ON THE GALOIS STRUCTURE OF ARITHMETIC COHOMOLOGY I: COMPACTLY SUPPORTED p-ADIC COHOMOLOGY

DAVID BURNS

Abstract. We investigate the Galois structures of p-adic cohomology groups of general p-adic representations over finite extensions of number fields. We show, in particular, that as the field extensions vary over natural families the Galois modules formed by these cohomology groups always decompose as the direct sum of a projective module and a complementary module of bounded p-rank. We use this result to derive new (upper and lower) bounds on the changes in ranks of Selmer groups over extensions of number fields and descriptions of the explicit Galois structures of natural arithmetic modules.

Introduction

Let F/k be a finite Galois extension of number fields with group G. Let M be a motive defined over k and write $L_G(M, s)$ for the complex L-function of the base change M_F of M through F/k, regarded as defined over k and with coefficients the rational group ring $\mathbb{Q}[G]$.

The equivariant Tamagawa number conjecture predicts a precise connection between the leading term at $s = 0$ of $L_G(M, s)$ and an Euler characteristic that belongs to the relative algebraic K_0-group of the ring extension $\mathbb{Z}[G] \to \mathbb{R}[G]$ and encodes the various motivic cohomology groups, realisations, comparison isomorphisms and regulators that are associated to both M_F and its Kummer dual.

However, extracting fine and explicit predictions out of this technical formalism in any general setting requires detailed knowledge, for each prime p and a suitable full Galois-stable sublattice T_p of the p-adic realisation of M, of the structure as $\mathbb{Z}_p[G]$-modules of (depending on the approach used) either the Bloch-Kato Selmer group $\mathrm{Sel}_F(T_p)$ of T_p over F or of the compactly supported p-adic étale cohomology groups $H^i_c(\mathcal{O}_{F,\Sigma}, T_p)$ for any finite set of places Σ of k that contains all archimedean places, all places which divide p and all places at which M_F has bad reduction.

In special cases there are also other strong reasons to investigate the explicit Galois structure of such cohomology groups.

For example, if $T_p = \mathbb{Z}_p(1)$, then $H^2_c(\mathcal{O}_{F,\Sigma}, T_p)$ identifies with the Galois group of the maximal abelian pro-p extension of F that is unramified outside Σ and aspects of the detailed Galois structures of such groups are linked to the validity, or otherwise, of Leopoldt's Conjecture. In this context such Galois structures have been much studied in the literature,

Mathematics Subject Classification: 11R34, 11R23, 20C11.

both in relatively simple cases and in more involved Iwasawa-theoretic contexts (see, for example, the recent work of Khare and Wintenberger [12]).

In another concrete direction, if T_p is the p-adic Tate module of an abelian variety A over k, then an investigation of the structure of $\mathrm{Sel}_F(T_p)$ as a $\mathbb{Z}_p[G]$-module can in certain circumstances be used to extract useful information concerning the changes in rank of $A(F')$ as F' varies over intermediate fields of F/k and to shed light on various 'equivariant' refinements of the Birch and Swinnerton-Dyer conjecture for A over F that are studied in the literature (see, for example, the results of Macias Castillo, Wuthrich and the present author in this direction in [6] and in the references contained therein).

Unfortunately, however, despite the interest in such investigations, understanding the explicit Galois structure of arithmetic cohomology groups in any general setting is a very difficult problem, not least because the relevant theory of integral representations is notoriously complicated (see, for example, Heller and Reiner [10]).

Notwithstanding the above difficulties, in this short series of articles our aim is to show that if p is odd, then it is possible to prove some interesting, and arithmetically useful, results concerning the structures of the $\mathbb{Z}_p[G]$-modules $\mathrm{Sel}_F(T_p)$, $H^i(\mathcal{O}_{F,\Sigma}, T_p)$ and $H^i_c(\mathcal{O}_{F,\Sigma}, T_p)$ as F varies in natural families of Galois extensions.

In this first note we shall establish a general 'bound' on the complexity of $\mathbb{Z}_p[G]$-modules of the form $H^i(\mathcal{O}_{F,\Sigma}, T_p)$ and $H^i_c(\mathcal{O}_{F,\Sigma}, T_p)$ by showing that in all cases they contain a projective direct summand with a complement the p-rank of which can be explicitly bounded (for a precise statement see Theorem 1.1).

This observation has several interesting, and (to us) quite surprising, consequences. For example, it leads to general 'finiteness results' concerning indecomposable $\mathbb{Z}_p[G]$-lattices occurring as direct summands of the lattices obtained by considering $H^i(\mathcal{O}_{F,\Sigma}, T_p)$ and $H^i_c(\mathcal{O}_{F,\Sigma}, T_p)$ modulo their torsion subgroups and hence, upon specialisation, to concrete structure results concerning natural arithmetic modules including unit groups, higher algebraic K-groups and ray class groups (see, for example, Corollaries 3.1 and 4.1, Theorem 4.3 and the computations in §4.3).

In another direction, we show the result gives concrete, and very general, information about the change in rank of the Selmer groups of T_p over F and k (see Corollary 1.2).

In subsequent articles we develop in greater detail two aspects of this general approach. Firstly, in joint work with Kumon [5], we explain how structure results for ray class groups of the sort discussed here can be used to extract concrete results and predictions from the formalism of the equivariant Tamagawa number conjecture for $h^0(\mathrm{Spec}(F))(1)$ and, in addition, to shed new light on the validity of Leopoldt's Conjecture. Secondly, by using Selmer complexes defined by Nekovář in the role played here by compactly supported p-adic cohomology complexes, in [2] we prove analogous results about the explicit Galois structure of the Bloch-Kato Selmer groups of critical motives and so extend the results obtained by Macias Castillo, Wuthrich and the present author in [6].

We thank Daniel Macias Castillo and Christian Wuthrich for helpful discussions.

1. Statement of the main results

1.1. At the outset we fix a number field k, an algebraic closure k^c of k, an odd prime p and a finite set of places Σ of k containing the sets Σ_∞ of all archimedean places and Σ_p of all

p-adic places and we set $\Sigma_f := \Sigma \setminus \Sigma_\infty$. We also write $M_{k,\Sigma}$ for the maximal extension of k in k^c that is unramified outside Σ and set $G_{k,\Sigma} := \mathrm{Gal}(M_{k,\Sigma}/k)$.

We assume to be given a finitely generated free $\mathbb{Z}_p$-module T and a continuous homomorphism of the form

$$\rho : G_{k,\Sigma} \to \mathrm{Aut}_{\mathbb{Z}_p}(T). \tag{1}$$

We write $T^*(1)$ for the linear dual $\mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$, endowed with the diagonal action of $G_{k,\Sigma}$ that is induced by ρ.

If L is a finite extension of k, then for any set of places Σ' of k we write Σ'_L for the set of places of L above Σ' and, if Σ' contains Σ_∞, we write $\mathcal{O}_{L,\Sigma'}$ for the subring of L comprising elements that are integral at all places of L outside Σ'_L and $\mathrm{Cl}_{\Sigma'}(L)$ for the ideal class group of $\mathcal{O}_{L,\Sigma'}$.

We identify T and $T^*(1)$ with étale pro-sheaves on $\mathrm{Spec}(\mathcal{O}_{L,\Sigma})$ in the usual way and for any such sheaf B we abbreviate the groups $H^i(\mathrm{Spec}(\mathcal{O}_{L,\Sigma})_{\text{ét}}, B)$ and $H^i_c(\mathrm{Spec}(\mathcal{O}_{L,\Sigma})_{\text{ét}}, B)$ to $H^i(\mathcal{O}_{L,\Sigma}, B)$ and $H^i_c(\mathcal{O}_{L,\Sigma}, B)$ respectively.

For a Galois extension F/E we usually abbreviate the group $\mathrm{Gal}(F/E)$ to $G_{F/E}$.

1.2. In the sequel we write μ_p for the group of p-th roots of unity in k^c and k_T for the finite Galois extension of $k(\mu_p)$ corresponding to the kernel of the action of $G_{k(\mu_p),\Sigma}$ on T/p induced by ρ (and hence also of the induced action of $G_{k(\mu_p),\Sigma}$ on $T^*(1)/p \cong (T/p)^\vee(1)$). For any extension F of k in k^c we then write F_T for the compositum $k_T F$ of k_T and F.

We write $\mathbb{F}_p$ for the finite field of cardinality p and for any finitely generated $\mathbb{Z}_p$-module M we write $\mathrm{rk}_p(M)$ for its 'p-rank' $\dim_{\mathbb{F}_p}(M/p)$.

We can now state our main result.

Theorem 1.1. *Let F/E be a Galois extension of fields with $k \subseteq E \subseteq F \subset k^c$, F/k finite and F/E unramified outside Σ_E. Then in each degree i there are decompositions of $\mathbb{Z}_p[G_{F/E}]$-modules*

$$H^i(\mathcal{O}_{F,\Sigma}, T) = P^i_{F/E,T} \oplus R^i_{F/E,T} \quad \text{and} \quad H^i_c(\mathcal{O}_{F,\Sigma}, T) = P^i_{F/E,T,c} \oplus R^i_{F/E,T,c}$$

where the modules $P^i_{F/E,T}$ and $P^i_{F/E,T,c}$ are projective and one has

$$\mathrm{rk}_p(R^i_{F/E,T}) \leq m^i_{F/E,T} \cdot \mathrm{rk}(T) \text{ and } \mathrm{rk}_p(R^i_{F/E,T,c}) \leq m^i_{F/E,T,c} \cdot \mathrm{rk}(T)$$

for integers $m^i_{F/E,T}$ and $m^i_{F/E,T,c}$ that depend only on i, $[F:E]$, $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T))$ and $\#\Sigma_{f,F}$.

Explicit expressions for the integers $m^i_{F/E,T}$ and $m^i_{F/E,T,c}$ will be given in the course of the proof of Theorem 1.1 in §2.3.

This result has some interest since the $\mathbb{Z}_p$-ranks of $H^i(\mathcal{O}_{F,\Sigma}, T)$ and $H^i_c(\mathcal{O}_{F,\Sigma}, T)$ are in general unbounded as F varies, whilst it is often possible to give universal bounds for both $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T))$ and $\#\Sigma_{f,F}$ as F ranges over natural families of extensions of k of unbounded degree (see, for example, Example 3.2 and the proof of Proposition 4.2).

In addition, in §3 we show that for representations ρ of the form (1) that have pro-p image one can often weaken the explicit dependence of the bounds given in Theorem 1.1 on either ρ or the behaviour of class groups (for details see Corollary 3.1).

In §3 we also deduce the following result showing that Theorem 1.1 gives concrete information about changes in the $\mathbb{Z}_p$-rank $\mathrm{rk}(\mathrm{Sel}_F(T))$ of the Bloch-Kato Selmer groups of T

over finite extensions F of k. (Note that if T is the p-adic Tate module of an abelian variety over k for which the classical Tate-Shafarevic group over F is finite, then $\mathrm{rk}(\mathrm{Sel}_F(T))$ agrees with that of the Mordell-Weil group of A over F).

Corollary 1.2. *For each natural number r there exists a finite Galois extension $k_{\Sigma,r}$ of k in $M_{k,\Sigma}$ with the following property: as T ranges over p-adic representations of $G_{k,\Sigma}$ that have pro-p image and rank at most r and F/E over finite p-power degree Galois extensions of fields with $k \subseteq E \subseteq F \subset k^c$, E/k finite and F/E unramified outside Σ_E, one has*

$$[F:E]\cdot \mathrm{rk}(\mathrm{Sel}_E(T)) - n_1 \leq \mathrm{rk}(\mathrm{Sel}_F(T)) \leq [F:E]\cdot \mathrm{rk}(\mathrm{Sel}_E(T)) + n_2$$

where n_1 and n_2 are integers that depend only on $[F:\mathbb{Q}]$, $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(k_{\Sigma,r}F))$ and $\#\Sigma_f$ and are made explicit in §3.2 below.

Remark 1.3. The degree of $k_{\Sigma,r}$ over k can be large (see the proof of Corollary 3.1 below). As a special case, Corollary 1.2 implies the existence of constants m_1 and m_2 depending only on k, Σ and r such that for any p-adic representation T of $G_{k,\Sigma}$ with pro-p image and rank at most r and any Galois extension F of k of p-power degree in $k_{\Sigma,r}$ one has

$$[F:k]\cdot \mathrm{rk}(\mathrm{Sel}_k(T)) - m_1 \leq \mathrm{rk}(\mathrm{Sel}_F(T)) \leq [F:k]\cdot \mathrm{rk}(\mathrm{Sel}_k(T)) + m_2.$$

This strongly restricts the structure of $\mathrm{Sel}_F(T)$. For instance, if F/k has degree p, then a classical result of Diederichsen [7] gives an isomorphism of $\mathbb{Z}_p[G_{F/k}]$-modules

$$\mathrm{Sel}_F(T)_{\mathrm{tf}} \cong \mathbb{Z}_p[G_{F/k}]^{a_F(T)} \oplus (\mathbb{Z}_p[G_{F/k}]/(\sum_{g\in G_{F/k}} g))^{b_F(T)} \oplus \mathbb{Z}_p^{c_F(T)}$$

for suitable non-negative integers $a_F(T), b_F(T)$ and $c_F(T)$ and the above inequalities imply that $-m_1/(p-1) \leq b_F(T) - c_F(T) \leq m_2/(p-1)$.

Finally we note that Theorem 1.1 has concrete consequences concerning natural arithmetic modules (including unit groups, higher algebraic K-groups and ray class groups) and that in special cases our methods can be used to give much more explicit structural results concerning such modules. These aspects of the theory are considered in §4.

2. The proof of Theorem 1.1

In this section we first prove a purely algebraic result that may itself be of some independent interest. We then combine this result with some general properties of p-adic étale cohomology to prove Theorem 1.1.

For any $\mathbb{Z}_p$-module M we write M_{tor} for the torsion submodule of M, M_{tf} for the quotient of M by M_{tor}, M^* for the linear dual $\mathrm{Hom}_{\mathbb{Z}_p}(M,\mathbb{Z}_p)$ and $M^\vee$ for the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(M,\mathbb{Q}_p/\mathbb{Z}_p)$. If M is endowed with the action of a finite group G, then we always endow both M^* and $M^\vee$ with the natural contragredient action of G.

For any abelian group M we write $M[p]$ for the subgroup of M comprising elements annihilated by p. For any finitely generated $\mathbb{Z}_p$-module M we set $\mathrm{rk}(M) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M)$ and note that $\mathrm{rk}_p(M) = \dim_{\mathbb{F}_p}(M[p]) + \mathrm{rk}(M)$. In the sequel we also often use, without explicit comment, the fact that for any exact sequence of finitely generated $\mathbb{Z}_p$-modules $M_1 \xrightarrow{\theta_1} M_2 \xrightarrow{\theta_2} M_3$ one has $\mathrm{rk}_p(\mathrm{im}(\theta_i)) \leq \mathrm{rk}_p(M_2) \leq \mathrm{rk}_p(M_1) + \mathrm{rk}_p(M_3)$ for $i = 1$ and $i = 2$.

For a finite group G we write tr_G for the 'trace' element $\sum_{g\in G} g$ of $\mathbb{Z}[G]$.

2.1. The following result is key to our approach and may also itself be of some independent interest (see, for example, Remark 2.2).

Proposition 2.1. *Let G be a finite p-group, X a $\mathbb{Z}_p[G]$-lattice and $\{x_i\}_{1\leq i\leq t}$ a finite subset of X. Then the images in $H^0(G,X)/p$ of the elements $\{\mathrm{tr}_G(x_i)\}_{1\leq i\leq t}$ are linearly independent over $\mathbb{F}_p$ if and only if the $\mathbb{Z}_p[G]$-submodule of X generated by $\{x_i\}_{1\leq i\leq t}$ is both a direct summand of X and free of rank t.*

Proof. Write $\mathcal{X}$ for the $\mathbb{Z}_p[G]$-submodule of X generated by $\{x_i\}_{1\leq i\leq t}$.

If $\mathcal{X}$ is free of rank t, then $H^0(G,\mathcal{X}) = \mathrm{tr}_G(\mathcal{X})$ is a free $\mathbb{Z}_p$-module of rank t and is generated by the elements $\{\mathrm{tr}_G(x_i)\}_{1\leq i\leq t}$. The images in $H^0(G,\mathcal{X})/p$ of these elements are therefore linearly independent over $\mathbb{F}_p$. If, in addition, the $\mathbb{Z}_p[G]$-module $\mathcal{X}$ is a direct summand of X, then the $\mathbb{F}_p$-module $H^0(G,\mathcal{X})/p$ is a direct summand of $H^0(G,X)/p$ and so the images in $H^0(G,X)/p$ of the given elements are also linearly independent over $\mathbb{F}_p$, as claimed.

To prove the converse implication we use the homomorphism of $\mathbb{Z}_p[G]$-modules

$$\psi : \mathbb{Z}_p[G]^t \twoheadrightarrow \mathcal{X} \subseteq X$$

that sends each element b_i of the standard basis $\{b_i\}_{1\leq i\leq t}$ of $\mathbb{Z}_p[G]^t$ to x_i.

We write $\overline{\psi}$ for the homomorphism $\mathbb{F}_p[G]^t \to X/pX$ induced by ψ and note that if $\ker(\overline{\psi})$ is non-trivial, then $H^0(G,\ker(\overline{\psi}))$ is also non-trivial (as G is a p-group). However, the group $H^0(G,\mathbb{F}_p[G]^t)$ is generated by the images in $\mathbb{F}_p[G]^t$ of the elements $\mathrm{tr}_G(b_i)$ and so the non-triviality of $H^0(G,\ker(\overline{\psi}))$ would contradict the linear independence hypothesis on the elements $\mathrm{tr}_G(x_i)$. The map $\overline{\psi}$ is therefore injective and so one has $\ker(\psi) \subseteq p\cdot\mathbb{Z}_p[G]^t$.

On the other hand, $\mathcal{X}$ is a free $\mathbb{Z}_p$-module so the tautological exact sequence of $\mathbb{Z}_p$-modules $0 \to \ker(\psi) \to \mathbb{Z}_p[G]^t \to \mathcal{X} \to 0$ splits and one has $\ker(\psi) = \ker(\psi)\cap p\cdot\mathbb{Z}_p[G]^t = p\cdot\ker(\psi)$. This shows that $\ker(\psi)$ vanishes and hence that $\mathcal{X}$ is a free $\mathbb{Z}_p[G]$-module of rank t (as claimed).

In addition, the fact that $\mathcal{X}$ is a free G-module implies both that $H^0(G,\mathcal{X}) = \mathrm{tr}_G(\mathcal{X})$ and that the group $H^1(G,\mathcal{X})$ vanishes. Thus, writing ι for the inclusion $\mathcal{X}\subseteq X$, the long exact sequence of G-cohomology associated to the tautological sequence

$$0 \to \mathcal{X} \xrightarrow{\iota} X \to \mathrm{cok}(\iota) \to 0 \tag{2}$$

gives an exact sequence of $\mathbb{Z}_p$-modules

$$0 \to \mathrm{tr}_G(\mathcal{X}) \to H^0(G,X) \to H^0(G,\mathrm{cok}(\iota)) \to 0. \tag{3}$$

Now, the images in $H^0(G,X)/p$ of the generating elements $\{\mathrm{tr}_G(x_i)\}_{1\leq i\leq t}$ of $\mathrm{tr}_G(\mathcal{X})$ are, by assumption, linearly independent over $\mathbb{F}_p$ and so can be extended to an $\mathbb{F}_p$-basis of $H^0(G,X)/p$. Nakayama's Lemma therefore implies that the elements $\{\mathrm{tr}_G(x_i)\}_{1\leq i\leq t}$ belong to a basis of the $\mathbb{Z}_p$-module $H^0(G,X)$ and, given this, the exact sequence (3) implies that the $\mathbb{Z}_p$-module $H^0(G,\mathrm{cok}(\iota))$ is free. This in turn implies that the module $H^0(G,\mathrm{cok}(\iota))_{\mathrm{tor}} = H^0(G,\mathrm{cok}(\iota)_{\mathrm{tor}})$ vanishes, and hence, since G is a p-group, that the module $\mathrm{cok}(\iota)_{\mathrm{tor}}$ itself vanishes.

Then, as $\mathrm{cok}(\iota)$ is free over $\mathbb{Z}_p$, the exact sequence (2) induces, upon taking linear duals, an exact sequence of $\mathbb{Z}_p[G]$-modules $0 \to \mathrm{cok}(\iota)^* \to X^* \xrightarrow{\iota^*} \mathcal{X}^* \to 0$. Since the $\mathbb{Z}_p[G]$-module

$\mathbb{Z}_p[G]^*$ is free of rank one, the $\mathbb{Z}_p[G]$-module $\mathcal{X}^*$ is free of rank t and so this sequence splits. Thus, upon taking linear duals, one deduces that (2) also splits as a sequence of $\mathbb{Z}_p[G]$-modules, as required to complete the proof. □

Remark 2.2. The result of Proposition 2.1 leads immediately to the following observation regarding indecomposable lattices: if G is any finite p-group and I any indecomposable $\mathbb{Z}_p[G]$-lattice, then either $\mathrm{tr}_G(I) \subseteq p \cdot H^0(G, I)$ or I is isomorphic to $\mathbb{Z}_p[G]$.

2.2. In this section we fix an odd prime p and data $F/E, \Sigma$ and T as in Theorem 1.1 and set $G := G_{F/E}$. For any noetherian ring R we write $D(R)$ for the derived category of left R-modules and $D^{\mathrm{p}}(R)$ for the full triangulated subcategory of $D(R)$ comprising perfect complexes.

In the following result we record some relevant (and essentially well-known) properties of the compactly supported étale cohomology complexes $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ that arise in the context of Theorem 1.1. We recall that these complexes are defined so as to lie in natural exact triangles in $D(\mathbb{Z}_p[G])$ of the form

$$R\Gamma_c(\mathcal{O}_{F,\Sigma}, T) \to R\Gamma(\mathcal{O}_{F,\Sigma}, T) \to \bigoplus_{w \in \Sigma_F} R\Gamma(F_w, T) \to R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)[1], \tag{4}$$

with the second arrow denoting the natural diagonal localisation map.

In the sequel we also set $B_F(T) := \bigoplus_{w \in \Sigma_{\infty,F}} H^0(F_w, T)$.

Proposition 2.3. *For data $F/E, \Sigma, T$ and G as above the following claims are valid.*

(i) *Let J be a normal subgroup of G. Then there are natural isomorphisms in $D(\mathbb{Z}_p[G_{F^J/E}])$*

$$\begin{cases} \mathbb{Z}_p[G_{F^J/E}] \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} R\Gamma(\mathcal{O}_{F,\Sigma}, T) \cong R\Gamma(\mathcal{O}_{F^J,\Sigma}, T), \\ \mathbb{Z}_p[G_{F^J/E}] \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} R\Gamma_c(\mathcal{O}_{F,\Sigma}, T) \cong R\Gamma_c(\mathcal{O}_{F^J,\Sigma}, T). \end{cases}$$

(ii) *The complexes $R\Gamma(\mathcal{O}_{F,\Sigma}, T)$ and $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ are respectively acyclic outside degrees zero, one and two and degrees one, two and three. In addition, there is an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$H^1_c(\mathcal{O}_{F,\Sigma}, T) \cong B_F(T) \oplus H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^* \tag{5}$$

and for both $i = 2$ and $i = 3$ a canonical short exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \to (H^{4-i}(\mathcal{O}_{F,\Sigma}, T^*(1))_{\mathrm{tor}})^\vee \to H^i_c(\mathcal{O}_{F,\Sigma}, T) \to H^{3-i}(\mathcal{O}_{F,\Sigma}, T^*(1))^* \to 0. \tag{6}$$

(iii) *$R\Gamma(\mathcal{O}_{F,\Sigma}, T)$ and $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ belong to $D^{\mathrm{p}}(\mathbb{Z}_p[G])$.*

(iv) *The Euler characteristic of $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ in $K_0(\mathbb{Z}_p[G])$ vanishes.*

Proof. The first isomorphism in claim (i) is the standard 'projection formula' isomorphism in étale cohomology. The second isomorphism then results by combining this with the analogous isomorphisms for the complexes $R\Gamma(F_w, T)$ and the definition of compactly supported cohomology via the triangles (4) for F and F^J.

Next we note that, since p is odd, the complex $R\Gamma(\mathcal{O}_{F,\Sigma}, T)$ is well-known to be acyclic outside degrees zero, one and two. In addition, in this case the Artin-Verdier Duality Theorem implies there is a canonical exact triangle in $D(\mathbb{Z}_p[G])$

$$B_F(T)[-1] \to R\Gamma_c(\mathcal{O}_{F,\Sigma}, T) \to \mathrm{Hom}_{\mathbb{Z}_p}(R\Gamma(\mathcal{O}_{F,\Sigma}, T^*(1)), \mathbb{Z}_p[-3]) \to B_F(T)[0] \tag{7}$$

(see, for example, [4, Lem. 12b)]). By using the universal coefficient spectral sequence one can also compute the cohomology groups of the third term in the above triangle in terms of those of the complex $R\Gamma(\mathcal{O}_{F,\Sigma}, T^*(1))$.

In this way one finds that the long exact sequence of cohomology of (7) implies $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ is acyclic outside degrees one, two and three and gives rise both to the exact sequences (6) and also to a short exact sequence $0 \to B_F(T) \to H^1_c(\mathcal{O}_{F,\Sigma}, T) \to H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^* \to 0$. In addition, since $B_F(T)$ is a projective $\mathbb{Z}_p[G]$-module (by Lemma 2.4(i) below) and the module $H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*$ is torsion-free, the same argument as used at the end of the proof of Proposition 2.1 shows this sequence of $\mathbb{Z}_p[G]$-modules splits to give an isomorphism of the form (5), as required to complete the proof of claim (ii).

Finally, we note that claims (iii) and (iv) are special cases of a result of Flach [8, Th. 5.1] and of Flach and the present author [4, Lem. 7] respectively. □

In the sequel we will also find the following observations to be useful.

Lemma 2.4. *For data $F/E, T$ and G as in Proposition 2.3 the following claims are valid.*

(i) *$B_F(T)$ is a projective $\mathbb{Z}_p[G]$-module.*

(ii) *If J is any subgroup of G of odd order, then* $\mathrm{rk}(B_F(T)) = \#J \cdot \mathrm{rk}(B_{F^J}(T))$.

Proof. For each place v in $\Sigma_{\infty,E}$ we choose a corresponding embedding $\sigma_v : E \to E_v$ and write G_v for the decomposition subgroup in G of a fixed place of F above v. Then there is a natural isomorphism of $\mathbb{Z}_p[G]$-modules

$$B_F(T) \cong \bigoplus_{v \in \Sigma_{\infty,E}} H^0(G_v, T \otimes_{\mathbb{Z}_p} \prod\nolimits_{\Sigma_v} \mathbb{Z}_p)$$

where Σ_v denotes the set of embeddings $F \to (E_v)^c$ that extend σ_v and on the tensor product G_v acts diagonally (via post-composition with elements of Σ_v) and G acts only on the second factor (via pre-composition with elements of Σ_v).

This isomorphism immediately implies claim (i) since each $\mathbb{Z}_p[G]$-module $T \otimes_{\mathbb{Z}_p} \prod_{\Sigma_v} \mathbb{Z}_p$ is free and the order of each subgroup G_v is prime to p.

If $\#J$ is odd, then each place v in $\Sigma_{\infty,E}$ is totally split in F/F^J. This implies that there are isomorphisms of $\mathbb{Z}_p$-modules

$$B_F(T) = \bigoplus_{w \in \Sigma_{\infty,F}} H^0(G_w, T) \cong \mathbb{Z}_p[J] \otimes_{\mathbb{Z}_p} \Big(\bigoplus_{s \in \Sigma_{\infty,F^J}} H^0(G_s, T) \Big) = \mathbb{Z}_p[J] \otimes_{\mathbb{Z}_p} B_{F^J}(T).$$

Claim (ii) follows immediately from this composite isomorphism. □

2.3. Turning now to the proof of Theorem 1.1 we proceed by a number of reductions.

In the sequel we often use, without explicit comment, the fact that $\mathrm{rk}(T)$ and $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T))$ are unchanged if one replaces T by $T^*(1)$.

Lemma 2.5. *It is enough to prove the result of Theorem 1.1 as it applies to $H^2_c(\mathcal{O}_{F,\Sigma}, T)$.*

Proof. At the outset we note $H^0(\mathcal{O}_{F,\Sigma}, T)$ is a submodule of T and hence that in this case the claim of Theorem 1.1 is obviously true with $P^0_{F/E,T} = 0$ and $m^0_{F/E,T} = 1$.

Next, the long exact cohomology sequence of the sequence $0 \to T \xrightarrow{p} T \to T/p \to 0$ induces both a surjective homomorphism $H^0(\mathcal{O}_{F,\Sigma}, T/p) \to H^1(\mathcal{O}_{F,\Sigma}, T)[p]$ and an isomorphism $H^2(\mathcal{O}_{F,\Sigma}, T)/p \cong H^2(\mathcal{O}_{F,\Sigma}, T/p)$, implying $\mathrm{rk}_p(H^1(\mathcal{O}_{F,\Sigma}, T)[p]) \leq \mathrm{rk}(T)$ and $\mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T)) = \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T/p))$ respectively.

The inequality $\mathrm{rk}_p(H^1(\mathcal{O}_{F,\Sigma}, T)[p]) \leq \mathrm{rk}(T)$ combines with the exact sequences (6) (with T replaced by $T^*(1)$) to give two consequences.

Firstly, it implies a decomposition of the required sort for $H^3_c(\mathcal{O}_{F,\Sigma}, T)$ with $P^3_{F/E,T,c} = 0$ and $m^3_{F/E,T,c} = 2$.

Secondly, since (6) implies $H^1(\mathcal{O}_{F,\Sigma}, T)_{\mathrm{tf}}$ is naturally isomorphic to $H^2_c(\mathcal{O}_{F,\Sigma}, T^*(1))^*$, it shows that a decomposition of the claimed sort for $H^2_c(\mathcal{O}_{F,\Sigma}, T^*(1))$ implies a corresponding decomposition of $H^1(\mathcal{O}_{F,\Sigma}, T)$ with $m^1_{F/E,T} = m^2_{F/E,T,c} + 1$.

We now note that, since the complexes $R\Gamma(\mathcal{O}_{F_T,\Sigma}, T)$ and $R\Gamma(\mathcal{O}_{F,\Sigma}, T)$ are acyclic in degrees greater than two the first descent isomorphism in Proposition 2.3(i) induces an identification $H_0(G_{F_T/F}, H^2(\mathcal{O}_{F_T,\Sigma}, T)) \cong H^2(\mathcal{O}_{F,\Sigma}, T)$ and hence implies that

$$\begin{aligned}(8)\quad \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T)) &\leq \mathrm{rk}_p(H^2(\mathcal{O}_{F_T,\Sigma}, T)) = \mathrm{rk}_p(H^2(\mathcal{O}_{F_T,\Sigma}, T/p)) \\ &= \mathrm{rk}(T) \cdot \mathrm{rk}_p(H^2(\mathcal{O}_{F_T,\Sigma}, \mu_p)) = \mathrm{rk}(T) \cdot (\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + \#\Sigma_{f,F_T} - 1)\end{aligned}$$

where the second equality follows from the fact that over F_T the module T/p is isomorphic to a direct sum of $\mathrm{rk}(T)$ copies of μ_p and the last from a standard computation of $H^2(\mathcal{O}_{F_T,\Sigma}, \mu_p)$ using class field theory.

This immediately gives a decomposition for $H^2(\mathcal{O}_{F,\Sigma}, T)$ of the required sort with $P^2_{F/E,T} = 0$ and $m^2_{F/E,T} = \mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + [F_T : F] \cdot \#\Sigma_{f,F} - 1$.

We observe finally this decomposition (with T replaced by $T^*(1)$) combines with the isomorphism (5) to give a corresponding decomposition of $H^1_c(\mathcal{O}_{F,\Sigma}, T)$ with $m^1_{F/E,T,c} = m^2_{F/E,T}$. □

Since we can now focus on $H^2_c(\mathcal{O}_{F,\Sigma}, T)$ we abbreviate it to M. We also set $G := G_{F/E}$.

Lemma 2.6. *Theorem 1.1 is valid if and only if* $\mathrm{rk}_p(\hat{H}^0(G, M_{\mathrm{tf}}))$ *is bounded by an explicit multiple of* $\mathrm{rk}(T)$ *that depends only on* $\#G$, $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T))$ *and* $\#\Sigma_{f,F}$.

Proof. Necessity of the given condition is clear. To prove sufficiency we note first that the exact sequence (6) implies

$$(9)\qquad \mathrm{rk}_p(M_{\mathrm{tor}}) = \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))_{\mathrm{tor}}) \leq \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))).$$

This combines with the bound (8) (with T replaced by $T^*(1)$) to show that M has a decomposition of the form stated in Theorem 1.1 if and only if the lattice M_{tf} has the same sort of decomposition.

To analyse M_{tf} we fix a Sylow p-subgroup P of G and note the natural restriction map $\hat{H}^0(G, M_{\mathrm{tf}}) \to \hat{H}^0(P, M_{\mathrm{tf}})$ is bijective.

We set

$$r := \mathrm{rk}(H^0(P, M_{\mathrm{tf}})) \quad \text{and} \quad r_p := \mathrm{rk}_p(\hat{H}^0(P, M_{\mathrm{tf}})) = \mathrm{rk}_p(\hat{H}^0(G, M_{\mathrm{tf}})),$$

note that the integer

$$d := r - r_p = \mathrm{rk}_p(H^0(P, M_{\mathrm{tf}})/p) - \mathrm{rk}_p(H^0(P, M_{\mathrm{tf}})/(p, \mathrm{tr}_P(M_{\mathrm{tf}})))$$

is non-negative and choose a set of elements $\{m_i\}_{1\leq i\leq d}$ of M such that the images in $H^0(P, M_{\mathrm{tf}})/p$ of the elements $\mathrm{tr}_P(m_i)$ are linearly independent over $\mathbb{F}_p$.

By applying Proposition 2.1 to this data we deduce that the $\mathbb{Z}_p[P]$-submodule M' of M generated by $\{m_i\}_{1\leq i\leq d}$ is both free of rank d and a direct summand of M. Fixing a complement M'' to the direct summand M' in M one has

$$\begin{aligned}(10)\quad \mathrm{rk}(M'') = \mathrm{rk}(M) - \mathrm{rk}(M') &= \mathrm{rk}(M) - \#P \cdot d \\ &= (\mathrm{rk}(M) - \#P \cdot \mathrm{rk}(H^0(P, M))) + \#P \cdot r_p.\end{aligned}$$

Now, if J denotes either P or the identity subgroup of G, then one has

$$\begin{aligned}\mathrm{rk}(H^0(J, M)) =& \mathrm{rk}(H^2_c(\mathcal{O}_{F^J,\Sigma}, T)) \\ =& \mathrm{rk}(H^1_c(\mathcal{O}_{F^J,\Sigma}, T)) + \mathrm{rk}(H^3_c(\mathcal{O}_{F^J,\Sigma}, T)) \\ =& \mathrm{rk}(B_{F^J}(T)) + \mathrm{rk}(H^2(\mathcal{O}_{F^J,\Sigma}, T^*(1))) + \mathrm{rk}(H^0(\mathcal{O}_{F^J,\Sigma}, T^*(1))).\end{aligned}$$

(The second equality here is a consequence of Proposition 2.3(iv) and the third a consequence of the descriptions given in Proposition 2.3(ii)).

Taken in conjunction with Lemma 2.4(ii), the last displayed equality implies that

$$\begin{aligned}\mathrm{rk}(M) - \#P \cdot \mathrm{rk}(H^0(P, M)) &\leq \mathrm{rk}(M) - \#P \cdot \mathrm{rk}(B_{F^P}(T)) \\ &= \mathrm{rk}(M) - \mathrm{rk}(B_F(T)) \\ &= \mathrm{rk}(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))) + \mathrm{rk}(H^0(\mathcal{O}_{F,\Sigma}, T^*(1))) \\ &\leq \mathrm{rk}(T)(m^2_{F/E,T} + 1),\end{aligned}$$

where $m^2_{F/E,T}$ is the explicit integer defined in the proof of Lemma 2.5.

This fact combines with (10) to imply there is an isomorphism of $\mathbb{Z}_p[G]$-modules

$$(11)\qquad \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M \cong M_1 \oplus M_2$$

where $M_1 := \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M'$ is free and $M_2 := \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M''$ satisfies

$$(12)\qquad \mathrm{rk}(M_2) = [G : P] \cdot \mathrm{rk}(M'') \leq [G : P]\mathrm{rk}(T)(m^2_{F/E,T} + 1) + \#G \cdot r_p.$$

Next we claim M_{tf} is a direct summand of the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M_{\mathrm{tf}}$. To see this write t for the index of P in G and choose a set of coset representatives $\{c_i\}_{1\leq i\leq t}$ for P in G. Then t is prime to p and the map of $\mathbb{Z}_p[G]$-modules $M_{\mathrm{tf}} \to \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M_{\mathrm{tf}}$ that sends each m to $t^{-1} \sum_{i=1}^{i=t} c_i^{-1} \otimes c_i(m)$ is a section to the natural surjective map $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} M_{\mathrm{tf}} \to M_{\mathrm{tf}}$, as required.

In particular, if one decomposes M_{tf} as a direct sum of $\mathbb{Z}_p[G]$-modules $\Pi \oplus \Pi'$ where Π is projective and Π' is a direct sum of non-projective indecomposable modules, then the isomorphism (11) and upper bound (12) combine with the Krull-Schmidt Theorem to imply Π' is isomorphic to a direct summand of M_2 and hence is of $\mathbb{Z}_p$-rank at most $[G : P]\mathrm{rk}(T)(m^2_{F/E,T} + 1) + \#G \cdot r_p$.

The claimed result now follows immediately from Lemma 2.5. □

In view of Lemma 2.6 the proof of Theorem 1.1 is completed by the following result.

Lemma 2.7. $\mathrm{rk}_p(\hat{H}^0(G, M_{\mathrm{tf}})) \leq \mathrm{rk}(T) \cdot (2 + (1 + (\#G)^2)(\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + \#\Sigma_{f,F_T} - 1))\#G$.

Proof. Since $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ is perfect over $\mathbb{Z}_p[G]$, acyclic outside degrees one, two and three and $\mathbb{Z}_p$-free in degree one (by Proposition 2.3) a standard argument of homological algebra shows that it is isomorphic in $D(\mathbb{Z}_p[G])$ to a complex of finitely generated projective $\mathbb{Z}_p[G]$-modules of the form $Q^1 \xrightarrow{d^1} Q^2 \xrightarrow{d^2} Q^3$ where each module Q^i occurs in degree i. This representative gives rise to tautological short exact sequences

$$\begin{cases} 0 \to M^1 \to Q^1 \to \mathrm{im}(d^1) \to 0, & 0 \to \mathrm{im}(d^1) \to \ker(d^2) \to M^2 \to 0, \\ 0 \to \ker(d^2) \to Q^2 \to \mathrm{im}(d^2) \to 0, & 0 \to \mathrm{im}(d^2) \to Q^3 \to M^3 \to 0, \end{cases}$$

where we set $M^i := H^i_c(\mathcal{O}_{F,\Sigma}, T)$ in each degree i (so $M^2 = M$).

Since the modules Q^1, Q^2 and Q^3 are cohomologically-trivial over G, the long exact cohomology sequences of these sequences combine to give an exact sequence

$$\hat{H}^{-2}(G, M^3) \to \hat{H}^0(G, M) \to \hat{H}^2(G, H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*).$$

Here we also use the fact that Lemma 2.4(i) combines with the isomorphism (5) to imply the groups $\hat{H}^2(G, M^1)$ and $\hat{H}^2(G, H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*)$ are naturally isomorphic.

In addition, the tautological exact sequence $0 \to M_{\mathrm{tor}} \to M \to M_{\mathrm{tf}} \to 0$ also gives rise to an exact sequence $\hat{H}^0(G, M) \to \hat{H}^0(G, M_{\mathrm{tf}}) \to H^1(G, M_{\mathrm{tor}})$ and this combines with the last displayed exact sequence to imply $\mathrm{rk}_p(\hat{H}^0(G, M_{\mathrm{tf}}))$ is at most

$$\begin{aligned} &\mathrm{rk}_p(\hat{H}^0(G, M)) + \mathrm{rk}_p(H^1(G, M_{\mathrm{tor}})) \\ \leq &\mathrm{rk}_p(\hat{H}^{-2}(G, M^3)) + \mathrm{rk}_p(\hat{H}^2(G, H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*)) + \mathrm{rk}_p(H^1(G, M_{\mathrm{tor}})) \\ \leq &\#G \cdot \mathrm{rk}_p(M^3) + (\#G)^3 \cdot \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*) + \#G \cdot \mathrm{rk}_p(M_{\mathrm{tor}}) \\ \leq &\#G(\mathrm{rk}_p(M^3) + (\#G)^2 \cdot \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*) + \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1)))) \\ \leq &\#G \cdot \mathrm{rk}(T)(2 + ((\#G)^2 + 1)(\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + \#\Sigma_{f,F_T} - 1)) \end{aligned}$$

where the second inequality is obtained by three applications of Lemma 2.8 below, the third follows from (9) and the last is a consequence of the bound $\mathrm{rk}_p(M^3) \leq 2 \cdot \mathrm{rk}(T)$ obtained in the course of proving Lemma 2.5 and the bound for $\mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*) \leq \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1)))$ given by (8). This proves the claimed result. □

Lemma 2.8. *Let $\mathcal{G}$ be a finite group and M a finitely generated $\mathbb{Z}_p$-module. Then for each integer i one has* $\mathrm{rk}_p(\hat{H}^i(\mathcal{G}, M)) \leq (\#\mathcal{G})^{|i+1|} \cdot \mathrm{rk}_p(M)$.

Proof. The tensor product $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}]$ is endowed with a natural diagonal action of $\mathcal{G}$ and lies in two natural short exact sequences of $\mathbb{Z}_p[\mathcal{G}]$-modules

$$\begin{cases} 0 \to M \xrightarrow{\iota_M} M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}] \to \mathrm{cok}(\iota_M) \to 0 \\ 0 \to \ker(\pi_M) \to M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}] \xrightarrow{\pi_M} M \to 0. \end{cases}$$

These sequences imply the p-ranks of $\mathrm{cok}(\iota_M)$ and $\ker(\iota_M)$ are at most $\mathrm{rk}_p(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}])$ $= \#\mathcal{G} \cdot \mathrm{rk}_p(M)$. In addition, since $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}]$ is a cohomologically-trivial G-module, the long exact cohomology sequences associated to these sequences induce isomorphisms

$$\hat{H}^i(\mathcal{G}, M) \cong \hat{H}^{i-1}(\mathcal{G}, \mathrm{cok}(\iota_M)) \quad \text{and} \quad \hat{H}^i(\mathcal{G}, M) \cong \hat{H}^{i+1}(\mathcal{G}, \ker(\pi_M)). \tag{13}$$

In particular, if i is non-negative, resp. strictly negative, then after repeatedly applying isomorphisms of the first, resp. second, kind in (13) one finds that

$$\mathrm{rk}_p(\hat{H}^i(\mathcal{G}, M)) = \mathrm{rk}_p(\hat{H}^{-1}(\mathcal{G}, M_i)),$$

where M_i is a $\mathbb{Z}_p[\mathcal{G}]$-module which satisfies $\mathrm{rk}_p(M_i) \leq (\#\mathcal{G})^{|i+1|} \cdot \mathrm{rk}_p(M)$.

The claimed result thus follows from the last displayed equality because $\mathrm{rk}_p(\hat{H}^{-1}(\mathcal{G}, M_i))$ is a subquotient of M_i and hence satisfies $\mathrm{rk}_p(\hat{H}^{-1}(\mathcal{G}, M_i)) \leq \mathrm{rk}_p(M_i)$. □

3. Representations with pro-p image

In this section we discuss applications of Theorem 1.1 in the setting of representations with pro-p image.

3.1. We start by deducing a result which shows that, in certain natural cases, one can weaken the explicit dependence of the bounds given in Theorem 1.1 on either the given p-adic representation or the behaviour of class groups.

In the sequel we write $M^p_{k,\Sigma}$ for the maximal pro-p extension of k in $M_{k,\Sigma}$ and $M^{p,\mathrm{ab}}_{k,\Sigma}$ for the maximal abelian extension of k in $M^p_{k,\Sigma}$.

Corollary 3.1. *Fix an abstract finite group $\mathcal{G}$, a finite set Σ of places of k containing $\Sigma_\infty \cup \Sigma_p$ and natural numbers r and b.*

Then there exists a finite Galois extension $k_{\Sigma,r}$ of k in $M_{k,\Sigma}$ with the following property: as T ranges over all p-adic representations of $G_{k,\Sigma}$ that have pro-p image and rank at most r and F/E over all $\mathcal{G}$-extensions of number fields that contain k, are unramified outside Σ_E and such that $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(k_{\Sigma,r}F)) + \#\Sigma_{f,F} \leq b$, there are, up to projective direct summands, only finitely many isomorphism classes of $\mathbb{Z}_p[\mathcal{G}]$-modules that can arise from the modules $H^i(\mathcal{O}_{F,\Sigma}, T)_{\mathrm{tf}}$ and $H^i_c(\mathcal{O}_{F,\Sigma}, T)_{\mathrm{tf}}$ for any choice of degree i.

Proof. If ρ is a representation $G_{k,\Sigma} \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ with pro-p image and rank at most r, then the kernel of the induced modular representation $G_{k,\Sigma} \to \mathrm{Aut}_{\mathbb{Z}_p}(T/p)$ can be computed as the kernel of a homomorphism $G_{k,\Sigma} \to \mathrm{GL}_r(\mathbb{F}_p)$ with pro-p image and so has index dividing the maximal power p^{ir} of p that divides $\#\mathrm{GL}_r(\mathbb{F}_p)$. The field k_T that occurs in Theorem 1.1 is thus the compositum of $k(\mu_p)$ and a Galois extension k'_T of k in $M_{k,\Sigma}$ of exponent dividing p^{ir}.

Write $k'_{\Sigma,r}$ for the compositum of the fields k'_T as ρ runs over all such representations. Then $k'_{\Sigma,r}$ is a Galois extension of k in $M^p_{k,\Sigma}$ of exponent dividing p^{ir} and, since $G_{M^p_{k,\Sigma}/k}$ is topologically finitely generated, this implies $k'_{\Sigma,r}$ is a finite extension of k. We thus obtain a finite Galois extension of k in $M_{k,\Sigma}$ by setting $k_{\Sigma,r} := k'_{\Sigma,r}(\mu_p)$.

The proof of Theorem 1.1 shows that the same bounds on $\mathrm{rk}_p(R^i_{F/E,T})$ and $\mathrm{rk}_p(R^i_{F/E,T,c})$ are valid if one replaces F_T with the larger field $F_{\Sigma,r} := k_{\Sigma,r}F$. Hence, since the given bound on $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_{\Sigma,r})) + \#\Sigma_{f,F}$ implies a bound on both $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_{\Sigma,r}))$ and $\#\Sigma_{f,F}$, this argument gives a bound on the $\mathbb{Z}_p$-ranks of the lattices $R^i_{F/E,T,\mathrm{tf}}$ and $R^i_{F/E,T,c,\mathrm{tf}}$.

The claimed result now follows since there are, up to isomorphism, only finitely many $\mathbb{Z}_p[\mathcal{G}]$-lattices of any given rank. □

For a concrete arithmetical application of this result for the representations $T = \mathbb{Z}_p(a)$ see Corollary 4.1 (and Proposition 4.2).

In general, the following example shows the bounds required by Corollary 3.1 arise in natural families of extensions.

In the sequel we write E_{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of a number field E.

Example 3.2. Assume k contains μ_p, fix a pro-p p-adic analytic extension K of k containing k_{cyc} and unramified outside Σ and set $E_{\Sigma,r} := k_{\Sigma,r}E$ for each subfield E of K. Fix a finite group $\mathcal{G}$ of p-power order and a natural number e and write $\mathrm{Ext}(\mathcal{G}, K/k, e)$ for the family of Galois extensions F/E with $G_{F/E}$ isomorphic to $\mathcal{G}$, $k \subseteq E \subset F \subset K$, E/k finite and $[E : E \cap k_{\mathrm{cyc}}] \leq e$. For any such F/E the degree over k_{cyc} of the Galois closure of F_{cyc} over k_{cyc} is at most the maximal power p^m of p that divides $(e\#\mathcal{G})!$ In addition, since in this case $K_{\Sigma,r}$ is a pro-p p-adic analytic extension of k_{cyc}, the compositum $K_{r,m}$ of $k_{\Sigma,r}$ with the largest Galois extension of k_{cyc} in K of exponent dividing p^m is of finite p-power degree over k_{cyc}. Now $(F_{\Sigma,r})_{\mathrm{cyc}}$ is one of the finitely many intermediate fields L of $K_{r,m}/k_{\mathrm{cyc}}$ and if the Iwasawa μ-invariant of k_{cyc} vanishes (as conjectured by Iwasawa [11]) one can show $G_{M^{p,\mathrm{ab}}_{L,\Sigma}/L}$ is a finitely generated $\mathbb{Z}_p$-module for each such L. By using [15, Prop. 13.23] this gives a finite upper bound on $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_{\Sigma,r}))$ that depends only on $K_{r,m}/k$. Since every place in Σ_f is only finitely decomposed in $K_{r,m}/k$ one can also give a similar bound on $\#\Sigma_{f,F}$ and so Corollary 3.1 applies to the family $\mathrm{Ext}(\mathcal{G}, K/k, e)$.

3.2. In this section we prove Corollary 1.2. To do so we first recall details concerning the finite support cohomology and Selmer groups introduced by Bloch and Kato.

With $\mathcal{F}$ denoting either T or $W := (\mathbb{Q}_p/\mathbb{Z}_p)\otimes_{\mathbb{Z}_p} T$, for each place w of each finite extension L of k in k^c we write $H^1_f(L_w, \mathcal{F})$ for the 'finite support cohomology' subgroup of $H^1(L_w, \mathcal{F})$ defined in [1]. Then the Bloch-Kato Selmer group $\mathrm{Sel}_L(W)$ of W over L is defined to be the kernel of the natural diagonal localisation map

$$H^1(\mathcal{O}_{L,\Sigma}, W) \to \bigoplus_{w\in\Sigma_L} \frac{H^1(L_w, W)}{H^1_f(L_w, W)}.$$

Setting $\mathrm{Sel}_L(T) := \mathrm{Sel}_L(W)^\vee$, Artin-Verdier Duality gives rise (via, for example, the computations of [3, pp. 86-87]) to an exact sequence of finitely generated $\mathbb{Z}_p$-modules

$$\bigoplus_{w\in\Sigma_{f,L}} H^1_f(L_w, T) \to H^2_c(\mathcal{O}_{L,\Sigma}, T) \to \mathrm{Sel}_L(T) \to 0$$

and hence to an inequality

$$\mathrm{rk}(H^2_c(\mathcal{O}_{L,\Sigma}, T)) - \sum_{w\in\Sigma_{f,L}} \mathrm{rk}(H^1_f(L_w, T)) \leq \mathrm{rk}(\mathrm{Sel}_L(T)) \leq \mathrm{rk}(H^2_c(\mathcal{O}_{L,\Sigma}, T)). \tag{14}$$

It is also well known that for each $w \in \Sigma_{f,L}$ one has

$$\text{rk}(H^1_f(L_w,T)) \leq \begin{cases} \text{rk}(T)([L_w:\mathbb{Q}_p]+1), & \text{if } w \text{ is } p\text{-adic,} \\ \text{rk}(T), & \text{otherwise} \end{cases} \tag{15}$$

(for example, this follows directly from [3, (1.5) and (1.7)] and the fact that if w is p-adic, then the $\mathbb{Q}_p$-dimension of the tangent space of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ over L_w is at most $[L_w:\mathbb{Q}_p]\cdot\text{rk}(T)$).

Turning to the proof of Corollary 1.2 we assume the notation and hypotheses of that result, we set $G := G_{F/E}$ and we fix a decomposition $H^2_c(\mathcal{O}_{F,\Sigma},T) = P^2_{F/E,T,c} \oplus R^2_{F/E,T,c}$ of the form stated in Theorem 1.1.

As G is here assumed to be a p-group, the $\mathbb{Z}_p[G]$-module $P^2_{F/E,T,c}$ is free and so $\text{rk}(P^2_{F/E,T,c})$ $= \#G\cdot\text{rk}(H^0(G,P^2_{F/E,T,c}))$. In addition, since the isomorphism in Proposition 2.3(i) induces an identification of $\mathbb{Q}_p$-spaces $H^0(G,\mathbb{Q}_p\otimes_{\mathbb{Z}_p} H^2_c(\mathcal{O}_{F,\Sigma},T)) \cong \mathbb{Q}_p\otimes_{\mathbb{Z}_p} H^2_c(\mathcal{O}_{E,\Sigma},T)$, one has

$$\begin{aligned}\text{rk}(H^0(G,P^2_{F/E,T,c})) &= \text{rk}(H^0(G,H^2_c(\mathcal{O}_{F,\Sigma},T))) - \text{rk}(H^0(G,R^2_{F/E,T,c})) \\ &= \text{rk}(H^2_c(\mathcal{O}_{E,\Sigma},T)) - \text{rk}(H^0(G,R^2_{F/E,T,c}))\end{aligned}$$

and hence

$$\begin{aligned}\text{rk}(H^2_c(\mathcal{O}_{F,\Sigma},T)) =& \text{rk}(P^2_{F/E,T,c}) + \text{rk}(R^2_{F/E,T,c}) \\ =& \#G\cdot\text{rk}(H^0(G,P^2_{F/E,T,c})) + \text{rk}(R^2_{F/E,T,c}) \\ =& \#G(\text{rk}(H^2_c(\mathcal{O}_{E,\Sigma},T)) - \text{rk}(H^0(G,R^2_{F/E,T,c})) + \text{rk}(R^2_{F/E,T,c}) \\ =& \#G\cdot\text{rk}(H^2_c(\mathcal{O}_{E,\Sigma},T)) + \delta_{F/E,T}\end{aligned}$$

with $\delta_{F/E,T} := \text{rk}(R^2_{F/E,T,c}) - \#G\cdot\text{rk}(H^0(G,R^2_{F/E,T,c}))$ so that

$$-\#G\cdot\text{rk}_p(R^2_{F/E,T,c,\text{tf}}) \leq \delta_{F/E,T} \leq \text{rk}_p(R^2_{F/E,T,c,\text{tf}}).$$

These facts combine with (14) and (15) (for both $L=F$ and $L=E$) to give inequalities

$$\begin{aligned}\text{rk}(\text{Sel}_F(T)) \leq& \text{rk}(H^2_c(\mathcal{O}_{F,\Sigma},T)) \\ =& \#G\cdot\text{rk}(H^2_c(\mathcal{O}_{E,\Sigma},T)) + \delta_{F/E,T} \\ \leq& \#G(\text{rk}(\text{Sel}_E(T)) + \text{rk}(T)(\#\Sigma_{f,E} + [E:\mathbb{Q}])) + \delta_{F/E,T} \\ \leq& \#G\cdot\text{rk}(\text{Sel}_E(T)) + \text{rk}(T)(\#G\cdot\#\Sigma_{f,F} + [F:\mathbb{Q}]) + \text{rk}_p(R^2_{F/E,T,c,\text{tf}}) \\ \leq& \#G\cdot\text{rk}(\text{Sel}_E(T)) + r(\#G\cdot\#\Sigma_{f,F} + [F:\mathbb{Q}]) + \text{rk}_p(R^2_{F/E,T,c,\text{tf}})\end{aligned}$$

and

$$\begin{aligned}\text{rk}(\text{Sel}_F(T)) \geq& \text{rk}(H^2_c(\mathcal{O}_{F,\Sigma},T)) - \text{rk}(T)(\#\Sigma_{f,F} + [F:\mathbb{Q}]) \\ =& \#G\cdot\text{rk}(H^2_c(\mathcal{O}_{E,\Sigma},T)) + \delta_{F/E,T} - \text{rk}(T)(\#\Sigma_{f,F} + [F:\mathbb{Q}]) \\ \geq& \#G\cdot\text{rk}(\text{Sel}_E(T)) - \text{rk}(T)(\#\Sigma_{f,F} + [F:\mathbb{Q}]) - \#G\cdot\text{rk}_p(R^2_{F/E,T,c,\text{tf}}) \\ \geq& \#G\cdot\text{rk}(\text{Sel}_E(T)) - r(\#\Sigma_{f,F} + [F:\mathbb{Q}]) - \#G\cdot\text{rk}_p(R^2_{F/E,T,c,\text{tf}}).\end{aligned}$$

To deduce Corollary 1.2 from these explicit inequalities it is enough to note that the argument of Corollary 3.1 gives an upper bound on $\mathrm{rk}_p(R^2_{F/E,T,c,\mathrm{tf}})$ that depends only on $\#G$, $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(k_{\Sigma,r}F))$ and $\#\Sigma_{f,F}$.

4. The representations $T = \mathbb{Z}_p(r)$

By means of concrete arithmetic examples, in this section we explore consequences of Theorem 1.1 for the representations $T = \mathbb{Z}_p(r)$. We also show that in this context, and for special classes of extensions F/E, our methods can lead to very explicit structural results.

4.1. We first record a general consequence of Corollary 3.1 in this case.

For any abstract finite group $\mathcal{G}$, any finite set of rational places Σ that contains p and any natural number b we write $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$ for the family of Galois extensions of number fields F/E that satisfy all of the following properties

$$\begin{cases} G_{F/E} \text{ is isomorphic to } \mathcal{G}, \\ E \text{ contains } \mu_p, \\ F/E \text{ is unramified outside } \Sigma_E, \\ \mathrm{rk}_p(\mathrm{Cl}_\Sigma(F)) + \#\Sigma_{f,F} \leq b. \end{cases}$$

Then Corollary 3.1 has the following concrete consequence concerning Galois structures in these families.

Corollary 4.1. *Fix data $\mathcal{G}$, Σ and b as above. Then, as F/E ranges over $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$ there are, up to projective direct summands, only finitely many isomorphism classes of $\mathbb{Z}_p[\mathcal{G}]$-modules that arise from either $\mathrm{Gal}(M^{p,\mathrm{ab}}_{F,\Sigma}/F)_{\mathrm{tf}}$ or $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))_{\mathrm{tf}}$ for any non-negative integer a.*

Proof. If $T = \mathbb{Z}_p(a)$ for any integer a, then the associated p-adic representation of $G_{\mathbb{Q}(\mu_p),\Sigma}$ has pro-p image and for every field F as above one has $F_T = F$.

The claimed result thus follows directly from the proof of Corollary 3.1 (with k replaced by $\mathbb{Q}(\mu_p)$) and the fact that there are canonical isomorphisms of $\mathbb{Z}_p[G_{F/E}]$-modules

$$\begin{cases} H^1(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{F,\Sigma} = \mathbb{Z}_p \otimes_{\mathbb{Z}} K_1(\mathcal{O}_{F,\Sigma}), \\ H^1(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1+a)) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}) \ \text{ for } \ a > 0, \\ H^2_c(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1)) \cong \mathrm{Gal}(M^{p,\mathrm{ab}}_{F,\Sigma}/F). \end{cases} \tag{16}$$

(The first isomorphism here is induced by Kummer theory, the second by the Chern class homomorphism $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}) \to H^1(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1+a))$ whose bijectivity is guaranteed by the known validity of the Quillen-Lichtenbaum Conjecture, and the third by the Artin-Verdier duality theorem.) □

The interest of Corollary 4.1 is explained by the following result.

Proposition 4.2. *Let $\mathcal{G}$ be a finite group of odd order that has a commutator subgroup of p-power order. Then for any large enough finite set of rational places Σ and any large enough integer b the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(M^{p,\mathrm{ab}}_{F,\Sigma}/F)_{\mathrm{tf}}$, and of $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))_{\mathrm{tf}}$ for any non-negative integer a, is unbounded as F/E ranges over $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$.*

Proof. As any such group $\mathcal{G}$ is both solvable and of order prime to the number of roots of unity in $\mathbb{Q}$ there exists a Galois extension F of $\mathbb{Q}$ for which $G_{F/\mathbb{Q}}$ is isomorphic to $\mathcal{G}$ and p is unramified in F (see Neukirch [13, Cor. 2, p. 156]). We write Σ for the set of rational places comprising ∞, p and those primes that ramify in $F/\mathbb{Q}$.

For each natural number m we write E_m for the field generated over $\mathbb{Q}$ by a primitive p^m-th root of unity, set $F_m := FE_m$ and claim that for any large enough integer b the extensions F_m/E_m all belong to $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$.

At the outset it is clear E_m contains μ_p, F_m/E_m is unramified outside Σ and, as $E_m/\mathbb{Q}$ is disjoint from $F/\mathbb{Q}$ (since p is unramified in F), G_{F_m/E_m} is isomorphic to $\mathcal{G}$.

We next write F_∞ for the union of the fields F_m for $m > 0$. Then each rational prime has open decomposition group in $G_{F_\infty/\mathbb{Q}}$ and so $\#\Sigma_{f,F_m}$ is bounded independently of m. In addition, since F_1 is (by our assumption on the commutator subgroup of $\mathcal{G}$) a Galois extension of p-power degree of an abelian field, the Iwasawa μ-invariant of F_∞/F_1 vanishes and so $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_m))$ is bounded independently of m (by [15, Prop. 13.23]).

At this stage we know that, for any sufficiently large integer b, the extensions F_m/E_m all belong to $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$. It is thus enough to note that, since the number of complex places of F_m is $[F_m : \mathbb{Q}]/2$, one has $\mathrm{rk}(\mathrm{Gal}(M^{p,\mathrm{ab}}_{F_m,\Sigma}/F_m)_{\mathrm{tf}}) \geq [F_m : \mathbb{Q}]/2 - 1$ and, for any non-negative integer a, also $\mathrm{rk}((\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F_m,\Sigma}))_{\mathrm{tf}}) \geq [F_m : \mathbb{Q}]/2$. □

4.2. In this section we explain how techniques developed in [6] can be used to make the structure results of Corollary 4.1 more precise in the case of cyclic extensions of p-power degree. We thus fix such an extension F/k, set $G := G_{F/k}$ and $[F : k] = p^n$ and for each integer i with $0 \leq i \leq n$, let F_i denote the unique extension of k in F of degree p^i.

For any non-negative integer a and intermediate field F_i of F/k we write $\mathrm{cap}^a_{F,i,\Sigma}$ for the 'p-primary capitulation kernel'

$$\begin{cases} \mathbb{Z}_p \otimes_{\mathbb{Z}} \ker(\mathrm{Cl}_\Sigma(F_i) \to \mathrm{Cl}_\Sigma(F)), & \text{if } a = 0, \\ \mathbb{Z}_p \otimes_{\mathbb{Z}} \ker(K_{2a}(\mathcal{O}_{F_i,\Sigma}) \to K_{2a}(\mathcal{O}_{F,\Sigma})), & \text{if } a > 0 \end{cases}$$

where the arrows denote the respective homomorphisms that are induced by the ring inclusion $\mathcal{O}_{F_i,\Sigma} \subseteq \mathcal{O}_{F,\Sigma}$

We write $r_{1,E}$ and $r_{2,E}$ for the number of real and complex places of a number field E.

Theorem 4.3. *Fix a non-negative integer a for which $H^0(G_{k,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ vanishes.*

Then the isomorphism class of the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma})$ is uniquely determined (in the sense described in [6, §3.2.1]*) by the diagram*

$$\mathrm{cap}^a_{F,0,\Sigma} \leftrightarrows \mathrm{cap}^a_{F,1,\Sigma} \leftrightarrows \cdots \leftrightarrows \mathrm{cap}^a_{F,n-1,\Sigma}, \tag{17}$$

where the upper and lower arrows are the homomorphisms induced by the field-theoretic norms $F_{i+1}^\times \to F_i^\times$ and inclusions $\mathcal{O}_{F_i,\Sigma} \subseteq \mathcal{O}_{F_{i+1},\Sigma}$ respectively, together with knowledge of

$$\begin{cases} \#\Sigma_{F_i} \text{ for each } i \text{ with } 0 \leq i \leq n, & \text{if } a = 0 \\ r_{2,k}, & \text{if } a > 0 \text{ and } a \text{ is odd} \\ r_{1,k} + r_{2,k}, & \text{if } a > 0 \text{ and } a \text{ is even.} \end{cases}$$

Proof. Fix a non-negative integer a and an integer i with $0 \leq i \leq n$. Then the assumed vanishing of $H^0(G_{k,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ implies $H^0(G_{F_i,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ vanishes. This implies $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma})$ is $\mathbb{Z}_p$-free and also combines with the description of Proposition 2.3(ii), the exact sequence (6) and the isomorphisms $H^2(\mathcal{O}_{F_i,\Sigma}, \mathbb{Z}_p(1))_{\mathrm{tor}} \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Cl}_\Sigma(F_i)$ and $H^2(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1+a)) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a}(\mathcal{O}_{F,\Sigma})$ for $a > 0$ that are respectively induced by class field theory and the canonical Chern class homomorphism, to imply that the complex $C_i(a) := R\Gamma_c(\mathcal{O}_{F_i,\Sigma}, \mathbb{Z}_p(-a))$ is acyclic outside one and two and is such that there is a canonical short exact sequence

$$0 \to B_i^a \to H^2(C_i(a))) \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F_i,\Sigma}))^* \to 0$$

with $B_i^0 := (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Cl}_\Sigma(F_i))^\vee$ and $B_i^a := (\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a}(\mathcal{O}_{F,\Sigma}))^\vee$ for $a > 0$. In addition, since $C_i(a)$ is acyclic in degrees greater than two the descent isomorphism $\mathbb{Z}_p[G_{F_i/k}] \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} C_n(a) \cong C_i(a)$ from Proposition 2.3(i) induces an identification $H_0(G_{F/F_i}, H^2(C_n(a))) \cong H^2(C_i(a))$.

Given these facts, one can simply follow the argument of [6, §3.2.1] (with the terms $\overline{X}$ and $Ш_i$ in loc. cit. respectively replaced by $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))^*$ and B_i^a) to deduce that the isomorphism class of the $\mathbb{Z}_p[G]$-lattice $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))^*$, and hence also of $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))_{\mathrm{tf}} = \mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma})$, is uniquely determined, in a sense made precise in loc. cit., by the (Pontryagin dual of the) diagram (17) together with knowledge of the rank $r_i^a := \mathrm{rk}(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F_i,\Sigma}))$ for each i.

The claimed result thus follows from the fact that for each i one has $r_i^0 = \#\Sigma_{F_i} - 1$ and if $a > 0$ is odd, respectively even, also $r_i^a = r_{2,F_i} = p^i \cdot r_{2,k}$, respectively $r_i^a = r_{1,F_i} + r_{2,F_i} = p^i(r_{1,k} + r_{2,k})$. □

Remark 4.4. An important special case of Theorem 4.3 arises when $\mathrm{cap}^a_{F,i,\Sigma}$ vanishes for each i with $0 \leq i < n$. In this case a closer analysis of the argument in [6, §3.2.1] shows that $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma})$ is a free $\mathbb{Z}_p[G]$-module if $a > 0$ and is isomorphic to the direct sum $\bigoplus_{j=0}^{j=n} \mathbb{Z}_p[G_{F_j/k}]^{m_j}$ if $a = 0$, where the non-negative integers m_j are determined by the equalities $\sum_{j=0}^{j=n} m_j \cdot p^{\min\{j,b\}} = \#\Sigma_{F_b} - 1$ for each b with $0 \leq b \leq n$.

4.3. In this final section we show that, in special cases, our approach can be used to make the result of Theorem 4.3 much more explicit.

To do this we fix an odd prime p and for each number field k and non-negative integer n write k_n for the unique subfield of k_{cyc} that has degree p^n over k. For each such n we also fix a primitive p^n-th root of unity ζ_n in $\mathbb{Q}^c$ with $\zeta_n^p = \zeta_{n-1}$.

We assume throughout that the following hypothesis is satisfied.

Hypothesis 4.5. *k is disjoint from $\mathbb{Q}_{\mathrm{cyc}}$ and does not contain a p-th root of $\omega \cdot p$ for any root of unity ω.*

Remark 4.6. It is straightforward to check that this hypothesis is satisfied if, for example, the absolute ramification index of some p-adic place of k is prime to p.

We write Σ for the set of places of k that are either archimedean or p-adic and for each n we study the structure of the $\mathbb{Z}_p[G_{k_n/k}]$-module $H^1(\mathcal{O}_{k_n,\Sigma}, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{k_n,\Sigma}^\times$.

To do this we define an element of $\mathcal{O}_{k_n,\Sigma}^\times$ by setting

$$\epsilon_n := \mathrm{Norm}_{\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}_n}(\zeta_n - 1).$$

Proposition 4.7. *Let k be any number field satisfying Hypothesis 4.5. Then for each natural number n the element ϵ_n generates a $\mathbb{Z}_p[G_{k_n/k}]$-submodule of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma}$ that is both a direct summand and isomorphic to $\mathbb{Z}_p[G_{k_n/k}]$.*

Proof. The fact that k is disjoint from $\mathbb{Q}_{\mathrm{cyc}}$ implies that the restriction map $G_{k_n/k} \to G_{\mathbb{Q}_n/\mathbb{Q}}$ is bijective and hence that $\mathrm{Norm}_{k_n/k}(\epsilon_n) = \mathrm{Norm}_{\mathbb{Q}_n/\mathbb{Q}}(\epsilon_n) = p$.

Since k does not contain a p-th root of $\omega \cdot p$ for any root of unity ω, this equality implies that the image $\epsilon^0_{n,p}$ of $\mathrm{Norm}_{k_n/k}(\epsilon_n)$ in the lattice $(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k,\Sigma})_{\mathrm{tf}}$ is not divisible by p.

We set $\Gamma_n := G_{k_n/k}$, $U_{n,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma}$ and $\mu_{n,p} := (U_{n,p})_{\mathrm{tor}}$. Then by applying the functor $H^0(\Gamma_n, -)$ to the tautological exact sequence $1 \to \mu_{n,p} \to U_{n,p} \to (U_{n,p})_{\mathrm{tf}} \to 1$ one obtains an exact sequence of abelian groups

$$0 \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k,\Sigma})_{\mathrm{tf}} \xrightarrow{\iota_{n,p}} H^0(\Gamma_n, (U_{n,p})_{\mathrm{tf}}) \to H^1(\Gamma_n, \mu_{n,p}).$$

Let us assume for the moment that the group $H^1(\Gamma_n, \mu_{n,p})$ vanishes. Then the sequence shows that $\iota_{n,p}$ is bijective and so the above considerations imply that the image $\epsilon_{n,p}$ of ϵ_n in $(U_{n,p})_{\mathrm{tf}}$ is such that $\mathrm{tr}_{\Gamma_n}(\epsilon_{n,p}) = \iota_{n,p}(\epsilon^0_{n,p})$ is not divisible by p in $H^0(\Gamma_n, (U_{n,p})_{\mathrm{tf}})$. Given this, we can apply Proposition 2.1 to the data $G = \Gamma_n, X = (U_{n,p})_{\mathrm{tf}}, t = 1$ and $x_1 = \epsilon_{n,p}$ to deduce that $\epsilon_{n,p}$ generates a $\mathbb{Z}_p[G_{k_n/k}]$-submodule of $(U_{n,p})_{\mathrm{tf}}$ that is both a direct summand and isomorphic to $\mathbb{Z}_p[G_{k_n/k}]$. It is then clear that ϵ_n generates a $\mathbb{Z}_p[G_{k_n/k}]$-submodule of $U_{n,p}$ that is a direct summand and isomorphic to $\mathbb{Z}_p[G_{k_n/k}]$, as claimed.

It therefore suffices to check $H^1(\Gamma_n, \mu_{n,p})$ vanishes and this is clear if k does not contain ζ_1 since then the group $\mu_{n,p}$ vanishes.

If, on the other hand, k contains ζ_1, then (as k is disjoint from $\mathbb{Q}_{\mathrm{cyc}}$) the torsion subgroup $H^0(\Gamma_n, \mu_{n,p})$ of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k,\Sigma}$ is generated by ζ_1 and the group $\mu_{n,p}$ by ζ_{n+1}. Since $\mathrm{Norm}_{k_n/k}(\zeta_{n+1}) = \zeta_1$ this shows that the Tate cohomology group $\hat{H}^0(\Gamma_n, \mu_{n,p})$ vanishes, and hence also (since Γ_n is cyclic) that the group $H^1(\Gamma_n, \mu_{n,p})$ vanishes, as required. □

This result implies some very explicit structural results. To explain this we start with an easy special case.

Corollary 4.8. *Let k be $\mathbb{Q}$ or an imaginary quadratic field in which p is not split. Then for each natural number n the $\mathbb{Z}_p[G_{k_n/k}]$-module $(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma})_{\mathrm{tf}}$ is free of rank one.*

Proof. The stated conditions on k imply it satisfies Hypothesis 4.5 and in addition that k_n has p^n archimedean places and a unique p-adic place and hence that $\mathrm{rk}(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma})$ is equal to $(p^n - 1) + 1 = \mathrm{rk}(\mathbb{Z}_p[G_{k_n/k}])$. In these cases, therefore, the result of Proposition 4.7 implies $(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma})_{\mathrm{tf}}$ is equal to $\mathbb{Z}_p[G_{k_n/k}] \cdot \epsilon_{n,p}$ and so is a free $\mathbb{Z}_p[G_{k_n/k}]$-module of rank one. □

In the rest of this section we consider the next simplest case by assuming that k is a real quadratic field in which p is inert.

In this case k satisfies Hypothesis 4.5 and $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma}$ is a free $\mathbb{Z}_p$-module of rank $2p^n$ so that Proposition 4.7 implies there is an isomorphism of $\mathbb{Z}_p[k_n/k]$-modules

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^\times_{k_n,\Sigma} \cong \mathbb{Z}_p[G_{k_n/k}] \oplus V_{k_n/k} \tag{18}$$

with $\mathrm{rk}(V_{k_n/k}) = p^n$.

For each pair of integers i and j with $0 \leq i \leq j \leq n$ we now write

$$\mathrm{cap}^{k_j}_{k_i,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \ker(\mathrm{Cl}(k_i) \to \mathrm{Cl}(k_j))$$

for the p-primary part of the kernel of the classical 'capitulation' map on ideal classes. Then, in terms of the notation in Theorem 4.3, for all such i and j there are natural isomorphisms

$$\hat{H}^{-1}(G_{k_j/k_i}, V^*_{k_j/k}) \cong \hat{H}^{-1}(G_{k_j/k_i}, (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_j,\Sigma})^*) \cong (\mathrm{cap}^0_{k_j,i,\Sigma})^{\vee} \cong (\mathrm{cap}^{k_j}_{k_i,p})^{\vee} \tag{19}$$

where the first follows directly from the $\mathbb{Z}_p$-linear dual of the isomorphism (18) (with n replaced by j), the second from the argument of [6, Prop. 3.1] (modified as per the $a = 0$ case of the proof of Theorem 4.3) and the third follows trivially from the fact that p is inert in k and so the unique prime ideals of k_i and k_j above p are principal.

To further analyse the structure of $V_{k_n/k}$ we now restrict to the case $n = 2$ and use the Heller-Reiner classification of indecomposable $\mathbb{Z}_p[G_{k_2/k}]$-lattices from [9]. In fact, for our purposes, the relevant properties of these lattices are conveniently displayed in [14, Table 2] and so in the following result we shall use the same notation for indecomposable lattices as in loc. cit.

Corollary 4.9. *Let k be a real quadratic field in which p is inert. Set $G := G_{k_2/k}$ and write Q for the quotient of G of order p and Z_p for the set of integers i with $1 \leq i \leq p-2$. For integers a and b in $\{0,1,2\}$ with $a \leq b$ abbreviate $\mathrm{cap}^{k_b}_{k_a,p}$ to cap^b_a.*

Then there is an isomorphism of $\mathbb{Z}_p[G]$-lattices $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_2,\Sigma} \cong \mathbb{Z}_p[G] \oplus V^*$ where the lattice V is such that precisely one of the following cases arises.

(i) $V = (R_2, R_1 \oplus \mathbb{Z}_p, 1 \oplus 1)$ *and* $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = |\mathrm{cap}^2_1| = p$.
(i)$_i$ $V = (R_2, R_1 \oplus \mathbb{Z}_p, 1 \oplus \lambda^i_0)$ *with* $i \in Z_p$, $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = p$ *and* $|\mathrm{cap}^2_1| = p^i$.
(ii) $V = \mathbb{Z}_p[G]$ *and* $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = |\mathrm{cap}^2_1| = 1$.
(ii)$_i$ $V = (R_2, \mathbb{Z}_p[Q], \lambda^i_0)$ *with* $i \in Z_p \cup \{p-1\}$, $|\mathrm{cap}^1_0| = 1$, $|\mathrm{cap}^2_0| = p$ *and* $|\mathrm{cap}^2_1| = p^i$.
(iii) $V = (R_2, \mathbb{Z}_p, 1) \oplus R_1$, $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = p$ *and* $|\mathrm{cap}^2_1| = p^{p-1}$.
(iv) $V = R_2 \oplus \mathbb{Z}_p[Q]$, $|\mathrm{cap}^1_0| = 1$, $|\mathrm{cap}^2_0| = p$ *and* $|\mathrm{cap}^2_1| = p^p$.
(v) $V = R_2 \oplus R_1 \oplus \mathbb{Z}_p$, $|\mathrm{cap}^1_0| = p$, $\mathrm{cap}^2_0 \cong (\mathbb{Z}/p)^2$ *and* $|\mathrm{cap}^2_1| = p^p$.
(vi) $V = (R_2, R_1, 1)$, $|\mathrm{cap}^1_0| = p$, $\mathrm{cap}^2_0 \cong \mathbb{Z}/p^2$ *and* $|\mathrm{cap}^2_1| = p$.
(vi)$_i$ $V = (R_2, R_1, \lambda^i_0)$ *with* $i \in Z_p$, $|\mathrm{cap}^1_0| = p$, $\mathrm{cap}^2_0 \cong (\mathbb{Z}/p)^2$ *and* $|\mathrm{cap}^2_1| = p^{i+1}$.

Proof. The given conditions on k imply it satisfies Hypothesis 4.5 and so (18) gives an isomorphism of the form $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_2,\Sigma} \cong \mathbb{Z}_p[G] \oplus V^*$ with $V = V^*_{k_2/k}$. For each $a \in \{0,1,2\}$ this decomposition implies that $\mathrm{rk}(V^{J_a}) = \mathrm{rk}(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_{2-a},\Sigma}) - \mathrm{rk}(\mathbb{Z}_p[G/J_a]) = p^{2-a}$, where we write J_a for the subgroup of G of order p^a.

The stated list of possibilities for V is then obtained by explicitly comparing these rank conditions and the cohomology computations in (19) with the basic properties of the set of isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices, as recorded in [14, Table 2]. Since this process is entirely routine we leave all further details to the reader. □

Remark 4.10.
(i) Inspection of the list in Corollary 4.9 leads to several concrete observations about both Galois structures and capitulation kernels (under the given hypotheses). For example, the list combines with (18) to imply $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_2,\Sigma}$ decomposes, in all cases, as a direct sum of

ideals of $\mathbb{Z}_p[G]$ (whilst the Heller-Reiner classification implies that this is not true of every $\mathbb{Z}_p[G]$-lattice). It also implies that

$$\mathrm{cap}_0^2 = 0 \Longleftrightarrow \mathrm{cap}_1^2 = 0 \Longleftrightarrow V \cong \mathbb{Z}_p[G]$$

(as occurs, for example, whenever the class number of k is prime to p), that

$$\mathrm{cap}_0^1 = 0 \Longleftrightarrow V \cong \mathbb{Z}_p[G] \text{ or } V \cong R_2 \oplus \mathbb{Z}_p[Q] \text{ or } V \cong (R_2, \mathbb{Z}_p[Q], \lambda_0^i)$$

for some i in Z_p, that

$$\mathrm{cap}_0^2 \text{ has an element of order } p^2 \Longleftrightarrow |\mathrm{cap}_1^2| \leq |\mathrm{cap}_0^1| \Longleftrightarrow V \cong (R_2, R_1, 1)$$

and that in all cases one has $|\mathrm{cap}_0^2| \leq p \cdot |\mathrm{cap}_0^1|$.

(ii) Corollary 4.9 also shows that the structure of the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{k_2,\Sigma}^{\times}$ is completely determined by the abstract structures of the groups $\mathrm{cap}_{k_a,p}^{k_2}$ and $\mathrm{cap}_{k,p}^{k_1}$. In particular, contrary to the more general result of Theorem 4.3, in this case one does not require any information about maps between these groups.

References

[1] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, in The Grothendieck Festschrift Vol I, Progress in Math. Vol 86, Birkhäuser (1990), 333-400.

[2] D. Burns, On the Galois structure of arithmetic cohomology III: Selmer groups of critical motives, to appear in Kyoto J. Math.

[3] D. Burns, M. Flach, Motivic L-functions and Galois module structures, Math. Ann. **305** (1996) 65-102.

[4] D. Burns, M. Flach, Equivariant Tamagawa numbers for motives with (non-commutative) coefficients, Doc. Math. **6** (2001) 501-570.

[5] D. Burns, A. Kumon, On the Galois structure of arithmetic cohomology II: ray class groups, submitted for publication.

[6] D. Burns, D. Macias Castillo, C. Wuthrich, On the Galois structure of Selmer groups, Int. Math. Res. Notices **2015** (2015) 11909-11933.

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

[8] M. Flach, Euler characteristics in relative K-groups, Bull. London Math. Soc. **32** (2000) 272-284.

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

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

[11] K. Iwasawa, On the μ-invariants of $\mathbb{Z}_\ell$-extensions, In: Number Theory, Algebraic Geometry and Commutative Algebra, Kinokuniya, Tokyo 1973, 1-11.

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

[13] J. Neukirch, On solvable extensions of number fields, Invent. Math. **53** (1979), 135-164.

[14] M. Rzedowski-Calderón, G. D. Villa Salvador, M. L. Madan, Galois module structure of rings of integers, Math. Zeit. **204** (1990) 401-424.

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

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