpretation of the validity of Leopoldt's Conjecture in terms of the cohomological-triviality, as Galois modules, of a natural family of ray class groups.

In particular, in our first result we shall give a new interpretation of Leopoldt's Conjecture in terms of the basic properties of canonical 'étale' and 'cyclotomic' Yoneda extension classes that we shall introduce (in §2.2).

We then prove some detailed results about the explicit Galois structure of ray class groups and discuss consequences of these results for the validity of Leopoldt's Conjecture (see, for example, Theorem 2.15 and Remark 2.16).

Finally, as a concrete application of this general approach, we combine our results on Yoneda extensions and explicit Galois structures to prove several new results

Mathematics Subject Classification: 11G35 (primary), 11R33, 11R34 (secondary)
Keywords: Ray class groups, Galois structure, Leopoldt's Conjecture, Dirichlet L-series.

concerning the arithmetic of cyclotomic fields of conductor a power of any prime p that validates Vandiver's Conjecture.

These results include establishing families of explicit congruence relations between the values at $s = 1$ of the Dirichlet L-series associated to characters of p-power conductor after normalisation by a natural p-adic logarithmic resolvent if the character is odd and by a canonical $\mathcal{L}$-invariant (which is defined by comparing archimedean and p-adic logarithm maps) if the character is even.

We also prove a natural analogue of the classical fact that Stickelberger ideals account for all Galois relations in the ideal class groups of fields of p-power conductor (see Washington [27, §10.3]) in which ideal class groups are replaced by the torsion subgroups of ray class groups and Stickelberger elements by the values at $s = 1$ of Dirichlet L-series of even characters (normalised by the canonical $\mathcal{L}$-invariants). For more details of these results see Theorem 2.19 and Remark 2.20.

For convenience of the reader, we collect together the statements of all of our main results in §2. These results are then proved in the remainder of the paper.

The authors are grateful to Daniel Macias Castillo for pointing out an error in an earlier version of this article.

2. Statement of the main results

At the outset we fix an odd prime p and write $\mathbb{F}_p$ for the field of cardinality p.

For any abelian group M we write $M_{[p]}$ for its subgroup of elements of order dividing p and $M_{\rm tor}$ for its torsion subgroup and set $\overline{M} := M/M_{\rm tor}$.

If M is finitely generated over $\mathbb{Z}_p$, then we set $\mathrm{rk}_{\mathbb{Z}_p}(M) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M)$ and write $\mathrm{rk}_p(M)$ for the p-rank $\dim_{\mathbb{F}_p}(M/p) = \dim_{\mathbb{F}_p}(M_{[p]}) + \mathrm{rk}_{\mathbb{Z}_p}(M)$ of M.

For any commutative noetherian ring R we write $D(R)$ for the derived category of R-modules and $D^{\rm perf}(R)$ for the full triangulated subcategory of $D(R)$ comprising perfect complexes.

We denote the Galois group of a Galois extension of fields F/E by $G_{F/E}$.

2.1. Some general field notation.

We fix an extension of number fields L/K. We write $L^{\rm cyc}$ for the cyclotomic $\mathbb{Z}_p$-extension of L and set

$$\Gamma_L := G_{L^{\rm cyc}/L}.$$

We write Σ_p for the set of p-adic places of K. We fix a finite set of places Σ of K that contains Σ_p and write M_L^Σ for the maximal abelian pro-p extension of L that is unramified outside all places above those in Σ.

We then set

$$A_L^\Sigma := G_{M_L^\Sigma/L}$$

and

$$B_L^\Sigma := G_{M_L^\Sigma/L^{\rm cyc}}.$$

If L/K is Galois, then we regard both of these groups as $\mathbb{Z}_p[G_{L/K}]$-modules via the natural conjugation action of $G_{L/K}$.

In the special case that $\Sigma = \Sigma_p$ we often abbreviate $M_L^{\Sigma_p}$, $A_L^{\Sigma_p}$ and $B_L^{\Sigma_p}$ to M_L^p, A_L^p and B_L^p respectively.

2.2. The cyclotomic and étale extension classes.

For any finite group G, any non-negative integer n and $\mathbb{Z}_p[G]$-modules M and N we write $\mathrm{YExt}^n_G(N, M)$ for the group which classifies Yoneda n-extensions of N by M.

2.2.1. Then, after fixing a topological generator γ_L of $G_{L^{\rm cyc}/L}$, the canonical extension

$$0 \to B_L^\Sigma \to A_L^\Sigma \to \Gamma_L \to 0 \tag{1}$$

gives rise to an element $c_{L/K}^{\Sigma,\gamma_L}$ of the group

$$\mathrm{YExt}^1_{G_{L/K}}(\Gamma_L, B_L^\Sigma) \cong \mathrm{YExt}^1_{G_{L/K}}(\mathbb{Z}_p, B_L^\Sigma) \cong H^1(G_{L/K}, B_L^\Sigma)$$

where the first isomorphism is induced by the choice of γ_L and the second isomorphism is canonical.

We refer to $c_{L/K}^{\Sigma,\gamma_L}$ as the 'cyclotomic extension class' associated to the data $L/K, \Sigma$ and γ_L.

2.2.2. We next write $\mathcal{O}_{L,\Sigma}$ for the subring of L comprising elements that are integral at all non-archimedean places which do not lie above a place in Σ. We regard the Tate module $\mathbb{Z}_p(1)$ as an étale pro-sheaf on $\mathrm{Spec}(\mathcal{O}_{L,\Sigma})$ in the natural way and write $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ for the associated complex of compactly supported étale cohomology.

If L/K is Galois and Σ contains all places which ramify in L/K, then the action of G on $\mathcal{O}_{L,\Sigma}$ means that $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ is naturally an object of $D(\mathbb{Z}_p[G_{L/K}])$. In addition, since the truncated complex

$$\tau^{\geq 2} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)) \tag{2}$$

is acyclic outside degrees two and three and has cohomology in these degrees which identifies with A_L^Σ and $\mathbb{Z}_p$ respectively (see Lemma 3.1 below), it gives rise in this case to a canonical element $c_{L/K}^{\Sigma,\text{ét}}$ of

$$\mathrm{YExt}^2_{G_{L/K}}(\mathbb{Z}_p, A_L^\Sigma) \cong H^2(G_{L/K}, A_L^\Sigma).$$

We refer to $c_{L/K}^{\Sigma,\text{ét}}$ as the 'étale extension class' associated to L/K and Σ.

Remark 2.1. In [6, Th. 3.1(ii)] it is shown that the Shafarevic-Weil Theorem gives an alternative, and more concrete, description of the extension class $c_{L/K}^{\Sigma,\text{ét}}$.

2.2.3. Our first main result gives an explicit reinterpretation of the validity of Leopoldt's Conjecture at p in terms of the extension classes $c_{L/K}^{\Sigma,\gamma_L}$ and $c_{L/K}^{\Sigma,\text{ét}}$.

Theorem 2.2. *Let L/K be a finite Galois extension of number fields and Σ a finite set of places of K which contains all p-adic places and all which ramify in L/K. Then the following conditions are equivalent.*

(i) *Leopoldt's Conjecture is valid at p.*

(ii) *For all L/K and Σ as above the complex $\tau^{\geq 2} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ belongs to the category $D^{\rm perf}(\mathbb{Z}_p[G_{L/K}])$.*

(iii) *For all L/K and Σ as above one has both*

  (a) *$c_{L/K}^{\Sigma,\gamma_L}$ generates $H^1(G_{L/K}, B_L^\Sigma)$, and*

  (b) *$c_{L/K}^{\Sigma,\text{ét}}$ generates $H^2(G_{L/K}, A_L^\Sigma)$ and has order $|G_{L/K}|$.*

Remark 2.3. The proof of Theorem 2.2 given in §3.2 below shows that claim (iii) is equivalent to asserting that the $G_{L/K}$-module A_L^Σ is a class module with fundamental class $c_{L/K}^{\Sigma,\text{ét}}$ (as defined, for example, in [21, Chap. III, Def. (3.1.3)]). This statement constitutes a natural p-adic analogue of the fact that the Σ-idele class group of L is a class module for $G_{L/K}$.

In §3.3 we will show that Theorem 2.2 has the following concrete consequence.

Corollary 2.4. *Let L/K and Σ be as in Theorem 2.2 and assume that Leopoldt's Conjecture is valid at p. Then the following conditions are equivalent.*

(i) *$c_{L/K}^{\Sigma,\gamma_L}$ vanishes (and so the canonical extension (1) splits).*
(ii) *The $G_{L/K}$-module B_L^Σ is cohomologically-trivial.*
(iii) *For any given Sylow p-subgroup P of $G_{L/K}$ and every subgroup C of P of order p the transfer map $G_{M_K^\Sigma/K} \to G_{M_L^\Sigma/L}$ is injective on the subgroup $G_{M_K^\Sigma/L^{\rm cyc}}$.*

To end this section we record an important special case of this result.

Corollary 2.5. *Assume that Leopoldt's Conjecture is valid at p. Then for any number field K the conditions of Corollary 2.4(i), (ii) and (iii) are satisfied by any proper subfield L of $K^{\rm cyc}$.*

Proof. Let L be a proper subfield of $K^{\rm cyc}$, with $[L:K]=p^n$ say, and fix an element γ of $G_{M_L^\Sigma/K}$ which projects to give a topological generator of Γ_K.

Then the element γ^{p^n} belongs to A_L^Σ, is central in $G_{M_L^\Sigma/K}$ and projects to give a topological generator γ' of $\Gamma_L=\Gamma_K^{p^n}$. The unique homomorphism of $\mathbb{Z}_p$-modules $\Gamma_L\to A_L^\Sigma$ which sends γ' to γ^{p^n} is therefore a homomorphism of $\mathbb{Z}_p[G_{L/K}]$-modules which splits the extension (1).

This shows that the element $c_{L/K}^{\Sigma,\gamma_L}$ vanishes and so the claimed result is a direct consequence of Corollary 2.4. $\square$

2.3. **The structure of $\overline{A_L^\Sigma}$ in cyclic p-extensions.** To consider the Galois structure of A_L^Σ in greater detail we first restrict to the case that L/K is a cyclic extension of p-power degree.

For each intermediate field F of L/K we set

$$T_{L/F}^\Sigma := \mathrm{cok}(G_{M_L^\Sigma/L,\mathrm{tor}} \to G_{M_F^\Sigma/L,\mathrm{tor}}),$$

where the arrow denotes the natural restriction map. This is a finite group and is naturally isomorphic to $G_{(L^{\max}\cap M_F^\Sigma)/L,\mathrm{tor}}$ where we write $L^{\max}$ for the maximal $\mathbb{Z}_p$-power extension of L.

We write r_F for the number of complex places of F and δ_F for the p-adic 'Leopoldt defect' of F. We recall that δ_F is a non-negative integer which vanishes if and only if Leopoldt's Conjecture is valid for F at p and that

$$\mathrm{rk}_{\mathbb{Z}_p}(B_F^\Sigma)=\mathrm{rk}_{\mathbb{Z}_p}(A_F^\Sigma)-1=r_F+\delta_F$$

(cf. [21, (10.3.7) Corollary]).

Theorem 2.6. *Assume that L/K is cyclic of degree p^n and unramified outside Σ. For each integer i with $0\le i\le n$ let L_i denote the unique field with $K\subseteq L_i\subseteq L$ and $[L:L_i]=p^i$.*

Then the $\mathbb{Z}_p[G_{L/K}]$-lattice $\overline{A_L^\Sigma}$ is determined up to isomorphism (in a sense to be made precise in §4 below) by r_K, the integers δ_{L_i} for each i with $0\le i\le n$ and *the diagrams of finite groups*

$$\begin{cases} T^{\Sigma}_{L/L_1} \to T^{\Sigma}_{L/L_2} \to \cdots\cdots \to T^{\Sigma}_{L/L_n} \\ T^{\Sigma}_{L/L_1} \leftarrow T^{\Sigma}_{L/L_2} \leftarrow \cdots\cdots \leftarrow T^{\Sigma}_{L/L_n}. \end{cases} \tag{3}$$

Here each homomorphism $T^{\Sigma}_{L/L_i} \to T^{\Sigma}_{L/L_{i+1}}$ *is induced by the natural restriction map* $G_{M^{\Sigma}_{L_i}/L} \to G_{M^{\Sigma}_{L_{i+1}}/L}$ *and each homomorphism* $T^{\Sigma}_{L/L_{i+1}} \to T^{\Sigma}_{L/L_i}$ *by the map* $G_{M^{\Sigma}_{L_{i+1}}/L} \to G_{M^{\Sigma}_{L_i}/L}$ *which sends* x *to* $\sum_{c\in G_{L_i/L_{i+1}}} c(\tilde{x})$ *where* $\tilde{x}$ *is any lift of* x *to* $G_{M^{\Sigma}_{L_i}/L}$ *and we use the natural conjugation action of* $G_{L_i/L_{i+1}}$ *on* $G_{M^{\Sigma}_{L_i}/L}$.

Remark 2.7. A key ingredient in the proof of Theorem 2.6 is provided by a representation theoretic result of Yakovlev [28]. At the expense of only a little extra effort (and by using the results of [29] rather than [28]), all of the results discussed here extend to the setting of Galois extensions L/K for which only the Sylow p-subgroups of $G_{L/K}$ are assumed to be cyclic. However, the essential ideas are the same and so, for simplicity of exposition, we prefer not to deal with this more general case.

Remark 2.8. The finite groups $A^{\Sigma}_{L,\mathrm{tor}}$ have been extensively studied in the literature following seminal work of G. Gras. In particular, by using the explicit computation of $A^{\Sigma}_{L,\mathrm{tor}}$ made by Hemard in [13] one can often compute groups of the form $T^{\Sigma}_{L/F}$. (For an explicit example of such a computation see the proof of Lemma 6.1.)

Remark 2.9. If L/K is a cyclic extension of degree either p or p^2, then the indecomposable $\mathbb{Z}_p[G_{L/K}]$-lattices have been classified explicitly (see Remark 2.13 below) and this can be used to give a much more explicit version of Theorem 2.6. If L/K has degree p such an analysis is effectively carried out by Miki and Sato in [19] (see the proof of Proposition 5.1 below for more details). However, if L/K has degree p^2 the analysis is much more involved and is discussed in the upcoming thesis of the second author.

We record here two concrete consequences of Theorem 2.6.

Corollary 2.10. *Let* L/K *be a cyclic extension of* p*-power degree that is unramified outside* Σ *and set* $G := G_{L/K}$.

Then the group $T^{\Sigma}_{L/E}$ *vanishes for every intermediate field* E *of* L/K *if and only if there exists for each subgroup* H *of* G *a non-negative integer* n_H *for which there is an isomorphism of* $\mathbb{Z}_p[G]$*-modules of the form*

$$\overline{A^{\Sigma}_L} \cong \bigoplus_{H\leq G} \mathbb{Z}_p[G/H]^{n_H}.$$

If this is the case and, in addition, Leopoldt's Conjecture is valid for K *at* p*, then the right hand side of this isomorphism must have the form* $\mathbb{Z}_p[G]^{r_K} \oplus \mathbb{Z}_p[G/H]$ *for some subgroup* H *of* G.

Remark 2.11. It is clear that $T^{\Sigma}_{L/E}$ vanishes if $A^{\Sigma}_{E,\mathrm{tor}}$ vanishes and the latter condition is already well understood: for example, under the assumption that Leopoldt's Conjecture is valid at p, Gras [10, Th. I 2, Cor. 1] has characterised fields E for which $A^{p}_{E,\mathrm{tor}}$ vanishes. (Note that it is also clear that $T^{\Sigma}_{L/E}$ can vanish even if $A^{\Sigma}_{E,\mathrm{tor}}$ is non-trivial since, for example, if L is totally-real, then Leopoldt's Conjecture implies $\overline{A^{\Sigma}_L}$ is isomorphic to $\mathbb{Z}_p$ (as a trivial G-module) and hence, via Corollary 2.10, that $T^{\Sigma}_{L/E}$ vanishes). For a useful characterisation of the vanishing of $T^{\Sigma}_{L/E}$ in terms of '$\mathbb{Z}_p$-extendable' extensions see §4.4.

Before stating a second consequence of Theorem 2.6 we introduce some convenient notation.

For each non-negative number n we write C_n for the cyclic group $\mathbb{Z}/p^n$. For each non-negative integer m with $m \le n$ we regard C_m as a quotient of C_n in the obvious way. We then also fix a set $\mathrm{IM}_{p,n}$ of representatives of the isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices which do not contain $\mathbb{Z}_p[C_m]$ for any integer m with $0 \le m \le n$.

For each profinite extension of number fields F/E that is unramified outside p, each natural number n and each lattice I in $\mathrm{IM}_{p,n}$ we write $m_I(F/E)$ for the maximal multiplicity with which I occurs as a direct summand of $\overline{A^p_L}$ as L/K ranges over cyclic extensions of degree p^n with $E \subseteq K \subseteq L \subset F$ and K/E finite and, in each case, A^p_L is regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $G_{L/K}$ with C_n.

Finally, for each natural number d we define an integer

$$\kappa^d_n := \sum_{J_1\times\cdots\times J_n} \prod_{i=1}^{i=n-1} c_{J_i} c_{J_{i+1}},$$

where in the sum each J_i runs over a set of representatives of the isomorphism classes of finite abelian p-groups of exponent dividing p^i and p-rank at most d and c_{J_i} denotes the number of conjugacy classes in $\mathrm{Aut}(J_i)$ comprising elements of order dividing p^n.

Corollary 2.12. *Let E_∞ be a $\mathbb{Z}_p$-extension of a number field E for which all p-adic places of E have open decomposition groups in $G_{E_\infty/E}$ and the Iwasawa μ-invariant of the extension $E_\infty(\zeta_p)/E(\zeta_p)$ vanishes, where ζ_p is a choice of primitive p-th root of unity in E^c. Let F be a finite p-extension of E_∞ that is both unramified outside p and Galois over E.*

Then there exists an integer d which depends only upon F/E and is such that for any natural number n one has

$$\sum_{I\in \mathrm{M}_{p,n}} m_I(F/E) \le p^{n(n-1)d^2} \cdot \kappa^d_n. \tag{4}$$

In particular, for each n only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices can occur as direct summands of $\overline{A^p_L}$ as L/K runs over cyclic degree p^n extensions with $E \subseteq K \subset L \subset F$ and K/E finite and, in each case, A^p_L is regarded as a C_n-module via some choice of isomorphism of $G_{L/K}$ with C_n.

Remark 2.13. In the context of the inequality (4) Diederichsen [8] has shown that $\mathrm{IM}_{p,1}$ can be taken as the singleton $\{\mathbb{Z}_p[C_1]/(\sum_{g\in C_1} g)\}$ and Heller and Reiner [11] have explicitly described $\mathrm{IM}_{p,2}$ showing that $\#\mathrm{IM}_{p,2} = 4p-2$. However, if $n > 2$, then Heller and Reiner have shown in [12] that $\mathrm{IM}_{p,n}$ is infinite and, even now, there is still no explicit description of these sets.

Remark 2.14. The finiteness assertion in the final paragraph of Corollary 2.12 is of interest since $\mathrm{rk}_{\mathbb{Z}_p}(\overline{A^p_L})$ is in general unbounded as L ranges over finite extensions of E in F. This assertion also raises the question of whether there are general conditions under which one can explicitly describe the indecomposable $\mathbb{Z}_p[C_n]$-lattices which arise, up to isomorphism, as direct summands of these lattices. This question is similar in spirit to that considered in a different context by Elder in [9, §7] but appears to be difficult.

2.4. **The structure of A_L^Σ over p-rational fields.** If now L is any finite Galois extension of K that is unramified outside Σ, then the results of §2.3 can be used to study each of the $\mathbb{Z}_p[G_{E/E'}]$-modules $\overline{A_E^\Sigma}$ as E/E' ranges over cyclic p-power degree extensions with $K \subseteq E' \subseteq E \subseteq L$. These results can often then be combined to give strong information about the structure of $\overline{A_L^\Sigma}$ as a $\mathbb{Z}_p[G_{L/K}]$-module.

As an example, the next result uses this approach to give an explicit description of the Galois structure of A_L^Σ in the case that L/K is a p-extension and the group A_K^Σ is as small as possible (following Movahhedi and Nguyen Quang Do [20] such fields K are said to be 'p-rational').

Theorem 2.15. *Assume K validates Leopoldt's Conjecture at p and that the group A_K^Σ is torsion-free. Let L be any finite Galois p-extension of K that is unramified outside Σ and set $G := G_{L/K}$.*

Then the following claims are valid.

(i) *L validates Leopoldt's Conjecture at p.*
(ii) *The $\mathbb{Z}_p[G]$-module B_L^Σ is free of rank r_K.*
(iii) *The cyclotomic extension class $c_{L/K}^{\Sigma,\gamma_L}$ vanishes.*
(iv) *Assume that L/K is cyclic of order p^n and fix an element γ of $G_{M_L^\Sigma/K}$ which projects to give a generator of G. Then γ^{p^n} is central in $G_{M_L^\Sigma/K}$ and belongs to A_L^Σ and the $\mathbb{Z}_p[G]$-module $A_L^\Sigma/\langle\gamma^{p^n}\rangle$ is free of rank r_K.*

Remark 2.16. The result of Theorem 2.15(i) is not new. It has been proved both by Miki [18, Th. 3] and by Jaulent and Nguyen Quang Do [14, Cor. 1.5] by means of arguments that are different from ours because they make critical use of Shafarevic's description [25] of the minimal number of generators and relations of the Galois group of the maximal pro-p extension of K unramified outside Σ. If L/K is Galois of degree p it has also been proved by Miki and Sato in [19] by a method closer in spirit to ours but still reliant on Sharaferevich's results. Finally note that Theorem 2.15(i) is of interest since it implies the validity of Leopoldt's Conjecture for L at p can be deduced from its validity for the subfield K.

Remark 2.17. Fix a regular prime p. Then any abelian field K of p-power conductor is both p-rational (by [14, Cor. 1.3(ii)]) and validates Leopoldt's Conjecture (by Brumer [4]). Theorem 2.15 can therefore be applied in this setting. In particular, if one takes K and L to be the fields generated over $\mathbb{Q}$ by a primitive p-th root of unity and by a primitive p^n-th root of unity (for any natural number n) respectively, then Theorem 2.15 implies B_L^p is a free $\mathbb{Z}_p[G_{L/K}]$-module of rank $(p-1)/2$. In the next section we describe a natural extension of this result.

Remark 2.18. The modified ray class groups $A_L^\Sigma/\langle\gamma^{p^n}\rangle$ that occur in Theorem 2.15(iv) play a key role in the approach of Macias Castillo and the first author in [6] where they are used to give an explicit reinterpretation of the validity of Leopoldt's Conjecture at p.

2.5. **Extensions of prime power conductor.** For each natural number n we now fix a primitive p^n-th root of unity ζ_{p^n} in $\mathbb{Q}^c$ with the property that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for all $n > 1$.

In this section we assume that p does not divide the class number of the maximal real subfield of $\mathbb{Q}(\zeta_p)$. (We recall that the latter condition is automatically satisfied by regular primes and that Vandiver's Conjecture asserts it is satisfied by all primes.)

In this case we state several results concerning the arithmetic of abelian fields of p-power conductor that are obtained by specialisation of the general approach discussed above.

These include a natural generalisation of the result observed in Remark 2.17, a natural analogue concerning ray class groups of Washington's determination of the explicit Galois structure of ideal class groups of such fields [27, Th. 10.14] and new families of explicit congruence relations between the (suitably normalised) values at $s = 1$ of Dirichlet L-series associated to characters of p-power conductor.

2.5.1. We first fix some more general notation.

For each natural number n we set $L_n := \mathbb{Q}(\zeta_{p^n})$, $G_n := G_{L_n/\mathbb{Q}}$ and $P_n := G_{L_n/L_1}$. We also write H_n for the unique subgroup of G_n of order $p-1$ and use the restriction map $G_n \to G_1$ to identify H_n with G_1.

For each finite abelian group Γ we set $\Gamma^* := \mathrm{Hom}(\Gamma, \mathbb{Q}_p^{c\times})$ and for each ϕ in Γ^* we write e_ϕ for the idempotent $|\Gamma|^{-1}\sum_{\gamma\in\Gamma}\phi(\gamma)\gamma^{-1}$ of $\mathbb{Q}_p^c[\Gamma]$. We write $\mathbf{1}_\Gamma$ for the trivial element of Γ^* and often abbreviate the idempotent $e_{\mathbf{1}_\Gamma}$ to e_Γ. For each element x of $\mathbb{C}_p[\Gamma]$ and each ϕ in Γ^* we write x^ϕ for the unique element of $\mathbb{C}_p$ that is defined by the equality $x = \sum_{\phi\in\Gamma^*} x^\phi e_\phi$.

We use the fact that the natural direct product decomposition $G_n = P_n \times H_n$ implies each element of G_n^* can be written uniquely as a product $\psi\phi$ with ψ in P_n^* and ϕ in H_n^* and also that for each ϕ in H_n^* the idempotent e_ϕ belongs to $\mathbb{Z}_p[H_n]$.

We write τ_n for the (unique) complex conjugation in H_n and for any $\mathbb{Z}_p[G_n]$-module M we write M^+ and M^- for the submodules upon which τ_n acts as multiplication by $+1$ and -1 respectively. In particular, E^+ denotes the maximal real subfield of each subfield E of L_n.

We also write $G_n^{*,-}$ and $G_n^{*,+}$ for the subsets of G_n^* comprising characters that are odd (that is, satisfy $\chi(\tau_n) = -1$) and even (satisfy $\chi(\tau_n) = 1$) respectively. We define subsets $H_n^{*,+}$ and $H_n^{*,-}$ of H_n^* in a similar way and write ω for the Teichmuller character in $H_n^{*,-} = G_1^{*,-}$.

For any integer i and any $\mathbb{Z}_p[G_n]$-module M we write $M^{(i)}$ for the ω^i-isotypic component $e_{\omega^i}(M)$ of M.

2.5.2. To define the necessary logarithmic resolvents and $\mathcal{L}$-invariants we fix an isomorphism of fields j between $\mathbb{C}$ and the completion $\mathbb{C}_p$ of an algebraic closure of $\mathbb{Q}_p$ and, to ease notation, often suppress explicit reference to this isomorphism in what follows.

We also fix an embedding $\sigma_n : L_n \to \mathbb{Q}^c$, set $L_{n,p} := \mathbb{Q}_p \otimes_{\mathbb{Q}} L_n$ (which we identify with the pro-p completion of L_n at its unique p-adic place) and $\mathbb{Z}_p\hat{\otimes}L_{n,p}^\times$ for the pro-p completion of $L_{n,p}^\times$.

For any element π of $\mathbb{Z}_p\hat{\otimes}L_{n,p}^\times$ and any character χ in $G_n^{*,-}$ we then define a normalised logarithmic resolvent by setting

$$\mathcal{LR}_\pi^\chi := \frac{1}{j(2\pi i)} \sum_{g\in G_n} \chi(g)^{-1}\log_p(\sigma_n(g(\pi))) \in \mathbb{C}_p.$$

To define $\mathcal{L}$-invariants we use the composite homomorphisms of G_n-modules

$$\log_\infty^n : \mathcal{O}_{L_n^+}^\times \to \prod_\sigma \mathbb{R}^\times \xrightarrow{(\log)_\sigma} \prod_\sigma \mathbb{R} = \mathbb{R}\otimes_{\mathbb{Q}} L_n^+,$$

where σ runs over the set of all embeddings $L_n^+ \to \mathbb{Q}^c$ and the first arrow is the diagonal embedding, and

$$\log_p^n : \mathcal{O}_{L_n^+}^\times \to \mathcal{O}_{L_{n,p}^+}^\times \xrightarrow{\log_p} L_{n,p}^+ = \mathbb{Q}_p \otimes_{\mathbb{Q}} L_n^+$$

where the first arrow is the obvious embedding and $\log_p$ denotes Iwasawa's p-adic logarithm.

We write $L_{n,0}^+$ for the kernel $(1-e_{G_n})L_n^+$ of the field-theoretic trace map $L_n^+ \to \mathbb{Q}$. Then $\mathrm{im}(\log_\infty^n)$ is a full $\mathbb{Z}[G_n]$-lattice in $\mathbb{R}\otimes_{\mathbb{Q}} L_{n,0}^+$ and $\mathbb{Z}_p\cdot \mathrm{im}(\log_p^n)$ is a full $\mathbb{Z}_p[G_n]$-lattice in $\mathbb{Q}_p\otimes_{\mathbb{Q}} L_{n,0}^+$ and so for any generator x of the $\mathbb{Q}[G_n]$-module $\mathbb{Q}\cdot\mathcal{O}_{L_n^+}^\times$ there is in $(\mathbb{C}_p\otimes_{\mathbb{Q}} L_{n,0}^+)\oplus \mathbb{C}_p e_{G_n}$ an equality

$$(j\otimes \mathrm{id}_{L_{n,0}^+})(\log_\infty^n(x)) + e_{G_n} = \mathcal{L}_{\infty,p}^n \cdot (\log_p^n(x) + e_{G_n})$$

for an '$\mathcal{L}$-invariant' $\mathcal{L}_{\infty,p}^n$ in $\mathbb{C}_p[G_n]^{+,\times}$ that is easily seen to be independent of the choice of x.

For each character ψ in G_n^* we usually abbreviate the scalar $\mathcal{L}_{\infty,p}^{n,\psi}$ to $\mathcal{L}_{\infty,p}^{\psi}$.

2.5.3. In order to state the main result of this section we fix a topological generator $\gamma_{\mathbb{Q}}$ of $\Gamma_{\mathbb{Q}}$. Noting that G_n/H_n can be identified with the quotient of $\Gamma_{\mathbb{Q}}$ of order p^{n-1} we also fix a generating element γ_n of G_n which projects to the same element of G_n/H_n as does $\gamma_{\mathbb{Q}}$.

We write $\chi_{\mathbb{Q}}$ for the cyclotomic character of $\Gamma_{\mathbb{Q}}$ and define an element

$$\epsilon_{\gamma_{\mathbb{Q}}}^n := \sum_{\psi\in G_n^*} \epsilon_{\gamma_{\mathbb{Q}}}^\psi e_\psi$$

of $\mathbb{Q}_p[G_n]^\times$ by setting for each ψ in G_n^*

$$\epsilon_{\gamma_{\mathbb{Q}}}^\psi := \begin{cases} \log_p(\chi_{\mathbb{Q}}(\gamma_{\mathbb{Q}}))^{-1}, & \text{if } \psi = 1_{G_n},\\ (1-\psi(\gamma_n))^{-1}, & \text{if } \psi(H_n) = 1 \neq \psi(\gamma_n),\\ 1, & \text{otherwise.}\end{cases}$$

Finally we set

$$\theta_n^*(1) := (1-p^{-1})e_{\mathbf{1}_{G_n}} + \sum_{\psi\in G_n^*\setminus\{\mathbf{1}_{G_n}\}} L(\psi,1)\cdot e_\psi \in \mathbb{C}_p[G_n]^\times$$

(and we note that this element is equal to the leading term at $z=1$ of the p-truncated Dedekind zeta function that is naturally attached to the extension $L_n/\mathbb{Q}$).

The following result will be proved in §6.

Theorem 2.19. *Assume p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$. Then the following claims are valid for every natural number n.*

(i) *There are isomorphisms of* $\mathbb{Z}_p[G_n]$*-modules* $A^p_{L_n} \cong B^p_{L_n} \oplus \mathbb{Z}_p$ *and* $\overline{B^p_{L_n}} \cong \mathbb{Z}_p[G_n]^-$.

(ii) *The groups* $A^p_{L_n,\mathrm{tor}}$ *and* $B^{p,+}_{L_n}$ *coincide, the product* $\theta^*_n(1)\cdot\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}$ *belongs to* $\mathbb{Z}_p[G_n]^+ \cap (\mathbb{C}_p[G_n]^+)^\times$ *and there is an isomorphism of* $\mathbb{Z}_p[G_n]$*-modules*

$$A^p_{L_n,\mathrm{tor}} \cong \mathbb{Z}_p[G_n]^+/(\theta^*_n(1)\cdot\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}).$$

(iii) *Fix an even integer* i *with* $0 \le i \le p-3$ *and for each* ψ *in* P^*_n *set*

$$L^*(\psi\omega^i,1) := \begin{cases} 1-p^{-1}, & \textit{if } \psi = 1_{P_n} \textit{ and } i=0,\\ L(\psi\omega^i,1), & \textit{otherwise.}\end{cases}$$

(a) *If* p *divides the generalised Bernoulli number* $B_{1,\omega^{i-1}}$*, then the group* $A^{p,(i)}_{L_n,\mathrm{tor}}$ *has order at least* p^n*, the product* $\epsilon^{\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\omega^i}_{\infty,p}\cdot L^*(\omega^i,1)$ *belongs to* $p\cdot\mathbb{Z}_p$ *and for every element* g *in* G_n *the congruence*

$$\sum_{\psi\in P^*_n}(\psi\omega^i)(g)\epsilon^{\psi\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\psi\omega^i}_{\infty,p}\cdot L^*(\psi\omega^i,1) \equiv 0 \pmod{|G|\cdot\mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

(b) *If* p *does not divide* $B_{1,\omega^{i-1}}$*, then the group* $A^{p,(i)}_{L_n,\mathrm{tor}}$ *is trivial, the product* $\epsilon^{\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\omega^i}_{\infty,p}\cdot L^*(\omega^i,1)$ *belongs to* $\mathbb{Z}_p^\times$ *and for every element* g *of* G_n *the congruence*

$$\sum_{\psi\in P^*_n}(\psi\omega^i)(g)\epsilon^{\psi\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\psi\omega^i}_{\infty,p}\cdot L^*(\psi\omega^i,1) \equiv 0 \pmod{|G|\cdot\mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

(iv) *Fix an element* π *of* $(\mathbb{Z}_p\hat{\otimes}L^\times_{n,p})^-$ *which the reciprocity map sends to a generator of the (cyclic)* $\mathbb{Z}_p[G_n]^-$*-module* $\overline{B^p_{L_n}}$*. Then for every odd integer* i *with* $1 \le i \le p-2$ *the product* $\mathcal{LR}^{\omega^i}_\pi\cdot L(\omega^i,1)$ *belongs to* $\mathbb{Z}_p^\times$ *and for every element* g *of* G_n *the congruence*

$$\sum_{\psi\in P^*_n}(\psi\omega^i)(g)\mathcal{LR}^{\psi\omega^i}_\pi\cdot L(\psi\omega^i,1) \equiv 0 \pmod{|G|\cdot\mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

Remark 2.20. The known validity in this case of the p-adic Stark conjecture at $z=1$ (as discussed by Tate in [26, Chap. VI, §5] where it is attributed to Serre [24]) implies that each of the expressions $\mathcal{L}^{\psi\omega^i}_{\infty,p}\cdot L^*(\psi\omega^i,1)$ in Theorem 2.19(iii) can be replaced by the leading term at $z=1$ of the p-adic L-function of $\psi\omega^i$. A similar change can be made to the term $\theta^*_n(1)\cdot\mathcal{L}^n_{\infty,p}$ that occurs in the displayed isomorphism in Theorem 2.19(ii) and shows that this isomorphism gives a strong refinement of the main results of Oriat in [22]. However we have preferred not to state Theorem 2.19 in this way in order to stress the similarity between the results obtained for odd and even characters.

3. The proofs of Theorem 2.2 and Corollary 2.4

3.1. **Compactly supported étale cohomology.** In this section we use the notation and hypotheses of Theorem 2.2.

We also write Σ_L for the set of all complex embeddings $L \to \mathbb{C}$ and consider the direct sum $\bigoplus_{\Sigma_L} \mathbb{C}$ as a $G_{L/K} \times G_{\mathbb{C}/\mathbb{R}}$-module where $G_{L/K}$ acts on Σ_L via pre-composition and $G_{\mathbb{C}/\mathbb{R}}$ acts both on $\mathbb{C}$ naturally and on Σ_L via post-composition. We write W_L for the $G_{L/K}$-submodule of $\bigoplus_{\Sigma_L} 2\pi i\cdot\mathbb{Z} \subset \bigoplus_{\Sigma_L} \mathbb{C}$ comprising elements that are invariant under the action of $G_{\mathbb{C}/\mathbb{R}}$.

The basic properties of the complex $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ introduced in §2.2.2 that we shall need in the sequel are recorded in the next result (and are certainly well known - see, for example, the argument of [2, §4]).

Lemma 3.1. *Let L/K be a finite Galois extension of number fields and set $G := G_{L/K}$. Fix a finite set of places Σ of K that contains all p-adic places and all which ramify in L/K. Set $C_{L,\Sigma} := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$.*

(i) *$C_{L,\Sigma}$ is an object of the subcategory $D^{\text{perf}}(\mathbb{Z}_p[G])$ of $D(\mathbb{Z}_p[G])$.*

(ii) *$C_{L,\Sigma}$ is acyclic outside degrees one, two and three. There are natural identifications $H^2(C_{L,\Sigma}) = A_L^{\Sigma}$ and $H^3(C_{L,\Sigma}) = \mathbb{Z}_p$ and a natural exact sequence*

$$0 \to \mathbb{Z}_p \otimes W_L \to H^1(C_{L,\Sigma}) \to \mathbb{Z}_p \otimes \mathcal{O}_L^\times \xrightarrow{\lambda_{L,p}} \bigoplus_w \mathbb{Z}_p \hat{\otimes} L_w^\times$$

where in the direct sum w runs over all p-adic places of L and $\lambda_{L,p}$ denotes the natural diagonal map.

Remark 3.2. Leopoldt's Conjecture asserts that the map $\lambda_{L,p}$ in Lemma 3.1(ii) is injective and hence that $H^1(C_{L,\Sigma})$ identifies with the explicit module $\mathbb{Z}_p \otimes W_L$.

In each degree i we set $H^i_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)) := H^i(R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)))$.

3.2. **The proof of Theorem 2.2.** The key to our proof of Theorem 2.2 is provided by the following result of Macias Castillo and the first author (from [6, §5]).

Lemma 3.3. *Leopoldt's Conjecture is valid at p if and only if for every Galois extension L/K and set of places Σ as in the statement of Theorem 2.2, the $G_{L/K}$-module $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ is cohomologically-trivial.*

To apply this result we fix data L/K and Σ as in Theorem 2.2 and set $G := G_{L/K}$ and $C^\bullet := \tau^{\geq 2} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$.

Since the complex $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ is acyclic in degrees less than one (by Lemma 3.1), there exists a natural exact triangle in $D(\mathbb{Z}_p[G])$ of the form

$$H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))[-1] \to R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)) \to C^\bullet \to H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))[0].$$

As $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ belongs to $D^{\text{perf}}(\mathbb{Z}_p[G])$ (by Lemma 3.1), this triangle implies $C^\bullet$ belongs to $D^{\text{perf}}(\mathbb{Z}_p[G])$ if and only if the complex $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))[-1]$ belongs to $D^{\text{perf}}(\mathbb{Z}_p[G])$.

In addition, since the $\mathbb{Z}_p[G]$-module $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ is finitely generated, it is clear that $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))[-1]$ belongs to $D^{\text{perf}}(\mathbb{Z}_p[G])$ if and only if the $\mathbb{Z}_p[G]$-module $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ has a finite projective resolution, or equivalently (by the argument of [3, Chap. VI, Th. (8.12)]) that $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ is a cohomologically-trivial G-module.

The equivalence of conditions (i) and (ii) in Theorem 2.2 now follows directly upon combining these observations with the result of Lemma 3.3.

To further analyse condition (ii) of Theorem 2.2 we may choose a complex $\widehat{C}^\bullet$ of finitely generated $\mathbb{Z}_p[G]$-modules which represents $C^\bullet$ and has the form $M \xrightarrow{d} P$, where M occurs in degree two and P is free. Such a representative gives rise to (tautological) short exact sequences of $\mathbb{Z}_p[G]$-modules

$$0 \to A_L^\Sigma \to M \to \mathrm{im}(d) \to 0 \tag{5}$$

and

$$0 \to \mathrm{im}(d) \to P \to \mathbb{Z}_p \to 0 \tag{6}$$

and hence, in each degree i and for each subgroup J of G, to connecting homomorphisms in Tate cohomology

$$\kappa_{J,1}^i : \hat{H}^i(J, \mathrm{im}(d)) \to \hat{H}^{i+1}(J, A_L^\Sigma), \quad \kappa_{J,2}^i : \hat{H}^i(J, \mathbb{Z}_p) \to \hat{H}^{i+1}(J, \mathrm{im}(d)).$$

Now by an argument similar to that used above (to prove equivalence of the conditions (i) and (ii)) it is clear that the complex $\widehat{C}^\bullet$, and hence also $C^\bullet$, belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ if and only if M is a cohomologically-trivial G-module. In addition, by [3, Chap. VI, Th. (8.9)], the latter condition is satisfied if and only if for every subgroup J of G the group $\hat{H}^i(J, M)$ vanishes for both $i = 1$ and $i = 2$. By analysing the long exact cohomology sequence of (5) one finds that the latter condition is equivalent to requiring that $\kappa_{J,1}^0$ is surjective, $\kappa_{J,1}^1$ is bijective and $\kappa_{J,1}^2$ is injective.

We next note that the group $\hat{H}^a(J, \mathbb{Z}_p)$ vanishes for $a = -1$ and $a = 1$ and is isomorphic to $\mathbb{Z}_p/|J|$ if $a = 0$. Since each homomorphism $\kappa_{J,1}^i$ is bijective (as the module P that occurs in (6) is a free $\mathbb{Z}_p[G]$-module), it follows easily that $\kappa_{J,1}^2$ is injective, that $\kappa_{J,1}^0$ is surjective if and only if $\hat{H}^1(J, A_L^\Sigma)$ vanishes and that $\kappa_{J,1}^1$ is bijective if and only if $(\kappa_{J,1}^1 \circ \kappa_{J,2}^0)(1_{|J|})$ has order $|J|$ and generates $\hat{H}^2(J, A_L^\Sigma)$ where we write $1_{|J|}$ for the image of 1 in $\mathbb{Z}_p/|J|$.

In addition, the composite $\kappa_{J,1}^1 \circ \kappa_{J,2}^0$ coincides, up to sign, with the map given by taking cup product with the element $c_{L/L^J}^{\Sigma,\text{ét}}$ of

$$\hat{H}^2(J, A_L^\Sigma) = H^2(J, A_L^\Sigma) \cong \mathrm{YExt}_J^2(\mathbb{Z}_p, A_L^\Sigma)$$

that is defined by the complex $\mathrm{res}_{\mathbb{Z}_p[J]}^{\mathbb{Z}_p[G]} C^\bullet$ and so one has $(\kappa_{J,1}^1 \circ \kappa_{J,2}^0)(1_{|J|}) = \pm c_{L/L^J}^{\Sigma,\text{ét}}$. The bijectivity of $\kappa_{J,1}^1$ is thus equivalent to the condition of Theorem 2.2(iii)(b) with K replaced by L^J.

To complete the proof that the validity of Leopoldt's Conjecture at p is equivalent to the conditions stated in Theorem 2.2(iii) it is thus enough to show that the group $\hat{H}^1(J, A_L^\Sigma)$ vanishes if and only if $c_{L/L^J}^{\Sigma,\gamma_L}$ generates $H^1(J, B_L^\Sigma)$. This equivalence in turn follows easily from the fact that the long exact sequence of cohomology of (1) gives an exact sequence

$$\hat{H}^0(J, \mathbb{Z}_p) \xrightarrow{\alpha} H^1(J, B_L^\Sigma) \to H^1(J, A_L^\Sigma) \to H^1(J, \mathbb{Z}_p)$$

in which α sends the element $1_{|J|}$ of $\hat{H}^0(J, \mathbb{Z}_p) = \mathbb{Z}_p/|J|$ to $c_{L/L^J}^{\Sigma,\gamma_L}$ and the group $H^1(J, \mathbb{Z}_p)$ vanishes.

This completes the proof of Theorem 2.2.

3.3. **The proof of Corollary 2.4.** We again fix L/K and Σ as in Theorem 2.2 and set $G := G_{L/K}$.

If B_L^Σ is a cohomologically-trivial G-module, then $H^1(G, B_L^\Sigma)$ vanishes and so the sequence (1) obviously splits.

To prove the converse we assume Leopoldt's Conjecture to be valid at p and hence (by Theorem 2.2) that for any subgroup J of G the group $H^1(J, B_L^\Sigma)$ is generated by the element $c_{L/L^J}^{\Sigma,\gamma_L}$. In this case the vanishing of $c_{L/L^J}^{\Sigma,\gamma_L}$ therefore implies that $H^1(J, B_L^\Sigma)$ vanishes.

We assume for the moment that J has order p. Then, since p is odd, one has $r_L = |J| \cdot r_{L^J}$ and so

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot B_L^\Sigma) = r_L = |J| \cdot r_{L^J} = |J| \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot B_{L^J}^\Sigma) = |J| \cdot \dim_{\mathbb{Q}_p}(H_0(J, \mathbb{Q}_p \cdot B_L^\Sigma)),$$

where the last equality is valid because the result of Lemma 3.4(ii) below (with F replaced by L^J) applies to L/L^J and implies $H_0(J, B_L^\Sigma)$ identifies with an open subgroup of $B_{L^J}^\Sigma$.

Since every finitely generated $\mathbb{Q}_p[J]$-module is isomorphic to a direct sum of the form $\mathbb{Q}_p^a \oplus (\mathbb{Q}_p[J]/(\sum_{g\in J} g))^b$ for suitable non-negative integers a and b, the above formula for $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot B_L^\Sigma)$ implies that $\mathbb{Q}_p \cdot B_L^\Sigma$ is a free $\mathbb{Q}_p[J]$-module. The periodicity of Tate cohomology over J can therefore be combined with the vanishing of $H^1(J, B_L^\Sigma)$ and a Herbrand Quotient argument to deduce that the group $\hat{H}^a(J, B_L^\Sigma)$ vanishes in all degrees a.

Now any subgroup J' of G of p-power order contains a normal subgroup J of order p and so the associated Hochschild-Serre spectral sequence in Tate cohomology $\hat{H}^a\big(J'/J, \hat{H}^b(J, B_L^\Sigma)\big) \Longrightarrow \hat{H}^{a+b}\big(J', B_L^\Sigma\big)$ implies $\hat{H}^a\big(J', B_L^\Sigma\big)$ vanishes in all degrees a. This fact combines with [3, Chap. VI, Prop. (8.8)] to imply that B_L^Σ is a cohomologically-trivial G-module, as required.

This argument shows the equivalence of the conditions (i) and (ii) in Corollary 2.4 and further that (ii) is satisfied if and only if for every group C as in (iii) the group $H^1(C, B_L^\Sigma) \cong \hat{H}^{-1}(C, B_L^\Sigma)$ vanishes. By its very definition, the latter group vanishes if and only if the map $T_C : H_0(C, B_L^\Sigma) \to B_L^\Sigma$ induced by the action of $\sum_{c\in C} c$ is injective.

To show that this is equivalent to the stated condition in (iii) it now suffices to use the description of $H_0(C, B_L^\Sigma)$ given in Lemma 3.4(ii) below, with $F = L^C$, and the fact that in this case the following diagram commutes

$$\begin{array}{ccc} G_{M_F^\Sigma/L^{\mathrm{cyc}}} & \xrightarrow{\subset} & A_F^\Sigma \\ {\scriptstyle T_C}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{ver}} \\ B_L^\Sigma & \xrightarrow{\subset} & A_L^\Sigma, \end{array}$$

where ver is the natural transfer map from $A_F^\Sigma = (G_{M_L^\Sigma/F})^{\mathrm{ab}}$ to $(G_{M_L^\Sigma/L})^{\mathrm{ab}} = A_L^\Sigma$.

This completes the proof of Corollary 2.4.

Lemma 3.4. *Let L/F be a finite cyclic extension of p-power degree that is unramified outside a finite set of places Σ of F and set $G = G_{L/F}$.*

(i) *Then $H_0(G, A_L^\Sigma)$ identifies with $G_{M_F^\Sigma/L}$.*

(ii) *If $L \cap F^{\mathrm{cyc}}$ is equal to either F or L (as is automatically the case if L/F has degree p), then $H_0(G_{L/F}, B_L^\Sigma)$ identifies with $G_{M_F^\Sigma/L^{\mathrm{cyc}}}$.*

Proof. Claim (i) follows easily from the fact that G is cyclic and that M_F^Σ is the maximal extension of L inside M_L^Σ that is abelian over F.

To prove claim (ii) we assume first that $L\cap F^{\rm cyc}=F$. In this case the natural restriction maps induce identifications $\Gamma_L=\Gamma_F$ and $G_{L^{\rm cyc}/F^{\rm cyc}}=G$ and so lead to the following commutative diagram.

$$\begin{tikzcd}
 & & M_L^\Sigma \arrow[dl, dash, "B_L^\Sigma"'] \arrow[ddl, dash, "G_{M_L^\Sigma/F^{\rm cyc}}"] \\
 & L^{\rm cyc} \arrow[dl, dash, "\Gamma_F"'] \arrow[d, dash, "G"'] & \\
L \arrow[d, dash, "G"'] & F^{\rm cyc} \arrow[dl, dash, "\Gamma_F"] & \\
F & &
\end{tikzcd}$$

We write E for the intermediate field of $M_L^\Sigma/L^{\rm cyc}$ with $G_{E/L^{\rm cyc}}=H_0(G,B_L^\Sigma)$. Then $L^{\rm cyc}\subset M_F^\Sigma\subseteq E$ and so it suffices to show that E/F is abelian (and hence that $E=M_F^\Sigma$). But, since G is cyclic, E is automatically abelian over $F^{\rm cyc}$. Then, since Γ_F is pro-cyclic it suffices to show that the conjugation action of Γ_F on $G_{E/F^{\rm cyc}}$ is trivial and this follows easily from the above diagram and the fact that E is contained in M_L^Σ which is abelian over L.

We now assume $L\cap F^{\rm cyc}=L$ and hence that $L\subset F^{\rm cyc}$. In this case the exact sequence of $\mathbb{Z}_p[G]$-modules (1) splits (by Corollary 2.5) and so induces an exact sequence of $\mathbb{Z}_p$-modules

$$0\to H_0(G,B_L^\Sigma)\to H_0(G,A_L^\Sigma)\to\Gamma_L\to 0.$$

Taking account of claim (i) this sequence identifies $H_0(G,B_L^\Sigma)$ with $G_{M_F^\Sigma/L^{\rm cyc}}$, as required. □

4. The proof of Theorem 2.6 and Corollaries 2.10 and 2.12

4.1. **A result of Yakovlev.** A key role in these arguments is played by a purely representation-theoretic result of Yakovlev in [28].

To recall this result we fix a cyclic group Γ of order p^n and for each integer i with $0\le i\le n$ write Γ_i for the subgroup of Γ of order p^i.

Then the results of [28, Th. 2.4 and Lem. 5.2] combine to imply that if M and N are any $\mathbb{Z}_p[\Gamma]$-lattices for which, for each integer i with $1\le i<n$, there exists an isomorphism of $\mathbb{Z}_p[\Gamma/\Gamma_i]$-modules $\theta_i:\hat H^{-1}(\Gamma_i,M)\to\hat H^{-1}(\Gamma_i,N)$ that lies in commutative diagrams

$$\begin{tikzcd}
\hat H^{-1}(\Gamma_i,M) \arrow[r, "\kappa_M^i"] \arrow[d, "\theta_i"'] & \hat H^{-1}(\Gamma_{i+1},M) \arrow[d, "\theta_{i+1}"] & \hat H^{-1}(\Gamma_i,M) \arrow[d, "\theta_i"'] & \hat H^{-1}(\Gamma_{i+1},M) \arrow[l, "\rho_M^i"'] \arrow[d, "\theta_{i+1}"] \\
\hat H^{-1}(\Gamma_i,N) \arrow[r] & \hat H^{-1}(\Gamma_{i+1},N) & \hat H^{-1}(\Gamma_i,N) & \hat H^{-1}(\Gamma_{i+1},N) \arrow[l]
\end{tikzcd} \tag{7}$$

where the horizontal arrows are the natural corestriction and restriction homomorphisms, then there are isomorphisms of $\mathbb{Z}_p[\Gamma]$-modules of the form

$$M \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[\Gamma/\Gamma_i]^{a_i} \qquad \text{and} \qquad N \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[\Gamma/\Gamma_i]^{b_i} \tag{8}$$

for a suitable $\mathbb{Z}_p[\Gamma]$-lattice R and suitable non-negative integers a_i and b_i.

4.2. **The proof of Theorem 2.6.** We use the notation and hypotheses of Theorem 2.6. We also set $\overline{A} := \overline{A^{\Sigma}_{L}}$ and $G := G_{L/K}$ and for each integer i with $0 \le i \le n$ also $G_i := G_{L/L_i}$ and $T_i := T^{\Sigma}_{L/L_i}$.

We start by making a useful technical observation.

Lemma 4.1. *Fix an integer i with $0 \le i \le n$.*

(i) *The group T_i is naturally isomorphic as a $\mathbb{Z}_p\big[G/G_i\big]$-module to $\hat{H}^{-1}\big(G_i, \overline{A}\big)$.*

(ii) *If $i < n$, then the corestriction map $\hat{H}^{-1}\big(G_i, \overline{A}\big) \to \hat{H}^{-1}\big(G_{i+1}, \overline{A}\big)$ corresponds, under the isomorphisms in claim (i), to the homomorphism $T_i \to T_{i+1}$ that is induced by the natural restriction map $A^{\Sigma}_{L_i} \to A^{\Sigma}_{L_{i+1}}$.*

(iii) *If $i > 0$, then the restriction map $\hat{H}^{-1}\big(G_i, \overline{A}\big) \to \hat{H}^{-1}\big(G_{i-1}, \overline{A}\big)$ corresponds, under the isomorphisms in claim (i), to the homomorphism $T_i \to T_{i-1}$ that is induced by the map $G_{M^{\Sigma}_{L_i}/L} \to G_{M^{\Sigma}_{L_{i-1}}/L}$ which sends x to $\sum_{c\in G_{L_{i-1}/L_i}} c(\tilde{x})$ where $\tilde{x}$ is any lift of x to $G_{M^{\Sigma}_{L_{i-1}}/L}$.*

Proof. Upon taking G_i-coinvariants of the tautological exact sequence

$$0 \to A^{\Sigma}_{L,\mathrm{tor}} \to A^{\Sigma}_{L} \to \overline{A^{\Sigma}_{L}} \to 0,$$

recalling that $H_0(G_i, A^{\Sigma}_{L})$ identifies with $G_{M^{\Sigma}_{L_i}/L}$ (by Lemma 3.4(i)) and then passing to torsion subgroups in the resulting exact sequence one obtains an exact sequence of $\mathbb{Z}_p[G/G_i]$-modules

$$A^{\Sigma}_{L,\mathrm{tor}} \xrightarrow{\pi^{L}_{L_i}} G_{M^{\Sigma}_{L_i}/L,\mathrm{tor}} \to H_0(G_i, \overline{A^{\Sigma}_{L}})_{\mathrm{tor}} \to 0.$$

Given this exact sequence and the definition of T_i as the cokernel of $\pi^{L}_{L_i}$, the isomorphism in claim (i) follows from the fact that $H_0(G_i, \overline{A^{\Sigma}_{L}})_{\mathrm{tor}}$ is equal to $\hat{H}^{-1}(G_i, \overline{A^{\Sigma}_{L}})$. Indeed, since $\hat{H}^{-1}(G_i, \overline{A^{\Sigma}_{L}})$ is finite and $\overline{A^{\Sigma}_{L}}$ is $\mathbb{Z}_p$-free, the latter equality follows immediately from the tautological exact sequence

$$0 \to \hat{H}^{-1}(G_i, \overline{A^{\Sigma}_{L}}) \xrightarrow{\subseteq} H_0(G_i, \overline{A^{\Sigma}_{L}}) \to H^0(G_i, \overline{A^{\Sigma}_{L}}) \to \hat{H}^0(G_i, \overline{A^{\Sigma}_{L}}) \to 0$$

where the third arrow is induced by the action of the element $\sum_{g\in G_i} g$ of $\mathbb{Z}_p[G]$.

Given these isomorphisms, the assertions of claims (ii) and (iii) follow by straightforward computation (which we leave to the reader). □

To prove Theorem 2.6 we now apply the result of Yakovlev recalled in §4.1 with $\Gamma = G$ and $M = \overline{A}$. In this context Lemma 4.1 implies that the upper rows of the diagrams (7) for each integer i collectively correspond to the diagrams that are described in (3).

Given Yakovlev's theorem, the proof of Theorem 2.6 will therefore be complete if we show that, given an isomorphism of $\mathbb{Z}_p[G]$-modules of the form $\overline{A} \cong R \oplus R'$ in which R is uniquely determined up to isomorphism and R' is a module of the form $\bigoplus_{i=0}^{i=n} \mathbb{Z}_p[G/G_i]^{a_i}$ for suitable non-negative integers a_i, then R' is determined up to isomorphism as a $\mathbb{Z}_p[G]$-module by r_K and the integers δ_{L_i} for each integer i with $0 \le i \le n$.

But the explicit structure of the module R' makes it clear that it is determined up to isomorphism by the integers $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R'))$ for each integer i with $0 \le i \le n$, and so the required fact follows from the equalities

$$\begin{aligned}\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R')) &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, \overline{A})) - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R))\\ &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A^{\Sigma}_{L_i}) - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R))\\ &= r_{L_i} + \delta_{L_i} - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R))\\ &= p^{n_i} \cdot r_K + \delta_{L_i} - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R)),\end{aligned}$$

where the second equality is true because Lemma 3.4(i) implies that the $\mathbb{Q}_p$-spaces $\mathbb{Q}_p \cdot H^0(G_i, \overline{A}) \cong \mathbb{Q}_p \cdot H_0(G_i, A)$ and $\mathbb{Q}_p \cdot A^{\Sigma}_{L_i}$ are isomorphic.

This completes the proof of Theorem 2.6.

4.3. **The proof of Corollary 2.10.** If, in the notation of §4.1, M is any lattice for which $\hat{H}^{-1}(\Gamma_i, M)$ vanishes for each integer i, then in the decomposition (8) we may take the lattice N, and hence also R, to be the zero module and therefore deduce that M is itself a direct sum of modules of the form $\mathbb{Z}_p[\Gamma/\Gamma_i]$.

The first assertion of Corollary 2.10 follows directly by combining the latter observation with $\Gamma = G$ and $M = \overline{A^{\Sigma}_L}$ together with the explicit computation of Lemma 4.1(i).

To prove the second assertion of Corollary 2.10 we note that the stated conditions imply that the $\mathbb{Z}_p[G]$-module $\overline{A^{\Sigma}_L}$ is isomorphic to a direct sum of the form $\bigoplus_{i=1}^{i=d} \mathbb{Z}_p[Q_i]$ for suitable (not necessarily distinct) quotients Q_i of G. This isomorphism implies that

$$\begin{aligned}d &= \sum_{i=1}^{i=d} \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G, \mathbb{Z}_p[Q_i]))\\ &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot \bigoplus_{i=1}^{i=d} H^0(G, \mathbb{Z}_p[Q_i]))\\ &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G, \overline{A^{\Sigma}_L}))\\ &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot \overline{A^{\Sigma}_K})\\ &= 1 + r_K,\end{aligned}$$

where the first and second equalities are clear, the third follows from the stated isomorphism, the fourth from Lemma 3.4(i) and the last from the assumed validity of Leopoldt's Conjecture for K at p.

Since $r_L = |G| \cdot r_K$, this equality in turn implies that

$$\sum_{i=1}^{i=1+r_K} |Q_i| = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot \overline{A^{\Sigma}_L}) = 1 + r_L + \delta_L = 1 + |G| \cdot r_K + \delta_L \ge 1 + |G| \cdot r_K.$$

The second assertion of Corollary 2.10 now follows because an easy exercise shows this inequality implies that at least r_K of the quotients Q_i must be equal to G.

This completes the proof of Corollary 2.10.

4.4. **The vanishing of $T^{\Sigma}_{L/K}$.** We recall that an extension of number fields L/K is said to be '$\mathbb{Z}_p$-extendable' if there exists a Galois extension L' of K which contains L and is such that $G_{L'/K}$ is isomorphic to $\mathbb{Z}_p$. Such extensions have been extensively investigated in the literature, for example by Seo in [23].

It is clear that A^{Σ}_K is torsion-free if and only if all cyclic degree p extensions of K that are unramified outside Σ are $\mathbb{Z}_p$-extendable.

In the following result we use the concept of $\mathbb{Z}_p$-extendability to give a useful criterion for the vanishing of the groups $T^{\Sigma}_{L/K}$ which occur in Theorem 2.6 and Corollary 2.10.

Lemma 4.2. *Assume that L/K is cyclic of finite p-power degree and unramified outside a finite set of places Σ which contains all p-adic places.*

(i) *Then $T^{\Sigma}_{L/K}$ vanishes if and only if any degree p extension of L that is Galois over K is $\mathbb{Z}_p$-extendable if and only if it is contained in a $\mathbb{Z}_p$-extension of L that is abelian over K.*

(ii) *If L/K is $\mathbb{Z}_p$-extendable, then $T^{\Sigma}_{L/K}$ is equal to the cokernel of the restriction map $A^{\Sigma}_{L,\mathrm{tor}} \to A^{\Sigma}_{K,\mathrm{tor}}$. In this case $T^{\Sigma}_{L/K}$ vanishes if and only if for any degree p Galois extension K' of K that is not $\mathbb{Z}_p$-extendable the extension LK'/K is not $\mathbb{Z}_p$-extendable.*

Proof. As remarked earlier, $T^{\Sigma}_{L/K}$ is naturally isomorphic to the torsion subgroup of $G_{(M^{\Sigma}_K \cap L^{\max})/L}$ with $L^{\max}$ denoting the maximal $\mathbb{Z}_p$-power extension of L. It follows that $T^{\Sigma}_{L/K}$ vanishes if and only if $G_{(M^{\Sigma}_K \cap L^{\max})/L}$ is torsion-free. The latter condition is satisfied if and only if every degree p subextension of $(M^{\Sigma}_K \cap L^{\max})/L$ is contained in a $\mathbb{Z}_p$-extension of L that is contained in M^{Σ}_K. The assertion of claim (i) follows directly from this observation.

The first assertion of claim (ii) is true because if L/K is $\mathbb{Z}_p$-extendable, then $L \subseteq K^{\max}$ and so $G_{M^{\Sigma}_K/L,\mathrm{tor}} = G_{M^{\Sigma}_K/K^{\max}}$. This implies $T^{\Sigma}_{L/K}$ is isomorphic to $G_{(M^{\Sigma}_K \cap L^{\max})/K^{\max}}$ and this group vanishes if and only if $M^{\Sigma}_K \cap L^{\max} = K^{\max}$.

The latter condition is satisfied if and only if for any degree p extension L' of L that is abelian over K the extension L'/L is $\mathbb{Z}_p$-extendable if and only if $L' \subseteq K^{\max}$. If L'/K is cyclic, then it is itself $\mathbb{Z}_p$-extendable (since L/K is). If L'/K is not cyclic, then it has p intermediate fields K' that are of degree p over K and such that $L' = LK'$ and either all such extensions K'/K are $\mathbb{Z}_p$-extendable (in which case $L' \subseteq K^{\max}$ and L'/L is $\mathbb{Z}_p$-extendable) or no such extension K'/K is $\mathbb{Z}_p$-extendable (in which case $L' \not\subseteq K^{\max}$).

It is now straightforward to check that $M^{\Sigma}_K \cap L^{\max} = K^{\max}$ if and only if the condition stated in claim (ii) is satisfied, as required. □

4.5. **The proof of Corollary 2.12.** We continue for the moment to use the notation of §4.1.

For any natural number d we also write Lat_d for the set of $\mathbb{Z}_p[\Gamma]$-lattices N for which $\mathrm{rk}_p(\hat{H}^{-1}(\Gamma_i, N)) \leq d$ for all i with $1 \leq i \leq n$. For each I in $\mathrm{IM}_{p,n}$ we write m^d_I for the maximal multiplicity with which I occurs as a direct summand of any lattice N that belongs to Lat^d_{Γ}.

Then the key point in the proof of Corollary 2.12 is that Yakovlev's theorem combines with an analysis of the diagrams (7) to show that

$$\sum_{I\in \mathrm{IM}_{p,n}} m_I^d \le p^{n(n-1)d^2}\cdot \kappa_n^d$$

where κ_n^d is the integer defined just prior to the statement of Corollary 2.12 (for a proof of this fact see [5, Lem. 3.2]).

To deduce the claimed inequality (4) from this it is thus enough to show that the stated conditions imply the existence of an integer d which depends only on F/E and is such that $\mathrm{rk}_p(\hat{H}^{-1}(G_{L/K},\overline{A_L^p}))\le d$ for all cyclic degree p^n extensions L/K with $E\subseteq K\subset L\subset F$ and E/K finite.

In view of the description of the groups $\hat{H}^{-1}(G_{L/K},\overline{A_L^p})$ given in Lemma 4.1(i), it is therefore enough to show the existence of such an integer d for which one has

$$\mathrm{rk}_p(A^p_{L,\mathrm{tor}})\le d$$

for all finite extensions L of E in F.

We derive such an inequality as a simple consequence of the formula

$$\mathrm{rk}_p(A^p_{L,\mathrm{tor}}) = g(L)-\nu(L)+\mathrm{rk}_p(\mathrm{Cl}'_{L(\zeta_p)})-\delta_L \tag{9}$$

proved by Gras in [10, Th. I2]. Here $g(L)$ is the number of p-adic places of L, $\nu(L)$ is either 0 or 1 (depending on whether L contains ζ_p or not) and $\mathrm{Cl}'_{L(\zeta_p)}$ is a subquotient of the ideal class group $\mathrm{Cl}_{L(\zeta_p)}$ of $L(\zeta_p)$.

Since the stated assumption on the decomposition behaviour of p-adic places in F/E implies $g(L)$ is bounded above (independently of L) as L varies over finite extensions of E in F the formula (9) implies it suffices to show that the same is true of the p-ranks of the groups $\mathrm{Cl}_{L(\zeta_p)}$.

For any extension E' of E we write $X_{E'}$ for the Galois group of the maximal unramified abelian pro-p extension of E'.

We note that, for any L as above, the compositum of $L(\zeta_p)$ and E_∞ is an intermediate field of $F(\zeta_p)/E_\infty(\zeta_p)$ that is a $\mathbb{Z}_p$-extension of $L(\zeta_p)$. Since there are only finitely many intermediate fields of $F(\zeta_p)/E_\infty(\zeta_p)$ a standard Iwasawa-theoretic argument means it will be enough for us to show that, for each such intermediate field D, the $\mathbb{Z}_p$-module X_D is finitely generated.

To show this we note each such D is a finite p-extension of $E_\infty(\zeta_p)$ and hence that one can choose a finite chain of subgroups

$$G_{F(\zeta_p)/D} = J_0 \trianglelefteq J_1 \trianglelefteq \cdots \trianglelefteq J_n = G_{F(\zeta_p)/E_\infty(\zeta_p)}$$

with $|J_{i+1}/J_i| = p$ for all i with $0\le i<n$. For each such i we set $D_i := D^{J_i}$. Then $D_0 = D$, $D_n = E_\infty(\zeta_p)$ and each extension D_i/D_{i+1} is Galois of degree p.

Now the assumptions of Corollary 2.12 imply each field D_i has only finitely many p-adic places and that $X_{D_n} = X_{E_\infty(\zeta_p)}$ is a finitely generated $\mathbb{Z}_p$-module. The required result can therefore be obtained by successively applying the result of Lemma 4.3 below to each of the extensions D_i/D_{i+1} starting at $i = n-1$ and descending to $i = 0$.

This completes the proof of the inequality (4). To complete the proof of Corollary 2.12 it is enough to note that the finiteness assertion in its final paragraph is true because (4) implies directly that $m_I(F/E)$ can be non-zero for only finitely many indecomposable lattices I.

Lemma 4.3. *Let D be a number field with only finitely many p-adic places and D' a Galois extension of D of degree p. Then if the $\mathbb{Z}_p$-module X_D is finitely generated so is $X_{D'}$.*

Proof. Write $M_{D'}$ and M_D for the maximal unramified abelian pro-p extensions of D' and D and set $\Delta := G_{D'/D}$.

Then the extension $M_{D'}/D$ is Galois and $H_0(\Delta, X_{D'})$ identifies with $G_{M/D}$ where M denotes the maximal abelian extension of D in $M_{D'}$.

In addition, the inertia degree in M/D of each of the finitely many p-adic places of D is at most p and so the subgroup I of $G_{M/D}$ that is generated by the inertia subgroups of these places is finite.

The fixed field M^I is a subfield of M_D and so there is a surjective homomorphism of $\mathbb{Z}_p$-modules from X_D to the quotient $H_0(\Delta, X_{D'})/I$. Since X_D is finitely generated and I and Δ are both finite, this surjective homomorphism combines with Nakayama's Lemma to imply the $\mathbb{Z}_p$-module $X_{D'}$ is also finitely generated, as required. □

5. The proof of Theorem 2.15

We start the proof by making an important technical observation.

Proposition 5.1. *Let L/K be a cyclic extension of degree p^n that is unramified outside Σ and set $G := G_{L/K}$. Fix an element γ of $G_{M^\Sigma_L/K}$ that has infinite order and projects to give a generator of G. For each integer i with $0 \le i \le n$ write L_i for the intermediate field of L/K that has degree p^i over K and γ_i for the image of γ^{p^i} in $A^\Sigma_{L_i}$.*

If both K validates Leopoldt's Conjecture at p and the group A^Σ_K is torsion-free, then L validates Leopoldt's Conjecture at p and for each integer i the groups $A^\Sigma_{L_i}$ and $A^\Sigma_{L_i}/\langle\gamma_i\rangle$ are torsion-free.

Proof. For integers i and j with $0 \le i < j \le n$ we set $A_i := A^\Sigma_{L_i}$, $D_i := A^\Sigma_{L_i}/\langle\gamma_i\rangle$ and $Q_{j,i} := G_{L_j/L_i}$.

For each integer i as above one can use the multiplication-by-p map on the tautological exact sequence $0 \to \langle\gamma_i\rangle \to A_i \to D_i \to 0$ to obtain an exact sequence

$$0 \to A_{i,[p]} \to D_{i,[p]} \to \langle\gamma_i\rangle/\langle\gamma_i^p\rangle \xrightarrow{d_i} A_i/(A_i)^p.$$

Since the image of γ_i generates G_{L_{i+1}/L_i} one has $\gamma_i \notin (A_i)^p$. The map d_i is thus injective and so the above sequence implies that the natural map $A_{i,[p]} \to D_{i,[p]}$ is bijective. This implies, in particular, that the group D_i is torsion-free if and only if the group A_i is torsion-free.

Until further notice, we now assume that the integer i is such that the following hypothesis is satisfied.

$(*)_i$ L_i validates Leopoldt's Conjecture at p and the group $D_i = A_i/\langle\gamma_i\rangle$ is torsion-free.

In this case, for each integer j with $i < j \le n$ the group $H_0(Q_{j,i}, A_j)$ identifies with a subgroup of A_i and the torsion subgroup of $H_0(Q_{j,i}, D_j) = H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle$ is equal to

$$(A_i/\langle\gamma_i^{p^{j-i}}\rangle)_{\rm tor} \cap H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle = \langle\gamma_i\rangle/\langle\gamma_i^{p^{j-i}}\rangle \cap H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle.$$

Furthermore, this group vanishes since for any integer a with $0 \le a < j-i$ the element $\gamma_i^{p^a}$ does not act trivially on L_j and so does not lie in $H_0(Q_{j,i}, A_j)$.

It follows that under hypothesis $(*)_i$ the group $H_0(Q_{j,i}, D_j)$ is torsion-free and hence, by the same argument as used in the proof of Lemma 4.1, the group $\hat{H}^{-1}(Q_{j,i}, \overline{D_j})$ vanishes.

In the case $j = i+1$ we set $Q_i := Q_{j,i}$. Then, since Q_i has order p, there are only three isomorphism classes of indecomposable $\mathbb{Z}_p[Q_i]$-lattices, represented by $\mathbb{Z}_p, \mathbb{Z}_p[Q_i]$ and $\mathbb{Z}_p[Q_i]/(\sum_{g\in Q_i} g)$, each being endowed with the natural Q_i-action (cf. Remark 2.13). One also knows that the groups $\hat{H}^{-1}(Q_i, \mathbb{Z}_p)$ and $\hat{H}^{-1}(Q_i, \mathbb{Z}_p[Q_i])$ vanish and that $\hat{H}^{-1}(G, \mathbb{Z}_p[Q_i]/(\sum_{g\in Q_i} g))$ has order p.

Thus, since $\hat{H}^{-1}(Q_i, \overline{D_{i+1}})$ vanishes, the Krull-Schmidt theorem implies that the $\mathbb{Z}_p[Q_i]$-module $\overline{D_{i+1}}$ is isomorphic to a direct sum of the form $\mathbb{Z}_p^a \oplus \mathbb{Z}_p[Q_i]^b$ for suitable (non-negative) integers a and b.

Now

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_{i+1}) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A_{i+1}) - 1 = r_{L_{i+1}} + \delta_{L_{i+1}} \ge r_{L_{i+1}} = p \cdot r_{L_i}$$

whilst, since (under hypothesis $(*)_i$) we are assuming that L_i validates Leopoldt's Conjecture at p, one also has $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_i) = r_{L_i}$. This gives an inequality

$$\begin{aligned} a + p\cdot b = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_{i+1}) &\ge p \cdot r_{L_i} \\ &= p \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_i) = p \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H_0(Q_i, D_{i+1})) = p(a+b) \end{aligned}$$

and hence implies that $a = 0$ and $b = r_{L_i}$. This shows both that L_{i+1} validates Leopoldt's Conjecture at p and also that $\overline{D_{i+1}}$ is a free $\mathbb{Z}_p[Q_i]$-module.

Then, since $\overline{D_{i+1}}$ is a free $\mathbb{Z}_p[Q_i]$-module, the tautological exact sequence

$$0 \to (D_{i+1})_{\mathrm{tor}} \to D_{i+1} \to \overline{D_{i+1}} \to 0$$

splits as a sequence of $\mathbb{Z}_p[Q_i]$-modules and so $H_0(Q_i, (D_{i+1})_{\mathrm{tor}})$ is isomorphic to a finite submodule of $H_0(Q_i, D_{i+1})$. We have already shown the latter module to be torsion-free and so $H_0(Q_i, (D_{i+1})_{\mathrm{tor}})$ vanishes. By Nakayama's Lemma, this fact then implies that $(D_{i+1})_{\mathrm{tor}}$, and hence also $(A_{i+1})_{\mathrm{tor}}$, vanishes.

At this stage we have shown that the validity of hypothesis $(*)_i$ implies the validity of hypothesis $(*)_{i+1}$.

Thus, since the stated assumptions on $L_0 = K$ are equivalent to the validity of hypothesis $(*)_0$, an induction on i shows that hypothesis $(*)_i$ is true for all integers i with $0 \le i \le n$ and this fact is equivalent to the claimed result. □

To prove Theorem 2.15 we now simply proceed as follows. Let J be any subgroup of G of order p and set $F := L^J$. Then, since G is a p-group, there exists a finite chain of subgroups $\mathrm{id} = J_0 \trianglelefteq J_1 \trianglelefteq \cdots \trianglelefteq J_n = G$ in which $|J_{i+1}/J_i| = p$ for all i with $0 \le i < n$ and $J_1 = J$. For each such i we set $F^i := F^{J_i}$. Then by successively applying Proposition 5.1 to each of the extensions F^i/F^{i+1} for $0 \le i < n$ we deduce that L validates Leopoldt's Conjecture at p and that the groups A_L^Σ and A_F^Σ are torsion-free. In particular, this proves claim (i).

To prove claim (ii) we note first that it suffices to show B_L^Σ is a cohomologically-trivial G-module. Indeed, if this is true then, since B_L^Σ is also torsion-free (as a submodule of A_L^Σ), it must therefore be a free $\mathbb{Z}_p[G]$-module (by an application of, for example, [3, Chap. VI, (8.7), (8.8) and (8.10)]). Then, since Leopoldt's Conjecture is valid for L at p the rank of B_L^Σ over $\mathbb{Z}_p[G]$ is equal to r_K, as required.

Next we note that, by the same argument as used in §3.3, to prove B_L^Σ is a cohomologically-trivial G-module it suffices to show that $\hat{H}^{-1}(J, B_L^\Sigma)$ vanishes for any subgroup J of G of order p. We further claim that, for any given such J, the group $\hat{H}^{-1}(J, B_L^\Sigma)$ vanishes because $A_{L^J}^\Sigma$ is torsion-free. This is because $\hat{H}^{-1}(J, B_L^\Sigma)$ is a finite subgroup of $H_0(J, B_L^\Sigma)$ whilst, since L/L^J has degree p and hence satisfies the hypotheses of Lemma 3.4(ii), that result identifies $H_0(J, B_L^\Sigma)$ with a subgroup of the torsion-free group $A_{L^J}^\Sigma$. This proves claim (ii).

Claim (iii) is clear since B_L^Σ is a free $\mathbb{Z}_p[G]$-module.

To prove claim (iv) it is enough to show that the group $D_L := A_L^\Sigma/\langle\gamma^{p^n}\rangle$ is a permutation module over $\mathbb{Z}_p[G]$ since then the equality

$$\mathrm{rk}_{\mathbb{Z}_p}(D_L) = r_L = p^n \cdot r_K$$

(which follows from the known validity of Leopoldt's Conjecture for L at p) implies that D_L is free of rank r_K. Thus, as D_L is torsion-free (by Proposition 5.1), the argument of Theorem 2.6 shows it is enough to prove that for each subgroup J of G the group $\hat{H}^{-1}(J, D_L)$ vanishes. We need therefore only recall that the latter groups were shown to vanish in the course of proving Proposition 5.1.

This completes the proof of Theorem 2.15.

6. The proof of Theorem 2.19

In this section we fix an odd prime p that does not divide the class number of $\mathbb{Q}(\zeta_p)^+$.

We adopt the general notation of §2.5. In addition, for each natural number n we abbreviate the groups $A_{L_n}^p$ and $B_{L_n}^p$ to A_n and B_n respectively, we set $R_n := \mathbb{Z}_p[G_n]$ and for any homomorphism ϕ in H_n^* and any R_n-module M we set $M^\phi := e_\phi(M)$ and regard this as a module over the ring R_n^ϕ in the natural way.

6.1. **The proof of Theorem 2.19(i).** The first claimed isomorphism of R_n-modules $A_{L_n}^p \cong B_{L_n}^p \oplus \mathbb{Z}_p$ is true because the same argument as used in the proof of Corollary 2.5 shows that the short exact sequence (1) with $L = L_n, K = \mathbb{Q}$ and $\Sigma = \{p\}$ splits.

We recall next that L_n, and hence also L_n^+, validates Leopoldt's Conjecture at p (by Brumer [4]) and therefore that the group $(\overline{B_n})^+ \cong \overline{B_{L_n^+}^p}$ vanishes. This implies that $\overline{B_n} = (\overline{B_n})^-$ and hence that the second isomorphism $\overline{B_n} \cong R_n^-$ in claim (i) is valid provided that $(\overline{B_n})^-$ is a free R_n^--module of rank one.

Now, since for each ϕ in $H_n^{*,-}$ the ring R_n^ϕ is local and the $\mathbb{Z}_p$-ranks of R_n^ϕ and $(\overline{B_n})^\phi$ are equal (by the validity of Leopoldt for L_n), it suffices to show that $\overline{B_n}$ is a projective $\mathbb{Z}_p[P_n]$-module. By means of the same reductions used in the proof of Theorem 2.15(ii), this will in turn follow if we can show $\overline{B_n}$ is a cohomologically-trivial module over $G_{L_n/L_{n-1}}$.

In addition, since the validity of Leopoldt's Conjecture implies $\overline{B_n}$ spans a free $\mathbb{Q}_p[G_{L_n/L_{n-1}}]$-module (by the argument at the beginning of §3.3), a Herbrand Quotient argument implies the required cohomological-triviality follows directly from the result of Lemma 6.1 below, as required to complete the proof of claim (i).

In the sequel, for a number field F we write P_F and H_F for the subgroups of $F^\times$ comprising p-units and those elements x for which the extension $F(\sqrt[p]{x})$ is unramified outside p respectively, and Cl_F^p for the quotient of the ideal class group of F by the subgroup generated by the classes of ideals above p. We use the fact that these groups are related by a natural exact sequence

$$0 \to P_F/P_F^p \to H_F(F^\times)^p/(F^\times)^p \xrightarrow{\Delta_F} \mathrm{Cl}^p_{F,[p]} \to 0 \tag{10}$$

(see, for example, the proof of [1, Prop. 2.4]).

Lemma 6.1. *If p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$, then the group $\hat{H}^{-1}(G_{L_n/L_{n-1}}, \overline{B_n})$ vanishes.*

Proof. If $n = 1$, then this follows immediately from the fact that $\overline{B_n}$ is a pro-p group and the order of $G_{L_n/L_{n-1}} = G_1$ is prime to p.

If $n > 1$, then, as already observed above, the exact sequence (1) splits and so the description of Lemma 4.1 shows it is enough to prove $T^p_{L_n/L_{n-1}}$ vanishes. Recalling Lemma 4.2(iii), it therefore suffices to show that for any degree p Galois extension E of L_{n-1} that is not $\mathbb{Z}_p$-extendable the extension L_nE/L_n is not $\mathbb{Z}_p$-extendable.

To check this condition we use the fact that if F is either L_n or L_{n-1} and x is any element of $F^\times$, then Bertrandias and Payan [1, Prop. 2.7] have shown that $F(\sqrt[p]{x})$ is $\mathbb{Z}_p$-extendable if and only if x belongs to $P_F(F^\times)^p$. From the sequence (10) it is thus enough to show that if x is any element of $L_{n-1}^\times$ with $\Delta_{L_{n-1}}(x) \neq 0$, then also $\Delta_{L_n}(x) \neq 0$.

Since there is a commutative diagram

$$\begin{array}{ccc} H_{L_n}(L_n^\times)^p/(L_n^\times)^p & \xrightarrow{\Delta_{L_n}} & \mathrm{Cl}^p_{L_n} \\ \uparrow & & \iota_n\uparrow \\ H_{L_{n-1}}(L_{n-1}^\times)^p/(L_{n-1}^\times)^p & \xrightarrow{\Delta_{L_{n-1}}} & \mathrm{Cl}^p_{L_{n-1}} \end{array}$$

where the left hand vertical map is induced by inclusion and ι_n is the natural inflation, it thus suffices to show ι_n is injective.

This is true because $\mathrm{Cl}^p_{L_{n-1}} = \mathrm{Cl}_{L_{n-1}}$ and $\mathrm{Cl}^p_{L_n} = \mathrm{Cl}_{L_n}$ (as all prime ideals of L_{n-1} and L_n above p are principal), because the groups $\mathrm{Cl}^+_{L_{n-1}}$ and $\mathrm{Cl}^+_{L_n}$ vanish (by the stated assumption on p) and because the natural inflation map $\mathrm{Cl}^-_{L_{n-1}} \to \mathrm{Cl}^-_{L_n}$ is injective (as is shown, for example, by Kida in [16, Prop. 1, (1.2)]). □

6.2. **The proof of Theorem 2.19(ii).** The key fact that we use in the proof of Theorem 2.19(ii) is the known validity (due to Flach and the first author) of the appropriate case of the equivariant Tamagawa number conjecture. However, we must also first prove several auxiliary results.

We recall that for each integer i the ring $e_{\omega^i}R_n$ is abbreviated to $R_n^{(i)}$. For convenience we also write e_n for the idempotent $e_{\omega^0} = e_{H_n}$ of $\mathbb{Z}_p[H_n]$.

6.2.1. *A useful exact triangle.* We fix an element γ of $G_{M^p_{L_n}/\mathbb{Q}}$ which restricts to give both the element γ_n of G_n and the element $\gamma_\mathbb{Q}$ of $\Gamma_\mathbb{Q}$ that are fixed at the beginning of §2.5.3.

We then write $C^\bullet_{n,\gamma}$ for the complex of projective R_n-modules

$$R_n^{(0)} \xrightarrow{d_\gamma} R_n^{(0)}$$

where the first term is placed in degree two and d_γ satisfies $d_\gamma(e_n) = (1-\gamma_n)e_n$. We identify the groups $H^2(C^\bullet_{n,\gamma}) = \ker(d_\gamma)$ and $H^3(C^\bullet_{n,\gamma}) = \mathrm{cok}(d_\gamma)$ with $\mathbb{Z}_p$ via the maps of R_n-modules $\iota : \mathbb{Z}_p \to R_n^{(0)}$ and $\epsilon : R_n^{(0)} \to \mathbb{Z}_p$ with $\iota(1) = \sum_{g\in P_n} ge_n$ and $\epsilon(ge_n) = 1$ for all $g \in G_n$.

Finally we set $W_{n,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} W_{L_n}$, where the module W_{L_n} is as defined at the beginning of §3.1, and write $C_n^\bullet$ for the complex

$$W_{n,p}[-1] \oplus R_n^-[-2].$$

The following result refines the description of $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1))$ that is given in Lemma 3.1.

Proposition 6.2. *Fix an element b of $B_n^- = A_n^-$ which projects to give a basis of the (free, rank one) R_n^--module $\overline{B_n}$. Then there exists a canonical exact triangle in $D^{\text{perf}}(R_n)$ of the form*

$$C_{n,\gamma}^\bullet \oplus C_n^\bullet \xrightarrow{\theta_\gamma\oplus\theta_b} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1)) \to A_{n,\text{tor}}[-2] \to (C_{n,\gamma}^\bullet \oplus C_b^\bullet)[1]$$

in which $H^2(\theta_\gamma)(1) = \gamma^{|G_n|} \in A_n$, $H^3(\theta_\gamma)$ is the identity on $\mathbb{Z}_p$, $H^1(\theta_b)$ is the canonical identification $W_{n,p} = H^1_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1))$ (see Remark 3.2) and $H^2(\theta_b)$ sends each element x of $\mathbb{Z}_p[G_n]^-$ to $x(b)$.

In particular, the G_n-module $A_{n,\text{tor}}$ is cohomologically-trivial.

Proof. Set $E_n^\bullet := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1))$.

Then the complex $C_{n,\gamma}^\bullet$ clearly belongs to $D^{\text{perf}}(R_n)$ and the same is true of $C_n^\bullet$ since $W_{n,p}$ is a free R_n^--module of rank one and of $E_n^\bullet$ by Lemma 3.1(i).

The descriptions of the cohomology of $E_n^\bullet$ given in Lemma 3.1(ii) then make it clear that there exists a unique morphism $\theta_b : C_n^\bullet \to E_n^\bullet$ in $D(R_n)$ with the given descriptions of $H^1(\theta_b)$ and $H^2(\theta_b)$. In addition, the construction of a morphism $\theta_\gamma : C_{n,\gamma}^\bullet \to E_n^\bullet$ in $D^{\text{perf}}(R_n)$ with the given descriptions of $H^2(\theta_\gamma)$ and $H^3(\theta_\gamma)$ is described by Macias Castillo and the first author in [6, Prop. 4.3].

Writing $D_n^\bullet$ for the mapping cone of the morphism $\theta_\gamma \oplus \theta_b$, it therefore suffices to show that the long exact cohomology sequence of this cone implies that it is acyclic outside degree two and is such that R_n-module $H^2(D_n^\bullet)$ is naturally isomorphic to $A_{n,\text{tor}}$.

This long exact sequence makes the vanishing of $H^i(D_n^\bullet)$ for $i \notin \{0,1,2,3\}$ immediately clear and shows that the vanishing of $H^0(D_n^\bullet)$ and $H^3(D_n^\bullet)$ follows directly from the (obvious) injectivity of $H^1(\theta_\gamma)$ and surjectivity of $H^3(\theta_\gamma)$ respectively, that the vanishing of $H^1(D_n^\bullet)$ follows from the (obvious) surjectivity of $H^1(\theta_\gamma)$ and injectivity of both $H^2(\theta_\gamma)$ and $H^2(\theta_b)$ and that the (obvious) injectivity of $H^3(\theta_\gamma)$ gives rise to a short exact sequence

$$0 \to \text{im}(H^2(\theta_\gamma \oplus \theta_b)) \to A_n \to H^2(D_n^\bullet) \to 0. \tag{11}$$

Now the group $\text{im}(H^2(\theta_\gamma \oplus \theta_b)) = \text{im}(H^2(\theta_\gamma)) \oplus \text{im}(H^2(\theta_b))$ is $\mathbb{Z}_p$-free and so disjoint from $A_{n,\text{tor}} = B_{n,\text{tor}}$. Since the element $H^2(\theta_\gamma)(1) = \gamma^{|G_n|}$ is a topological generator of Γ_{L_n} and our choice of element b implies $B_{n,\text{tor}} + \text{im}(H^2(\theta_b)) = B_n$, we therefore obtain a direct sum decomposition $A_n = A_{n,\text{tor}} \oplus \text{im}(H^2(\theta_\gamma \oplus \theta_b))$. Given this, the exact sequence (11) induces a natural isomorphism of R_n-modules $H^2(D_n^\bullet) \cong A_{n,\text{tor}}$, as required.

Finally we note that the given exact triangle implies $A_{n,\text{tor}}[-2]$ belongs to $D^{\text{perf}}(R_n)$. This in turn implies that the R_n-module $A_{n,\text{tor}}$ has finite projective dimension and hence that it is cohomologically-trivial over G_n, as claimed. $\square$

Remark 6.3. It will be seen later (in Lemma 6.5) that our assumption that p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$ implies $A^-_{n,\mathrm{tor}}$ vanishes. Since $C^{\bullet,-}_{n,\gamma}$ is clearly the zero complex, this shows that the exact triangle in Proposition 6.2 induces an isomorphism in $D^{\mathrm{perf}}(\mathbb{Z}_p[G_n])$ between $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1))^-$ and the explicit complex $C^\bullet_n$.

6.2.2. *The Fitting ideal.* In this section we combine the exact triangle constructed in Proposition 6.2 with the known validity, due to Flach and the first author, of the equivariant Tamagawa number conjecture for the pair $(h^0(\mathrm{Spec}(L_n))(1), \mathbb{Z}[G_n])$ to prove the following result.

Theorem 6.4. *Fix an element π of $(\mathbb{Z}_p\hat{\otimes}L^\times_{n,p})^-$ as in the statement of Theorem 2.19(iv) and set*

$$\mathcal{LR}_\pi := \sum_{\chi\in G_n^{*,-}} \mathcal{LR}^\chi_\pi \cdot e_\chi \in \mathbb{C}_p[G_n].$$

Then $\theta^*_n(1)(\mathcal{LR}_\pi + \epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p})$ belongs to R_n and generates the ideal $\mathrm{Fit}_{R_n}(A_{n,\mathrm{tor}})$.

Proof. For any commutative noetherian ring R we write $\mathrm{Det}_R(-)$ for the determinant functor defined by Knudsen and Mumford in [17]. We recall that this functor is well-defined on the category $D^{\mathrm{perf}}(R)$ and takes values in the category of graded invertible R-modules.

If R is semisimple, C is an object of $D^{\mathrm{perf}}(R)$ that is acyclic outside degrees i and $i+1$ for some integer i and μ is an isomorphism of R-modules $H^i(C)\cong H^{i+1}(C)$, then we write ϑ_μ for the composite isomorphism

$$\begin{aligned}\mathrm{Det}_R(C) &\cong \mathrm{Det}_R(H^i(C))^{(-1)^i}\otimes \mathrm{Det}_R(H^{i+1}(C))^{(-1)^{i+1}}\\ &\cong \mathrm{Det}_R(H^{i+1}(C))^{(-1)^i}\otimes \mathrm{Det}_R(H^{i+1}(C))^{(-1)^{i+1}}\\ &\cong (R,0)\end{aligned}$$

where the first map is the canonical 'passage to cohomology' isomorphism (which exists since R is semisimple), the second is $\mathrm{Det}_R(\mu)^{(-1)^i}\otimes\mathrm{id}$ and the third is induced by the evaluation pairing on $H^{i+1}(C)$.

To prove the stated result we set $E^\bullet_n := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma_p}, \mathbb{Z}_p(1))$ and use, without explicit comment, the descriptions of the cohomology groups $H^i(E^\bullet_n)$ that are given in Lemma 3.1 and Remark 3.2. We also write Λ_n for the semisimple algebra $\mathbb{C}_p\cdot R_n$.

It clearly suffices to show both that $(\theta^*_n(1)\mathcal{LR}_\pi)R^-_n = \mathrm{Fit}_{R^-_n}(A^-_{n,\mathrm{tor}})$ and that $(\theta^*_n(1)\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p})R^+_n = \mathrm{Fit}_{R^+_n}(A^+_{n,\mathrm{tor}})$.

To prove the first equality we note that the proof of Castillo and Jones [7, Prop. 2.2] (which depends on the result of Flach and the first author) describes an explicit isomorphism of Λ_n-modules $\Phi_n : \mathbb{C}_p\cdot H^2(E^\bullet_n)^-\cong \mathbb{C}_p\cdot H^1(E^\bullet_n)^-$ for which there is an equality of graded invertible R^-_n-modules

$$(\theta^*_n(1)\cdot R^-_n, 0) = \vartheta_{\Phi_n^{-1}}(\mathrm{Det}_{R^-_n}(E^{\bullet,-}_n))^{-1}. \tag{12}$$

To explicate this equality we write ϵ_π for the homomorphism of R_n-modules $H^1(E^\bullet_n) = W_{n,p}\to H^2(E^\bullet_n)$ which sends the R_n-generator

$$w_n := 2\pi i\cdot(\sigma_n - \sigma_n\circ\tau_n)$$

of $W_{n,p}$ to the image of the chosen element π under the global reciprocity map $(\mathbb{Z}_p\hat{\otimes}L^\times_{n,p})^-\to B^-_n = A^-_n = H^2(E^\bullet_n)^-$. Then an explicit comparison of the result of [7, Prop. 2.3] with our definition of the equivariant resolvent $\mathcal{LR}_\pi$ implies that

$$\det_{\Lambda_n}(\Phi_n \circ (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \epsilon_\pi)) = \mathcal{LR}_\pi.$$

Since our choice of π implies that the map $\mathbb{C}_p \otimes \epsilon_\pi$ is invertible, this equality combines with (12) to give an equality of graded invertible R_n^--modules

$$((\theta_n^*(1) \cdot \mathcal{LR}_\pi)R_n^-, 0) = \vartheta_{\mathbb{C}_p\otimes\epsilon_\pi}(\mathrm{Det}_{R_n^-}(E_n^{\bullet,-}))^{-1}. \tag{13}$$

To compute the right hand side of this equality we use the exact triangle constructed in Proposition 6.2 in the case that the element b is chosen to have the same image in $\overline{B_n}$ as does the image of π under the reciprocity map. In this case the image of $H^2(\theta_b)((1-\tau_n)/2)$ in $\overline{B_n}$ is equal to the image of $H^1(\theta_b)(w_n)$ under $\mathbb{C}_p \otimes \epsilon_\pi$. Thus, if we write μ_b for the isomorphism of (free rank one) R_n^--modules $W_{n,p} \to R_n^-$ which sends w_n to $(1-\tau_n)/2$, then one has

$$\begin{aligned}\vartheta_{\mathbb{C}_p\otimes\epsilon_\pi}(\mathrm{Det}_{R_n^-}(E_n^{\bullet,-})) =& \vartheta_{\mathbb{C}_p\otimes\mu_b}(\mathrm{Det}_{R_n^-}(C_n^{\bullet})) \otimes \mathrm{Det}_{R_n^-}(A_{n,\mathrm{tor}}^-[-2]) \\ =& \mathrm{Det}_{R_n^-}(A_{n,\mathrm{tor}}^-[-2]) \\ =& (\mathrm{Fit}_{R_n^-}(A_{n,\mathrm{tor}}^-)^{-1}, 0).\end{aligned} \tag{14}$$

Here the first equality follows from the exact triangle in Proposition 6.2 and the fact that $C_{n,\gamma}^{\bullet,-}$ is the zero complex; the second equality in (14) is true because

$$\begin{aligned}\vartheta_{\mathbb{C}_p\otimes\mu_b}(\mathrm{Det}_{R_n^-}(C_n^{\bullet})) &= (\vartheta_{\mathrm{ev}} \circ (\mathrm{Det}_R(\mu_b)^{-1} \otimes \mathrm{id}))((\mathrm{Hom}_{R_n^-}(W_{n,p}, R_n^-), -1) \otimes (R_n^-, 1)) \\ &= \vartheta_{\mathrm{ev}}((\mathrm{Hom}_{R_n^-}(R_n^-, R_n^-), -1) \otimes (R_n^-, 1)) \\ &= (R_n^-, 0)\end{aligned}$$

where ϑ_{ev} is induced by the evaluation pairing on R_n^- and the second equality follows from the fact that $\mu_b(W_{n,p}) = R_n^-$; the final equality in (14) follows from a general property of Fitting ideals since Proposition 6.2 implies that the finite R_n^--module $A_{n,\mathrm{tor}}^-$ is of projective dimension at most one.

The equalities (13) and (14) then combine to imply that $(\theta_n^*(1) \cdot \mathcal{LR}_\pi)R_n^-$ is equal to $\mathrm{Fit}_{R_n^-}(A_{n,\mathrm{tor}}^-)$, as required.

To prove $(\theta_n^*(1)\epsilon_{\gamma_{\mathbb{Q}}}^n \mathcal{L}_{\infty,p}^n)R_n^+ = \mathrm{Fit}_{R_n^+}(A_{n,\mathrm{tor}}^+)$ we note first that the homomorphisms $\log_\infty^n$ and $\log_p^n$ in §2.5.2 combine to give an isomorphism of $\mathbb{C}_p[G_n]$-modules

$$\log_{\infty,p}^n : \mathbb{C}_p \otimes_{\mathbb{Q}} L_{n,0}^+ \xrightarrow{(\mathbb{C}_p\cdot\log_\infty^n)^{-1}} \mathbb{C}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L_n^+}^\times \xrightarrow{\mathbb{C}_p\cdot\log_p^n} \mathbb{C}_p \otimes_{\mathbb{Q}} L_{n,0}^+,$$

and that, by the very definition of the $\mathcal{L}$-invariant $\mathcal{L}_{\infty,p}^n$, one has

$$\mathcal{L}_{\infty,p}^n = \det_{\mathbb{C}_p[G_n]}(\log_{\infty,p}^n). \tag{15}$$

We also note that $E_n^{\bullet,+}$ is acyclic outside degrees two and three and that there is a canonical composite isomorphism of $\mathbb{Q}_p[G_n]$-modules

$$\Xi_n : \mathbb{Q}_p \cdot H^2(E_n^{\bullet,+}) = \mathbb{Q}_p \cdot \Gamma_{L_n^+} \xrightarrow{\log_p\circ\chi_{\mathbb{Q}}} \mathbb{Q}_p = \mathbb{Q}_p \cdot H^3(E_n^{\bullet,+}).$$

Then, in terms of this notation, the validity of the equivariant Tamagawa number conjecture for $(h^0(\mathrm{Spec}(L_n^+))(1), \mathbb{Z}[G_n]^+)$ implies that

$$(\theta_n^*(1)\mathcal{L}_{\infty,p}^n \cdot R_n^+, 0) = \vartheta_{\Xi_n}(\mathrm{Det}_{R_n^+}(E_n^{\bullet,+}))^{-1}. \tag{16}$$

(This equality follows directly from the explicit computation of Breuning and the first author in [2, §5.3] after taking into account (15) and the fact that the isomorphism $\mathbb{Q}_p\cdot\mathbb{Z}_p^\times \cong \mathbb{Q}_p\cdot\Gamma_\mathbb{Q}$ induced by the reciprocity map is the inverse of the isomorphism $\mathbb{Q}_p\cdot\Gamma_\mathbb{Q}\cong\mathbb{Q}_p\cdot\mathbb{Z}_p^\times$ induced by $\chi_\mathbb{Q}$.)

In addition the exact triangle in Proposition 6.2 implies that

$$\vartheta_{\Xi_n}(\mathrm{Det}_{R_n^+}(E_n^{\bullet,+})) = \vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n^+}(C_{n,\gamma}^\bullet))\otimes \mathrm{Det}_{R_n^+}(A_{n,\mathrm{tor}}^+[-2]) \tag{17}$$

where we write Ξ_n^γ for the composite isomorphism

$$\mathbb{Q}_p\cdot H^2(C_{n,\gamma}^\bullet)\xrightarrow{\mathbb{Q}_p\otimes_{\mathbb{Z}_p}H^2(\theta_\gamma)}\mathbb{Q}_p\cdot H^2(E_n^{\bullet,+})\xrightarrow{\Xi_n}\mathbb{Q}_p\cdot H^3(E_n^{\bullet,+})=\mathbb{Q}_p\cdot H^3(C_{n,\gamma}^\bullet).$$

It now suffices to prove that

$$\vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n}(C_{n,\gamma}^\bullet)) = ((\epsilon_{\gamma_\mathbb{Q}}^n)^{-1}R_n^+,0), \tag{18}$$

since, if this is true, then it combines with (16) and (17) to directly imply the required equality

$$(\theta_n^*(1)\epsilon_{\gamma_\mathbb{Q}}^n\mathcal{L}_{\infty,p}^n\cdot R_n^+,0) = \mathrm{Det}_{R_n^+}(A_{n,\mathrm{tor}}^+[-2])^{-1} = (\mathrm{Fit}_{R_n^+}(A_{n,\mathrm{tor}}^+),0)$$

(where the last equality follows in just the same way as the last equality of (14)).

It is enough to prove the ω^a-component of (18) for every even integer a with $0\le a\le p-2$. Further, if $a\neq 0$, then $C_{n,\gamma}^{\bullet,(a)}$ is the zero complex and $e_{\omega^a}\epsilon_\gamma^n = \epsilon_\gamma^{\omega^a}e_{\omega^a}=e_{\omega^a}$ and so the ω^a-component of the equality is clear.

To compute $\vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n}(C_{n,\gamma}^\bullet))^{(0)}$ we note that $\mathrm{Det}_{R_n^{(0)}}(C_{n,\gamma}^{\bullet,(0)})$ is generated over $R_n^{(0)}$ by $x:=(e_n,1)\otimes(e_n^*,-1)$ where e_n^* is the dual of e_n in $\mathrm{Hom}_{R_n^{(0)}}(R_n^{(0)},R_n^{(0)})$.

Now, since $e_n=e_{G_n}+(e_n-e_{G_n})$, $\mathbb{Q}_p\cdot H^2(C_{n,\gamma}^\bullet)=\mathbb{Q}_p\cdot e_{G_n}$, $d_\gamma(e_n-e_{G_n}) = (1-\gamma_n)e_n$ and $\Xi_n^\gamma(e_{G_n})=\log_p(\chi_\mathbb{Q}(\gamma))=\log_p(\chi_\mathbb{Q}(\gamma_\mathbb{Q}))$ one has

$$\begin{aligned}\vartheta_{\Xi_n^\gamma}(x) &= ((1-\gamma_n)e_n,0)+(\vartheta'_{\mathrm{ev}}\circ(\mathrm{Det}_{\mathbb{Q}_p\cdot R_n^+}(\Xi_n^\gamma)\otimes\mathrm{id}))((e_{G_n},1)\otimes(e_{G_n}^*,-1)))\\ &= ((1-\gamma_n)e_n,0)+\vartheta'_{\mathrm{ev}}((\log_p(\chi_\mathbb{Q}(\gamma_\mathbb{Q}))e_{G_n},1)\otimes(e_{G_n}^*,-1))\\ &= ((1-\gamma_n)e_n+\log_p(\chi_\mathbb{Q}(\gamma_\mathbb{Q}))e_{G_n},0)\\ &= (e_n(\epsilon_{\gamma_\mathbb{Q}}^n)^{-1},0)\end{aligned}$$

where ϑ'_{ev} is induced by the evaluation pairing on $\mathbb{Q}_p\cdot e_{G_n}$, $e_{G_n}^*$ denotes the dual of e_{G_n} in $\mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p\cdot e_{G_n},\mathbb{Q}_p)$ and the last equality follows by explicit comparison with the definition of $\epsilon_{\gamma_\mathbb{Q}}^n$.

This completes the proof of Theorem 6.4. □

6.2.3. *Completion of the proof.* From Lemma 6.5 below one knows that the group $B_{n,\mathrm{tor}}^- = A_{n,\mathrm{tor}}^-$ vanishes and that the R_n-module $A_{n,\mathrm{tor}}=B_{n,\mathrm{tor}}^+$ is cyclic.

By a general property of Fitting ideals the latter fact implies $\mathrm{Fit}_{R_n}(A_{n,\mathrm{tor}})$ is equal to $\mathrm{Ann}_{R_n}(A_{n,\mathrm{tor}})$ and hence also then combines with the formula of Theorem 6.4 to imply that the R_n-module $A_{n,\mathrm{tor}}=A_{n,\mathrm{tor}}^+$ is isomorphic to

$$(R_n/(\theta_n^*(1)(\mathcal{L}\mathcal{R}_\pi+\epsilon_{\gamma_\mathbb{Q}}^n\mathcal{L}_{\infty,p}^n)))^+ = R_n^+/(\theta_n^*(1)\cdot\epsilon_{\gamma_\mathbb{Q}}^n\mathcal{L}_{\infty,p}^n).$$

This completes the proof of Theorem 2.19(ii).

Lemma 6.5. *Assume p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$ and fix an integer i with $0\le i\le p-2$. Then the group $B_{n,\mathrm{tor}}^{(i)}=A_{n,\mathrm{tor}}^{(i)}$ vanishes if either i is* *odd or if i is even and the generalised Bernoulli number $B_{1,\omega^{i-1}}$ is not divisible by p. In all other cases this group is a non-trivial cyclic $R_n^{(i)}$-module.*

Proof. Lemma 3.4(ii) implies the restriction map $B_n \to B_1$ induces an isomorphism of $R_1^{(i)}$-modules $H_0(P_n, B_n^{(i)}) \cong B_1^{(i)}$. Since the $R_n^{(i)}$-module $\overline{B_n^{(i)}}$ is projective (as a consequence of Theorem 2.19(i)) this isomorphism restricts to give an isomorphism $H_0(P_n, A_{n,\mathrm{tor}}^{(i)}) = H_0(P_n, B_{n,\mathrm{tor}}^{(i)}) \cong B_{1,\mathrm{tor}}^{(i)} = A_{1,\mathrm{tor}}^{(i)}$.

This isomorphism in turn induces a surjective homomorphism of $R_n^{(i)}$-modules

$$\mu_n^i : A_{n,\mathrm{tor}}^{(i)} \to H_0(P_n, A_{n,\mathrm{tor}}^{(i)}) \cong A_{1,\mathrm{tor}}^{(i)} \to A_{1,\mathrm{tor}}^{(i)}/p. \tag{19}$$

We write I_{P_n} for the augmentation ideal of $\mathbb{Z}_p[P_n]$ and define an ideal of R_n by setting $I_n := p \cdot R_n + I_{P_n} \cdot R_n$. Then $I_n^{(i)}$ is equal to the Jacobson radical of $R_n^{(i)}$ and is contained in $\ker(\mu_n^i)$ and the quotient $R_n^{(i)}/I_n^{(i)}$ is isomorphic to $\mathbb{F}_p$. This shows that the map μ_n^i induces an isomorphism of $\mathbb{F}_p$-modules $A_{n,\mathrm{tor}}^{(i)}/(I_n^{(i)} \cdot A_{n,\mathrm{tor}}^{(i)}) \cong A_{1,\mathrm{tor}}^{(i)}/p$ and hence that Nakayama's Lemma implies that the minimal number of generators of the $R_n^{(i)}$-module $A_{n,\mathrm{tor}}^{(i)}$ is equal to $\dim_{\mathbb{F}_p}(A_{1,\mathrm{tor}}^{(i)}/p)$.

We now compute

$$\begin{aligned}
&\dim_{\mathbb{F}_p}(A_{1,\mathrm{tor}}^{(i)}/p)\\
=&\dim_{\mathbb{F}_p}(A_1^{(i)}/p) - \dim_{\mathbb{F}_p}(\overline{A_1^{(i)}}/p)\\
=&\dim_{\mathbb{F}_p}((H_{L_1}(L_1^\times)/(L_1^\times)^p)^{(1-i)}) - \dim_{\mathbb{F}_p}(\overline{B_1^{(i)}}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}_p^{(i)}/p)\\
=&\dim_{\mathbb{F}_p}((P_{L_1}/P_{L_1}^p)^{(1-i)}) + \dim_{\mathbb{F}_p}(\mathrm{Cl}_{L_1}^{(1-i)}/p) - \dim_{\mathbb{F}_p}(\overline{B_1^{(i)}}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}_p^{(i)}/p)\\
=&\dim_{\mathbb{F}_p}(\langle\zeta_p\rangle^{(1-i)}) + \dim_{\mathbb{F}_p}((\mathcal{O}_{L_1^+}^\times/(\mathcal{O}_{L_1^+}^\times)^p)^{(1-i)}) + \dim_{\mathbb{F}_p}((\mathbb{Z}_p/p)^{(1-i)})\\
&\qquad\qquad + \dim_{\mathbb{F}_p}(\mathrm{Cl}_{L_1}^{(1-i)}/p) - \dim_{\mathbb{F}_p}(\overline{B_1^{(i)}}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}_p^{(i)}/p).
\end{aligned}$$

Here the first equality is obvious and the second is true because the definition of H_{K_1} (just prior to (10)) implies Kummer theory gives an isomorphism of $\mathbb{Z}_p[G_1]$-modules $A_1/p \cong \mathrm{Hom}(H_{K_1}(K_1^\times)/(K_1^\times)^p, \langle\zeta_p\rangle)$ and because the tautological exact sequence of $\mathbb{Z}_p[G_1]$-modules $0 \to B_1 \to A_1 \to \Gamma_{L_1} \to 0$ splits. The third equality follows by taking ω^{1-i}-isotypic components of the exact sequence (10) and the last equality is derived easily from the following facts: since the unique prime ideal of L_1 above p is principal there is an exact sequence of G_1-modules $0 \to \mathcal{O}_{L_1}^\times \to P_{L_1} \to \mathbb{Z} \to 0$ and, since $\mathcal{O}_{L_1}^\times = \mathcal{O}_{L_1^+}^\times \cdot \langle\zeta_p\rangle$ (by [27, Prop. 1.5]) there is a direct sum decomposition of $\mathbb{F}_p[G_1]$-modules $\mathcal{O}_{L_1}^\times/(\mathcal{O}_{L_1}^\times)^p = \mathcal{O}_{L_1^+}^\times/(\mathcal{O}_{L_1^+}^\times)^p \oplus \langle\zeta_p\rangle$.

Next we note that $\dim_{\mathbb{F}_p}(\langle\zeta_p\rangle^{(1-i)})$ and $\dim_{\mathbb{F}_p}(\mathbb{Z}_p^{(i)}/p)$ are both equal to 1 if $i = 0$ and to 0 otherwise, that [27, Prop. 8.13] implies $\dim_{\mathbb{F}_p}((\mathcal{O}_{L_1^+}^\times/(\mathcal{O}_{L_1^+}^\times)^p)^{(1-i)})$ is equal to 1 if i is both odd and bigger than 1 and to zero otherwise, that $\dim_{\mathbb{F}_p}((\mathbb{Z}_p/p)^{(1-i)})$ is equal to 1 if $i = 1$ and to 0 otherwise, that [27, Cor. 10.15] implies $\dim_{\mathbb{F}_p}(\mathrm{Cl}_{L_1}^{(1-i)}/p)$ is equal to 1 if i is even and such that $B_{1,\omega^{i-1}}$ is divisible by p and to 0 otherwise, and that Theorem 2.19(i) implies $\dim_{\mathbb{F}_p}(\overline{B_1^{(i)}}/p)$ is equal to 1 if i is odd and to 0 otherwise.

Upon substituting these facts into the above displayed formula for $\dim_{\mathbb{F}_p}(A^{(i)}_{1,\mathrm{tor}}/p)$ one finds that the minimal number of generators of the $R^{(i)}_n$-module $A^{(i)}_{n,\mathrm{tor}}$ is equal to

$$\dim_{\mathbb{F}_p}(A^{(i)}_{1,\mathrm{tor}}/p) = \begin{cases} 1, & \text{if } i \text{ is even and } p \text{ divides } B_{1,\omega^{i-1}}, \\ 0, & \text{otherwise,} \end{cases}$$

as required. □

6.3. **The proof of Theorem 2.19(iii).** In this section we fix an even integer i with $0 \le i \le p-3$.

We note that the first assertion of Theorem 2.19(iii)(b) follows immediately from Lemma 6.5.

To prove the first assertion of Theorem 2.19(iii)(a) we assume p divides $B_{1,\omega^{i-1}}$ and note that in this case Lemma 6.5 implies $A^{(i)}_{1,\mathrm{tor}}$ is non-trivial. We then set $M := A^{(i)}_{n,\mathrm{tor}}$ and also for each integer a with $0 \le a < n$ we set $P_{n-a} := G_{L_n/L_{a+1}}$ and consider the natural surjective homomorphisms

$$M = H_0(P_1, M) \twoheadrightarrow H_0(P_2, M) \twoheadrightarrow \cdots \twoheadrightarrow H_0(P_n, M) \cong A^{(i)}_{1,\mathrm{tor}},$$

where the isomorphism is from (19).

Now for each such a the kernel of the projection $H_0(P_a, R^{(i)}_n) \to H_0(P_{a+1}, R^{(i)}_n)$ is contained in the Jacobson radical of the ring $H_0(P_a, R^{(i)}_n)$. Thus, since $A^{(i)}_{1,\mathrm{tor}}$ does not vanish, Nakayama's Lemma implies that the kernel of each projection map $H_0(P_a, M) \to H_0(P_{a+1}, M)$ does not vanish and hence that the order of M is at least p^n, as required to prove the first assertion of claim (a).

To prove the remaining assertions of Theorem 2.19(iii) we note that Lemma 6.5 combines with the displayed isomorphism in Theorem 2.19(ii) to imply that the element $e_{(i)}\theta^*_n(1) \cdot \epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}$ belongs to $R^{(i)\times}_n$ if p does not divide $B_{1,\omega^{i-1}}$ and to $R^{(i)}_n \setminus R^{(i)\times}_n$ if p divides $B_{1,\omega^{i-1}}$.

We also note that $R^{(i)}_n$ is isomorphic to the ring $\mathbb{Z}_p[P_n]$ and that for each ψ in P^*_n one has $(e_{(i)}\theta^*_n(1) \cdot \epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p})^\psi = \epsilon^{\psi\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\psi\omega^i}_{\infty,p} \cdot L^*(\psi\omega^i, 1)$.

Given these facts, all remaining assertions of Theorem 2.19(iii) are obtained directly by applying the following result with $\Gamma = P_n$ and $x = e_{(i)}\theta^*_n(1) \cdot \epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}$.

Lemma 6.6. *Let Γ be a finite abelian p-group and fix x in $\mathbb{C}_p[\Gamma]$.*

(i) *Then x belongs to $\mathbb{Z}_p[\Gamma]$ if and only if for every γ in Γ the congruence*

$$\sum_{\psi\in\Gamma^*} \psi(\gamma)x^\psi \equiv 0 \pmod{|\Gamma| \cdot \mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

(ii) *If x belongs to $\mathbb{Z}_p[\Gamma]$, then x belongs to $\mathbb{Z}_p[\Gamma] \setminus \mathbb{Z}_p[\Gamma]^\times$, resp. to $\mathbb{Z}_p[\Gamma]^\times$, if and only if $x^{\mathbf{1}_\Gamma}$ belongs to $p \cdot \mathbb{Z}_p$, resp. to $\mathbb{Z}_p^\times$.*

Proof. To prove claim (i) note that

$$x = \sum_{\psi\in\Gamma^*} x^\psi e_\psi = \sum_{\psi\in\Gamma^*} x^\psi|\Gamma|^{-1}\sum_{\gamma\in\Gamma}\psi(\gamma)\gamma^{-1} = \sum_{\gamma\in\Gamma}|\Gamma|^{-1}(\sum_{\psi\in\Gamma^*}\psi(\gamma)x^\psi)\gamma^{-1}$$

and hence that x belongs to $\mathbb{Z}_p[\Gamma]$ if and only if for every element γ of Γ the sum $\sum_{\psi\in\Gamma^*}\psi(\gamma)x^\psi$ belongs to $|\Gamma| \cdot \mathbb{Z}_p$.

We note next that $\mathbb{Z}_p[\Gamma]$ is a local ring with maximal ideal equal to the set of elements $x = \sum_{\gamma\in\Gamma} x_\gamma \gamma$, with each x_γ in $\mathbb{Z}_p$, such that $\sum_{\gamma\in\Gamma} x_\gamma$ belongs to $p\cdot\mathbb{Z}_p$. This implies claim (ii) because

$$\sum_{\gamma\in\Gamma} x_\gamma = \sum_{\gamma\in\Gamma}\sum_{\psi\in\Gamma^*} |\Gamma|^{-1}\psi(\gamma)x^\psi = \sum_{\psi\in\Gamma^*} |\Gamma|^{-1}(\sum_{\gamma\in\Gamma}\psi(\gamma))x^\psi = x^{\mathbf{1}_\Gamma}.$$

□

6.4. **The proof of Theorem 2.19(iv).** Fix an odd integer i with $1 \le i \le p-3$.

In this case Lemma 6.5 implies that $A^{(i)}_{n,\mathrm{tor}}$ vanishes. It follows that the ideal $\mathrm{Fit}_{R_n}(A_{n,\mathrm{tor}})^{(i)} = \mathrm{Fit}_{R_n^{(i)}}(A^{(i)}_{n,\mathrm{tor}})$ is equal to $R_n^{(i)}$ and hence, via the equality of Theorem 6.4, that the element $e_{(i)}\theta_n^*(1)(\mathcal{LR}_\pi + \epsilon^n_{\gamma_\mathbb{Q}}\mathcal{L}^n_{\infty,p}) = e_{(i)}\theta_n^*(1)\cdot\mathcal{LR}_\pi$ is a unit of the ring $R_n^{(i)}$.

This fact implies Theorem 2.19(iv) via a simple application of Lemma 6.6 (in just the same way that it was used to prove Theorem 2.19(iii)(b)).

This completes the proof of Theorem 2.19.

References

[1] F. Bertrandias, J.-J. Payan, Γ-extensions et invariants cyclotomiques, Ann. Sci. Éc. Norm. Sup. **5** (1972) 517-543.

[2] M. Breuning, D. Burns, On Equivariant Dedekind Zeta-Functions at $s = 1$, Documenta Math., Extra Volume: Andrei A. Suslin's Sixtieth Birthday, 119-146 (2010).

[3] K. S. Brown, Cohomology of groups, Graduate Texts in Math. **87**, Springer, New York, 1992.

[4] A. Brumer, On the units of algebraic number fields, Mathematica **14** (1967) 121-124.

[5] D. Burns, On the Galois structure of arithmetic cohomology I: compactly supported p-adic cohomology, submitted for publication.
Available at http://www.mth.kcl.ac.uk/staff/dj_burns/newdbpublist.html.

[6] D. Burns, D. Macias Castillo, On p-adic L-series, p-adic cohomology and class field theory, to appear in J. reine u. angew. Math.

[7] H. Castillo, A. Jones, On the values of Dedekind Zeta functions at $s = 1$ and annihilation of class groups, Acta Arith. **160** (2013) 67-93.

[8] F. E. Diederichsen, Über die Ausreduktion ganzahliger Gruppendarstellungen bei arithmetischer Aquivalenz, Abh. Math. Sem. Univ. Hamburg **14** (1940) 357-412.

[9] G. G. Elder, On Galois structure of the integers in cyclic extensions of local number fields, J. Th. Nombres Bordeaux **14** (2002) 113-149.

[10] G. Gras, Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres, J. reine. u. angew. Math. **333** (1982) 86-132.

[11] A. Heller, I. Reiner, Representations of cyclic groups in rings of integers. I. Ann. Math. **76** (1962) 73-92.

[12] A. Heller, I. Reiner, Representations of cyclic groups in rings of integers. II. Ann. Math. **77** (1963) 318-328.

[13] D. Hemard, Modules galoisiennes de torsion et plongements dans les $\mathbb{Z}_p$-extensions, J. Number Theory **30** (1988) 357-374.

[14] J-F. Jaulent, T. Nguyen Quang Do, Corps p-rationnels, corps p-réguliers et ramification restreinte, J. Th. Nombres Bordeaux **5** (1993) 343-363.

[15] C. Khare, J-P. Wintenberger, Ramification in Iwasawa Theory and Splitting Conjectures, Int. Math. Res. Notices **2014**, 1 (2014) 194-223.

[16] Y. Kida, ℓ-Extensions of CM-Fields and Cyclotomic Invariants, J. Number Theory **12** (1980) 519-528.

[17] F. Knudsen, D. Mumford, The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div', Math. Scand. **39** (1976) 19-55.

[18] H. Miki, On the Leopoldt Conjecture on the p-adic regulators, J. Number Theory **26** (1987) 117-128.

[19] H. Miki, H. Sato, Leopoldt's conjecture and Reiner's theorem, J. Math. Soc. Japan **36** (1984) 47-52.

[20] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Sém. Th. Nombres Paris 1987/1988, Prog. in Math. **89** (1990) 155-200.

[21] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of number fields, (Springer-Verlag, Berlin, 2000).

[22] B. Oriat, Annulation de groupes de classes reelles, Nagoya Math. J. **81** (1981) 45-56.

[23] S. Seo, On first layers of $\mathbb{Z}_p$-extensions, J. Number Theory, **133** (2013) 4010-4023.

[24] J-P. Serre, Sur le résidue de la fonction zêta p-adique d'un corps de nombres, C.R. Acad. Sci. Paris **278** (1978) 183-188.

[25] I. R. Shafarevic, Extensions with prescribed ramification points, Publ. Math. I.H.E.S. **36** (1986) 71-95.

[26] J. Tate, Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$ (notes par D. Bernardi et N. Schappacher), Progress in Math., **47**, Birkhäuser, Boston, 1984.

[27] L.C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Math. **83**, Springer-Verlag, Berlin, 1982.

[28] A. V. Yakovlev, Homological definability of p-adic representations of a ring with power basis, Izvestia A N SSSR, ser. Math. **34** (1970), 321-342 (In Russian).

[29] A. V. Yakovlev, Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup, An. St. Univ. Ovidius Constanţa **4** (1996) 206-221.

King's College London, Department of Mathematics, London WC2R 2LS, U.K.
E-mail address: `david.burns@kcl.ac.uk`

King's College London, Department of Mathematics, London WC2R 2LS, U.K.
E-mail address: `asuka.kumon@kcl.ac.uk`