Nagoya Math. J., **239** (2020), 294–321
DOI 10.1017/nmj.2018.41

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, realizations, 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 realization 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.

Received December 15, 2016. Accepted August 5, 2017.
2010 Mathematics subject classification. 11R34, 11R23, 20C11.

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, both in relatively simple cases and in more involved Iwasawa-theoretic contexts (see, for example, the recent work of Khare and Wintenberger [15]).

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 [7] 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 [13]).

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 specialization, 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 Section 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. First, in joint work with Kumon [6], 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. Second, by using Selmer complexes defined by Nekovář in the role played here by compactly supported p-adic cohomology complexes, in [3] 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 [7].

§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 k_Σ for the maximal extension of k in k^c that is unramified outside Σ and set $G_{k,\Sigma} := \mathrm{Gal}(k_\Sigma/k)$.

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

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

We regard T as a left $\mathbb{Z}_p[G_{k,\Sigma}]$-module via ρ and write $T^*(1)$ for the linear Kummer dual $\mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$, regarded as a (left) $\mathbb{Z}_p[G_{k,\Sigma}]$-module via the action given by $(\sigma \circ \theta)(t) = \sigma(\theta(\rho(\sigma)^{-1}(t)))$ for all σ in $G_{k,\Sigma}$, θ in $T^*(1)$ and t in T.

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 both 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 $H^i(\mathrm{Spec}(\mathcal{O}_{L,\Sigma})_{\text{ét}}, B)$ 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 shall 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 pth roots of unity in k^c. We also write k_T for the finite Galois extension of $k(\mu_p)$ that corresponds to the kernel of the action of $G_{k(\mu_p),\Sigma}$ on T/p that is induced by ρ, and hence also to the kernel 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*

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

and

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

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

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

for integers $m^i_{F/E,T}$ and $m^i_{F/E,T,c}$ depending 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 Section 2.3.

This result is of interest as the dimensions of the $\mathbb{Q}_p$-spaces spanned by $H^i(\mathcal{O}_{F,\Sigma}, T)$ 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 Section 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 behavior of class groups (for details see Corollary 3.1).

In Section 3 we also deduce the following result showing that Theorem 1.1 gives concrete information about changes in the dimension $\mathrm{rk}(\mathrm{Sel}_F(T))$ of the $\mathbb{Q}_p$-space spanned by the Bloch–Kato Selmer group $\mathrm{Sel}_F(T)$ 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–Shafarevich group over F is finite, then $\mathrm{rk}(\mathrm{Sel}_F(T))$ coincides with the dimension of the rational space spanned by 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 k_Σ 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*

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

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 Section 3.2.

Remark 1.3. The degree of $k_{\Sigma,r}$ over k can be large (see the proof of Corollary 3.1). 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

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

This strongly restricts the structure of $\mathrm{Sel}_F(T)$. For instance, if F/k has degree p, then a classical result of Diederichsen [10] implies there exist nonnegative integers $a_F(T), b_F(T)$ and $c_F(T)$ and an isomorphism of $\mathbb{Z}_p[G_{F/k}]$-modules of the form

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

where $\mathrm{Sel}_F(T)_{\mathrm{tf}}$ denotes the quotient of $\mathrm{Sel}_F(T)$ by its torsion subgroup, and the above inequalities now imply that

$$-m_1/(p-1) \leqslant b_F(T) - c_F(T) \leqslant m_2/(p-1).$$

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

For any abelian group X we write $X[p]$ for the subgroup of X comprising elements annihilated by p. For any finitely generated $\mathbb{Z}_p$-module X we set $\mathrm{rk}(X) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} X)$ and note that $\mathrm{rk}_p(X) = \dim_{\mathbb{F}_p}(X[p]) + \mathrm{rk}(X)$. In the sequel we also often use, without explicit comment, the fact that for any exact sequence of finitely generated $\mathbb{Z}_p$-modules $X_1 \xrightarrow{\theta_1} X_2 \xrightarrow{\theta_2} X_3$ one has $\mathrm{rk}_p(\mathrm{im}(\theta_i)) \leqslant \mathrm{rk}_p(X_2) \leqslant \mathrm{rk}_p(X_1) + \mathrm{rk}_p(X_3)$ 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 $\mathbb{Z}[G]$. We recall that a "$\mathbb{Z}_p[G]$-lattice" is a finitely generated $\mathbb{Z}_p[G]$-module that is torsion-free.

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 group of p-power order, X a $\mathbb{Z}_p[G]$-lattice and $\{x_i\}_{1\leqslant i\leqslant t}$ a finite subset of X. Then the images in $H^0(G, X)/p$ of the elements $\{\mathrm{tr}_G(x_i)\}_{1\leqslant i\leqslant t}$ are linearly independent over $\mathbb{F}_p$ if and only if the $\mathbb{Z}_p[G]$-submodule of X that is generated by $\{x_i\}_{1\leqslant i\leqslant t}$ 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 $\{x_i\}_{1\leqslant i\leqslant t}$.

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 $\{\mathrm{tr}_G(x_i)\}_{1\leqslant i\leqslant t}$. 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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 $\{b_i\}_{1\leqslant i\leqslant t}$ 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 nontrivial, then $H^0(G, \ker(\overline{\psi}))$ is also nontrivial (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 nontriviality 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 $\{\mathrm{tr}_G(x_i)\}_{1\leqslant i\leqslant t}$ 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 $\{\mathrm{tr}_G(x_i)\}_{1\leqslant i\leqslant t}$ 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 (by, for example, [8, Theorem (10.29)]), 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 $\mathrm{tr}_G(I)$ is contained in $p \cdot H^0(G, I)$ 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

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

with the second arrow denoting the natural diagonal localization 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*

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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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

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

(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, setting $C := R\Gamma(\mathcal{O}_{F,\Sigma}, T^*(1))$, the Artin–Verdier duality theorem implies there is a canonical exact triangle in $D(\mathbb{Z}_p[G])$

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

(see, for example, [5, Lemma 12b]). By using the universal coefficient spectral sequence

$$E_2^{p,q} = \operatorname{Ext}^p_{\mathbb{Z}_p}(H^{3-q}(C), \mathbb{Z}_p) \Longrightarrow H^{p+q}(R\operatorname{Hom}_{\mathbb{Z}_p}(C, \mathbb{Z}_p[-3]))$$

(cf. [19, III.4.6.10]) one can also compute the cohomology groups of the third term in the above triangle in terms of those of C.

In this way one finds 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 [11, Theorem 5.1] and of Flach and the present author [5, Lemma 7], respectively. ∎

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 $\mathrm{rk}(B_F(T))$ is equal to $\#J \cdot \mathrm{rk}(B_{F^J}(T))$.*

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

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

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 postcomposition with elements of Σ_v) and G acts only on the second factor (via precomposition 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

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

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 the numbers $\mathrm{rk}(T)$ and $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T))$ are both 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 $H^2_c(\mathcal{O}_{F,\Sigma}, T)$.*

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 $H^2(\mathcal{O}_{F,\Sigma},T)/p\cong H^2(\mathcal{O}_{F,\Sigma},T/p)$, and hence implies $\mathrm{rk}_p(H^1(\mathcal{O}_{F,\Sigma},T)[p])\leqslant \mathrm{rk}(T)$ 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 $\mathrm{rk}_p(H^1(\mathcal{O}_{F,\Sigma},T)[p])\leqslant \mathrm{rk}(T)$ combines with the exact sequences (6) (with T replaced by $T^*(1)$) to give two consequences.

First, 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 $m^3_{F/E,T,c}=2$.

Second, 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

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

Here 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 follows by combining the canonical short exact sequence

$$0\to H^1(\mathcal{O}_{F_T,\Sigma},\mathbb{G}_m)/p\to H^2(\mathcal{O}_{F_T,\Sigma},\mu_p)\to H^2(\mathcal{O}_{F_T,\Sigma},\mathbb{G}_m)[p]\to 0$$

with the fact $H^1(\mathcal{O}_{F_T,\Sigma},\mathbb{G}_m)=\mathrm{Cl}_\Sigma(F_T)$ and an explicit computation of $H^2(\mathcal{O}_{F_T,\Sigma},\mathbb{G}_m)$ using class field theory (as, for example, in [16, Chapter III, Example 2.22, Case (f)]).

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 $m^1_{F/E,T,c} = m^2_{F/E,T}$. ∎

In the sequel, for any finite group Γ, any Γ-module Y and any integer i we write $\hat{H}^i(\Gamma, Y)$ for the Tate cohomology group of Y in degree i, as discussed for example in [1, Section 6].

Since Lemma 2.5 allows us to focus on the module $H^2_c(\mathcal{O}_{F,\Sigma}, T)$ we now set

$$X := H^2_c(\mathcal{O}_{F,\Sigma}, T).$$

We also abbreviate $G_{F/E}$ to G.

LEMMA 2.6. *Theorem 1.1 is valid if and only if* $\mathrm{rk}_p(\hat{H}^0(G, X_{\mathrm{tf}}))$ *is bounded by an explicit multiple of* $\mathrm{rk}(T)$ *depending 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

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

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

To analyse X_{tf} we fix a Sylow p-subgroup P of G and note the natural restriction map $\hat{H}^0(G, X_{\mathrm{tf}}) \to \hat{H}^0(P, X_{\mathrm{tf}})$ is bijective (as a consequence of [1, Proposition 8]).

We set

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

note that the integer

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

is nonnegative and choose a set of elements $\{x_i\}_{1 \leqslant i \leqslant d}$ of X such that the images in $H^0(P, X_{\mathrm{tf}})/p$ of the elements $\mathrm{tr}_P(x_i)$ are linearly independent over $\mathbb{F}_p$.

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

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

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

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

(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

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

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

$$\mathbb{Z}_p[G]\otimes_{\mathbb{Z}_p[P]} X \cong X_1\oplus X_2\tag{11}$$

where $X_1 := \mathbb{Z}_p[G]\otimes_{\mathbb{Z}_p[P]} X'$ is free and $X_2 := \mathbb{Z}_p[G]\otimes_{\mathbb{Z}_p[P]} X''$ satisfies

$$\mathrm{rk}(X_2) = [G:P]\cdot\mathrm{rk}(X'') \leqslant [G:P]\cdot\mathrm{rk}(T)\cdot(m^2_{F/E,T}+1) + \#G\cdot r_p.\tag{12}$$

We next claim that X_{tf} is a direct summand of the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G]\otimes_{\mathbb{Z}_p[P]} X_{\mathrm{tf}}$. To show this write t for the index of P in G and choose a set of coset representatives $\{c_i\}_{1\leqslant i\leqslant t}$ for P in G. Then t is prime to p

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

and the homomorphism of $\mathbb{Z}_p[G]$-modules $X_{\mathrm{tf}} \to \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} X_{\mathrm{tf}}$ that sends each x to $t^{-1}\sum_{i=1}^{i=t} c_i^{-1} \otimes c_i(x)$ is a section to the natural surjective map $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[P]} X_{\mathrm{tf}} \to X_{\mathrm{tf}}$, as required.

In particular, if one decomposes X_{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 nonprojective indecomposable modules, then the isomorphism (11) and upper bound (12) combine with the Krull–Schmidt theorem to imply that Π' is isomorphic to a direct summand of X_2 and hence that

$$\mathrm{rk}_p(X_2) \leqslant [G:P] \cdot \mathrm{rk}(T) \cdot (m_{F/E,T}^2 + 1) + \#G \cdot r_p.$$

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. *One has*

$$\begin{aligned}&\mathrm{rk}_p(\hat{H}^0(G, X_{\mathrm{tf}}))\\ &\quad\leqslant \mathrm{rk}(T) \cdot \#G \cdot (2 + (1 + \#G)(\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + \#\Sigma_{f,F_T} - 1)).\end{aligned}$$

Proof. Since Proposition 2.3 implies $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ is perfect over $\mathbb{Z}_p[G]$ and acyclic outside degrees one, two and three a standard argument of homological algebra (as, for example, in [9, Rapport, Lemma 4.7]) shows that this complex is isomorphic in $D(\mathbb{Z}_p[G])$ to a complex of finitely generated $\mathbb{Z}_p[G]$-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, the modules Q^2 and Q^3 are free and Q^1 is cohomologically trivial for G. This representative of $R\Gamma_c(\mathcal{O}_{F,\Sigma}, T)$ in turn gives rise to tautological short exact sequences of $\mathbb{Z}_p[G]$-modules

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

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

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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

exact sequence

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

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

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

$$\begin{aligned}
&\mathrm{rk}_p(\hat{H}^0(G, X)) + \mathrm{rk}_p(H^1(G, X_{\rm tor}))\\
&\quad\leqslant \mathrm{rk}_p(\hat{H}^{-2}(G, X^3)) + \mathrm{rk}_p(\hat{H}^2(G, H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*)) + \mathrm{rk}_p(H^1(G, X_{\rm tor}))\\
&\quad\leqslant \#G \cdot \mathrm{rk}_p(X^3) + (\#G)^2 \cdot \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*) + \#G \cdot \mathrm{rk}_p(X_{\rm tor})\\
&\quad\leqslant \#G \cdot [\mathrm{rk}_p(X^3) + \#G \cdot \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1))^*) + \mathrm{rk}_p(H^2(\mathcal{O}_{F,\Sigma}, T^*(1)))]\\
&\quad\leqslant \#G \cdot \mathrm{rk}(T) \cdot [2 + (\#G + 1)(\mathrm{rk}_p(\mathrm{Cl}_\Sigma(F_T)) + \#\Sigma_{f,F_T} - 1)],
\end{aligned}$$

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

LEMMA 2.8. *Let $\mathcal{G}$ be a finite group and X a finitely generated $\mathbb{Z}_p[\mathcal{G}]$-module. Then for each integer i one has*

$$\mathrm{rk}_p(\hat{H}^i(\mathcal{G}, X)) \leqslant (\#\mathcal{G})^{n_i} \cdot \mathrm{rk}_p(X)$$

with n_i equal to i if $i \geqslant 0$ and to $-(i+1)$ if $i < 0$.

Proof. The tensor product $X \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}]$ 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

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

These sequences imply $\mathrm{rk}_p(\mathrm{cok}(\iota_X))$ and $\mathrm{rk}_p(\ker(\pi_X))$ are both at most $\mathrm{rk}_p(X \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}]) = \#\mathcal{G} \cdot \mathrm{rk}_p(X)$. In addition, since $X \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathcal{G}]$ is a cohomologically trivial $\mathcal{G}$-module, the long exact cohomology sequences

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

associated to these sequences induce isomorphisms

$$(13)\ \hat{H}^i(\mathcal{G}, X) \cong \hat{H}^{i-1}(\mathcal{G}, \mathrm{cok}(\iota_X)) \quad \text{and} \quad \hat{H}^i(\mathcal{G}, X) \cong \hat{H}^{i+1}(\mathcal{G}, \ker(\pi_X)).$$

In particular, if $i \geqslant 0$, respectively $i < 0$, then after repeatedly applying isomorphisms of the first, respectively second, kind in (13) one finds that

$$\mathrm{rk}_p(\hat{H}^i(\mathcal{G}, X)) = \begin{cases} \mathrm{rk}_p(\hat{H}^0(\mathcal{G}, X_i)) & \text{if } i \geqslant 0, \\ \mathrm{rk}_p(\hat{H}^{-1}(\mathcal{G}, X_i)) & \text{if } i < 0, \end{cases}$$

where in each case X_i is a $\mathbb{Z}_p[\mathcal{G}]$-module with $\mathrm{rk}_p(X_i) \leqslant (\#\mathcal{G})^{n_i} \cdot \mathrm{rk}_p(X)$.

The claimed result thus follows from the last displayed equality since both of the groups $\hat{H}^0(\mathcal{G}, X_i)$ and $\hat{H}^{-1}(\mathcal{G}, X_i)$ are, by definition, subquotients of X_i and hence of p-rank at most $\mathrm{rk}_p(X_i)$. □

§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 behavior of class groups.

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

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 k_Σ 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 $\mathrm{rk}_p(\mathrm{Cl}_\Sigma(k_{\Sigma,r}F)) + \#\Sigma_{f,F} \leqslant b$, 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 $H_c^i(\mathcal{O}_{F,\Sigma}, T)_{\mathrm{tf}}$ 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^{i_r} 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 k_Σ of exponent dividing p^{i_r}.

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 k_Σ^p of exponent dividing p^{i_r} and, since $G_{k_\Sigma^p/k}$ 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 k_Σ 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, by the Jordan–Zassenhaus theorem [8, Theorem (24.2)], 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 $T = \mathbb{Z}_p(r)$ for varying integers r, 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 $[E : E \cap k_{\mathrm{cyc}}] \leqslant e$. 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 [14]) one can show $G_{L_\Sigma^{p,\mathrm{ab}}/L}$ is a finitely generated $\mathbb{Z}_p$-module for each such L. By using [20, Proposition 13.23] this gives a finite upper bound

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 [2]. Then the Bloch–Kato Selmer group $\mathrm{Sel}_L(W)$ of W over L is defined to be the kernel of the natural diagonal localization 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 [4, 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

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

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

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

(for example, this follows directly from [4, (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 $[L_w : \mathbb{Q}_p] \cdot \mathrm{rk}(T)$).

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 one has $\mathrm{rk}(P^2_{F/E,T,c}) = \#G \cdot \mathrm{rk}(H^0(G, P^2_{F/E,T,c}))$. 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

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

and hence

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

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

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

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

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

and

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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

To deduce Corollary 1.2 from these explicit inequalities it is enough to note 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 $T = \mathbb{Z}_p(r)$ for varying integers 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

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

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 the extension 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 arising from either $\mathrm{Gal}(F_\Sigma^{p,\mathrm{ab}}/F)_{\mathrm{tf}}$ or $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))_{\mathrm{tf}}$ for any nonnegative 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

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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

Here the first isomorphism is induced by Kummer theory, the second by the fact that the Chern class homomorphism

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}) \to H^1(\mathcal{O}_{F,\Sigma}, \mathbb{Z}_p(1+a))$$

is bijective (by the known validity of the Quillen–Lichtenbaum conjecture – see Weibel [21]) and the third by the Artin–Verdier duality theorem. □

In the sequel, for each natural number m and each number field E we shall write E^m for the field generated over E by a primitive p^mth root of unity.

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* $\mathrm{Gal}(F_\Sigma^{p,\mathrm{ab}}/F)_{\mathrm{tf}}$*, and of* $(\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma}))_{\mathrm{tf}}$ *for any nonnegative 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 [17, Corollary 2, p. 156]). We write Σ for the set of rational places comprising ∞, p and those primes that ramify in $F/\mathbb{Q}$.

We claim that for any large enough integer b, all of the extensions $F^m/\mathbb{Q}^m$ as m varies belong to $\mathrm{Ext}(\mathcal{G}, \Sigma, b)$.

At the outset it is clear $\mathbb{Q}^m$ contains μ_p, $F^m/\mathbb{Q}^m$ is unramified outside Σ and, as $\mathbb{Q}^m/\mathbb{Q}$ is disjoint from $F/\mathbb{Q}$ (since p is unramified in F), $G_{F^m/\mathbb{Q}^m}$ 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 [20, Proposition 13.23]).

At this stage we know that, for any sufficiently large integer b, the extensions $F^m/\mathbb{Q}^m$ 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 $\mathrm{rk}(\mathrm{Gal}((F^m)_\Sigma^{p,\mathrm{ab}}/F^m)_{\mathrm{tf}}) \geqslant [F^m : \mathbb{Q}]/2 - 1$ and, for any nonnegative integer a, also $\mathrm{rk}((\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F^m,\Sigma}))_{\mathrm{tf}}) \geqslant [F^m : \mathbb{Q}]/2$. □

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

4.2 In this section we explain how techniques developed in [7] 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 $0 \leqslant i \leqslant n$, let F_i denote the unique extension of k in F of degree p^i.

For any nonnegative 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 nonnegative integer a for which the cohomology group $H^0(G_{k,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ 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 [7, Section 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 $F^\times_{i+1} \to F^\times_i$ and inclusions $\mathcal{O}_{F_i,\Sigma} \subseteq \mathcal{O}_{F_{i+1},\Sigma}$, respectively, together with knowledge of

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

Proof. Fix a nonnegative integer a and an integer i with $0 \leqslant i \leqslant n$. Then the assumed vanishing of the group $H^0(G_{k,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ implies that $H^0(G_{F_i,\Sigma}, (\mathbb{Q}_p/\mathbb{Z}_p)(1+a))$ also vanishes. This in turn implies that the module $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{2a+1}(\mathcal{O}_{F,\Sigma})$ 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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 [7, Section 3.2.1] (with the terms $\overline{X}$ and $Ш_i$ that occur in that argument being 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 that is made precise in [7, Lemma 3.5], 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 $0 \leqslant i < n$. In this case a closer analysis of the argument in [7, Section 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 nonnegative 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 $0 \leqslant b \leqslant n$.

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 nonnegative 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^nth 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 pth root of $\omega \cdot p$ for any root of unity ω.*

REMARK 4.6. 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 $H^1(\mathcal{O}_{k_n,\Sigma}, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_n,\Sigma}$.

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

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

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

$$\mathrm{Norm}_{k_n/k}(\epsilon_n) = \mathrm{Norm}_{\mathbb{Q}_n/\mathbb{Q}}(\epsilon_n) = \mathrm{Norm}_{\mathbb{Q}^{n+1}/\mathbb{Q}}(\zeta_{n+1} - 1) = p.$$

Since k does not contain a pth root of $\omega \cdot p$ for any root of unity ω, this equality implies 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 this 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 either $\mathbb{Q}$ 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 that 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 $0 \leqslant i \leqslant j \leqslant n$ 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

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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

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 [7, Proposition 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 [12]. In fact, for our purposes, the relevant properties of these lattices are conveniently displayed in [18, Table 2] and so in the following result we shall use the same notation for indecomposable lattices as in that table.

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 $1 \leqslant i \leqslant p-2$. For integers a and b in $\{0,1,2\}$ with $a \leqslant b$ 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* $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = |\mathrm{cap}^2_1| = p$.
- $(\mathrm{i})_i$ $V = (R_2, R_1 \oplus \mathbb{Z}_p, 1 \oplus \lambda^i_0)$ *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* $|\mathrm{cap}^1_0| = |\mathrm{cap}^2_0| = |\mathrm{cap}^2_1| = 1$.
- $(\mathrm{ii})_i$ $V = (R_2, \mathbb{Z}_p[Q], \lambda^i_0)$ *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* $|\mathrm{cap}^2_1| = p$.
- $(\mathrm{vi})_i$ $V = (R_2, R_1, \lambda^i_0)$ *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 that 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

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press

$\mathbb{Z}_p[G]$-lattices, as recorded in [18, 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

$$\mathrm{cap}_0^1 = 0 \Longleftrightarrow V \cong \mathbb{Z}_p[G]$$

or

$$V \cong R_2 \oplus \mathbb{Z}_p[Q]$$

or

$$V \cong (R_2, \mathbb{Z}_p[Q], \lambda_0^i)$$

for some i in Z_p, that

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

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

(ii) Corollary 4.9 shows, in addition, that the structure of the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}^{\times}_{k_2,\Sigma}$ is completely determined by the abstract structures of the groups $\mathrm{cap}^{k_2}_{k_a,p}$ and $\mathrm{cap}^{k_1}_{k,p}$. 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.

Acknowledgments. It is a pleasure to thank Daniel Macias Castillo and Christian Wuthrich for helpful discussions and to thank the referees for several helpful suggestions.

REFERENCES

[1] M. F. Atiyah and C. T. C. Wall, "*Cohomology of groups*", Algebraic Number Theory, (eds. J. W. S. Cassels and A. Fröhlich) Academic Press, London, 1967, 94–115.

[2] S. Bloch and K. Kato, "*L-functions and Tamagawa numbers of motives*", in *The Grothendieck Festschrift, Vol. I*, Progress in Mathematics **86**, Birkhäuser, 1990, 333–400.
[3] D. Burns, *On the Galois structure of arithmetic cohomology III: Selmer groups of critical motives*, Kyoto J. Math. **58** (2018), 671–693.
[4] D. Burns and M. Flach, *Motivic L-functions and Galois module structures*, Math. Ann. **305** (1996), 65–102.
[5] D. Burns and M. Flach, *Equivariant Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570.
[6] D. Burns and A. Kumon, *On the Galois structure of arithmetic cohomology II: ray class groups*, J. Math. Soc. Japan **70** (2018), 481–517.
[7] D. Burns, D. Macias Castillo and C. Wuthrich, *On the Galois structure of Selmer groups*, Int. Math. Res. Not. **2015** (2015), 11909–11933.
[8] C. W. Curtis and I. Reiner, *Methods of Representation Theory, Vol. I*, John Wiley, New York, 1987.
[9] P. Deligne, *Seminaire de Geometrie Algebrique du Bois-Marie, SGA 4* 1/2, Lecture Note Math. **569**, Springer, New York, 1977.
[10] F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg **14** (1940), 357–412.
[11] M. Flach, *Euler characteristics in relative K-groups*, Bull. Lond. Math. Soc. **32** (2000), 272–284.
[12] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers. I*, Ann. of Math. (2) **76** (1962), 73–92.
[13] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers. II*, Ann. of Math. (2) **77** (1963), 318–328.
[14] K. Iwasawa, "*On the μ-invariants of $\mathbb{Z}_\ell$-extensions*", in *Number Theory, Algebraic Geometry and Commutative Algebra*, Kinokuniya, Tokyo, 1973, 1–11.
[15] C. Khare and J.-P. Wintenberger, *Ramification in Iwasawa theory and splitting conjectures*, Int. Math. Res. Not. **2014** (2014), 194–223.
[16] J. S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, 1980.
[17] J. Neukirch, *On solvable extensions of number fields*, Invent. Math. **53** (1979), 135–164.
[18] M. Rzedowski-Calderón, G. D. Villa Salvador and M. L. Madan, *Galois module structure of rings of integers*, Math. Z. **204** (1990), 401–424.
[19] J. L. Verdier, *Des Catégories Dérivées des Catégories Abéliennes*, Asterisque **239**, Société Mathématique de France, Montrouge, 1996.
[20] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer, Berlin, 1982.
[21] C. Weibel, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), 346–372.

King's College London
Department of Mathematics
London WC2R 2LS
UK

david.burns@kcl.ac.uk

https://doi.org/10.1017/nmj.2018.41 Published online by Cambridge University Press