On the Galois structure of arithmetic cohomology, III: Selmer groups of critical motives

David Burns

Abstract We investigate the explicit Galois structures of Bloch–Kato Selmer groups of p-adic realizations of critical motives. We show in particular that, under natural and relatively mild hypotheses, the Krull–Schmidt decompositions of the p-adic lattices arising from such Selmer groups are dominated by very simple indecomposable modules (even when the ranks are very large).

1. Introduction and statement of main results

1.1

Let M be a motive defined over a number field E. Fix a prime p and a full Galois stable sublattice T of the p-adic realization of M. For each Galois extension F of E, set $G_{F/E} := \mathrm{Gal}(F/E)$.

If F/E is finite, then the quotient by its torsion subgroup of the Bloch–Kato Selmer group of T over F is a lattice $\mathrm{Sel}_F(T)_{\mathrm{tf}}$ over the group ring $\mathbb{Z}_p[G_{F/E}]$, and obtaining information on the explicit Krull–Schmidt decomposition of this lattice would be interesting for several reasons. Such structures, for example, play an essential role in attempts to understand and investigate natural equivariant refinements of the Tamagawa number conjecture of Bloch and Kato for M over F. In another direction, an analysis of these structures can, in certain circumstances, be used to extract useful information concerning changes in rank of the global points of the Kummer dual of M over the intermediate fields of F/E.

In some rather restricted cases, such applications have already been worked out by Macias Castillo, Wuthrich, and the present author in the setting of motives arising from Abelian varieties and various equivariant refinements of the Birch and Swinnerton-Dyer conjecture that are associated to them (see [2] and the references contained therein).

Unfortunately, however, obtaining explicit descriptions of these lattices in any degree of generality is a very difficult problem and, aside from the few cases that are discussed in [2], essentially nothing is, as far as we are aware, known.

Kyoto Journal of Mathematics, Vol. 58, No. 3 (2018), 671–693
First published online June 26, 2018.
DOI 10.1215/21562261-2017-0034,
Received August 29, 2016. Accepted December 16, 2016.
2010 Mathematics Subject Classification: Primary 11G35; Secondary 11R33, 11R34.

In fact, even setting aside the considerable difficulties of describing Selmer groups explicitly (let alone the Galois action on them), the relevant theory of integral representations is also very complicated. For example, even if $G_{F/E}$ is a cyclic group of p-power order, the number of isomorphism classes of (finitely generated) indecomposable $\mathbb{Z}_p[G_{F/E}]$-lattices is infinite unless the order of $G_{F/E}$ divides p^2 (this is the main result of Heller and Reiner in [8]), and even today there is still no complete classification of these lattices.

Notwithstanding these difficulties, in this note we hope to convince the reader that in certain cases it is possible to prove fairly general results concerning the explicit multiplicities of indecomposable modules that occur in the Selmer groups of motives that are critical in the sense of Deligne [3].

We will do this by combining some rather delicate techniques of integral representation theory (due, in the main, to Yakovlev) together with observations of Fukaya and Kato [5] concerning the Selmer complexes that were introduced by Nekovář in [10].

At this stage these techniques lead directly only to explicit structure results for the Selmer groups that arise in families of cyclic Galois extensions F/E for which one has $k \subseteq E \subseteq F \subseteq K$ for some fixed pro-p p-adic analytic extension K/k of rank 1.

However, such families arise naturally in several ways (see, e.g., Remark 1.3) and, in addition, the algebraic results of Heller and Reiner [7], [8] make it clear that, even in these cases, studying Galois structures can be, a priori, extremely difficult.

Furthermore, it seems reasonable to hope that, with further effort, the approach used here can lead to explicit results that are both finer and more general.

For example, Macias Castillo [9] has already developed our approach to obtain much finer results in some interesting special cases. In addition, given any finite Galois extension of number fields F/E, the methods used here can be applied to all cyclic extensions F'/E' with $E \subseteq E' \subseteq F' \subseteq F$, and this strongly restricts (albeit, at the moment, inexplicitly) the multiplicities with which indecomposable $\mathbb{Z}_p[G_{F/E}]$-lattices can occur as direct summands of $\mathrm{Sel}_F(T)_{\mathrm{tf}}$.

1.2

To state our main results, we recall that if M satisfies the condition of Dabrowski–Panchishkin at p, as is the case (by Perrin-Riou [11]) if M has good ordinary reduction at each p-adic place of k, then for each such place v, with absolute Galois group G_{k_v}, there exists a (unique) largest G_{k_v}-submodule N of the p-adic realization V of M for which $D^0_{\mathrm{dR}}(k_v, N)$ vanishes. We write $V^0(v)$ for this subspace, and we set $V^0(v)^*(1) := \mathrm{Hom}_{\mathbb{Q}_p}(V^0(v), \mathbb{Q}_p(1))$, regarded as endowed with the standard diagonal action of G_{k_v}.

For each finite cyclic group G of p-power order, we fix a set $\mathrm{IM}_p(G)$ of representatives of the isomorphism classes of those indecomposable $\mathbb{Z}_p[G]$-lattices that are not isomorphic to $\mathbb{Z}_p[Q]$ for any quotient Q of G. For each such G, each

$\mathbb{Z}_p[G]$-lattice X, and each I in $\mathrm{IM}_p(G)$, we then write $m_I(X)$ for the number of direct summands in the Krull–Schmidt decomposition of X that are isomorphic to I.

Finally, for each pair of natural numbers n and d, we define an integer

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

where the sum J_i runs over a set of representatives of the isomorphism classes of (finite) Abelian groups of exponent dividing p^i and p-rank at most d, and c_{J_i} denotes the number of conjugacy classes in $\mathrm{Aut}(J_i)$ comprising elements of order dividing p^n. We can now state our main result (which will be proved in Section 3).

THEOREM 1.1

Let M be a motive over k that is both critical and satisfies the condition of Dabrowski–Panchishkin at an odd prime p. Let T be a full Galois stable sublattice of the p-adic realization V of M. Let K be a rank 1 pro-p p-adic analytic extension of k with the following properties:

(i) *K/k is ramified at only finitely many places;*

(ii) *K contains a $\mathbb{Z}_p$-extension k_∞ of k;*

(iii) *for any place v of k that divides either p, a rational prime that ramifies in $K/\mathbb{Q}$, or a rational prime at which M has bad reduction, the following conditions are satisfied:*

(a) *v has an open decomposition group in $G_{K/k}$;*

(b) *if v is not p-adic, then for any place w of K above v the space $H^0(K_w, V)$ vanishes;*

(c) *if v is p-adic, then for any place w of K above v both of the spaces $H^0(K_w, V/V^0(v))$ and $H^0(K_w, V^0(v)^*(1))$ vanish.*

For each intermediate field E of K/k, we set $E_\infty := Ek_\infty$, and then for each nonnegative integer a, we write E_a for the unique extension of E in E_∞ with $[E_a : E] = p^a$. Then there exist rational numbers μ and κ that depend only upon T and K/k and are such that for every cyclic extension F/E with $k \subseteq E \subset F \subset K$ and F/k finite and all sufficiently large integers a one has

$$\sum\nolimits_{I\in \mathrm{IM}_p(G_{F_a/E_a})} m_I\big(\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}\big) \le p^{n(n-1)d^2}\cdot \kappa_n^d, \tag{1}$$

where the degree of F_∞/E_∞ is p^n and we write d for $p^a[F:k]\cdot\mu+\kappa$.

REMARK 1.2

(i) The field k_∞ is unique since G_{K/k_∞} is the subset of $G_{K/k}$ comprising all elements of finite order. The hypothesis concerning open decomposition subgroups is automatically satisfied if, for example, k_∞ is the cyclotomic $\mathbb{Z}_p$-extension k_{cyc} of k.

(ii) The proof of Theorem 1.1 is constructive in that structures of natural Iwasawa modules can be used to give explicit formulas for μ and κ. In addition, while in the generality of Theorem 1.1 the resulting upper bounds on multiplicities can be coarse, Macias Castillo [9] has recently shown that in certain special cases a closer analysis of the methods introduced here can give much better bounds.

(iii) Let G be a cyclic group of p-power order. If $\#G = p$, then by a classical result of Diederichsen [4] one can take $\mathrm{IM}_p(G)$ to be the singleton $\{\mathbb{Z}_p[G]/(\sum_{g\in G} g)\}$. If $\#G = p^2$, then results of Heller and Reiner in [7] give an explicit description of $\mathrm{IM}_p(G)$ which implies that $\#\mathrm{IM}_p(G) = 4p-2$. However, if $\#G > p^2$, then Heller and Reiner show in [8] that $\mathrm{IM}_p(G)$ is infinite and, even now, no explicit description of $\mathrm{IM}_p(G)$ is known.

REMARK 1.3

Several natural families of extensions arise in the context of Theorem 1.1. For example, if $M^p_{k,\Sigma}$ is the maximal pro-p extension of k unramified outside Σ, then $G_{M^p_{k,\Sigma}/k}$ is topologically finitely generated and so for any natural number e the maximal Galois extension $M^{p,(e)}_{k,\Sigma}$ of k_{cyc} in $M^p_{k,\Sigma}$ of exponent dividing p^e is finite. In particular, for any fixed integer d, all cyclic extensions F/E of degree p^n with $F \subset M^p_{k,\Sigma}$, E/k finite, and $[E : E\cap k_{\mathrm{cyc}}] \le p^d$ are contained in the rank 1 pro-p p-adic analytic extension $M^{p,(n+d)}_{k,\Sigma}$ of k. In a similar way, if K is any pro-p p-adic analytic extension of k ramified at only finitely many places and containing k_{cyc}, then all cyclic extensions F/E of degree p^n with $F\subset K$, E/k finite, and $[E : E\cap k_{\mathrm{cyc}}] \le p^d$ are contained in a fixed rank 1 pro-p p-adic analytic extension of k that contains k_{cyc}.

Under certain additional hypotheses on T and K/k, the rational number μ in Theorem 1.1 can be taken to be zero. In such cases the integer $d = \kappa$ in Theorem 1.1 is independent of F, and this observation leads to results such as the following (which will be proved in Section 4). In the rest of this article, for any $\mathbb{Z}_p$-module M, we write $\mathbb{Q}_p \cdot M$ in place of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$.

COROLLARY 1.4

Let the representation T and field extension K/k be as in Theorem 1.1, and assume that for each intermediate field E of K/k_∞ the (Bloch–Kato) Tate–Shafarevich group of T over E is a finitely generated $\mathbb{Z}_p$-module. Then for any cyclic extension F/E with both $k\subseteq E\subset F\subset K$ and F/k finite and any sufficiently large integer a there is an isomorphism of $\mathbb{Z}_p[G_{F_a/E_a}]$-lattices

$$\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}} \cong \Big(\bigoplus_{H\le G_{F_a/E_a}} \mathbb{Z}_p[G_{F_a/E_a}/H]^{s_{F_a,H}}\Big) \oplus R_{F_a} \tag{2}$$

for suitable nonnegative integers $s_{F_a,H}$ and a lattice R_{F_a} with $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p\cdot R_{F_a}) \le \delta_{[F:E]}$ for an integer $\delta_{[F:E]}$ that depends only on T, K/k and $[F:E]$. In particular, for any such extension F_a/E_a, one has

$$\dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\cdot \mathrm{Sel}_{F_a}(T)\big) \le [F:E]\cdot \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\cdot \mathrm{Sel}_{E_a}(T)\big) + \delta_{[F:E]}. \tag{3}$$

REMARK 1.5

(i) For each natural number m, we write C_m for the cyclic group $\mathbb{Z}/p^m\mathbb{Z}$ of order p^m. Fix F/E as in Corollary 1.4, and write the degree of F_∞/E_∞ as p^n. Then G_{F_a/E_a} is isomorphic to C_n for all sufficiently large a and thus, since there are only finitely many isomorphism classes of $\mathbb{Z}_p[C_n]$-lattices of any given $\mathbb{Z}_p$-rank, the upper bound on $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot R_{F_a})$ in Corollary 1.4 implies that there are only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices that arise as direct summands of $\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}$ as a varies. This observation is itself nontrivial (since, even under the stated hypotheses, $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot \mathrm{Sel}_{F_a}(T))$ is usually unbounded as a varies) and raises natural questions. For instance, are there any natural conditions on M and K/k under which one can explicitly describe the indecomposable lattices that can arise in this way, or are there examples of M and K/k for which the conclusion of Corollary 1.4 is valid without any hypotheses on Tate–Shafarevich groups?

(ii) Despite the observation in Remark 1.2(ii), our methods do not give explicit information on the integers $\delta_{[F:E]}$ in Corollary 1.4. The reason is that, for any $\mathbb{Z}_p[C_n]$-lattice N, knowledge of the p-rank of $\hat{H}^{-1}(H,N)$ for each subgroup H of C_n does not imply an upper bound on $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot N)$. However, in this direction it can be shown that

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot N) \leq p^n \cdot \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p \cdot H^0(C_n,N)\big) + (p^n - 1) \cdot d$$

with d equal to the maximum of the p-ranks of $\hat{H}^{-1}(H,N)$ as H runs over subgroups of C_n.

REMARK 1.6

The arguments used to prove Theorem 1.1 and Corollary 1.4 will also show that these results remain true if one replaces all occurrences of Bloch–Kato Selmer groups by Selmer groups in the sense of Greenberg. (For more details, see Remark 4.3.)

2. Selmer groups and complexes for critical motives

In this section we review various definitions of Selmer groups and Selmer complexes in the context of Theorem 1.1.

In the rest of this article, for any $\mathbb{Z}_p$-module X we will write $X[p]$ for the submodule of X comprising elements annihilated by p, X_{tor} for the torsion submodule of X, and X_{tf} for the quotient of X by X_{tor}. We also write $X^\vee$ for the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ and, if X is finitely generated (resp., has an action of $\mathbb{Q}_p$), we write X^* for the linear dual $\mathrm{Hom}_{\mathbb{Z}_p}(X,\mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(X_{\mathrm{tf}},\mathbb{Z}_p)$ (resp., $\mathrm{Hom}_{\mathbb{Q}_p}(X,\mathbb{Q}_p)$), each dual being endowed with the natural contragredient action of any group that acts on X.

If X is finitely generated, we also set $\mathrm{rk}(X) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot X)$ and, with $\mathbb{F}_p$ denoting the finite field of order p, we write $\mathrm{rk}_p(X)$ for the p-rank $\dim_{\mathbb{F}_p}(X/p)$. We note that

$$\mathrm{rk}_p(X) = \dim_{\mathbb{F}_p}\big(X[p]\big) + \mathrm{rk}(X)$$

and 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, for both $i = 1$ and $i = 2$, inequalities

$$\mathrm{rk}_p\big(\mathrm{im}(\theta_i)\big) \leq \mathrm{rk}_p(X_2) \leq \mathrm{rk}_p(X_1) + \mathrm{rk}_p(X_3).$$

For a Noetherian ring R, we write $D(R)$ for the derived category of (left) R-modules and $D^{\mathrm{perf}}(R)$ for the full triangulated subcategory of $D(R)$ comprising complexes that are "perfect" (i.e., isomorphic in $D(R)$ to a bounded complex of finitely generated projective R-modules).

2.1

At the outset, we fix a Galois extension of fields K/k as in Theorem 1.1. We also fix an algebraic closure K^c of K and for each finite extension F of k in K and each place w of F an algebraic closure F_w^c of F_w and an embedding of fields $\iota_w : K^c \to F_w^c$. We set $G_F := G_{K^c/F}$ and $G_{F_w} := G_{F_w^c/F_w}$, and we identify G_{F_w} as a subgroup of G_F by means of the embedding induced by ι_w. For each such field F and each set of places Σ' of k, we write Σ'_F for the set of places of F that lie above those in Σ'.

For any $\mathbb{Z}_p$-module X that is endowed with a continuous action of either G_F or G_{F_w} for some w, and any integer a, we endow the tensor product $X(a) := X \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(a)$ with the natural diagonal action of either G_F or G_{F_w}. Here, and in the rest of this article, we write $\mathbb{Z}_p(a)$ for the module $\mathbb{Z}_p$ upon which G_F and G_{F_w} act via the ath power of the respective cyclotomic characters.

We fix a motive M that is defined over k, is critical in the sense of Deligne [3], and satisfies the condition of Dabrowski–Panchishkin at p, and we write V for its p-adic realization. Under the hypotheses of Theorem 1.1, we can fix a finite set of places Σ of k that satisfies all of the following hypotheses:

- Σ contains the set Σ^∞ of Archimedean places, the set Σ^p of p-adic places, all places at which M has bad reduction, and all places that divide rational primes which ramify in $K/\mathbb{Q}$;
- every v in Σ has an open decomposition group in $G_{K/k}$;
- for every v in $\Sigma \setminus \Sigma^p$ and any place w of K above v, the space $H^0(K_w, V)$ vanishes.

As in Theorem 1.1, we also continue to assume that, for every p-adic place w of K, the spaces $H^0(K_w, V/V^0(v))$ and $H^0(K_w, V^0(v)^*(1))$ both vanish.

We fix a full G_k-stable sublattice T of V. For each v in Σ^p, we set $T_v^0 := T \cap V^0(v)$ and then for each finite extension F of k in K and each w in Σ_F^p above v, we write $V^0(w)$ and T_w^0 for the G_{F_w}-modules obtained by restricting $V^0(v)$ and T_v^0, respectively.

2.2

We now review some relevant aspects of Nekovář's theory of Selmer complexes (see [10]), as used by Fukaya and Kato in [5].

For each profinite group $\mathcal{G}$ and topological Abelian group $\mathcal{T}$ that is endowed with a continuous action of $\mathcal{G}$, we write $C(\mathcal{G},\mathcal{T})$ for the standard complex of continuous cochains of $\mathcal{G}$ with values in $\mathcal{T}$. If $\mathcal{G}$ is the Galois group of the maximal algebraic extension of F unramified outside Σ_F (resp., is G_{F_w}), then we abbreviate $C(\mathcal{G},\mathcal{T})$ to $C(\Sigma_F,\mathcal{T})$ (resp., to $C(F_w,\mathcal{T})$).

With Σ and T as in Section 2.1, we define $\mathrm{SC}_F(\Sigma,T)$ to be the mapping fiber of the natural diagonal localization morphism

$$C(\Sigma_F,T) \to \bigoplus_{w\in\Sigma_F^p} C(F_w,T/T_w^0) \oplus \bigoplus_{w\in\Sigma_F\setminus\Sigma_F^p} C(F_w,T). \tag{4}$$

For each place w of F that is not p-adic, we write $C_f(F_w,T)$ for the subcomplex of $C(F_w,T)$ that agrees with $C(F_w,T)$ in degree 0, is equal to the kernel of $Z^1(F_w,T)\to H^1(F_w^{\mathrm{un}},T)$ in degree 1, and is zero in all degrees greater than 1.

Then, defining $\mathrm{SC}_F(T)$ to be the mapping fiber of the localization morphism

$$C(\Sigma_F,T) \to \bigoplus_{w\in\Sigma_F^p} C(F_w,T/T_w^0) \oplus \bigoplus_{v\in\Sigma_F\setminus\Sigma_F^p} C(F_w,T)/C_f(F_w,T)$$

one obtains a natural exact triangle

$$\mathrm{SC}_F(\Sigma,T)\to\mathrm{SC}_F(T)\to \bigoplus_{w\in\Sigma_F\setminus\Sigma_F^p} C_f(F_w,T)\to\mathrm{SC}_F(\Sigma,T)[1]. \tag{5}$$

In the following result, we record the basic properties of these complexes that will be used in the rest of this article.

LEMMA 2.1

Let K/k, T and Σ be as in Section 2.1. Let F/E be a finite Galois extension with $k\subseteq E\subseteq F\subset K$ and E/k finite. Set $G:=G_{F/E}$.

(i) *$\mathrm{SC}_F(\Sigma,T)$ is an object of $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ that is acyclic outside degrees 1, 2, and 3.*

(ii) *For every subgroup J of G there exists a canonical isomorphism in $D(\mathbb{Z}_p[G/J])$ of the form $\mathbb{Z}_p[G/J]\otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]}\mathrm{SC}_F(\Sigma,T)\cong\mathrm{SC}_{F^J}(\Sigma,T)$.*

(iii) *We have that $\mathrm{rk}_p(H^3(\mathrm{SC}_F(\Sigma,T)))\le\mathrm{rk}(T)$.*

(iv) *For every place w in $\Sigma_F\setminus\Sigma_F^p$, the group $H^1(C_f(F_w,T))$ is finite and one has $\mathrm{rk}_p(H^1(C_f(F_w,T)))\le\mathrm{rk}(T)$.*

Proof

The complex $\mathrm{SC}_F(\Sigma,T)$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ because it is defined as the mapping fiber of (4) and, since p is odd, the complexes $C(\Sigma_F,T)$, $C(F_w,T/T_w^0)$ and $C(F_w,T)$ each belong to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ (as a consequence, for example, of [5, Proposition 1.6.5(2)]).

The acyclicity of $\mathrm{SC}_F(\Sigma,T)$ outside degrees 1, 2, and 3 follows directly from the long exact cohomology sequence of the triangle (5) and the fact that $\mathrm{SC}_F(T)$ is acyclic outside the same degrees (as is shown in [5, Proposition 4.2.35(1)]).

The isomorphism in claim (ii) follows from [5, Proposition 1.6.5(3)] (as is explicitly noted in [5, Section 4.1.4(2)]).

To prove claim (iii), we note that the long exact cohomology sequence of (5) induces an isomorphism $H^3(\mathrm{SC}_F(\Sigma,T)) \cong H^3(\mathrm{SC}_F(T))$. Then one need only recall that the argument of [5, Proposition 4.2.35(2)] implies that $H^3(\mathrm{SC}_F(T))$ is isomorphic to a quotient of $T(-1)$ and hence that $\mathrm{rk}_p(H^3(\mathrm{SC}_F(T))) \leq \mathrm{rk}_p(T(-1)) = \mathrm{rk}(T)$.

To prove claim (iv), we recall that for each such w the complex $C_f(F_w,T)$ is naturally isomorphic to $H^0(I_w,T) \xrightarrow{1-\varphi_w} H^0(I_w,T)$, where the first term is placed in degree 0, I_w denotes the inertia subgroup of G_{F_w}, and φ_w denotes the Frobenius automorphism in G_{F_w}/I_w (cf. the discussion in [5, Section 4.2.11]). In particular, since the (assumed) vanishing of $H^0(K_{w'},V)$ for any place w' of K above w implies that $H^0(F_w,T) = H^0(C_f(F_w,T))$ vanishes, the group $H^1(C_f(F_w,T))$ is finite. Since $H^1(C_f(F_w,T))$ is isomorphic to a quotient of $H^0(I_w,T)$, it is then also clear that $\mathrm{rk}_p(H^1(C_f(F_w,T))) \leq \mathrm{rk}_p(H^0(I_w,T)) \leq \mathrm{rk}_p(T) = \mathrm{rk}(T)$, as claimed. $\square$

2.3

We now recall definitions of Greenberg's Selmer groups and Bloch–Kato Selmer groups. For each non-Archimedean place w of F, we write $H^1_{f,(1)}(F_w,T^\vee(1))$ for the kernel of the natural projection map $H^1(F_w,T^\vee(1)) \to H^1(F_w,(T^0_w)^\vee(1))$ if w is p-adic and of the restriction map $H^1(F_w,T^\vee(1)) \to H^1(F^{\mathrm{un}}_w,T^\vee(1))$ in all other cases, where F^{un}_w denotes the maximal unramified extension of F_w in F^c_w.

For each such w, we also write $H^1_{f,(2)}(F_w,T^\vee(1))$ for the image of the natural composite map $H^1_f(F_w,V^*(1)) \to H^1(F_w,V^*(1)) \to H^1(F_w,V^*(1)/T^*(1)) = H^1(F_w,T^\vee(1))$.

For $i=1,2$, we then define the Selmer group $\mathrm{Sel}_{F,(i)}(T^\vee(1))$ to be the kernel of the diagonal localization map

$$H^1\big(F,T^\vee(1)\big) \to \bigoplus_{w\in\Sigma_F^\infty} H^1\big(F_w,T^\vee(1)\big)$$

$$\oplus \bigoplus_{w\notin\Sigma_F^\infty} H^1\big(F_w,T^\vee(1)\big)/H^1_{f,(i)}\big(F_w,T^\vee(1)\big),$$

where in the second sum w runs over all non-Archimedean places of F.

We finally set

$$\mathrm{Sel}_F(T) := \mathrm{Sel}_{F,(2)}\big(T^\vee(1)\big)^\vee \quad \text{and} \quad \mathrm{Sel}'_F(T) := \mathrm{Sel}_{F,(1)}\big(T^\vee(1)\big)^\vee,$$

and we define the (Bloch–Kato) Tate–Shafarevich group of T by setting

$$Ш_F(T) := \mathrm{Sel}_F(T)_{\mathrm{tor}}.$$

REMARK 2.2

The above definitions of the groups $\mathrm{Sel}_{F,(1)}(T^\vee(1))$ and $\mathrm{Sel}_{F,(2)}(T^\vee(1))$ are due, respectively, to Greenberg [6] and to Bloch and Kato [1]. In particular, if T is the p-adic Tate module of an Abelian variety A over k that has good ordinary reduction at all p-adic places, then $\mathrm{Sel}_{F,(2)}(T^\vee(1))$ coincides with the classical Selmer group of A over F and hence, if the Tate–Shafarevich group of A over F is finite, then its p-primary part is canonically isomorphic to the group $\text{Ш}_F(T)$ defined above.

3. Proof of Theorem 1.1

3.1

A key role in this argument is played by a delicate representation-theoretic result of Yakovlev [12]. To explain this result, we fix a cyclic group G of order p^n and for each integer i with $0 \le i \le n$, we write G_i for the subgroup of G of order p^i.

Then, in terms of this notation, the results of [12, Theorem 2.4, Lemma 5.2] combine to imply that if M and N are any $\mathbb{Z}_p[G]$-lattices for which, for each integer i with $1 \le i < n$, there exists an isomorphism of $\mathbb{Z}_p[G]$-modules $\theta_i : \hat{H}^{-1}(G_i, M) \to \hat{H}^{-1}(G_i, N)$ that lies in commutative diagrams (of $\mathbb{Z}_p[G]$-modules)

$$(6)\quad \begin{array}{ccc} \hat{H}^{-1}(G_i,M) & \xrightarrow{\kappa^i_M} & \hat{H}^{-1}(G_{i+1},M) \\ {\scriptstyle\theta_i}\downarrow & & \downarrow{\scriptstyle\theta_{i+1}} \\ \hat{H}^{-1}(G_i,N) & \longrightarrow & \hat{H}^{-1}(G_{i+1},N) \end{array} \qquad \begin{array}{ccc} \hat{H}^{-1}(G_i,M) & \xleftarrow{\rho^i_M} & \hat{H}^{-1}(G_{i+1},M) \\ {\scriptstyle\theta_i}\downarrow & & \downarrow{\scriptstyle\theta_{i+1}} \\ \hat{H}^{-1}(G_i,N) & \longleftarrow & \hat{H}^{-1}(G_{i+1},N) \end{array}$$

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

$$(7)\qquad M \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[G/G_i]^{a_i} \quad\text{and}\quad N \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[G/G_i]^{b_i}$$

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

Taken in conjunction with the Krull–Schmidt theorem (for $\mathbb{Z}_p[G]$-lattices), these isomorphisms imply that for any modules M and N as above one must have $m_I(M) = m_I(R) = m_I(N)$ for all lattices I in $\mathrm{IM}_p(G)$.

In addition, for each such M and each subgroup G_i of G the isomorphism

$$\hat{H}^{-1}(G_i, M) \cong \bigoplus_{I \in \mathrm{IM}_p(G)} \hat{H}^{-1}(G_i, I)^{n_I}$$

implies that

$$(8)\qquad \mathrm{rk}_p\big(\hat{H}^{-1}(G_i, M)\big) = \sum_{I \in \mathrm{IM}_p(G)} n_I \cdot \mathrm{rk}_p\big(\hat{H}^{-1}(G_i, I)\big).$$

3.2

Before proceeding to the proof of Theorem 1.1, it is convenient to make some general observations about diagrams of the form (6). To do so we continue to assume that G is cyclic of order p^n, and we refer to finite "double chains" of homomorphisms of $\mathbb{Z}_p[G]$-modules

$$X_1 \xrightarrow{\theta_1} X_2 \xrightarrow{\theta_2} \cdots \xrightarrow{\theta_{t-2}} X_{t-1} \xrightarrow{\theta_{t-1}} X_t, \qquad X_1 \xleftarrow{\phi_1} X_2 \xleftarrow{\phi_2} \cdots \xleftarrow{\phi_{t-2}} X_{t-1} \xleftarrow{\phi_{t-1}} X_t$$

and

$$X_1' \xrightarrow{\theta_1'} X_2 \xrightarrow{\theta_2'} \cdots \xrightarrow{\theta_{t-2}'} X_{t-1}' \xrightarrow{\theta_{t-1}'} X_t', \qquad X_1' \xleftarrow{\phi_1'} X_2' \xleftarrow{\phi_2'} \cdots \xleftarrow{\phi_{t-2}'} X_{t-1}' \xleftarrow{\phi_{t-1}'} X_t'$$

as *equivalent* if there exist isomorphisms of $\mathbb{Z}_p[G]$-modules $\iota_i : X_i \to X_i'$ for each index i which together give commutative diagrams

$$\begin{array}{ccccccccc}
X_1 & \xrightarrow{\theta_1} & X_2 & \xrightarrow{\theta_2} & \cdots & \xrightarrow{\theta_{t-2}} & X_{t-1} & \xrightarrow{\theta_{t-1}} & X_t \\
{\scriptstyle \iota_1}\downarrow & & {\scriptstyle \iota_2}\downarrow & & & & {\scriptstyle \iota_{t-1}}\downarrow & & {\scriptstyle \iota_t}\downarrow \\
X_1' & \xrightarrow{\theta_1'} & X_2' & \xrightarrow{\theta_2'} & \cdots & \xrightarrow{\theta_{t-2}'} & X_{t-1}' & \xrightarrow{\theta_{t-1}'} & X_t'
\end{array}$$

and

$$\begin{array}{ccccccccc}
X_1 & \xleftarrow{\phi_1} & X_2 & \xleftarrow{\phi_2} & \cdots & \xleftarrow{\phi_{t-2}} & X_{t-1} & \xleftarrow{\phi_{t-1}} & X_t \\
{\scriptstyle \iota_1}\downarrow & & {\scriptstyle \iota_2}\downarrow & & & & {\scriptstyle \iota_{t-1}}\downarrow & & {\scriptstyle \iota_t}\downarrow \\
X_1' & \xleftarrow{\phi_1'} & X_2' & \xleftarrow{\phi_2'} & \cdots & \xleftarrow{\phi_{t-2}'} & X_{t-1}' & \xleftarrow{\phi_{t-1}'} & X_t'
\end{array}$$

We write $e(X)$ for the exponent of a finite Abelian p-group X. For natural numbers d and m, we fix a set of representatives Ab_d^m of the isomorphism classes of (finite) Abelian p-groups X with both $\mathrm{rk}_p(X) \le d$ and $e(X) \le m$. For natural numbers $d, m_1, m_2, \ldots, m_t$, we write $\Delta_d^{m_1,\ldots,m_t}$ for the number of nonequivalent double chains of homomorphisms of finite $\mathbb{Z}_p[G]$-modules

$$X_1 \to X_2 \to \cdots \to X_{t-1} \to X_t, \qquad X_1 \leftarrow X_2 \leftarrow \cdots \leftarrow X_{t-1} \leftarrow X_t$$

in which for each index i one has both $\mathrm{rk}_p(X_i) \le d$ and $e(X_i) \le m_i$.

LEMMA 3.1

For each set of natural numbers $d, m_1, m_2, \ldots, m_t$, one has

$$\Delta_d^{m_1,\ldots,m_t} \le \Big(\prod_{i=1}^{i=t-1} \min\{m_i, m_{i+1}\}\Big)^{2d^2} \cdot \sum_{J_1\times\cdots\times J_t} \prod_{i=1}^{i=t-1} c_{J_i} c_{J_{i+1}},$$

where each J_i runs over $\mathrm{Ab}_d^{m_i}$, and c_{J_i} denotes the number of conjugacy classes of $\mathrm{Aut}_{\mathbb{Z}_p}(J_i)$ comprising elements of order dividing p^n.

Proof

The category of (finite) $\mathbb{Z}_p[G]$-modules X satisfying both $\mathrm{rk}_p(X) \le d$ and $e(X) \le m$ is equivalent to the category of pairs $(\tilde{X}, \alpha)$, where $\tilde{X}$ is a finite Abelian p-

group satisfying $\mathrm{rk}_p(\tilde{X}) \le d$ and $e(\tilde{X}) \le m$, and α is an element of $\mathrm{Aut}_{\mathbb{Z}_p}(\tilde{X})$ of order dividing p^n.

If one fixes a generator g of G, then this equivalence is induced by the assignment $X \mapsto ([X], g_X)$, where $[X]$ is the Abelian group underlying X, g_X corresponds to the action of g on X, and $\mathbb{Z}_p[G]$-homomorphisms $\theta : X \to Y$ correspond to group homomorphisms $[\theta] : [X] \to [Y]$ which satisfy $[\theta] \circ g_X \circ [\theta]^{-1} = g_Y$.

This implies, in particular, that the isomorphism classes of $\mathbb{Z}_p[G]$-modules X satisfying both $\mathrm{rk}_p(X) \le d$ and $e(X) \le m$ are represented by pairs (J, β) as J runs over Ab_d^m and β over the set C_J of conjugacy classes of $\mathrm{Aut}_{\mathbb{Z}_p}(J)$ comprising elements of order dividing p^n.

Now if, for each index i with $1 \le i \le t$, one is given a pair of isomorphic $\mathbb{Z}_p[G]$-modules X_i and X_i', then any double chain of homomorphisms of $\mathbb{Z}_p[G]$-modules

$$X_1' \to X_2' \to \cdots \to X_{t-1}' \to X_t', \qquad X_1' \leftarrow X_2' \leftarrow \cdots \leftarrow X_{t-1}' \leftarrow X_t'$$

is equivalent to a double chain of homomorphisms of $\mathbb{Z}_p[G]$-modules of the form

$$X_1 \to X_2 \to \cdots \to X_{t-1} \to X_t, \qquad X_1 \leftarrow X_2 \leftarrow \cdots \leftarrow X_{t-1} \leftarrow X_t. \tag{9}$$

Taken in conjunction with the observations above, this implies that a set of representatives of the inequivalent chains of the form (9), in which each X_i is finite and satisfies both $\mathrm{rk}_p(X_i) \le d$ and $e(X_i) \le m_i$, is contained in the set $\Upsilon_d^{m_1,\dots,m_t}$ of double chains (9) in which each X_i is the $\mathbb{Z}_p[G]$-module $[J_i, \beta_i]$ that corresponds to some J_i in $\mathrm{Ab}_d^{m_i}$ and β_i in C_{J_i}. This fact implies that $\Delta_d^{m_1,\dots,m_t}$ is at most

$$\begin{aligned}
&\#\Upsilon_d^{m_1,\dots,m_t} \\
&\quad = \sum_{(J_1,\beta_1)\times\cdots\times(J_t,\beta_t)} \prod_{i=1}^{i=t-1} \#\mathrm{Hom}_{\mathbb{Z}_p[G]}\big([J_i,\beta_i],[J_{i+1},\beta_{i+1}]\big) \\
&\quad\quad \times \#\mathrm{Hom}_{\mathbb{Z}_p[G]}\big([J_{i+1},\beta_{i+1}],[J_i,\beta_i]\big) \\
&\quad \le \sum_{(J_1,\beta_1)\times\cdots\times(J_t,\beta_t)} \prod_{i=1}^{i=t-1} \#\mathrm{Hom}_{\mathbb{Z}_p}(J_i,J_{i+1})\#\mathrm{Hom}_{\mathbb{Z}_p}(J_{i+1},J_i) \\
&\quad = \sum_{J_1\times\cdots\times J_t} \prod_{i=1}^{i=t-1} c_{J_i}c_{J_{i+1}}\#\mathrm{Hom}_{\mathbb{Z}_p}(J_i,J_{i+1})\#\mathrm{Hom}_{\mathbb{Z}_p}(J_{i+1},J_i) \\
&\quad = \sum_{J_1\times\cdots\times J_t} \prod_{i=1}^{i=t-1} c_{J_i}c_{J_{i+1}}\#\big(J_{i+1}\big[e(J_i)\big]\big)^{\mathrm{rk}_p(J_i)}\#\big(J_i\big[e(J_{i+1})\big]\big)^{\mathrm{rk}_p(J_{i+1})} \\
&\quad \le \sum_{J_1\times\cdots\times J_t} \prod_{i=1}^{i=t-1} c_{J_i}c_{J_{i+1}}\big(\min\{e(J_i),e(J_{i+1})\}\big)^{2\,\mathrm{rk}_p(J_i)\,\mathrm{rk}_p(J_{i+1})},
\end{aligned}$$

where in each sum J_i runs over $\mathrm{Ab}_d^{m_i}$ and β_i over C_{J_i}.

Note that the first inequality above is true because $\mathrm{Hom}_{\mathbb{Z}_p[G]}([J_a,\beta_a],[J_b,\beta_b])$ is a subgroup of $\mathrm{Hom}_{\mathbb{Z}_p}(J_a,J_b)$ and the second because both $e(J_a[e(J_b)]) = \min\{e(J_a),e(J_b)\}$ and $\mathrm{rk}_p(J_a[e(J_b)]) = \mathrm{rk}_p(J_a)$ and hence $\#(J_a[e(J_b)]) \leq (\min\{e(J_a),e(J_b)\})^{\mathrm{rk}_p(J_a)}$. In addition, the first equality above is clear, the second is true because $c_{J_i} = \#C_{J_i}$ and $c_{J_{i+1}} = \#C_{J_{i+1}}$, and the third because, after choosing a minimal set of generators $\{x_{aj}\}_{1\leq j\leq \mathrm{rk}_p(J_a)}$ of the Abelian group J_a, any element θ of $\mathrm{Hom}_{\mathbb{Z}_p}(J_a,J_b)$ is uniquely specified by the elements $\theta(x_{aj})$, each of which must belong to $J_b[e(J_a)]$.

The claimed upper bound on $\Delta_d^{m_1,\ldots,m_t}$ now follows from the above displayed inequality by taking into account the fact that $\min\{e(J_i),e(J_{i+1})\} \leq \min\{m_i,m_{i+1}\}$ (since, by assumption, both $e(J_i)\leq m_i$ and $e(J_{i+1})\leq m_{i+1}$) and that $\mathrm{rk}_p(J_i)$ and $\mathrm{rk}_p(J_{i+1})$ are both, by assumption, at most d. □

For any natural number d, we write Lat_G^d for the set of $\mathbb{Z}_p[G]$-lattices N for which one has $\mathrm{rk}_p(\hat{H}^{-1}(G_i,N)) \leq d$ for all i with $1\leq i\leq n$.

In the next result, we show that for each indecomposable lattice I in $\mathrm{IM}_p(G)$ the maximal multiplicity m_I^d with which I occurs (up to isomorphism) as a direct summand of any lattice in Lat_G^d is both well defined and bounded by a quantity that depends only on n and d.

LEMMA 3.2

For each natural number d, one has

$$\sum_{I\in \mathrm{IM}_p(G)} m_I^d \leq p^{n(n-1)d^2}\cdot \kappa_n^d$$

with κ_n^d the integer defined just prior to the statement of Theorem 1.1.

Proof

For each N in Lat_G^d and each index i, one has $e(\hat{H}^{-1}(G_i,N)) \leq \#G_i = p^i$ and so, as N ranges over Lat_G^d, the number of inequivalent double chains of homomorphisms of $\mathbb{Z}_p[G]$-modules

$$(10)\quad \begin{cases} \hat{H}^{-1}(G_1,N) \to \hat{H}^{-1}(G_2,N) \to \cdots \to \hat{H}^{-1}(G_{n-1},N) \to \hat{H}^{-1}(G,N), \\ \hat{H}^{-1}(G_1,N) \leftarrow \hat{H}^{-1}(G_2,N) \leftarrow \cdots \leftarrow \hat{H}^{-1}(G_{n-1},N) \leftarrow \hat{H}^{-1}(G,N) \end{cases}$$

that arise is at most $\Delta_d^{p,p^2,\ldots,p^n}$. By applying Lemma 3.1 in this context (and recalling the explicit definition of κ_n^d), one also finds that

$$\Delta_d^{p,p^2,\ldots,p^n} \leq \Big(\prod_{i=1}^{i=n-1}\min\{p^i,p^{i+1}\}\Big)^{2d^2}\cdot\kappa_n^d = p^{n(n-1)d^2}\cdot\kappa_n^d.$$

Now, for each I in $\mathrm{IM}_p(G)$ and each integer a with $1\leq a\leq m_I^d$, the equality (8) implies that I^a belongs to Lat_G^d. In addition, for each I and J in $\mathrm{IM}_p(G)$ and each pair of natural numbers a and b, the observation made just after (7) implies that the homomorphism chains (10) corresponding to the modules $N = I^a$ and

$N = J^b$ (with the arrows representing the relevant restriction and corestriction maps) are equivalent if and only if both $I = J$ and $a = b$.

These observations imply that the modules $N = I^a$ for I in $\mathrm{IM}_p(G)$ and $1 \leq a \leq m_I^d$ account for at least $\sum_{I\in \mathrm{IM}_p(G)} m_I^d$ of the at most $p^{n(n-1)d^2} \cdot \kappa_n^d$ nonequivalent double chains of homomorphisms (10), and so one has $\sum_{I\in \mathrm{IM}_p(G)} m_I^d \leq p^{n(n-1)d^2} \cdot \kappa_n^d$, as claimed. □

3.3

In this section we fix data K/k, Σ, and T as in Section 2.1, and we prove the following reduction result regarding Theorem 1.1.

PROPOSITION 3.3

To prove Theorem 1.1 it suffices to show the existence of rational numbers μ and κ' that depend only upon K/k, Σ, and T, and are such that for all finite extensions F of k in K one has $\mathrm{rk}_p(H^2(\mathrm{SC}_{F_a}(\Sigma,T))_{\mathrm{tor}}) \leq p^a[F:k]\cdot\mu+\kappa'$ for all sufficiently large integers a.

Proof

The precise inequality in Theorem 1.1 will follow directly from Lemma 3.2 if we can show that, under the hypotheses of Theorem 1.1, there exist rational numbers μ and κ that depend only upon T and K/k and are such that

$$\mathrm{rk}_p\big(\hat{H}^{-1}\big(J,\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}\big)\big) \leq p^a[F:k]\cdot\mu+\kappa \tag{11}$$

for all cyclic extensions F/E with $k \subseteq E \subseteq F \subset K$ and F/k finite, all sufficiently large integers a, and all subgroups J of G_{F_a/E_a}.

To relate this condition to that given in the claimed result, we note first that the result of Lemma 3.4 below (with F/E replaced by F_a/E_a) implies that for each such extension F_a/E_a and subgroup J there exists a $\mathbb{Z}_p[G_{F_a/E_a}]$-module Q_{F_a} which satisfies $\mathrm{rk}_p(Q_{F_a}) \leq \#\Sigma^p_{F_a}\cdot\mathrm{rk}(T)$ and lies in an exact sequence of the form

$$\hat{H}^{-2}(J,Q_{F_a}) \to \hat{H}^{-1}\big(J,\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}\big) \to \hat{H}^{-1}\big(J,H^2\big(\mathrm{SC}_{F_a}(\Sigma,T)\big)_{\mathrm{tf}}\big).$$

This sequence implies an inequality

$$\begin{aligned}\mathrm{rk}_p\big(\hat{H}^{-1}\big(J,\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}\big)\big) &\leq \mathrm{rk}_p\big(\hat{H}^{-1}\big(J,H^2\big(\mathrm{SC}_{F_a}(\Sigma,T)\big)_{\mathrm{tf}}\big)\big)+\mathrm{rk}_p\big(\hat{H}^{-2}(J,Q_{F_a})\big)\\ &\leq \mathrm{rk}_p\big(\hat{H}^{-1}\big(J,H^2\big(\mathrm{SC}_{F_a}(\Sigma,T)\big)_{\mathrm{tf}}\big)\big)+\#\Sigma^p_{F_a}\cdot\mathrm{rk}(T)\\ &\leq \mathrm{rk}_p\big(H^2\big(\mathrm{SC}_{F_a^J}(\Sigma,T)\big)_{\mathrm{tor}}\big)+(1+\#\Sigma^p_{F_a})\cdot\mathrm{rk}(T),\end{aligned} \tag{12}$$

where the second inequality is valid because $\hat{H}^{-2}(J,Q_{F_a})$ is isomorphic to a subquotient of Q_{F_a} (as J is cyclic), and the third follows from Lemma 3.5 below (with F/E replaced by F_a/E_a).

Now, by explicit assumption in Theorem 1.1, the decomposition subgroup of each p-adic place is open in $G_{K/k}$ and so the cardinality of $\Sigma^p_{F_a}$ is bounded independently of F and a. The required inequality (11) will therefore follow directly from (12), provided that there exist rational numbers μ and κ' that depend only upon T, K/k, and Σ, and are such that $\mathrm{rk}_p(H^2(\mathrm{SC}_{F_a}(\Sigma,T))_{\mathrm{tor}}) \le p^a[F:k]\cdot\mu+\kappa'$ for all F and all sufficiently large a.

Note also that, while the rationals μ and κ' obtained in this way ostensibly depend on Σ (contrary to the assertion of Theorem 1.1), one can remove this dependence by simply choosing Σ to be equal to the union of Σ^∞, Σ^p, the set of places at which M has bad reduction, and the set of places that divide rational primes ramifying in $K/\mathbb{Q}$. This completes the proof of Proposition 3.3. □

LEMMA 3.4

For each cyclic extension F/E with $k\subseteq E\subseteq F\subset K$ and F/k finite there exists a natural exact sequence of $\mathbb{Z}_p[G_{F/E}]$-modules

$$0\to \mathrm{Sel}_F(T)_{\mathrm{tf}}\to H^2\big(\mathrm{SC}_F(\Sigma,T)\big)_{\mathrm{tf}}\to Q_F\to 0,$$

where Q_F is such that $\mathrm{rk}_p(Q_F)\le \#\Sigma_F^p\cdot\mathrm{rk}(T)$.

Proof

We note first that for each place w of F the group $H^1_{f,(2)}(F_w,T^\vee(1))$ is equal to the maximal divisible subgroup of $H^1_{f,(1)}(F_w,T^\vee(1))$. In fact, this follows directly from [5, Lemma 4.2.32(1)] if w is not p-adic and from [5, Lemma 4.2.32(2)] if w is p-adic since our assumption that the spaces $H^0(K_w,V/V^0(v))$ and $H^0(K_w, V^0(v)^*(1))$ vanish implies that both of the spaces $H^0(F_w,V/V^0(w))$ and $H^0(F_w, V^0(w)^*(1))$ also vanish.

This fact induces a natural inclusion $\mathrm{Sel}_{F,(2)}(T^\vee(1))\to\mathrm{Sel}_{F,(1)}(T^\vee(1))$ with $\mathbb{Z}_p$-torsion cokernel. By taking Pontryagin duals, this inclusion induces a surjective homomorphism with $\mathbb{Z}_p$-torsion kernel

$$\mathrm{Sel}'_F(T):=\mathrm{Sel}_{F,(1)}\big(T^\vee(1)\big)^\vee\to\mathrm{Sel}_{F,(2)}\big(T^\vee(1)\big)^\vee=:\mathrm{Sel}_F(T)$$

and hence also an identification of lattices $\mathrm{Sel}'_F(T)_{\mathrm{tf}}=\mathrm{Sel}_F(T)_{\mathrm{tf}}$. In addition, the long exact cohomology sequence of (5) gives an exact sequence

$$\bigoplus_{w\in\Sigma_F\setminus\Sigma_F^p} H^1\big(C_f(F_w,T)\big)\to H^2\big(\mathrm{SC}_F(\Sigma,T)\big)\to H^2\big(\mathrm{SC}_F(T)\big)\to 0 \tag{13}$$

and hence also, since each module $H^1(C_f(F_w,T))$ is finite by Lemma 2.1(iv), an identification of lattices $H^2(\mathrm{SC}_F(\Sigma,T))_{\mathrm{tf}}=H^2(\mathrm{SC}_F(T))_{\mathrm{tf}}$.

The key point now is that, as shown in the proof of [5, Proposition 4.2.35(2)], the local and global duality theorems combine to give an exact sequence

$$0\to\mathrm{Sel}'_F(T)\to H^2\big(\mathrm{SC}_F(T)\big)\to\bigoplus_{w\in\Sigma_F^p}H^2(F_w,T_w^0) \tag{14}$$

and hence also an induced exact sequence

$$0\to\mathrm{Sel}'_F(T)_{\mathrm{tf}}\to H^2\big(\mathrm{SC}_F(T)\big)_{\mathrm{tf}}\to Q_F\to 0$$

for a suitable subquotient Q_F of $\bigoplus_{w\in\Sigma_F^p}H^2(F_w,T_w^0)$. By local duality, each module $H^2(F_w,T_w^0)$ is isomorphic to $H^0(F_w,(T_w^0)^\vee(1))^\vee$ and hence to a quotient of $((T_w^0)^\vee(1))^\vee\cong T_w^0(-1)$. This in turn implies that

$$\begin{aligned}\mathrm{rk}_p(Q_F) &\le \mathrm{rk}_p\Big(\bigoplus_{w\in\Sigma_F^p} H^2(F_w,T_w^0)\Big) \le \bigoplus_{w\in\Sigma_F^p}\mathrm{rk}_p\big(T_w^0(-1)\big) = \bigoplus_{w\in\Sigma_F^p}\mathrm{rk}_p(T_w^0)\\ &\le \#\Sigma_F^p\cdot \mathrm{rk}(T),\end{aligned}$$

as required to prove the claimed inequality. □

LEMMA 3.5

Fix F/E as in Lemma 3.4, and set $G := G_{F/E}$. Then for each subgroup J of G one has $\mathrm{rk}_p(\hat{H}^{-1}(J, H^2(\mathrm{SC}_F(\Sigma,T))_{\mathrm{tf}})) \le \mathrm{rk}_p(H^2(\mathrm{SC}_{F^J}(\Sigma,T))_{\mathrm{tor}}) + \mathrm{rk}(T)$.

Proof

Set $M := H^2(\mathrm{SC}_F(\Sigma,T))$. Then, as $\hat{H}^{-1}(J,M_{\mathrm{tf}})$ is finite and M_{tf} is torsion-free, the group $\hat{H}^{-1}(J,M_{\mathrm{tf}})$ can be computed as the torsion subgroup of $H_0(J,M_{\mathrm{tf}})$. In particular, by taking J-coinvariants of the tautological exact sequence

$$0 \to M_{\mathrm{tor}} \to M \to M_{\mathrm{tf}} \to 0$$

and passing to torsion subgroups in the resulting sequence, one obtains a surjective homomorphism $H_0(J,M)_{\mathrm{tor}} \to \hat{H}^{-1}(J,M_{\mathrm{tf}})$ and hence an inequality

$$\mathrm{rk}_p\big(\hat{H}^{-1}(J,M_{\mathrm{tf}})\big) \le \mathrm{rk}_p\big(H_0(J,M)_{\mathrm{tor}}\big).$$

To compute the right-hand term here, we note that $\mathrm{SC}_F(\Sigma,T)$ is acyclic in degrees greater than three and hence that the hypertor spectral sequence combines with the isomorphism in Lemma 2.1(ii) to give an exact sequence

$$\mathrm{Tor}^2_{\mathbb{Z}_p[J]}\big(\mathbb{Z}_p, H^3\big(\mathrm{SC}_F(\Sigma,T)\big)\big) \to H_0(J,M)_{\mathrm{tor}} \to H^2\big(\mathrm{SC}_{F^J}(\Sigma,T)\big)_{\mathrm{tor}}$$

and hence an inequality

$$\begin{aligned}\mathrm{rk}_p\big(H_0(J,M)_{\mathrm{tor}}\big) \le{}& \mathrm{rk}_p\big(H^2\big(\mathrm{SC}_{F^J}(\Sigma,T)\big)_{\mathrm{tor}}\big)\\ &+ \mathrm{rk}_p\big(\mathrm{Tor}^2_{\mathbb{Z}_p[J]}\big(\mathbb{Z}_p, H^3\big(\mathrm{SC}_F(\Sigma,T)\big)\big)\big).\end{aligned}$$

Now, since J is cyclic, the group $\mathrm{Tor}^2_{\mathbb{Z}_p[J]}(\mathbb{Z}_p, H^3(\mathrm{SC}_F(\Sigma,T)))$ can be identified with the subquotient $\hat{H}^{-1}(J, H^3(\mathrm{SC}_F(\Sigma,T)))$ of $H^3(\mathrm{SC}_F(\Sigma,T))$. To deduce the claimed result from the above two displayed inequalities, it is thus enough to use the bound on $\mathrm{rk}_p(H^3(\mathrm{SC}_F(\Sigma,T)))$ given by Lemma 2.1(iii). □

3.4

We now deduce Theorem 1.1 from Proposition 3.3. For any finite extension L of k in K, we set $\Gamma_L := G_{L_\infty/L}$ and we write Λ_L for the associated Iwasawa algebra $\mathbb{Z}_p[[\Gamma_L]]$. We write $\mathrm{SC}_{L_\infty}(\Sigma,T)$ for the complex of Λ_L-modules constructed by taking the inverse limit over m of the complexes $\mathrm{SC}_{L_m}(\Sigma,T)$ with respect to the transition morphisms

$$\mathrm{SC}_{L_m}(\Sigma,T) \to \mathbb{Z}_p[G_{L_{m-1}/L}] \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_{L_m/L}]} \mathrm{SC}_{L_m}(\Sigma,T) \cong \mathrm{SC}_{L_{m-1}}(\Sigma,T)$$

that are induced by Lemma 2.1(ii). Then $\mathrm{SC}_{L_\infty}(\Sigma,T)$ belongs to $D^{\mathrm{perf}}(\Lambda_L)$ (as a consequence of Lemma 2.1(i)), and for each nonnegative integer n there is a natural isomorphism $\mathbb{Z}_p[G_{L_n/L}]\otimes^{\mathbb{L}}_{\Lambda_L}\mathrm{SC}_{L_\infty}(\Sigma,T)\cong\mathrm{SC}_{L_n}(\Sigma,T)$ in $D^{\mathrm{perf}}(\mathbb{Z}_p[G_{L_n/L}])$.

In particular, we may apply the result of Lemma 3.6 below to deduce that for each such n one has

$$\mathrm{rk}_p\big(H^2\big(\mathrm{SC}_{L_n}(\Sigma,T)\big)_{\mathrm{tor}}\big)\le p^n\cdot\mu_L(\Sigma,T)+\kappa_{L_\infty/L}(\Sigma,T), \tag{15}$$

where $\mu_L(\Sigma,T)$ is the μ-invariant of the (finitely generated) Λ_L-module $H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))$, and the nonnegative integer $\kappa_{L_\infty/L}(\Sigma,T)$ depends only on the structures of the Λ_L-modules $H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))$ and $H^3(\mathrm{SC}_{L_\infty}(\Sigma,T))$.

Now if L' is any other finite extension of k in K for which one has $L_\infty=L'_\infty$, then $\Gamma:=\Gamma_L\cap\Gamma_{L'}$ is an open subgroup of $G_{L_\infty/k}$ and

$$[\Gamma_L:\Gamma]\cdot\mu_L(\Sigma,T)=\mu_{(L_\infty)^\Gamma}(\Sigma,T)=[\Gamma_{L'}:\Gamma]\cdot\mu_{L'}(\Sigma,T),$$

and so the rational number

$$\begin{aligned}\mu_{L_\infty}(\Sigma,T):=\frac{\mu_L(\Sigma,T)}{[L:k]}&=\frac{[\Gamma_L:\Gamma]\cdot\mu_L(\Sigma,T)}{[\Gamma_L:\Gamma]\cdot[G_{L_\infty/k}:\Gamma_L]}\\&=\frac{[\Gamma_{L'}:\Gamma]\cdot\mu_{L'}(\Sigma,T)}{[G_{L_\infty/k}:\Gamma]}=\frac{\mu_{L'}(\Sigma,T)}{[G_{L_\infty/k}:\Gamma_{L'}]}=\frac{\mu_{L'}(\Sigma,T)}{[L':k]}\end{aligned}$$

depends only on the field L_∞ rather than L. In addition, if we write $[\Gamma_L:\Gamma]=p^n$ and $[\Gamma_{L'}:\Gamma]=p^{n'}$, then for any nonnegative integer b one has $L_{n+b}=L'_{n'+b}$.

For each of the finitely many intermediate fields E of K/k_∞, we now fix a finite extension E' of k in K with $E=E'_\infty$, and we write μ^* and κ^* for the maximum values of $\mu_E(\Sigma,T)$ and $\kappa_{E/E'}(\Sigma,T)$ as E ranges over this finite set. For any finite extension F of k in K, we write E'_F for the unique field E' as above, for which $E_F:=E'_{F,\infty}$ is equal to F_∞. Then for any large enough integer a, one has $F_a=E'_{F,m(a)}$ for some nonnegative integer $m(a)$ and so (15), with L_∞/L replaced by E_F/F, implies that

$$\begin{aligned}\mathrm{rk}_p\big(H^2\big(\mathrm{SC}_{F_a}(\Sigma,T)\big)_{\mathrm{tor}}\big)&=\mathrm{rk}_p\big(H^2\big(\mathrm{SC}_{E'_{F,m(a)}}(\Sigma,T)\big)_{\mathrm{tor}}\big)\\&\le p^{m(a)}\cdot\mu_{E'_F}(\Sigma,T)+\kappa_{E_F/E'_F}(\Sigma,T)\\&=[E'_{F,m(a)}:k]\cdot\mu_{E_F}(\Sigma,T)+\kappa_{E_F/E'_F}(\Sigma,T)\\&\le[F_a:k]\cdot\mu^*+\kappa^*,\end{aligned}$$

as required. This gives an inequality as in Proposition 3.3 (with $\mu=\mu^*$ and $\kappa'=\kappa^*$) and hence completes the proof of Theorem 1.1.

LEMMA 3.6

Let Γ be a group that is topologically isomorphic to $\mathbb{Z}_p$, and set $\Lambda:=\mathbb{Z}_p[[\Gamma]]$. Let $C^\bullet$ be an object of $D^{\mathrm{perf}}(\Lambda)$, and in each degree i write $\mu^i(C^\bullet)$ for the μ-invariant of the (finitely generated) Λ-module $H^i(C^\bullet)$. Then in each degree i there exists a nonnegative integer $\kappa^i(C^\bullet)$ that depends only on the Λ-module $H^i(C^\bullet)$ and the

Λ-torsion submodule of $H^{i+1}(C^\bullet)$ and is such that for each nonnegative integer n one has $\mathrm{rk}_p(H^i(\mathbb{Z}_p[\Gamma/\Gamma^{p^n}] \otimes^{\mathbb{L}}_\Lambda C^\bullet)_{\mathrm{tor}}) \le p^n \cdot \mu^i(C^\bullet) + \kappa^i(C^\bullet)$.

Proof

For any Λ-module N, we write N_{Tor} for its Λ-torsion submodule and N_{TF} for the quotient N/N_{Tor}. We recall that a finitely generated Λ-torsion module $\mathcal{E}$ is said to be *elementary* if $\mathcal{E} = \mathcal{E}_{\mathrm{tor}} \oplus \mathcal{E}_{\mathrm{tf}}$, where $\mathcal{E}_{\mathrm{tor}}$ is a direct sum of modules $\Lambda/(p^e)$ for suitable natural numbers e and $\mathcal{E}_{\mathrm{tf}}$ is a direct sum of modules $\Lambda/(f)$ for suitable distinguished polynomials f.

In each degree i, we set $M^i := H^i(C^\bullet)$. For each natural number n, we set $\Gamma^n := \Gamma^{p^n}$, write Λ_n for the Iwasawa algebra $\mathbb{Z}_p[[\Gamma^n]]$, and fix a topological generator γ_n of Γ^n. We note that the natural exact triangle $C^\bullet \xrightarrow{1-\gamma_n} C^\bullet \to \mathbb{Z}_p \otimes^{\mathbb{L}}_{\Lambda_n} C^\bullet \to C^\bullet[1]$ in $D^{\mathrm{p}}(\Lambda)$ induces an exact sequence of $\mathbb{Z}_p$-modules

$$0 \to H_0(\Gamma^n, M^i)_{\mathrm{tor}} \to H^i(\mathbb{Z}_p \otimes^{\mathbb{L}}_{\Lambda_n} C^\bullet)_{\mathrm{tor}} \to H^0(\Gamma^n, M^{i+1})_{\mathrm{tor}}$$

and hence an inequality

$$\mathrm{rk}_p\big(H^i(\mathbb{Z}_p \otimes^{\mathbb{L}}_{\Lambda_n} C^\bullet)_{\mathrm{tor}}\big) \le \mathrm{rk}_p\big(H_0(\Gamma^n, M^i)_{\mathrm{tor}}\big) + \mathrm{rk}_p\big(H^0(\Gamma^n, M^{i+1})_{\mathrm{tor}}\big). \tag{16}$$

We now study the two terms on the right-hand side of this inequality separately.

To study the first term, we note that $\mathrm{Tor}^1_{\Lambda_n}(\mathbb{Z}_p, M^i_{\mathrm{TF}})$ is isomorphic to $H^0(\Gamma^n, M^i_{\mathrm{TF}})$ and hence that the tautological exact sequence $0 \to M^i_{\mathrm{Tor}} \to M^i \to M^i_{\mathrm{TF}} \to 0$ induces an exact sequence of $\mathbb{Z}_p$-modules

$$H^0(\Gamma^n, M^i_{\mathrm{TF}}) \to H_0(\Gamma^n, M^i_{\mathrm{Tor}}) \to H_0(\Gamma^n, M^i) \to H_0(\Gamma^n, M^i_{\mathrm{TF}}) \to 0. \tag{17}$$

There is also an exact sequence of Λ-modules $0 \to M^i_{\mathrm{TF}} \to Y^i \to N^i_1 \to 0$ in which Y^i is free and N^i_1 is finite, and by taking Γ^n-coinvariants of this sequence one finds that $H^0(\Gamma^n, M^i_{\mathrm{TF}})$ vanishes and that there is an exact sequence of $\mathbb{Z}_p$-modules

$$0 \to H^0(\Gamma^n, N^i_1) \to H_0(\Gamma^n, M^i_{\mathrm{TF}}) \to H_0(\Gamma^n, Y^i).$$

In particular, since $H_0(\Gamma^n, Y^i)$ is $\mathbb{Z}_p$-free, these facts combine with (17) to give an exact sequence of finite $\mathbb{Z}_p$-modules $H_0(\Gamma^n, M^i_{\mathrm{Tor}})_{\mathrm{tor}} \to H_0(\Gamma^n, M^i)_{\mathrm{tor}} \to H^0(\Gamma^n, N^i_1)$, and hence to inequalities

$$\begin{aligned}
\mathrm{rk}_p\big(H_0(\Gamma^n, M^i)_{\mathrm{tor}}\big) &\le \mathrm{rk}_p\big(H_0(\Gamma^n, M^i_{\mathrm{Tor}})_{\mathrm{tor}}\big) + \mathrm{rk}_p\big(H^0(\Gamma^n, N^i_1)\big) \\
&\le \mathrm{rk}_p\big(H_0(\Gamma^n, M^i_{\mathrm{Tor}})\big) + \mathrm{rk}_p\big(H^0(\Gamma^n, N^i_1)\big) \qquad (18)\\
&\le \mathrm{rk}_p\big(H_0(\Gamma^n, N^i_2)\big) + \mathrm{rk}_p\big(H_0(\Gamma^n, \tilde{M}^i_{\mathrm{Tor}})\big) + \mathrm{rk}_p\big(H^0(\Gamma^n, N^i_1)\big).
\end{aligned}$$

Here N^i_2 denotes the maximal finite Λ-submodule of M^i and $\tilde{M}^i_{\mathrm{Tor}}$ denotes the quotient of M^i_{Tor} by N^i_2, the second inequality is obvious, and the third is a consequence of the obvious exact sequence $H_0(\Gamma^n, N^i_2) \to H_0(\Gamma^n, M^i_{\mathrm{Tor}}) \to H_0(\Gamma^n, \tilde{M}^i_{\mathrm{Tor}})$.

To compute an upper bound on $\mathrm{rk}_p(H_0(\Gamma^n, \tilde{M}^i_{\mathrm{Tor}}))$, we choose an exact sequence of Λ-modules $0 \to \tilde{M}^i_{\mathrm{Tor}} \to \mathcal{E}^i \to N^i_3 \to 0$ in which N^i_3 is finite and $\mathcal{E}^i$ elementary. Then the induced exact sequence $H^0(\Gamma^n, N^i_3) \to H_0(\Gamma^n, \tilde{M}^i_{\mathrm{Tor}}) \to H_0(\Gamma^n, \mathcal{E}^i)$ implies that

$$\begin{aligned}\mathrm{rk}_p\big(H_0(\Gamma^n,\tilde{M}^i_{\mathrm{Tor}})\big) &\le \mathrm{rk}_p\big(H^0(\Gamma^n,N_3^i)\big)+\mathrm{rk}_p\big(H_0(\Gamma^n,\mathcal{E}^i)\big)\\ &\le \mathrm{rk}_p\big(H^0(\Gamma^n,N_3^i)\big)+p^n\cdot\mu^i(C^\bullet)+\mathrm{rk}_p\big(H_0(\Gamma^n,\mathcal{E}^i_{\mathrm{tf}})\big),\end{aligned}$$

where the second inequality is true because the number of direct summands of $\mathcal{E}^i_{\mathrm{tor}}$ is at most the μ-invariant of $\mathcal{E}^i$ (which is equal to $\mu^i(C^\bullet)$) and for each such summand $\Lambda/(p^e)$ one has $\mathrm{rk}_p(H_0(\Gamma^n,\Lambda/(p^e)))=\mathrm{rk}_p((\mathbb{Z}_p/p^e)[\Gamma/\Gamma^n])=p^n$.

After substituting this bound on $\mathrm{rk}_p(H_0(\Gamma^n,\tilde{M}^i_{\mathrm{Tor}}))$ into (18), and recalling that the $\mathbb{Z}_p$-module $\mathcal{E}^i_{\mathrm{tf}}$ is finitely generated and that the modules N_1^i, N_2^i, and N_3^i are all finite, one finds that an upper bound on $\mathrm{rk}_p(H^i(\mathbb{Z}_p\otimes^{\mathbb{L}}_{\Lambda_n}C^\bullet)_{\mathrm{tor}})$ of the stated form will follow from (16), provided that the p-rank of $H^0(\Gamma^n,M^{i+1})_{\mathrm{tor}}$ is bounded independently of n. To show this, we use the equality $H^0(\Gamma^n,M^{i+1})_{\mathrm{tor}}=H^0(\Gamma^n,M^{i+1}_{\mathrm{Tor}})_{\mathrm{tor}}$ and the existence of an exact sequence of torsion Λ-modules $0\to N_4^{i+1}\to M^{i+1}_{\mathrm{Tor}}\to\mathcal{E}^{i+1}$, where N_4^{i+1} is finite and $\mathcal{E}^{i+1}$ is an elementary module. This sequence gives rise to an exact sequence of $\mathbb{Z}_p$-modules $0\to H^0(\Gamma^n,N_4^{i+1})\to H^0(\Gamma^n,M^{i+1}_{\mathrm{Tor}})\to H^0(\Gamma^n,\mathcal{E}^{i+1})$ and hence to an inequality

$$\begin{aligned}\mathrm{rk}_p\big(H^0(\Gamma^n,M^{i+1})_{\mathrm{tor}}\big)=\mathrm{rk}_p\big(H^0(\Gamma^n,M^{i+1}_{\mathrm{Tor}})_{\mathrm{tor}}\big)&\le \mathrm{rk}_p\big(H^0(\Gamma^n,M^{i+1}_{\mathrm{Tor}})\big)\\ &\le \mathrm{rk}_p\big(H^0(\Gamma^n,N_4^{i+1})\big)+\mathrm{rk}_p\big(H^0(\Gamma^n,\mathcal{E}^{i+1})\big)\\ &= \mathrm{rk}_p\big(H^0(\Gamma^n,N_4^{i+1})\big)+\mathrm{rk}_p\big(H^0(\Gamma^n,\mathcal{E}^{i+1}_{\mathrm{tf}})\big),\end{aligned}$$

where the equality is valid because $H^0(\Gamma^n,\mathcal{E}^{i+1}_{\mathrm{tor}})$ vanishes.

Since N_4^{i+1} is finite and $\mathcal{E}^{i+1}_{\mathrm{tf}}$ is a finitely generated $\mathbb{Z}_p$-module, this inequality gives an upper bound on $\mathrm{rk}_p(H^0(\Gamma^n,M^{i+1}_{\mathrm{Tor}})_{\mathrm{tor}})$ that is independent of n and hence completes the proof of the claimed result. □

4. Proof of Corollary 1.4

4.1

We start with a general observation.

For each finite extension L of k in K, we write $Ш_{L_\infty}(T)$, $\mathrm{Sel}_{L_\infty}(T)$, $\mathrm{Sel}'_{L_\infty}(T)$, and $H^2(\mathrm{SC}_{L_\infty}(T))$ for the respective inverse limits $\varprojlim_m Ш_{L_m}(T)$, $\varprojlim_m \mathrm{Sel}_{L_m}(T)$, $\varprojlim_m \mathrm{Sel}'_{L_m}(T)$, and $\varprojlim_m H^2(\mathrm{SC}_{L_m}(T))$ with the transition morphisms in each case taken to be the natural corestriction maps. We also fix a finite set of places Σ of k as in Section 2.1.

LEMMA 4.1

For each finite extension L of k in K, the conditions of Theorem 1.1 imply that the μ-invariants of the Λ_L-modules $H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))$ and $Ш_{L_\infty}(T)$ coincide.

Proof

Since $Ш_{L_n}(T)$ is defined to be the $\mathbb{Z}_p$-torsion subgroup of $\mathrm{Sel}_{L_n}(T)$, it suffices to show that $H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))$ has the same μ-invariant as does the Λ_L-module $\mathrm{Sel}_{L_\infty}(T)$. To do this, we adapt the argument of Lemma 3.4.

We note first that, by taking the inverse limit over $F=L_n$ of the sequences (13) and (14), one obtains exact sequences of Λ_L-modules

$$\begin{cases}\varprojlim_n \bigoplus_{w\in\Sigma_{L_n}\setminus\Sigma^p_{L_n}} H^1(C_f(L_{n,w},T))\to H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))\to H^2(\mathrm{SC}_{L_\infty}(T))\to 0,\\ 0\to \mathrm{Sel}'_{L_\infty}(T)\to H^2(\mathrm{SC}_{L_\infty}(T))\to \varprojlim_n \bigoplus_{w\in\Sigma^p_{L_n}} H^2(L_{n,w},T^0_w)\end{cases}$$

in which, since each place of K above Σ has an open decomposition group in $G_{K/k}$, each of the direct sums $\bigoplus_{w\in\Sigma_{L_n}\setminus\Sigma^p_{L_n}} H^1(C_f(L_{n,w},T))$ and $\bigoplus_{w\in\Sigma^p_{L_n}} H^2(L_{n,w},T^0_w)$ has bounded p-rank as n varies (the first as a consequence of Lemma 2.1(iv) and the second as a consequence of the argument in Lemma 3.4). By applying Lemma 4.2 below to these exact sequences, we can therefore deduce that the μ-invariants of the Λ_L-modules $H^2(\mathrm{SC}_{L_\infty}(\Sigma,T))$, $H^2(\mathrm{SC}_{L_\infty}(T))$ and $\mathrm{Sel}'_{L_\infty}(T)$ coincide.

To compare the μ-invariants of $\mathrm{Sel}'_{L_\infty}(T)$ and $\mathrm{Sel}_{L_\infty}(T)$, we first recall (from the proof of Lemma 3.4) that for each n and each place w of L_n the group $H^1_{f,(2)}(L_{n,w},T^\vee(1))$ is equal to the maximal divisible subgroup of $H^1_{f,(1)}(L_{n,w}, T^\vee(1))$ and hence that there is a natural exact sequence

$$\bigoplus_{w\notin\Sigma^\infty_{L_n}} \big(H^1_{f,(1)}\big(L_{n,w},T^\vee(1)\big)_{\mathrm{cotor}}\big)^\vee \to \mathrm{Sel}_{L_n}(T)\to \mathrm{Sel}'_{L_n}(T)\to 0, \tag{19}$$

where in the direct sum w runs over all non-Archimedean places of L_n, and we write X_{cotor} for the quotient of a $\mathbb{Z}_p$-module X by its maximal divisible subgroup.

Now, for each w outside $\Sigma^\infty_{L_n}\cup\Sigma^p_{L_n}$, the group $(H^1_{f,(1)}(L_{n,w},T^\vee(1))_{\mathrm{cotor}})^\vee$ is isomorphic to a subgroup of $(H^0(I_w,T^\vee(1))^\vee)_{\mathrm{tor}}$ and so vanishes unless w belongs to Σ_{L_n}, in which case

$$\begin{aligned}\mathrm{rk}_p\big(\big(H^1_{f,(1)}\big(L_{n,w},T^\vee(1)\big)_{\mathrm{cotor}}\big)^\vee\big) &\le \mathrm{rk}_p\big(H^0\big(I_w,T^\vee(1)\big)^\vee\big)\le \mathrm{rk}_p\big(\big(T^\vee(1)\big)^\vee\big)\\ &= \mathrm{rk}_p\big(T(-1)\big)=\mathrm{rk}(T).\end{aligned}$$

Also, for w in $\Sigma^p_{L_n}$ local duality implies $H^1_{f,(1)}(L_{n,w},T^\vee(1))_{\mathrm{cotor}}$ is isomorphic to a quotient of $(H^1(L_{n,w},T/T^0_w)_{\mathrm{tor}})^\vee\cong (H^0(L_{n,w},\mathbb{Q}_p/\mathbb{Z}_p\otimes_{\mathbb{Z}_p}T/T^0_w)_{\mathrm{cotor}})^\vee$ and hence to a subquotient of $(\mathbb{Q}_p/\mathbb{Z}_p\otimes_{\mathbb{Z}_p}T/T^0_w)^\vee\cong \ker(T^*\xrightarrow{\varrho}(T^0_w)^*)$, where ϱ is the natural restriction map, so that

$$\begin{aligned}\mathrm{rk}_p\big(\big(H^1_{f,(1)}\big(L_{n,w},T^\vee(1)\big)_{\mathrm{cotor}}\big)^\vee\big) &= \mathrm{rk}_p\big(H^1_{f,(1)}\big(L_{n,w},T^\vee(1)\big)_{\mathrm{cotor}}\big)\\ &\le \mathrm{rk}_p(T^*)=\mathrm{rk}(T).\end{aligned}$$

In particular, since our assumption on the decomposition subgroups of places in Σ implies that there exists an upper bound on the cardinality of Σ_{L_n} that is independent of n, the above observations combine to imply that the p-rank of the first module in (19) is also bounded independently of n.

Thus, by taking the inverse limit over n of these sequences (and again applying Lemma 4.2 below), we can deduce that $\mathrm{Sel}'_{L_\infty}(T)$ and $\mathrm{Sel}_{L_\infty}(T)$ have the same μ-invariant, as required. □

The following result is certainly well known, but for lack of a convenient reference we include a proof.

LEMMA 4.2
Let $\{\phi_m\}_{m\geq 0}$ be an inverse system of $\mathbb{Z}_p[G_{L_m/L}]$-module homomorphisms $\phi_m : X_m \to Y_m$ with the following properties.

(i) *The Λ_L-module $\varprojlim_m X_m$ is finitely generated.*
(ii) *The p-ranks of both $\ker(\phi_m)$ and $\mathrm{cok}(\phi_m)$ are bounded independently of m.*

Then the Λ_L-module $\varprojlim_m Y_m$ is finitely generated and has the same μ-invariant as $\varprojlim_m X_m$.

Proof
Set $X_\infty := \varprojlim_m X_m$, $Y_\infty := \varprojlim_m Y_m$, $Z_1 := \varprojlim_m \ker(\phi_m)$, and $Z_2 := \varprojlim_m \mathrm{cok}(\phi_m)$, and write M_{Tor} for the Λ_L-torsion submodule of any finitely generated Λ_L-module M. We will show that (ii) implies that Z_1 and Z_2 are finitely generated over $\mathbb{Z}_p$. Assuming for the moment that this is true, then the natural exact sequence

$$0 \to Z_1 \to X_\infty \to Y_\infty \to Z_2$$

combines with (i) to imply that Y_∞ is a finitely generated Λ_L-module and also induces an exact sequence of torsion Λ_L-modules

$$0 \to Z_1 \to (X_\infty)_{\mathrm{Tor}} \to (Y_\infty)_{\mathrm{Tor}} \to Z_2,$$

which shows that the μ-invariants of X_∞ and Y_∞ coincide (since μ-invariants are multiplicative on exact sequences of finitely generated torsion Λ_L-modules and the μ-invariants of Z_1 and Z_2 vanish).

To complete the proof, it therefore suffices to show that if U_n is any inverse system of $\mathbb{Z}_p$-modules for which there exists an integer d with $\mathrm{rk}_p(U_n) \leq d$ for all n, then the $\mathbb{Z}_p$-module $U_\infty := \varprojlim_n U_n$ is such that U_∞/p is isomorphic to a subgroup of U_m/p for some m. To do this, write the transition morphisms $U_n/p \to U_{n-1}/p$ as π_n, and note that U_∞/p can be computed as $\varprojlim_n (U_n/p)'$ with $(U_n/p)' := \bigcap_{i\geq 1} \mathrm{im}(\pi_{n+i}) \subseteq U_n/p$. Since each induced transition map $\pi'_n : (U_n/p)' \to (U_{n-1}/p)'$ is surjective, the p-ranks $\mathrm{rk}_p((U_n/p)')$ increase monotonically with n and hence (since they are each at most d) stabilize.

This in turn implies the existence of a natural number n_0 such that π'_n is bijective for each $n \geq n_0$ and so the natural projection map $U_\infty/p \to (U_{n_0}/p)'$ is bijective, as required. □

4.2

We now turn to the proof of Corollary 1.4. We note first that the given assumptions combine with Lemma 4.1 and the argument of Section 3.4 to imply that the rational number μ in Theorem 1.1 can be taken to be zero and hence that the natural number d in Theorem 1.1 is independent of F.

In addition, in this case the proof of Theorem 1.1 combines with the argument of Section 3.2 to prove a stronger version of the inequality (1). To state this, we write C_n for the cyclic group of order p^n and $m_I(K/k,T)$ for each I in $\mathrm{IM}_p(C_n)$ for the maximum multiplicity with which I occurs (up to isomorphism) as a direct summand in any lattice $\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}$ as F/E ranges over cyclic extensions with $k\subseteq E\subseteq F\subset K$, E/k finite, and F_∞/E_∞ of degree p^n, and a ranges over all sufficiently large integers, and in each case $\mathrm{Sel}_{F_a}(T)$ is regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $G_{F_a/E_a}\cong G_{F_\infty/E_\infty}$ with C_n. Then the argument of Section 3.2 combines with the fact that d is independent of n to prove an inequality

$$\sum_{I\in\mathrm{IM}_p(C_n)} m_I(K/k,T)\le p^{n(n-1)d^2}\cdot\kappa_n^d. \tag{20}$$

Now for each extension F_a/E_a as above, the Krull–Schmidt theorem gives an isomorphism of $\mathbb{Z}_p[C_n]$-modules of the form

$$\mathrm{Sel}_{F_a}(T)_{\mathrm{tf}}\cong\Big(\bigoplus_{0\le m\le n}\mathbb{Z}_p[C_m]^{s_{F_a,m}}\Big)\oplus\bigoplus_{I\in\mathrm{IM}_p(C_n)} I^{m_{F_a,I}}, \tag{21}$$

where each integer $s_{F_a,m}$ is nonnegative and each multiplicity $m_{F_a,I}:=m_I(\mathrm{Sel}_{F_a}(T))$ is at most $m_I(K/k,T)$.

In particular, since the inequality (20) implies that each $m_I(K/k,T)$ is at most $p^{n(n-1)d^2}\cdot\kappa_n^d$ and that there are only finitely many I's for which $m_I(K/k,T)$ can be nonzero, there exists a bound δ_{p^n} on the $\mathbb{Z}_p$-ranks of the modules

$$R_{F_a}:=\bigoplus_{I\in\mathrm{IM}_p(C_n)} I^{m_{F_a,I}}$$

that depends only upon K/k, T and n. The isomorphism (21) is therefore a decomposition of the required form (2), at least if one defines $\delta_{[F:E]}$ to be the maximum of δ_{p^m} for nonnegative integers m with $p^m\le[F:E]$.

To deduce the inequality (3), we now set $G:=G_{F_a/E_a}$ and simply note that $\mathbb{Q}_p\cdot\mathrm{Sel}_{E_a}(T)$ identifies with $H^0(G,\mathbb{Q}_p\cdot\mathrm{Sel}_{F_a}(T))$ and hence that the isomorphism (2) implies that

$$\begin{aligned}
[F:E]\cdot\dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\cdot\mathrm{Sel}_{E_a}(T)\big) &= [F:E]\cdot\dim_{\mathbb{Q}_p}\big(H^0\big(G,\mathbb{Q}_p\cdot\mathrm{Sel}_{F_a}(T)\big)\big)\\
&\ge \#G\cdot\sum_{H\le G}\dim_{\mathbb{Q}_p}\big(H^0\big(G,\mathbb{Q}_p[G/H]^{s_{F_a,H}}\big)\big)\\
&= \#G\cdot\sum_{H\le G}s_{F_a,H}\\
&\ge \sum_{H\le G}\dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p[G/H]^{s_{F_a,H}}\big)\\
&= \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\cdot\mathrm{Sel}_{F_a}(T)\big)-\dim_{\mathbb{Q}_p}(\mathbb{Q}_p\cdot R_{F_a})\\
&\ge \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\cdot\mathrm{Sel}_{F_a}(T)\big)-\delta_{[F:E]},
\end{aligned}$$

as required. This completes the proof of Corollary 1.4.

REMARK 4.3

A closer inspection of the arguments used (in Sections 3 and 4) to prove Theorem 1.1 and Corollary 1.4 shows that these results remain true if one replaces all occurrences of $\mathrm{Sel}_F(T)$ by either $H^2(\mathrm{SC}_F(\Sigma, T))$ or $H^2(\mathrm{SC}_F(T))$ or by Greenberg's Selmer group $\mathrm{Sel}'_F(T)$.

Acknowledgments. The author is grateful to both Daniel Macias Castillo and Christian Wuthrich for stimulating discussions. He is also very grateful to the referees for several helpful comments.

References

[1] S. Bloch and K. Kato, "L-functions and Tamagawa numbers of motives" in *The Grothendieck Festschrift, Vol. I*, Progr. Math. **86**, Birkhäuser, Boston, 1990, 333–400. MR 1086888.

[2] D. Burns, D. Macias Castillo, and C. Wuthrich, *On the Galois structure of Selmer groups*, Int. Math. Res. Not. IMRN **2015**, no. 22, 11909–11933. MR 3456708.

[3] P. Deligne, "Valeurs de fonctions L et périodes d'intégrales" in *Automorphic Forms, Representations and L-Functions, Part 2 (Corvallis, 1977)*, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, 1979, 313–346. MR 0546622.

[4] F.-E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Semin. Univ. Hambg. **13** (1940), 357–412. MR 0002133.

[5] T. Fukaya and K. Kato, "A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory" in *Proceedings of the St. Petersburg Mathematical Society, Vol. XII*, Amer. Math. Soc. Transl. Ser. 2 **219**, Amer. Math. Soc., Providence, 2006, 1–85. MR 2276851. DOI 10.1090/trans2/219/01.

[6] R. Greenberg, "Iwasawa theory for p-adic representations" in *Algebraic Number Theory*, Adv. Stud. Pure Math. **17**, Academic Press, Boston, 1989, 97–137. MR 1097613.

[7] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers, I*, Ann. of Math. (2) **76** (1962), 73–92. MR 0140575. DOI 10.2307/1970266.

[8] ———, *Representations of cyclic groups in rings of integers, II*, Ann. of Math. (2) **77** (1963), 318–328. MR 0144980. DOI 10.2307/1970218.

[9] D. Macias Castillo, *On the Krull-Schmidt decomposition of Mordell-Weil groups*, Tokyo J. Math. **40** (2017), 353–378. MR 3743724.

[10] J. Nekovář, *Selmer Complexes*, Astérisque **310**, Soc. Math. France, Paris, 2006. MR 2333680.

[11] B. Perrin-Riou, "Représentations p-adiques ordinaires" in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque **223**, Soc. Math. France, Paris, 1994, 185–220. MR 1293973.

[12] A. V. Yakovlev, *Homological determination of p-adic representations of rings with basis of powers* (in Russian), Izv. Ross. Akad. Nauk Ser. Mat. **34** (1970), 1000–1014; English translation in Izv. Math. **4** (1970), 321–342. MR 0282945.

King's College London, Department of Mathematics, London, United Kingdom;
david.burns@kcl.ac.uk