New York Journal of Mathematics

New York J. Math. **27** (2021) 437–467.

On Bloch–Kato Selmer groups and Iwasawa theory of p-adic Galois representations

Matteo Longo and Stefano Vigni

Abstract. A result due to R. Greenberg gives a relation between the cardinality of Selmer groups of elliptic curves over number fields and the characteristic power series of Pontryagin duals of Selmer groups over cyclotomic $\mathbb{Z}_p$-extensions at good ordinary primes p. We extend Greenberg's result to more general p-adic Galois representations, including a large subclass of those attached to p-ordinary modular forms of weight at least 4 and level $\Gamma_0(N)$ with $p \nmid N$.

Contents

1. Introduction

A classical result of R. Greenberg ([9, Theorem 4.1]) establishes a relation between the cardinality of Selmer groups of elliptic curves over number fields and the characteristic power series of Pontryagin duals of Selmer groups over cyclotomic $\mathbb{Z}_p$-extensions at good ordinary primes p. Our goal in this paper is to extend Greenberg's result to more general p-adic Galois representations, including a large subclass of those coming from p-ordinary modular forms of weight at least 4 and level $\Gamma_0(N)$ with p a prime number such that $p \nmid N$. This generalization of Greenberg's theorem will play a role in our

Received November 11, 2020.

2010 *Mathematics Subject Classification.* 11R23, 11F80.

Key words and phrases. Selmer groups, Iwasawa theory, p-adic Galois representations, modular forms.

The authors are supported by PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic" and by GNSAGA–INdAM.

ISSN 1076-9803/2021

forthcoming paper [17], in which we prove, under some general conjectures in the theory of motives and for all but finitely many ordinary primes p, the p-part of the equivariant Tamagawa number conjecture for Grothendieck motives of modular forms (in the sense of Scholl, *cf.* [28]) of even weight ≥ 4 in analytic rank 1.

Let us begin by recalling Greenberg's result. Let E be an elliptic curve defined over a number field F, let p be a prime number and suppose that E has good ordinary reduction at all primes of F above p. Moreover, assume that the p-primary Selmer group $\mathrm{Sel}_p(E/F)$ of E over F is finite. Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F, set $\Gamma := \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$ and write $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$ for the corresponding Iwasawa algebra with $\mathbb{Z}_p$-coefficients, which we identify with the power series $\mathbb{Z}_p$-algebra $\mathbb{Z}_p[\![W]\!]$. Since $\mathrm{Sel}_p(E/F)$ is finite, the p-primary Selmer group $\mathrm{Sel}_p(E/F_\infty)$ of E over F_∞ is Λ-cotorsion, *i.e.*, the Pontryagin dual of $\mathrm{Sel}_p(E/F_\infty)$ is a torsion Λ-module ([9, Theorem 1.4]). Greenberg's result that is the starting point for the present paper states that if $f_E \in \Lambda$ is the characteristic power series of the Pontryagin dual of $\mathrm{Sel}_p(E/F_\infty)$, then

$$f_E(0) \sim \frac{\#\,\mathrm{Sel}_p(E/F) \cdot \prod_{v \text{ bad}} c_v(E) \cdot \prod_{v|p} \#\big(\tilde{E}_v(\mathbb{F}_v)_p\big)^2}{\#\big(E(F)_p\big)^2}, \tag{1.1}$$

where the symbol $\sim$ means that the two quantities differ by a p-adic unit, $c_v(E)$ is the Tamagawa number of E at a prime v of bad reduction, $\mathbb{F}_v$ is the residue field of F at v, $\tilde{E}_v(\mathbb{F}_v)_p$ is the p-torsion of the group of $\mathbb{F}_v$-rational points of the reduction $\tilde{E}_v$ of E at v and $E(F)_p$ is the p-torsion subgroup of the Mordell–Weil group $E(F)$. Formula (1.1) is a special case of a result of Perrin-Riou (if E has complex multiplication, [23]) and of Schneider (in general, [27, §8]).

To the best of our knowledge, no generalization of this result is currently available to other settings of arithmetic interest, most notably that of modular forms of level $\Gamma_0(N)$ that are ordinary at a prime number $p \nmid N$ (see, however, [13, Theorem 3.3.1] for a result for Galois representations in an anticyclotomic imaginary quadratic context). In this article we offer a generalization of this kind. Now let us describe our main result in more detail.

Given a number field F with absolute Galois group $G_F := \mathrm{Gal}(\bar{F}/F)$ and an odd prime number p, we consider a p-ordinary (in the sense of Greenberg, *cf.* [7]) representation

$$\rho_V : G_F \longrightarrow \mathrm{Aut}_K(V) \simeq \mathrm{GL}_r(K)$$

where V is a vector space of dimension r over a finite extension K of $\mathbb{Q}_p$, equipped with a continuous action of G_F. We assume that ρ_V is crystalline at all primes of F above p, self-dual (*i.e.*, ρ_V is equivalent to the Tate twist of its contragredient representation) and unramified outside a finite set Σ of primes of F including those that either lie above p or are archimedean. Writing $\mathcal{O}$ for the valuation ring of K, we also fix a G_F-stable $\mathcal{O}$-lattice

T inside V, set $A := T \otimes_{\mathcal{O}} (K/\mathcal{O})$ and assume that there exists a non-degenerate, Galois-equivariant pairing

$$T \times A \longrightarrow \mu_{p^\infty},$$

where μ_{p^∞} is the group of p-power roots of unity, so that A and the Tate twist of the Pontryagin dual of T become isomorphic. Finally, we impose on V a number of technical conditions on invariant subspaces and quotients for the ordinary filtration at primes above p; the reader is referred to Assumption 2.1 for details. In particular, in §2.3 we show that, choosing the prime number p judiciously, these properties are enjoyed by the p-adic Galois representation attached by Deligne to a modular form of level $\Gamma_0(N)$ with $p \nmid N$.

As before, let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F and set $\Gamma := \mathrm{Gal}(F_\infty/F)$. Let $\Lambda := \mathcal{O}[\![\Gamma]\!]$ be the Iwasawa algebra of Γ with coefficients in $\mathcal{O}$, which we identify with the power series $\mathcal{O}$-algebra $\mathcal{O}[\![W]\!]$, where W is an indeterminate. Finally, let $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ be the Greenberg Selmer group of A over F_∞ and let $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ be the Bloch–Kato Selmer group of A over F. General control theorems due to Ochiai ([21]) relate $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ and $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)^\Gamma$, and one can think of our paper as a refinement of [21] in which we describe in some cases the (finite) kernel and cokernel of the natural restriction map $\mathrm{Sel}_{\mathrm{BK}}(A/F) \to \mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)^\Gamma$. If $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite, then $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ is a Λ-cotorsion module, *i.e.*, the Pontryagin dual $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)^\vee$ of $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ is a torsion Λ-module. Thus, when $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite we can consider the characteristic power series $\mathcal{F} \in \Lambda$ of $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)^\vee$.

Our main result (Theorem 6.1) is

Theorem 1.1. *If $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite, then $\mathcal{F}(0) \neq 0$ and*

$$\#\big(\mathcal{O}/\mathcal{F}(0)\cdot\mathcal{O}\big) = \#\,\mathrm{Sel}_{\mathrm{BK}}(A/F) \cdot \prod_{\substack{v\in\Sigma \\ v\nmid p}} c_v(A),$$

where $c_v(A)$ is the p-part of the Tamagawa number of A at v.

The Tamagawa numbers $c_v(A)$ are defined in §3.2. It is worth pointing out that our local assumptions at primes of F above p ensure that the term corresponding to $E(F)_p$ in (1.1) is trivial. Moreover, our conditions on the ordinary filtrations at primes v of F above p force all the terms corresponding to $\tilde{E}_v(\mathbb{F}_v)_p$ in (1.1) to be trivial as well. As will be apparent, our strategy for proving Theorem 1.1 is inspired by the arguments of Greenberg in [9, §4].

We conclude this introduction with a couple of remarks of a general nature. First of all, several of our arguments can be adapted to other $\mathbb{Z}_p$-extensions F_∞/F. However, in general this would require modifying the definition of Selmer groups at primes in Σ that are not finitely decomposed in F_∞. Suppose, for instance, that F is an imaginary quadratic field, T is the

p-adic Tate module of an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p and F_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of F. Since prime numbers that are inert in F split completely in F_∞, some of the arguments described in this paper (*e.g.*, the proof of Lemma 5.14) fail and one needs to work with subgroups (or variants) of $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ that are defined by imposing different conditions at primes in Σ that are inert in F. For instance, the definition of Selmer groups in [13, §2.2.3] in the imaginary quadratic case requires that all the local conditions at inert primes be trivial, while in [2] one assumes ordinary-type conditions at those primes. Since the precise local conditions needed depend on the arithmetic situation being investigated, in this paper we chose to work with the cyclotomic $\mathbb{Z}_p$-extension of F exclusively, thus considering only Bloch–Kato Selmer groups as defined below.

Finally, we remark that our interest in $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ instead of the Bloch–Kato Selmer group $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)$ of A over F_∞ is essentially motivated by the applications to [17] of the results in this paper. Actually, the results of Skinner–Urban on the Iwasawa main conjecture in the cyclotomic setting ([31]), which play a crucial role in [17], are formulated in terms of $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ rather than $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)$, which explains the focus of our article. However, alternative settings can certainly be considered; for example, [21, Theorem 2.4] establishes a relation between $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ and $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)^\Gamma$, and it would be desirable to prove a formula for the value at 0 of the characteristic power series of $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)$ analogous to that in Theorem 1.1.

Acknowledgements. We would like to thank Meng Fai Lim for his interest in our work and for valuable comments on a previous version of this paper. We also wish to express our gratitude to the anonymous referee for carefully reading our article and for several helpful remarks and suggestions.

2. Galois representations

We fix the Galois representations that we consider in this paper, specifying our working assumptions. We will then show that these conditions are satisfied by a large class of p-ordinary crystalline representations attached to modular forms.

2.1. Notation and terminology. To begin with, we introduce some general notation and terminology. If p is a prime number and M is a topological $\mathbb{Z}_p$-module, then we write

$$M^\vee := \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$$

for the Pontryagin dual of M. If M is a module over the Galois group $\mathrm{Gal}(E/L)$ of some (Galois) field extension E/L, where L is an extension of $\mathbb{Q}$ or $\mathbb{Q}_\ell$ for some prime ℓ, then we denote by $M(1)$ the Tate twist of M. Let L be a local field of characteristic 0, let $\bar{L}$ be a fixed algebraic closure of

L and let $G_L := \mathrm{Gal}(\bar{L}/L)$ be the absolute Galois group of L. If $\mu_{p^\infty} \subset \bar{L}$ is the group of p-power roots of unity in $\bar{L}$, then local Tate duality

$$\langle \cdot,\cdot \rangle : H^i(G_L, M) \times H^{2-i}\big(G_L, M^\vee(1)\big) \longrightarrow H^2(G_L, \mu_{p^\infty}) \simeq \mathbb{Q}_p/\mathbb{Z}_p$$

identifies $H^i(G_L, M)$ with $H^{2-i}\big(G_L, M^\vee(1)\big)$ for $i = 0, 1$.

Let F be a number field, let $\bar{F}$ be a fixed algebraic closure of F and let

$$G_F := \mathrm{Gal}(\bar{F}/F)$$

be its absolute Galois group. For every prime v of F let F_v be the completion of F at v and let $\mathcal{O}_v$ be the valuation ring of F_v. Moreover, let

$$G_v := \mathrm{Gal}(\bar{F}_v/F_v)$$

be the absolute Galois group of F_v and let $I_v \subset G_v$ be the inertia subgroup.

Let T be a continuous G_F-module, which we assume to be free of finite rank r over the valuation ring $\mathcal{O}$ of a finite extension K of $\mathbb{Q}_p$, where p is an odd prime number. Fix a uniformizer π of $\mathcal{O}$ and set $\mathbb{F} := \mathcal{O}/(\pi)$ for the residue field of K, which is a finite field of characteristic p. Define $V := T \otimes_{\mathcal{O}} K$ and $A := V/T = T \otimes_{\mathcal{O}} (K/\mathcal{O})$, so that T is an $\mathcal{O}$-lattice inside V. Then $A \simeq (K/\mathcal{O})^r$ and $V \simeq K^r$ as groups and vectors spaces, respectively. Moreover, for every integer $n \geq 0$ there is an isomorphism of G_F-modules $T/\pi^n T \simeq A[\pi^n]$, where $A[\pi^n]$ is the π^n-torsion $\mathcal{O}$-submodule of A. Set

$$T^* := \mathrm{Hom}_{\mathbb{Z}_p}(A, \mu_{p^\infty}) = A^\vee(1), \quad V^* := T^* \otimes_{\mathcal{O}} K.$$

Observe that V^* is the Tate twist of the contragredient representation of V. Set also

$$A^* := V^*/T^* = T^* \otimes_{\mathcal{O}} (K/\mathcal{O}).$$

The representation V is *self-dual* if there exists an isomorphism

$$V \simeq V^*$$

of G_F-representations. Let us assume that V is self-dual and fix an isomorphism $\nu : V \xrightarrow{\simeq} V^*$ as above. Suppose that $\nu(T)$ is homothetic to T^*, which means that there exists $\lambda \in K^\times$ such that $\lambda \cdot \nu(T) = T^*$ in V^*; this is an identification of G_F-modules, as the action of G_F is $\mathcal{O}$-linear. The composition of ν with the multiplication-by-λ map on V^* induces an isomorphism of G_F-modules between the quotients $A = V/T$ and $A^* = V^*/T^*$.

The representation V is *ordinary* (in the sense of Greenberg, *cf.* [7]) at a prime $v \,|\, p$ if there exists a filtration $F^i(V)$ of K-vector spaces of V (where $i \in \mathbb{Z}$) such that

- $F^{i+1}(V) \subset F^i(V)$ for all $i \in \mathbb{Z}$;
- there are $j_1, j_2 \in \mathbb{Z}$ such that $F^i(V) = V$ for all $i \leq j_1$ and $F^i(V) = 0$ for all $i \geq j_2$;

- $F^i(V)$ is G_v-stable and I_v acts on the i-th graded piece
$$\mathrm{gr}^i(V) = F^i(V)/F^{i+1}(V)$$
by the i-th power of the cyclotomic character.

If we define $V^+ := \bigcup_{i>0} F^i(V)$, then V^+ admits a filtration on whose graded pieces I_v acts via positive powers of the cyclotomic character. Also, there is a short exact sequence of G_v-representations
$$0 \longrightarrow V^+ \longrightarrow V \longrightarrow V^- \longrightarrow 0 \tag{2.1}$$
such that V^- has a filtration on whose graded pieces I_v acts by non-positive powers of the cyclotomic character. The exact sequence (2.1) is called the *Panchishkin filtration* of V, see [21, Definition 2.2], [22, §5.4]. Define the integers $r^+ := \dim_K(V^+)$ and $r^- := \dim_K(V^-)$. Set $T^+ := V^+ \cap T$ and $T^- := T/T^+$, which are free $\mathcal{O}$-modules of ranks r^+ and r^-, respectively. Finally, identify T^- with its image in V^-, then set
$$A^+ := V^+/T^+ \simeq (K/\mathcal{O})^{r^+}$$
and
$$A^- := V^-/T^- \simeq (K/\mathcal{O})^{r^-}.$$

2.2. Assumptions. Notation being as in §2.1, write
$$\rho_V : G_F \longrightarrow \mathrm{Aut}_K(V) \simeq \mathrm{GL}_r(K)$$
and
$$\rho_T : G_F \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T) \simeq \mathrm{GL}_r(\mathcal{O})$$
for the Galois representations associated with V and T, respectively.

We work under the following assumption, which is slightly more restrictive than the one appearing in [21].

Assumption 2.1.
(1) ρ_V is unramified outside a finite set of primes of F;
(2) ρ_V is crystalline at all primes $v \mid p$;
(3) ρ_V is self-dual;
(4) ρ_V is ordinary at all primes $v \mid p$;
(5) there is a G_F-equivariant, non-degenerate pairing
$$T \times A \longrightarrow \boldsymbol{\mu}_{p^\infty}$$
that induces a non-degenerate pairing $T/p^mT \times A[p^m] \to \boldsymbol{\mu}_{p^m}$ for every integer $m \geq 1$, where $\boldsymbol{\mu}_{p^m}$ is the group of p^m-th roots of unity; in particular, this gives an isomorphism $T^\vee(1) \simeq A$.
(6) for each prime $v \mid p$, one has:
   (a) $H^0(F_v, A) = 0$,
   (b) $H^0(I_v, A^-) = 0$,
   (c) $H^0\big(F_v, (T^-)^\vee(1)\big) = 0$,

(d) there exists a suitable basis such that G_{F_v} acts on A^+ diagonally via non-trivial characters $\eta_1, \dots, \eta_{r^+}$ that do not coincide with the cyclotomic character.

Let us define

$$\Sigma := \{\text{primes of } F \text{ at which } V \text{ is ramified}\} \cup \{\text{primes of } F \text{ above } p\} \cup \{\text{archimedean primes of } F\}, \tag{2.2}$$

which is a finite set.

Remark 2.2. We list some consequences of Assumption 2.1.

(1) Suppose that $\mathrm{gr}^0(V) = F^0(V)/F^1(V) \neq 0$. Then V^- has a subspace where inertia acts trivially, which is ruled out by (6b).
(2) If $H^0(F_v, A) = 0$, then the Galois-equivariant isomorphism $A \simeq T^\vee(1)$ ensures that $H^0\big(F_v, T^\vee(1)\big) = 0$ as well.
(3) If the isomorphism $V \simeq V^*$ induces an isomorphism $(T^\pm)^\vee(1) \simeq A^\mp$ (which is always true in the case of ordinary modular forms considered below), then the condition $H^0\big(F_v, (T^-)^\vee(1)\big) = 0$ is equivalent to the condition $H^0(F_v, A^+) = 0$, which is implied by (6d).
(4) Note that (6b) is not satisfied in the important class of examples of elliptic curves; however, as already observed, our results are well known in the weight 2 case, which is one of the reasons why in the present article we are primarily concerned with higher weight modular forms.

2.3. The case of modular forms. We want to check that if the prime number p is chosen carefully, then Assumption 2.1 is satisfied by the p-adic Galois representation attached to a newform. Let $f(q) = \sum_{n\geq 1} a_n(f)q^n$ be a newform of even weight $k \geq 4$ and level $\Gamma_0(N)$. Let $\mathbb{Q}_f := \mathbb{Q}\big(a_n(f) \mid n \geq 1\big)$ be the Hecke field of f, which is a totally real number field. It is well known that the Fourier coefficients $a_n(f)$ are algebraic integers.

Let p be a prime number such that $p \nmid 2N$ and fix a prime $\mathfrak{p}$ of $\mathbb{Q}_f$ above p. We assume that

$$\mathfrak{p} \text{ is ordinary for } f. \tag{2.3}$$

In other words, we require $a_p(f)$ to be a $\mathfrak{p}$-adic unit, *i.e.*, $a_p(f) \in \mathcal{O}^\times$.

Remark 2.3. Let us say that a prime number p is *ordinary* for f if $p \nmid a_p(f)$. Thanks to results of Serre on eigenvalues of Hecke operators ([30, §7.2]), one can prove that if $k = 2$, then the set of primes that are ordinary for f has density 1, so it is infinite (see, *e.g.*, [5, Proposition 2.2]). On the other hand, it is immediate to check that if p is an ordinary prime for f that is unramified in $\mathbb{Q}_f$, then there exists a prime $\wp$ of $\mathbb{Q}_f$ above p such that f is $\wp$-ordinary. As a consequence, a weight 2 newform satisfies (2.3) with a suitable $\mathfrak{p}$ for infinitely many primes p (in fact, the set of such primes has density 1). On the contrary, the existence of infinitely many ordinary primes for a modular form of weight larger than 2 is, as far as we are aware of, still an open question.

We also assume that

$$a_p(f) \not\equiv 1 \pmod{\mathfrak{p}}. \tag{2.4}$$

Write K for the completion of $\mathbb{Q}_f$ at $\mathfrak{p}$ and $\mathcal{O}$ for the valuation ring of K. As before, set $\mathbb{F} := \mathcal{O}/\mathfrak{p}\mathcal{O}$. Let V be the self-dual twist of the representation $V_{f,\mathfrak{p}}$ of $G_\mathbb{Q}$ attached by Deligne to f and $\mathfrak{p}$ ([4]), so that $V = V_{f,\mathfrak{p}}(k/2)$. Choose a $G_\mathbb{Q}$-stable $\mathcal{O}$-lattice $T \subset V$. The $\mathfrak{p}$-adic representations

$$\rho_{f,\mathfrak{p}} : G_\mathbb{Q} \longrightarrow \mathrm{Aut}_K(V) \simeq \mathrm{GL}_2(K)$$

and

$$\rho_{f,\mathfrak{p},T} : G_\mathbb{Q} \longrightarrow \mathrm{Aut}_\mathcal{O}(T) \simeq \mathrm{GL}_2(\mathcal{O})$$

will play the roles of ρ_V and ρ_T, respectively. In particular, $F = \mathbb{Q}$ in the notation of §2.2.

Now we show that Assumption 2.1 is satisfied by the representation V. First of all, it is well known that V is unramified at all primes $\ell \nmid Np$ and crystalline at p: these properties correspond to conditions (1) and (2) in Assumption 2.1. Furthermore, V is the self-dual twist of $V_{f,\mathfrak{p}}$, so (3) in Assumption 2.1 is satisfied. On the other hand, (5) in Assumption 2.1 corresponds to [18, Proposition 3.1, (2)].

Next, we show that (4) and (6) in Assumption 2.1 are satisfied. If $\ell \nmid Np$ and Frob_ℓ is a geometric Frobenius at ℓ, then the characteristic polynomial of $\rho_V(\mathrm{Frob}_\ell)$ is the Hecke polynomial $X^2 - a_\ell(f)X + \ell^{k-1}$. Let $\alpha \in \mathcal{O}^\times$ be the unit root of $X^2 - a_p(f)X + p^{k-1}$, which exists because f satisfies (2.3), and let δ be the unramified character of the decomposition group $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ given by $\delta(\mathrm{Frob}_p) := \alpha$, where $\mathrm{Frob}_p \in G_p/I_p$ is as above the geometric Frobenius. It is a classical result of Deligne and of Mazur–Wiles (see, *e.g.*, [20, §1.3.5], or [21, Proposition 3.2]) that the restriction of $V_{f,\mathfrak{p}}$ to G_p is equivalent to a representation of the form

$$\begin{pmatrix} \delta & c \\ 0 & \delta^{-1} \cdot \chi_{\mathrm{cyc}}^{1-k} \end{pmatrix},$$

where c is a 1-cocycle with values in $\mathcal{O}$ and $\chi_{\mathrm{cyc}} : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. It follows that the restriction of $V = V_{f,\mathfrak{p}}(k/2)$ to G_p is equivalent to a representation of the form

$$\begin{pmatrix} \delta \cdot \chi_{\mathrm{cyc}}^{k/2} & c \cdot \chi_{\mathrm{cyc}}^{k/2} \\ 0 & \delta^{-1} \cdot \chi_{\mathrm{cyc}}^{1-k/2} \end{pmatrix}.$$

Thus, (4) in Assumption 2.1 is satisfied and there is an exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \longrightarrow V^+ \longrightarrow V \longrightarrow V^- \longrightarrow 0$$

such that V^+ and V^- are 1-dimensional K-vector spaces on which $G_{\mathbb{Q}_p}$ acts via the characters $\delta \cdot \chi_{\mathrm{cyc}}^{k/2}$ and $\delta^{-1} \cdot \chi_{\mathrm{cyc}}^{1-k/2}$, respectively. Since δ is non-trivial, we see that (6d) in Assumption 2.1 is satisfied. Now, I_p acts on $A^- \simeq K/\mathcal{O}$ via the $(1-k/2)$-th power of the cyclotomic character; if $k>2$, then this power is non-trivial, so (6b) in Assumption 2.1 holds. As for (6c), see part (3) of Remark 2.2.

Finally, we prove that (6a) is satisfied. Suppose that $H^0(\mathbb{Q}_p, A) \neq 0$. Then one can find an element $a \in A[\mathfrak{p}]$ such that $\sigma(a) = a$ for all $\sigma \in G_p$. Since $T/\mathfrak{p}T \simeq A[\mathfrak{p}]$, we may regard a as an element of $T/\mathfrak{p}T$. Choose a basis $\{e_1\}$ of the 1-dimensional $\mathbb{F}$-vector space $T^+/\mathfrak{p}T^+$ and complete it to a $\mathbb{F}$-basis $\{e_1, e_2\}$ of $T/\mathfrak{p}T$. The action of $\sigma \in G_p$ on $T/\mathfrak{p}T$ is then given by the matrix

$$\bar{\rho}_{f,\mathfrak{p}}(\sigma) = \begin{pmatrix} \left(\delta \cdot \chi_{\mathrm{cyc}}^{k/2}\right)(\sigma) & \left(c \cdot \chi_{\mathrm{cyc}}^{k/2}\right)(\sigma) \\ 0 & \left(\delta^{-1} \cdot \chi_{\mathrm{cyc}}^{1-k/2}\right)(\sigma) \end{pmatrix} \pmod{\mathfrak{p}}.$$

Write $a = x_1 e_1 + x_2 e_2$ with $x_1, x_2 \in \mathbb{F}$. Let $v \mid p$ be a prime of F, set $\bar{F}_v := \bar{\mathbb{Q}}_p$ and let $G_v := \mathrm{Gal}(\bar{F}_v/F_v) \subset G_p$. The action of $\sigma \in G_v$ on a is given by

$$\sigma(a) = \Big(x_1\big(\delta\cdot\chi_{\mathrm{cyc}}^{k/2}\big)(\sigma) + x_2\big(c\cdot\chi_{\mathrm{cyc}}^{k/2}\big)(\sigma)\Big)e_1 + x_2\Big(\delta^{-1}\cdot\chi_{\mathrm{cyc}}^{1-k/2}\Big)(\sigma)e_2 \pmod{\mathfrak{p}}. \tag{2.5}$$

Then, in light of (2.4), one easily shows from (2.5) that $\sigma(a) \neq a$. First suppose that $x_2 = 0$. Then $x_1 \neq 0$ because $a \neq 0$, so it is enough to find $\sigma \in G_p$ such that $x_1\big(\delta \cdot \chi_{\mathrm{cyc}}^{k/2}\big)(\sigma) \neq 1$. Let $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p)$ be a geometric Frobenius. If $k=2$, then $\mathrm{Frob}_p^j(a) = x_1\bar{\alpha}^j e_1$ for all integers j, where $\bar{\alpha} = \alpha \pmod{\mathfrak{p}}$. Since $\bar{\alpha} \neq 1$, one may find j such that $x_1\bar{\alpha}^j \neq 1$, and so $\sigma(a) \neq a$. If $k > 2$, then a similar argument works. Namely, choose an integer j such that $x_1\alpha^j \neq 1$, pick a lift $F \in G_p$ of Frob_p^j and let $\bar{F}$ be the image of F in $\mathrm{Gal}\big(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p\big)$, so that $\chi_{\mathrm{cyc}}(F) = \chi_{\mathrm{cyc}}(\bar{F})$. If $x_1\alpha^j \cdot \chi_{\mathrm{cyc}}^{k/2}(F) \neq 1$, then we are done; otherwise, since $x_1\alpha^j \neq 1$, we see that $\chi_{\mathrm{cyc}}^{k/2}(\bar{F}) \neq 1$, so the map $\sigma \mapsto \chi_{\mathrm{cyc}}^{k/2}$ is not the trivial character. It follows that $\chi_{\mathrm{cyc}}^{k/2} : \mathrm{Gal}\big(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p\big) \to \mathbb{F}_p^\times$ is surjective, and therefore we can find $\sigma \in I_p$ such that $\chi_{\mathrm{cyc}}^{k/2}(\sigma) \neq 1$. Then

$$\begin{aligned} x_1\big(\delta \cdot \chi_{\mathrm{cyc}}^{k/2}\big)(F\sigma) &= x_1\alpha^j \cdot \chi_{\mathrm{cyc}}^{k/2}(F\sigma) \\ &= x_1\alpha^j \cdot \chi_{\mathrm{cyc}}^{k/2}(F) \cdot \chi_{\mathrm{cyc}}^{k/2}(\sigma) = \chi_{\mathrm{cyc}}^{k/2}(\sigma) \neq 1, \end{aligned}$$

and we are done. The case $x_2 \neq 0$ is similar; in fact, it suffices to show that there exists σ such that $x_2\big(\delta^{-1} \cdot \chi_{\mathrm{cyc}}^{1-k/2}\big)(\sigma) \neq 1$. Choose j such that $x_2\bar{\alpha}^{-j} \neq 1$ and fix a lift $F \in G_p$ of Frob_p^j. If $x_2\alpha^{-j} \cdot \chi_{\mathrm{cyc}}^{1-k/2}(F) \neq 1$, then we are done, otherwise $\chi_{\mathrm{cyc}}^{1-k/2} : \mathrm{Gal}\big(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p\big) \to \mathbb{F}_p^\times$ is surjective, so we can find $\sigma \in I_p$ such that $\chi_{\mathrm{cyc}}^{1-k/2}(\sigma) \neq 1$. It follows that

$$\begin{aligned} x_2\big(\delta \cdot \chi_{\mathrm{cyc}}^{k/2}\big)(F\sigma) &= x_2\alpha^{-j} \cdot \chi_{\mathrm{cyc}}^{1-k/2}(F\sigma) \\ &= x_2\alpha^{-j} \cdot \chi_{\mathrm{cyc}}^{1-k/2}(F) \cdot \chi_{\mathrm{cyc}}^{1-k/2}(\sigma) = \chi_{\mathrm{cyc}}^{1-k/2}(\sigma) \neq 1, \end{aligned}$$

and the proof of (6a) in Assumption 2.1 is complete.

3. Selmer groups

Notation from §2.1 is in force; moreover, we work under Assumption 2.1. As before, let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F. Set $\Gamma := \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$, choose a topological generator γ of Γ and let $\Lambda := \mathcal{O}[\![\Gamma]\!]$ be the Iwasawa algebra of Γ with coefficients in $\mathcal{O}$, which can be identified with the formal power series $\mathcal{O}$-algebra $\mathcal{O}[\![W]\!]$ by sending γ to $W+1$. For every integer $n \geq 0$ write F_n for the n-th layer of F_∞/F, *i.e.*, the unique extension F_n of F such that $F_n \subset F_\infty$ and $\mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$ (in particular, $F_0 = F$). For every prime v of F_n denote by $F_{n,v}$ the completion of F_n at v, let $G_{n,v} := \mathrm{Gal}(\bar{F}_{n,v}/F_{n,v})$ be the absolute Galois group of $F_{n,v}$ and let $I_{n,v} \subset G_{n,v}$ be the inertia subgroup. If $n = 0$, in the previous notation we have $G_v = G_{0,v}$ and $I_v = I_{0,v}$. We also set $G_{\infty,v} := \mathrm{Gal}(\bar{F}_v/F_{\infty,v})$ and denote by $I_{\infty,v}$ its inertia subgroup.

3.1. Local conditions at $\ell \neq p$. Fix an integer $n \geq 0$. Fix also a prime number $\ell \neq p$ and a prime $v \,|\, \ell$ of F_n. For $\star \in \{V, A\}$, define

$$H^1_{\mathrm{ur}}(F_{n,v},\star) := \ker\Big(H^1(F_{n,v},\star) \longrightarrow H^1(I_{n,v},\star)\Big).$$

Here, as customary, $H^1(F_{n,v},\star)$ stands for $H^1(G_{n,v},\star)$. By functoriality, there is a map $H^1(F_{n,v},V) \to H^1(F_{n,v},A)$; set

$$\begin{aligned} H^1_f(F_{n,v},V) &:= H^1_{\mathrm{ur}}(F_{n,v},V),\\ H^1_f(F_{n,v},A) &:= \mathrm{im}\Big(H^1_f(F_{n,v},V) \longrightarrow H^1(F_{n,v},A)\Big). \end{aligned}$$

The commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & H^1_{\mathrm{ur}}(F_{n,v},V) & \longrightarrow & H^1(F_{n,v},V) & \longrightarrow & H^1(I_{n,v},V) \\ & & & \downarrow & & \downarrow \\ 0 \longrightarrow & H^1_{\mathrm{ur}}(F_{n,v},A) & \longrightarrow & H^1(F_{n,v},A) & \longrightarrow & H^1(I_{n,v},A) \end{array}$$

shows that $H^1_f(F_{n,v},A) \subset H^1_{\mathrm{ur}}(F_{n,v},A)$.

3.2. Local Tamagawa numbers. For every prime v of F we introduce the p-part of the Tamagawa number of A at v. As we shall see, the product of these integers will appear in our main result.

Lemma 3.1. *The index $\big[H^1_{\mathrm{ur}}(F_v,A) : H^1_f(F_v,A)\big]$ is finite.*

Proof. See [25, Lemma 1.3.5]. □

The following notion is well defined thanks to Lemma 3.1.

Definition 3.2. Let v be a prime of F. The integer

$$c_v(A) := \big[H^1_{\mathrm{ur}}(F_v, A) : H^1_f(F_v, A)\big]$$

is the *p-part of the Tamagawa number of A at v.*

Recall the finite set Σ from (2.2).

Lemma 3.3. *If $v \notin \Sigma$, then $c_v(A) = 1$.*

Proof. Since T is unramified outside Np, this is [25, Lemma 1.3.5, (iv)]. □

3.3. Local conditions at p. Fix an integer $n \geq 0$ and let $v \,|\, p$ be a prime of F_n.

3.3.1. The Bloch–Kato condition. Let $\mathbf{B}_{\mathrm{cris}}$ be Fontaine's crystalline ring of periods. Define

$$H^1_f(F_{n,v}, V) := \ker\Big(H^1(F_{n,v}, V) \longrightarrow H^1(F_{n,v}, V \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{cris}})\Big)$$

and

$$H^1_f(F_{n,v}, A) := \mathrm{im}\Big(H^1_f(F_{n,v}, V) \longrightarrow H^1(F_{n,v}, A)\Big),$$

where the second arrow is induced by the canonical map $H^1(F_{n,v}, V) \to H^1(F_{n,v}, A)$.

3.3.2. The Greenberg condition. As in §2.1, let $T^+ := T \cap V^+$, $A^+ := V^+/T^+$, $A^- := A/A^+$. For $\star \in \{V, A\}$, define

$$H^1_{\mathrm{ord}}(F_{n,v}, \star) := \ker\Big(H^1(F_{n,v}, \star) \longrightarrow H^1(I_{n,v}, \star^-)\Big),$$

the map being induced by restriction and the canonical projection $\star \twoheadrightarrow \star^-$.

3.3.3. Comparison between local conditions. Let $\mathbf{B}_{\mathrm{dR}}$ be Fontaine's de Rham ring of periods. Define

$$H^1_g(F_{n,v}, V) := \ker\Big(H^1(F_{n,v}, V) \longrightarrow H^1(F_{n,v}, V \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{dR}})\Big).$$

Since $\mathbf{B}_{\mathrm{cris}}$ is a subring of $\mathbf{B}_{\mathrm{dR}}$, there is an inclusion $H^1_f(F_{n,v}, V) \subset H^1_g(F_{n,v}, V)$. Since V is crystalline at p, by [19, Proposition 12.5.8], one has $\mathbf{D}_{\mathrm{cris},F_{n,v}}(V^-) = 0$ (here, as usual, $\mathbf{D}_{\mathrm{cris},F_{n,v}}(W) := (W \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{cris}})^{G_{F_{n,v}}}$ for a $G_{F_{n,v}}$-representation W). Then it follows from [19, Proposition 12.5.7, (2), (ii)] that

$$H^1_f(F_{n,v}, V) = H^1_g(F_{n,v}, V). \tag{3.1}$$

Moreover, by a result of Flach ([6, Lemma 2]; see also [21, Proposition 4.2]), there is an equality

$$H^1_g(F_{n,v}, V) = H^1_{\mathrm{ord}}(F_{n,v}, V). \tag{3.2}$$

Combining (3.1) and (3.2) then yields

$$H^1_f(F_{n,v}, V) = H^1_{\mathrm{ord}}(F_{n,v}, V). \tag{3.3}$$

Finally, in light of (3.3), the commutativity of the square

$$\begin{array}{ccc} H^1(F_{n,v},V) & \longrightarrow & H^1(F_{n,v},A) \\ \downarrow & & \downarrow \\ H^1(I_{n,v},V^-) & \longrightarrow & H^1(I_{n,v},A^-) \end{array}$$

shows that $H^1_f(F_{n,v},A) \subset H^1_{\mathrm{ord}}(F_{n,v},A)$.

3.4. Selmer groups. Now we introduce Selmer groups in the sense of Bloch–Kato and of Greenberg.

3.4.1. The Bloch–Kato Selmer group. Fix an integer $n \geq 0$. The *Bloch–Kato Selmer group of A over F_n* is

$$\mathrm{Sel}_{\mathrm{BK}}(A/F_n) := \ker\left(H^1(F_n,A) \longrightarrow \prod_v \frac{H^1(F_{n,v},A)}{H^1_f(F_{n,v},A)}\right),$$

where v varies over all primes of F_n and the arrow is induced by the localization maps. Moreover, define the *Bloch–Kato Selmer group of A over F_∞* as

$$\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty) := \varinjlim_n \mathrm{Sel}_{\mathrm{BK}}(A/F_n),$$

the direct limit being taken with respect to the usual restriction maps in Galois cohomology.

3.4.2. The Greeenberg Selmer group. Fix an integer $n \geq 0$. The *Greenberg Selmer group of A over F_n* is

$$\mathrm{Sel}_{\mathrm{Gr}}(A/F_n) := \ker\left(H^1(F_n,A) \longrightarrow \prod_{v\nmid p} \frac{H^1(F_{n,v},A)}{H^1_{\mathrm{ur}}(F_{n,v},A)} \times \prod_{v\mid p} \frac{H^1(F_{n,v},A)}{H^1_{\mathrm{ord}}(I_{n,v},A)}\right),$$

where v varies over all primes of F_n and the arrow is induced by the localization maps. Moreover, define the *Greenberg Selmer group of A over F_∞* as

$$\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty) := \varinjlim_n \mathrm{Sel}_{\mathrm{Gr}}(A/F_n), \tag{3.4}$$

the direct limit being taken again with respect to the restriction maps.

Remark 3.4. For Galois representations associated with modular forms, the Selmer group considered in [31] is the Greenberg Selmer group. In many cases, the *strict* Selmer group, which is defined as the Greenbebrg Selmer group with the difference that the local condition at a prime v above p is taken to be the kernel of the map

$$H^1(F_n,A) \longrightarrow \frac{H^1(F_{n,v},A)}{H^1_{\mathrm{ord}}(F_{n,v},A)},$$

is equal to the Bloch–Kato Selmer group (see, *e.g.*, [12, (23)]).

4. Characteristic power series

As before, let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F and put

$$\Gamma := \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p.$$

With notation as in (3.4), set

$$S := \mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty).$$

Furthermore, let

$$X := S^\vee = \mathrm{Hom}(S, \mathbb{Q}_p/\mathbb{Z}_p)$$

be the Pontryagin dual of S. By the topological version of Nakayama's lemma (see, *e.g.*, [1, p. 226, Corollary]), the Λ-module X is finitely generated.

4.1. Invariants and coinvariants of Selmer groups. In what follows, S^Γ (respectively, S_Γ) denotes the $\mathcal{O}$-module of Γ-invariants (respectively, Γ-coinvariants) of S.

Proposition 4.1. *If* $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ *is finite, then* S^Γ *is finite and* S *is a cotorsion* Λ*-module.*

Recall that, by definition, S is Λ-cotorsion if X is Λ-torsion.

Proof. By [21, Theorem 2.4], which can be applied in our setting using [19, Lemma 12.5.7], $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite if and only if $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)^\Gamma$ is. On the other hand, by [21, Proposition 4.2] combined with (3.3), $\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)^\Gamma$ is finite if and only if S^Γ is. Now fix a topological generator γ of Γ. By Pontryagin duality, the finiteness of S^Γ is equivalent to the finiteness of $X/(\gamma-1)X$. By [1, p. 229, Theorem], it follows that X is Λ-torsion, which means that S is a cotorsion Λ-module. □

Remark 4.2. The proof of Proposition 4.1 actually shows that the finiteness of $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is equivalent to the finiteness of S^Γ. Moreover, by [6, Theorem 3] and [21, Proposition 4.1, (1)], for every $n \geq 0$ the finiteness of $\mathrm{Sel}_{\mathrm{BK}}(A/F_n)$ is equivalent to the finiteness of $\mathrm{Sel}_{\mathrm{Gr}}(A/F_n)$.

In particular, when $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite we can consider the characteristic power series $\mathcal{F} \in \mathcal{O}[\![W]\!]$ of X.

Proposition 4.3. *If* S^Γ *is finite, then* S_Γ *is finite,* $\mathcal{F}(0) \neq 0$ *and*

$$\#\big(\mathcal{O}/\mathcal{F}(0)\mathcal{O}\big) = \#S^\Gamma/\#S_\Gamma.$$

Proof. Proceed as in the proof of [9, Lemma 4.2], which only deals with the $\mathcal{O} = \mathbb{Z}_p$ case but carries over to our more general setting in a straightforward way. □

Remark 4.4. Since Γ has cohomological dimension 1 and S is a direct limit of torsion groups, $H^2(\Gamma, S) = 0$; moreover, since $\Gamma \simeq \mathbb{Z}_p$, we have $H^1(\Gamma, S) = S_\Gamma$. It follows that

$$\#S^\Gamma/\#S_\Gamma = \#H^0(\Gamma, S)/\#H^1(\Gamma, S)$$

is the Euler characteristic of M.

From now on we work under

Assumption 4.5. The group $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is finite.

In light of Assumption 4.5, it follows from Propositions 4.1 and 4.3 that

$$S \text{ is } \Lambda\text{-cotorsion, } S^{\Gamma} \text{ and } S_{\Gamma} \text{ are finite, } \mathcal{F}(0) \neq 0 \tag{4.1}$$

and

$$\#\big(\mathcal{O}/\mathcal{F}(0)\cdot\mathcal{O}\big) = \frac{\# S^{\Gamma}}{\# S_{\Gamma}}. \tag{4.2}$$

In the following sections we shall study the quotient on the right hand side of (4.2).

5. Relating $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ and S^{Γ}

We know from §3.1 and §3.3.3 with $n = 0$ that $H^1_f(F_v, A) \subset H^1_{\mathrm{ur}}(F_v, A)$ if $v \nmid p$ and $H^1_f(F_v, A) \subset H^1_{\mathrm{ord}}(F_v, A)$ if $v \mid p$. It follows that there is an inclusion $\mathrm{Sel}_{\mathrm{BK}}(A/F) \subset \mathrm{Sel}_{\mathrm{Gr}}(A/F)$, which can be composed with the canonical map $\mathrm{Sel}_{\mathrm{Gr}}(A/F) \to S$ to produce a map

$$\mathrm{Sel}_{\mathrm{BK}}(A/F) \longrightarrow S. \tag{5.1}$$

Finally, it is straightforward to check that the image of (5.1) is contained in the submodule of Γ-invariants of S, so we obtain a natural map

$$s : \mathrm{Sel}_{\mathrm{BK}}(A/F) \longrightarrow S^{\Gamma}. \tag{5.2}$$

Remark 5.1. Again by §3.1 and §3.3.3, for every $n \geq 0$ there is an inclusion $\mathrm{Sel}_{\mathrm{BK}}(A/F_n) \subset \mathrm{Sel}_{\mathrm{Gr}}(A/F_n)$, so taking direct limits yields an injection

$$\mathrm{Sel}_{\mathrm{BK}}(A/F_\infty) \hookrightarrow S. \tag{5.3}$$

The map s in (5.2) can be equivalently recovered by pre-composing (5.3) with the canonical map $\mathrm{Sel}_{\mathrm{BK}}(A/F) \to \mathrm{Sel}_{\mathrm{BK}}(A/F_\infty)$ and observing that, as above, the image of the resulting map is contained in the submodule of Γ-invariants of S.

Now recall that Assumption 4.5 is in force. As remarked in (4.1), S^{Γ} is finite as well. Then

$$\# S^{\Gamma} = \frac{\#\,\mathrm{Sel}_{\mathrm{BK}}(A/F)\cdot \#\,\mathrm{coker}(s)}{\#\,\ker(s)}. \tag{5.4}$$

Our next goal is to study the orders of the kernel and of the cokernel of s.

5.1. The map r. Set

$$\mathcal{P}_{\mathrm{BK}}(A/F) := \prod_v \frac{H^1(F_v, A)}{H^1_f(F_v, A)}$$

and for every integer $n \geq 0$ set also

$$\mathcal{P}_{\mathrm{Gr}}(A/F_n) := \prod_{v \nmid p} \frac{H^1(F_{n,v}, A)}{H^1_{\mathrm{ur}}(F_{n,v}, A)} \times \prod_{v \mid p} \frac{H^1(F_{n,v}, A)}{H^1_{\mathrm{ord}}(F_{n,v}, A)},$$

where products are taken over all primes of F and of F_n, respectively. With this notation, we can write

$$\mathrm{Sel}_{\mathrm{BK}}(A/F) = \ker\Big(H^1(F, A) \longrightarrow \mathcal{P}_{\mathrm{BK}}(A/F)\Big)$$

and

$$\mathrm{Sel}_{\mathrm{Gr}}(A/F_n) = \ker\Big(H^1(F_n, A) \longrightarrow \mathcal{P}_{\mathrm{Gr}}(A/F_n)\Big).$$

Finally, we define

$$\mathcal{P}_{\mathrm{Gr}}(A/F_\infty) := \varinjlim_n \mathcal{P}_{\mathrm{Gr}}(A/F_n) = \prod_{v \nmid p} \frac{H^1(F_{\infty,v}, A)}{H^1_{\mathrm{ur}}(F_{\infty,v}, A)} \times \prod_{v \mid p} \frac{H^1(F_{\infty,v}, A)}{H^1_{\mathrm{ord}}(F_{\infty,v}, A)} \tag{5.5}$$

where the direct limit is taken with respect to the restriction maps; we also note that if a prime of F_n splits completely in F_m for $m \geq n$, then the corresponding map is the diagonal embedding. By definition, there is an equality

$$\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty) = \ker\Big(H^1(F_\infty, A) \longrightarrow \mathcal{P}_{\mathrm{Gr}}(A/F_\infty)\Big),$$

By construction (see §3.4 and (5.5)), there are natural maps $\mathcal{P}_{\mathrm{BK}}(A/F) \to \mathcal{P}_{\mathrm{Gr}}(A/F)$ and $\mathcal{P}_{\mathrm{Gr}}(A/F) \to \mathcal{P}_{\mathrm{Gr}}(A/F_\infty)$, which produce a map

$$r : \mathcal{P}_{\mathrm{BK}}(A/F) \longrightarrow \mathcal{P}_{\mathrm{Gr}}(A/F_\infty).$$

For every prime v of F let w be a prime of F_∞ above v. The map r is given by a product $r = \prod_{v,w} r_{v,w}$, where

$$r_{v,w} : \frac{H^1(F_v, A)}{H^1_f(F_v, A)} \longrightarrow \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ur}}(F_{\infty,w}, A)}$$

if $v \nmid p$, while

$$r_{v,w} : \frac{H^1(F_v, A)}{H^1_f(F_v, A)} \longrightarrow \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ord}}(F_{\infty,w}, A)}$$

if $v \mid p$. Our next goal is to study the kernel of r prime by prime.

5.1.1. The map $r_{v,w}$ for $v \nmid p$. Assume that $v \nmid p$. Let Σ be the finite set of primes of F introduced in (2.2). We will distinguish two cases: $v \notin \Sigma$ and $v \in \Sigma$.

Lemma 5.2. *If $v \notin \Sigma$, then $r_{v,w}$ is injective.*

Proof. By Lemma 3.3, the kernel of $r_{v,w}$ is the kernel of the restriction map

$$\frac{H^1(F_v, A)}{H^1_{\mathrm{ur}}(F_v, A)} \longrightarrow \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ur}}(F_{\infty,w}, A)}. \tag{5.6}$$

With self-explaining notation, there are injections

$$\frac{H^1(F_v, A)}{H^1_{\mathrm{ur}}(F_v, A)} \hookrightarrow H^1(I_v, A) = \mathrm{Hom}(I_v, A)$$

and

$$\frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ur}}(F_{\infty,w}, A)} \hookrightarrow H^1(I_{\infty,w}, A) = \mathrm{Hom}(I_{\infty,w}, A),$$

where the equalities are a consequence of the fact that A is unramified at v. Therefore, the kernel of (5.6) is contained in the kernel of the natural map

$$\mathrm{Hom}(I_v, A) \longrightarrow \mathrm{Hom}(I_{\infty,w}, A). \tag{5.7}$$

Since v is unramified, $F_{\infty,w}$ is the unramified $\mathbb{Z}_p$-extension of F_v. Thus, $I_v = I_{\infty,w}$ and (5.7) is injective, which concludes the proof. □

It follows from Lemma 5.2 that $\ker(r)$ is the subgroup of $\mathcal{P}_{\mathrm{BK}}(A/F)$ consisting of elements s such that $r_{v,w}(s) = 0$ for all $w \mid v$ with $v \in \Sigma$. Thus, upon setting

$$\mathcal{P}^{\Sigma}_{\mathrm{BK}}(A/F) := \prod_{v\in\Sigma} \frac{H^1(F_v, A)}{H^1_f(F_v, A)}$$

and

$$\mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty) := \prod_{\substack{w\mid v\\ v\in\Sigma,\, v\nmid p}} \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ur}}(F_{\infty,w}, A)} \times \prod_{w\mid v\mid p} \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ord}}(F_{\infty,w}, A)},$$

it follows that $\ker(r) \subset \mathcal{P}^{\Sigma}_{\mathrm{BK}}(A/F)$; more precisely, $\ker(r)$ coincides with the kernel of the restriction map

$$g : \mathcal{P}^{\Sigma}_{\mathrm{BK}}(A/F) \longrightarrow \mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty)^{\Gamma}. \tag{5.8}$$

We conclude that

$$\#\ker(r) = \prod_{\substack{w\mid v\\ v\in\Sigma}} \#\ker(r_{v,w}). \tag{5.9}$$

Lemma 5.3. *If $v \in \Sigma$ and $v \nmid p$, then $\#\ker(r_{v,w}) = c_v(A)$.*

Proof. The map $r_{v,w}$ splits as a composition

$$r_{v,w} : H^1(F_v, A)\big/H^1_f(F_v, A) \longrightarrow H^1(F_v, A)\big/H^1_{\mathrm{ur}}(F_v, A) \longrightarrow H^1(F_{\infty,w}, A)\big/H^1_{\mathrm{ur}}(F_{\infty,w}, A).$$

Thus, since $\#\big(H^1_{\mathrm{ur}}(F_v, A)/H^1_f(F_v, A)\big) = c_v(A)$, it suffices to show that the map

$$H^1(F_v, A)\big/H^1_{\mathrm{ur}}(F_v, A) \longrightarrow H^1(F_{\infty,w}, A)\big/H^1_{\mathrm{ur}}(F_{\infty,w}, A) \tag{5.10}$$

is injective. Let F_v^{ur} be the maximal unramified extension of F_v and set

$$G_v^{\mathrm{ur}} := \mathrm{Gal}(F_v^{\mathrm{ur}}/F_v).$$

There is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_{\mathrm{ur}}(F_v, A) & \longrightarrow & H^1(F_v, A) & \longrightarrow & H^1(I_v, A)^{G_v^{\mathrm{ur}}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1_{\mathrm{ur}}(F_{\infty,w}, A) & \longrightarrow & H^1(F_{\infty,w}, A) & \longrightarrow & H^1(I_{\infty,w}, A) & & \end{array} \tag{5.11}$$

with exact rows. Notice that, since $G_v^{\mathrm{ur}} \simeq \prod_\ell \mathbb{Z}_\ell$, the surjectivity of the right non-trivial map in the top row of (5.11) stems from the vanishing of $H^2(G_v^{\mathrm{ur}}, A)$ ([26, Proposition 1.4.10, (2)]). It follows that the kernel of the map in (5.10) can be identified with the kernel of the rightmost vertical map in (5.11), which is isomorphic (by the inflation-restriction exact sequence) to $H^1\big(I_v/I_{\infty,w}, A^{I_{\infty,w}}\big)^{G_v^{\mathrm{ur}}}$. Since $F_{\infty,w}/F_v$ is unramified if $v \nmid p$, we have $I_v = I_{\infty,w}$, so

$$H^1\big(I_v/I_{\infty,w}, A^{I_{\infty,w}}\big) = 0.$$

It follows that (5.10) is injective, which completes the proof. □

5.1.2. The map $r_{v,w}$ for $v \,|\, p$. Now we study the local conditions at a prime $v \,|\, p$. Recall that, by (3.3), we have $H^1_{\mathrm{ord}}(F_v, V) = H^1_f(F_v, V)$. Moreover, as explained in §3.3.3, there is an inclusion $H^1_f(F_v, A) \subset H^1_{\mathrm{ord}}(F_v, A)$.

The lemma below, whose proof uses in a crucial way the triviality of local invariants from part (6a) in Assumption 2.1, forces the terms corresponding to $\tilde{E}_v(\mathbb{F}_v)$ in (1.1) to be trivial for all primes v of F above p.

Lemma 5.4. *If $v \,|\, p$, then $r_{v,w}$ is injective.*

Proof. To begin with, note that the map $r_{v,w}$ can be written as the composition

$$r_{v,w} : \frac{H^1(F_v, A)}{H^1_f(F_v, A)} \longrightarrow \frac{H^1(F_v, A)}{H^1_{\mathrm{ord}}(F_v, A)} \longrightarrow \frac{H^1(F_{\infty,w}, A)}{H^1_{\mathrm{ord}}(F_{\infty,w}, A)}, \tag{5.12}$$

where the first arrow is induced by the identity map of $H^1(F_v, A)$ and the second by the obvious (restriction) map $H^1(F_v, A) \to H^1(F_{\infty,w}, A)$. Our strategy is to prove that both maps appearing in (5.12) are injective. As we shall see, the proof of the injectivity of the second map is, thanks to Assumption 2.1, straightforward, while dealing with the first map is much more delicate.

We first take care of the second map in (5.12). Let us consider the commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 \longrightarrow & H^1_{\mathrm{ord}}(F_v, A) & \longrightarrow & H^1(F_v, A) & \longrightarrow & H^1(I_v, A^-) \\
& \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & H^1_{\mathrm{ord}}(F_{\infty,w}, A) & \longrightarrow & H^1(F_{\infty,w}, A) & \longrightarrow & H^1(I_{\infty,w}, A^-).
\end{array}$$

The kernel of the rightmost vertical arrow is isomorphic (by the inflation-restriction exact sequence) to $H^1\big(I_v/I_{\infty,w}, (A^-)^{I_{\infty,w}}\big)$. We claim that the group $H^1\big(I_v/I_{\infty,w}, (A^-)^{I_{\infty,w}}\big)$ is trivial. First, observe that $(A^-)^{I_{\infty,w}} = A^-$, because the action of I_v on V factors through the cyclotomic $\mathbb{Z}_p$-extension of F_v, which is totally ramified over v. Since $I_v/I_{\infty,w} \simeq \mathbb{Z}_p$ has cohomological dimension 1, it is enough to show that $H^1\big(I_v/I_{\infty,w}, V^-\big) = 0$. Using the definition of V^-, it can be checked that if γ is a topological generator of $I_v/I_{\infty,w}$, then $V^-/(\gamma - 1) \cdot V^-$ is trivial (*cf.* part (1) of Remark 2.2). On the other hand, $H^1\big(I_v/I_{\infty,w}, V^-\big) \simeq V^-/(\gamma-1)V^-$, so $H^1\big(I_v/I_{\infty,w}, (A^-)^{I_{\infty,w}}\big) = 0$, as claimed. It follows that the second arrow in (5.12) is injective, so $\ker(r_{v,w})$ is equal to the kernel of the first map in (5.12). We tackle the study of this map by adapting arguments from [6] and [21, Proposition 4.2]. Of course, proving that the above-mentioned map is injective amounts to showing that $H^1_f(F_v, A) = H^1_{\mathrm{ord}}(F_v, A)$.

Let us consider the commutative diagram with exact rows

$$\begin{array}{ccccccc}
& & & \dfrac{H^1(F_v,T)}{H^1(F_v,T)_{\mathrm{tors}}} & \xrightarrow{a} & \left(\dfrac{H^1(I_v,T)}{H^1(I_v,T)_{\mathrm{tors}}}\right)^{G_v^{\mathrm{ur}}} \\
& & & \downarrow & & \downarrow \\
0 \longrightarrow & H^1_f(F_v, V) = H^1_{\mathrm{ord}}(F_v, V) & \longrightarrow & H^1(F_v, V) & \xrightarrow{b} & H^1(I_v, V^-)^{G_v^{\mathrm{ur}}} \\
& \downarrow \qquad \searrow g & & \downarrow & & \downarrow \\
& H^1_f(F_v, A) & & & & \\
& \hookdownarrow & & & & \\
0 \longrightarrow & H^1_{\mathrm{ord}}(F_v, A) & \xrightarrow{d} & H^1(F_v, A) & \xrightarrow{c} & H^1(I_v, A^-)^{G_v^{\mathrm{ur}}} \\
& & & \downarrow & & \downarrow \\
& & & H^2(F_v, T)_{\mathrm{tors}} & \longrightarrow & H^2(I_v, T^-)^{G_v^{\mathrm{ur}}}_{\mathrm{tors}}.
\end{array}$$

The map b splits as a composition

$$b : H^1(F_v, V) \xrightarrow{b'} H^1(F_v, V^-) \xrightarrow{b''} H^1(I_v, V^-)^{G_v^{\mathrm{ur}}}.$$

The cokernel of b' injects into $H^2(F_v, V^+)$ and local Tate duality gives an isomorphism $H^2(F_v, V^+) \simeq H^0\big(F_v, (V^-)^\vee(1)\big)$. Since $H^0\big(F_v, (T^-)^\vee(1)\big) = 0$ by part (6c) of Assumption 2.1, $H^0\big(F_v, (V^-)^\vee(1)\big)$ is trivial. On the other hand, the cokernel of b'' injects into $H^2\big(G_v^{\mathrm{ur}}, (V^-)^{I_v}\big)$, which is trivial by [26, Proposition 1.4.10, (2)]. Therefore, the map b is surjective. Moreover, local Tate duality identifies $H^2(F_v, T)$ with $H^0\big(F_v, T^\vee(1)\big)$, which is trivial by Assumption 2.1 (*cf.* part (2) of Remark 2.2), hence $H^2(F_v, T) = 0$. The snake lemma then gives an isomorphism $\mathrm{coker}(a) \simeq \mathrm{coker}(g)$. Now we study the cokernel of a. Let us consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(F_v, T)_{\mathrm{tors}} & \longrightarrow & H^1(F_v, T) & \longrightarrow & \dfrac{H^1(F_v, T)}{H^1(F_v, T)_{\mathrm{tors}}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle a} & & \\
0 & \longrightarrow & H^1(I_v, T^-)^{G_v^{\mathrm{ur}}}_{\mathrm{tors}} & \longrightarrow & H^1(I_v, T^-)^{G_v^{\mathrm{ur}}} & \xrightarrow{e} & \left(\dfrac{H^1(I_v, T^-)}{H^1(I_v, T^-)_{\mathrm{tors}}}\right)^{G_v^{\mathrm{ur}}} & . &
\end{array}$$

The cokernel of e is (isomorphic to) a subgroup of $H^1\big(G_v^{\mathrm{ur}}, H^1(I_v, T^-)_{\mathrm{tors}}\big)$. The group $H^1(I_v, T^-)_{\mathrm{tors}}$ is (isomorphic to) the largest cotorsion quotient of $H^0(I_v, A^-)$; since $H^0(I_v, A^-) = 0$ by part (6b) of Assumption 2.1, the group $H^1\big(G_v^{\mathrm{ur}}, H^1(I_v, T^-)_{\mathrm{tors}}\big)$ is trivial too, and so is $\mathrm{coker}(e)$. It follows that the natural map $\mathrm{coker}(h) \to \mathrm{coker}(a)$ is surjective. On the other hand, the map h can be written as

$$h : H^1(F_v, T) \xrightarrow{h'} H^1(F_v, T^-) \xrightarrow{h''} H^1(I_v, T^-)^{G_v^{\mathrm{ur}}}.$$

The cokernel of h' injects into $H^2(F_v, T^+)$, whose dual $H^0\big(F_v, (T^-)^\vee(1)\big)$ is trivial thanks to part (6c) of Assumption 2.1. Moreover, the cokernel of h'' injects into $H^2\big(G_v^{\mathrm{ur}}, (T^-)^{I_v}\big)$, which is trivial by [26, Proposition 1.4.10, (2)]. Thus, the map h is surjective, and we conclude that the cokernel of a is trivial. Since $\mathrm{coker}(a)$ is isomorphic to $\mathrm{coker}(g)$, it follows that the cokernel of g is trivial as well. This means that g is surjective, *i.e.*, $H^1_f(F_v, A) = H^1_{\mathrm{ord}}(F_v, A)$, as was to be shown. □

If follows from a combination of equality (5.9) and Lemmas 5.3 and 5.4 that

$$\#\ker(r) = \prod_{\substack{v \in \Sigma \\ v \neq p}} c_v(A). \tag{5.13}$$

5.2. Surjectivity of restriction. Denote by F_Σ the maximal extension of F unramified outside Σ, and for any $\mathrm{Gal}(F_\Sigma/F)$-module M set

$$H^i(F_\Sigma/F, M) := H^i\big(\mathrm{Gal}(F_\Sigma/F), M\big).$$

The symbol $H^i(F_\Sigma/F_\infty, M)$ will have an analogous meaning. It follows from Lemma 5.2 that

$$\mathrm{Sel}_{\mathrm{BK}}(A/F) = \ker\Big(H^1(F_\Sigma/F, A) \xrightarrow{\delta_\Sigma} \mathcal{P}^\Sigma_{\mathrm{BK}}(A/F)\Big)$$

and

$$\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty) = \ker\Big(H^1(F_\Sigma/F_\infty, A) \xrightarrow{\delta_{\infty,\Sigma}} \mathcal{P}^\Sigma_{\mathrm{Gr}}(A/F_\infty)\Big),$$

where δ_Σ and $\delta_{\infty,\Sigma}$ are the restriction maps. For notational convenience, if M is a G_F-module and F' is an algebraic extension of F, then we set $M(F') := H^0(F', M)$.

The following lemma, whose proof uses (a global consequence of) part (6a) of Assumption 2.1, implies that the term corresponding to $E(F)_p$ in (1.1) is trivial.

Lemma 5.5. $A(F_\infty) = 0$.

Proof. Since $A = \varinjlim_n A[\pi^n]$, it suffices to show that $A[\pi](F_\infty) = 0$. Recall that $A[\pi]$ is a finite-dimensional vector space over the finite field $\mathbb{F}$ of characteristic p; in particular, $A[\pi]$ is finite. It follows that if $x \in A[\pi]$, then the stabilizer of x in G_F is a closed and finite index subgroup of G_F, so it is equal to $G_{F'}$ for a suitable finite extension F' of F. If, moreover, $x \in A[\pi](F_\infty)$, then $F' \subset F_\infty$, hence $F' = F_n$ for a suitable $n \geq 0$ and $x \in A[\pi](F_n)$. Thus, we are reduced to showing that $A[\pi](F_n) = 0$ for all $n \geq 0$. Since $A[\pi](F) = 0$ by part (6a) of Assumption 2.1 and $[F_{m+1} : F_m] = p$ for all $m \geq 0$, the triviality of $A[\pi](F_n)$ for all $n \geq 0$ follows from [29, Proposition 26] by induction on n. □

Remark 5.6. If we imposed additional assumptions on the representation ρ_V, then we could avoid using part (6a) of Assumption 2.1 to deduce that $A(F_\infty) = 0$. For example, if we required the reduction of ρ_T modulo $\mathfrak{p}$ to be irreducible with non-solvable image (which in the case of non-CM modular forms is true for all but finitely many p, *cf.* [15, Lemma 3.9], [24, §2]), then we could show that $A(F_\infty)$ is trivial by proceeding as in the proof of [16, Lemma 2.4] (see also [15, Lemma 3.10, (2)]). However, the local vanishing from part (6a) of Assumption 2.1 plays a much more delicate role in the proof of Lemma 5.4, which is the reason why we decided to assume this condition right from the outset.

Lemma 5.7. *The map δ_Σ is surjective.*

Proof. We apply some results from [9, Section 4], so we first recall the setting of [9]. Let M be a G_F-module isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^d$ for some integer $d \geq 1$. As in [9], define

$$\begin{aligned} T^* &:= \mathrm{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty}) = M^\vee(1), \\ V^* &:= T^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \\ M^* &:= V^*/T^* = T^* \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p). \end{aligned}$$

Let

$$H^1(F_v, M) \times H^1(F_v, T^*) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

be the local Tate pairing, which is perfect. Suppose that for each $v \in \Sigma$ we have a divisible subgroup L_v of $H^1(F_v, M)$, then consider the Selmer group

$$\mathrm{Sel}(M/F) := \ker\left(H^1(F_\Sigma/F, M) \xrightarrow{\vartheta} \prod_{v\in\Sigma} \frac{H^1(F_v, M)}{L_v} \right), \tag{5.14}$$

where $\vartheta = \prod_{v\in\Sigma} \vartheta_v$ is the product of the maps $\vartheta_v : H^1(F_\Sigma/F, M) \to H^1(F_v, M)/L_v$ obtained by composing the canonical restriction map

$$H^1(F_\Sigma/F, M) \longrightarrow H^1(F_v, M)$$

and the projection $H^1(F_v, M) \to H^1(F_v, M)/L_v$. Furthermore, denote by U_v^* the orthogonal complement of L_v under the local Tate pairing. Write L_v^* for the image in $H^1(F_v, M^*)$ of the $\mathbb{Q}_p$-subspace of $H^1(F_v, V^*)$ generated by the image of U_v^* under the natural map $H^1(F_v, T^*) \to H^1(F_v, V^*)$. Set

$$\mathrm{Sel}(M^*/F) := \ker\left(H^1(F_\Sigma/F, M^*) \longrightarrow \prod_{v\in\Sigma} \frac{H^1(F_v, M^*)}{L_v^*} \right).$$

The arguments in [9, pp. 100–101] show that if the Selmer group $\mathrm{Sel}(M^*/F)$ is finite and $H^0(F_\Sigma/F, M^*)$ is trivial, then ϑ in (5.14) is surjective.

Now we return to our setting, with $M = A$, T and V as in Assumption 2.1. To apply the results explained above, recall that, by Assumption 2.1, the image of T in $V^* = V^\vee(1)$ under the isomorphism $V \simeq V^*$ is homothetic to T^*. Furthermore, the Bloch–Kato conditions $H^1_f(F_v, A)$ and $H^1_f(F_v, A^*)$ are orthogonal under local Tate duality ([3, Proposition 3.8]). Thus,

$$\mathrm{Sel}_{\mathrm{BK}}(A/F) \simeq \mathrm{Sel}_{\mathrm{BK}}(A^*/F),$$

so the finiteness of $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ is equivalent to that of $\mathrm{Sel}_{\mathrm{BK}}(A^*/F)$. To conclude the proof we only need to check that $H^0(F_\Sigma/F, A^*)$ is trivial. Since T and T^* are homothetic, and $A = V/T$, $A^* = V^*/T^*$, it is enough to show that $H^0(F_\Sigma/F, A)$ is trivial. Since A is unramified outside Σ, we have $A = H^0(F_\Sigma, A)$, so $H^0(F_\Sigma/F, A)$ is isomorphic to $H^0(F, A)$, and it is enough to show that $H^0(F, A) = 0$. By Lemma 5.5, $H^0(F_\infty, A) = 0$ and, *a fortiori*, $H^0(F, A) = 0$, concluding the proof. □

5.3. An application of the snake lemma. It follows from Lemma 5.7 that there is a commutative diagram

$$\begin{CD}
0 @>>> \mathrm{Sel}_{\mathrm{BK}}(A/F) @>>> H^1(F_\Sigma/F, A) @>\delta_\Sigma>> \mathcal{P}^\Sigma_{\mathrm{BK}}(A/F) @>>> 0\\
@. @VVsV @VVhV @VVgV \\
0 @>>> S^\Gamma @>>> H^1(F_\Sigma/F_\infty, A)^\Gamma @>\delta^\Gamma_{\infty,\Sigma}>> \mathcal{P}^\Sigma_{\mathrm{Gr}}(A/F_\infty)^\Gamma
\end{CD} \tag{5.15}$$

with exact rows, where s is as in (5.2), h is restriction, g is as in (5.8) and $\delta^{\Gamma}_{\infty,\Sigma}$ is the map induced by $\delta_{\infty,\Sigma}$ between Γ-invariants.

Lemma 5.8. *The map h is an isomorphism and the map s is injective.*

Proof. By inflation-restriction, there is an exact sequence

$$0 \longrightarrow H^1\big(\Gamma, A(F_\infty)\big) \longrightarrow H^1(F_\Sigma/F, A) \xrightarrow{h} H^1(F_\Sigma/F_\infty, A)^\Gamma \longrightarrow H^2\big(\Gamma, A(F_\infty)\big),$$

and we conclude thanks to Lemma 5.5 and the injection $\ker(s) \hookrightarrow \ker(h)$. □

Recall from (4.1) that S^Γ is finite, so $\mathrm{coker}(s)$ is finite.

Lemma 5.9. $\# S^\Gamma = \# \mathrm{Sel}_{\mathrm{BK}}(A/F) \cdot \# \ker(g)$.

Proof. From (5.15), the snake lemma gives an exact sequence

$$\ker(h) \longrightarrow \ker(g) \longrightarrow \mathrm{coker}(s) \longrightarrow \mathrm{coker}(h). \tag{5.16}$$

On the other hand, by Lemma 5.8, both $\ker(h)$ and $\mathrm{coker}(h)$ are trivial, so (5.16) yields an isomorphism $\ker(g) \simeq \mathrm{coker}(s)$. In particular, $\# \mathrm{coker}(s) = \# \ker(g)$, and the searched-for equality follows immediately from (5.4). □

The proposition below provides a crucial step towards our main result.

Proposition 5.10. $\# S^\Gamma = \# \mathrm{Sel}_{\mathrm{BK}}(A/F) \cdot \prod_{\substack{v \in \Sigma \\ v \nmid p}} c_v(A)$.

Proof. Combine Lemma 5.9, the equality $\ker(r) = \ker(g)$ and (5.13). □

5.4. Finite index Λ-submodules. Our present goal is to generalize [9, Proposition 4.9], which shows that if $E_{/F}$ is an elliptic curve, then the group $H^1(F_\Sigma/F, E[p^\infty])$ does not have proper Λ-submodules of finite index. As a consequence, we will see that $S_\Gamma = 0$. As was pointed out to us by the referee, both the fact that $H^1(F_\Sigma/F_\infty, A)$ has no proper Λ-submodules of finite index and (using the finiteness of S_Γ) the vanishing of S_Γ can be alternatively deduced from [10, Proposition 4.1.1]. However, we believe that the more explicit results we shall prove along our way to Proposition 5.15 and Corollary 5.19 may be of independent interest, so we decided to maintain our self-contained exposition in force.

In order to prove this non-existence result, we need four lemmas.

Lemma 5.11. *The map g is surjective.*

Proof. Using the fact that Γ has cohomological dimension 1, one can check that each of the local components defining g is surjective. □

The second lemma we are interested in is a generalization of [9, Lemma 2.3].

Lemma 5.12. *Let v_n be the prime of F_n above p, denote by F_{n,v_n} the completion of F_n at v_n and set $G_{F_{n,v_n}} := \mathrm{Gal}(\bar{\mathbb{Q}}_p/F_{n,v_n})$. Let $\psi : G_{F_v} \to \mathcal{O}^\times$ be a character and write $(K/\mathcal{O})(\psi)$ for the group $K/\mathcal{O}$ with G_{F_v}-action given by ψ. If $\psi|_{G_{F_{n,v_n}}}$ is non-trivial and does not coincide with the cyclotomic character, then the $\mathcal{O}$-corank of $H^1\big(F_{n,v_n}, (K/\mathcal{O})(\psi)\big)$ is $[F_{n,v_v} : \mathbb{Q}_p]$.*

Proof. To simplify the notation, put $C := (K/\mathcal{O})(\psi)$, $M := F_{n,v_n}$ and

$$G_M := \mathrm{Gal}(\bar{\mathbb{Q}}_p/M).$$

Let $T(C)$ be the p-adic Tate module of C, set $V(C) := T(C) \otimes_{\mathcal{O}} K$ and define

$$h_i := \dim_{\mathbb{Q}_p}\Big(H^i\big(M, V(C)\big)\Big)$$

for $i = 0, 1, 2$. Since $\dim_{\mathbb{Q}_p}\big(V(C)\big) = [K : \mathbb{Q}_p]$, the Euler characteristic of $V(C)$ over M is given by the formula

$$h_0 - h_1 + h_2 = -[M : \mathbb{Q}_p] \cdot [K : \mathbb{Q}_p]. \tag{5.17}$$

Let $K(\psi)$ denote K (viewed as a vector space over itself) equipped with the G_{F_v}-action induced by ψ. There is an isomorphism $V(C) \simeq K(\psi)$, so $H^0\big(M, V(C)\big) = 0$, where the restriction of ψ to G_M is non-trivial by assumption. Let $\mathbb{Q}_p(1)$ be the Tate twist of $\mathbb{Q}_p$ and define

$$V(C)^* := \mathrm{Hom}_{\mathbb{Q}_p}\big(V(C), \mathbb{Q}_p(1)\big).$$

The $H^0\big(M, V(C)^*\big) = 0$ because $V(C) \simeq K(\psi)$ and ψ does not coincide with the cyclotomic character. Poitou–Tate duality implies that $H^2\big(M, V(C)\big)$ is dual to $H^0\big(M, V(C)^*\big)$. Since $H^0\big(M, V(C)^*\big) = 0$, we conclude that $H^2\big(M, V(C)\big) = 0$. Therefore, $h_0 = h_2 = 0$ and it follows from (5.17) that $h_1 = [M : \mathbb{Q}_p] \cdot [K : \mathbb{Q}_p]$.

We want to prove that the $\mathbb{Z}_p$-corank of $H^1(M, C)$ is equal to h_1. This completes the proof of the lemma because, by what we have just shown, the $\mathbb{Z}_p$-corank of $H^1(M, C)$ is then equal to $[M : \mathbb{Q}_p] \cdot [K : \mathbb{Q}_p]$ and so its $\mathcal{O}$-corank must be equal to $[M : \mathbb{Q}_p]$. To prove this claim, note that the short exact sequence

$$0 \longrightarrow T(C) \longrightarrow V(C) \longrightarrow C \longrightarrow 0$$

induces an exact sequence

$$H^1\big(M, T(C)\big) \longrightarrow H^1\big(M, V(C)\big) \longrightarrow H^1(M, C) \longrightarrow H^2\big(M, T(C)\big).$$

Set $T(C)^* := \mathrm{Hom}\big(T(C), \mu_{p^\infty}\big)$. By Poitou–Tate duality, $H^2\big(M, T(C)\big)$ is identified with $H^0\big(M, T(C)^*\big)$. Since the action of G_M on $T(C)$ is via ψ, we get an isomorphism

$$H^0\big(M, T(C)^*\big) \simeq H^0\big(M, (K/\mathcal{O})(\chi_{\mathrm{cyc}}\psi^{-1})\big),$$

where $(K/\mathcal{O})(\chi_{\mathrm{cyc}}\psi^{-1})$ is $K/\mathcal{O}$ with Galois action twisted by $\chi_{\mathrm{cyc}}\psi^{-1}$. On the other hand, $\psi \neq \chi_{\mathrm{cyc}}$ by assumption, so $H^0\big(M, T(C)^*\big) = 0$. Thus, $H^2\big(M, V(C)\big)$ is also trivial. Now, by [32, Proposition 2.3], the image of $H^1\big(M,T(C)\big)$ in $H^1\big(M,V(C)\big)$ is a lattice, say P, so the quotient of $H^1\big(M,V(C)\big)$ by P, which is just $H^1(M,C)$ because $H^2\big(M,T(C)\big)=0$, is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{h_1}$. Taking $\mathbb{Z}_p$-duals shows that the $\mathbb{Z}_p$-corank of $H^1(M,C)$ is h_1, as was to be proved. □

Lemma 5.13. *If $v\nmid p$, then $H^0(F_v,A)$ is finite.*

Proof. If $H^0(F_v,A)$ is not finite, then there exists a p-divisible subgroup $B\subset A$ that is fixed by G_{F_v}. Let us choose an element $b\in B[p^M]\smallsetminus\{0\}$ for some integer $M\geq 1$. By part (4) of Assumption 2.1, for every integer $m\geq 1$ there is a G_F-equivariant, non-degenerate pairing

$$(\cdot,\cdot)_m : A[p^m]\times A[p^m]\longrightarrow \boldsymbol{\mu}_{p^m}.$$

Choose $c\in A[p^M]$ such that $(c,b)_M=\zeta_{p^r}$ for a non-trivial, primitive p^r-th root of unity ζ_{p^r} (so $r\leq M$). Using the fact that the representation ρ_T is continuous and $T/p^mT\simeq A[p^m]$ for all $m\geq 1$, there is a finite extension H/F_v with $b,c\in H^0(H,A)$. Since B is divisible, for every $N\geq M$ we can pick an element $b_N\in B[p^N]$ with the property that $p^{N-M}b_N=b$. Then $(c,b_N)_N=\zeta_{p^N}$ for some p^N-th root of unity ζ_{p^N} such that $\zeta_{p^N}^{N-M}=\zeta_{p^r}$; in particular, ζ_{p^N} is a primitive p^{N-M+r}-th root of unity. By assumption, $b_N\in H^0(H,A)$, and then the Galois-equivariance of $(\cdot,\cdot)_N$ ensures that

$$(c,b_N)_N=\sigma(\zeta_{p^N})$$

for all $\sigma\in G_H$. Since N is arbitrary and ζ_{p^N} is a primitive p^{N-M+r}-th root of unity, this implies that H contains the cyclotomic $\mathbb{Z}_p$-extension of F_v, which is impossible because the extension H/F_v is finite. □

The proof of the next lemma, which follows from [7, Propositions 1 and 2], proceeds along the lines of the arguments in [9, p. 94]

Lemma 5.14. *The Λ-corank of $\mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty)$ is $(r-r^+)\cdot[F:\mathbb{Q}]=r^-\cdot[F:\mathbb{Q}]$.*

Proof. Let $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F_\infty)$ denote the factor in $\mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty)$ corresponding to the place v. For $v\nmid p$, $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F_\infty)$ is Λ-cotorsion by [7, Proposition 1]. This result is clear if the prime v is archimedean, as in this case this module has exponent 2. For finite primes $v\nmid p$, $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F)$ is finite: this is a consequence of [7, Proposition 2] combined with Lemma 5.13 and the isomorphism $A\simeq A^\vee(1)$. Since the map $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F)\to\mathcal{P}^{v}_{\mathrm{Gr}}(A/F_\infty)^\Gamma$ is surjective by Lemma 5.11, $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F_\infty)^\Gamma$ is finite as well, which implies that $\mathcal{P}^{v}_{\mathrm{Gr}}(A/F_\infty)$ is Λ-cotorsion; here we are using [9, (2), p. 79] and the fact that all the primes in Σ are finitely decomposed in F_∞.

Now let $v\,|\,p$ be a place of F_∞ and let Γ_v be the corresponding decomposition group. By [7, Proposition 1], the $\mathbb{Z}_p[\![\Gamma_v]\!]$-corank of $H^1(F_{\infty,v},A)$ is equal to

$$r\cdot[F_v:\mathbb{Q}_p]\cdot[K:\mathbb{Q}_p]$$

(to apply this result, note that $K/\mathcal{O} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{[K:\mathbb{Q}_p]}$ as groups). Thus, the $\mathcal{O}[\![\Gamma_v]\!]$-corank of $H^1(F_{\infty,v}, A)$ is $r \cdot [F_v : \mathbb{Q}_p]$. Recall that there is an isomorphism of $\mathcal{O}$-modules $A^+ \simeq (K/\mathcal{O})^{r^+}$, and the action of G_{F_v} on A^+ is via the characters $\eta_1, \dots, \eta_{r^+}$, which are non-trivial and do not coincide with the cyclotomic character by condition (6d) in Assumption 2.1. If v_n denotes the prime of F_n above p, then Lemma 5.12 guarantees that the $\mathcal{O}$-corank of $H^1(F_{n,v_n}, A^+)$ is $r^+ \cdot [F_{n,v_n} : \mathbb{Q}_p]$. This implies that $H^1(F_{\infty,v}, A^+)$ has $\mathcal{O}[\![\Gamma_v]\!]$-corank $r^+ \cdot [F_v : \mathbb{Q}_p]$. Consequently, the $\mathcal{O}[\![\Gamma_v]\!]$-corank of the quotient $H^1(F_{\infty,v}, A)\big/H^1_{\mathrm{ord}}(F_{\infty,v}, A)$ is $(r - r^+) \cdot [F_v : \mathbb{Q}_p]$. Finally, the well-known formula

$$\sum_{v|p} [F_v : \mathbb{Q}_p] = [F : \mathbb{Q}]$$

(see, *e.g.*, [14, p. 39, Corollary 1]) concludes the proof. □

Now we can prove a result establishing, in particular, the non-existence of proper Λ-submodules of finite index of $H^1(F_\Sigma/F_\infty, A)$.

Proposition 5.15. *The Λ-module $H^1(F_\Sigma/F_\infty, A)$ is cofinitely generated of rank $r^- \cdot [F : \mathbb{Q}]$ and has no proper Λ-submodules of finite index.*

Proof. Since $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ is Λ-cotorsion by Proposition 4.1, it follows from Lemma 5.14 that the Λ-corank of $H^1(F_\Sigma/F_\infty, A)$ is at most $r^- \cdot [F : \mathbb{Q}]$. By [7, Proposition 3 and (34)], the Λ-corank of $H^1(F_\Sigma/F_\infty, A)$ is $r^- \cdot [F : \mathbb{Q}]$ and the Λ-corank of $H^2(F_\Sigma/F_\infty, A)$ is 0. Since $H^2(F_\Sigma/F_\infty, A)$ is Λ-cofree by [7, Proposition 4], we deduce that $H^2(F_\Sigma/F_\infty, A) = 0$. The lemma is a consequence of [7, Proposition 5]. □

Remark 5.16. The rank part of Proposition 5.15 corresponds essentially to the so-called *weak Leopoldt conjecture* (see, *e.g.*, [8]).

5.5. Triviality of coinvariants. Recall that $S = \mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$. Our goal here is to prove that $S_\Gamma = 0$. First of all, we need a lemma on the interaction between Pontryagin duals and torsion submodules, which is valid in a slightly more general context.

Lemma 5.17. *Let N be a Λ-algebra, let I be an ideal of Λ and write $N[I]$ for the I-torsion submodule of N. There is an isomorphism of Λ-modules*

$$N^\vee/IN^\vee \simeq N[I]^\vee.$$

Proof. Write $I = (x_1, \dots, x_n)$ and consider the map

$$\xi : N \longrightarrow \prod_{i=1}^n x_i N, \qquad n \longmapsto (x_i n)_{i=1,\dots,n},$$

whose kernel is equal to $N[I]$. If $i : N[I] \hookrightarrow N$ denotes inclusion then Pontryagin duality gives an exact sequence of Λ-modules

$$\left(\prod_{i=1}^n x_i N\right)^\vee \xrightarrow{\xi^\vee} N^\vee \xrightarrow{i^\vee} N[I]^\vee \longrightarrow 0. \tag{5.18}$$

On the other hand, sending $(\varphi_1,\dots,\varphi_n)$ to $\sum_i \varphi_i$ gives an isomorphism between $\prod_i (x_iN)^\vee$ and $\bigl(\prod_i x_iN\bigr)^\vee$, so we can rewrite (5.18) as

$$\prod_{i=1}^n (x_iN)^\vee \xrightarrow{\xi^\vee} N^\vee \xrightarrow{i^\vee} N[I]^\vee \longrightarrow 0. \tag{5.19}$$

In light of (5.19), we want to check that $\mathrm{im}(\xi^\vee) = IN^\vee$. First of all, let

$$\varphi = \sum_{i=1}^n x_i\varphi_i \in IN^\vee,$$

with $\varphi_i \in N^\vee$ for all $i = 1,\dots,n$. Then

$$\varphi = \xi^\vee\bigl((\varphi_1|_{x_1N},\dots,\varphi_n|_{x_nN})\bigr),$$

which shows that $\varphi \in \mathrm{im}(\xi^\vee)$. Conversely, let $\varphi \in \mathrm{im}(\xi^\vee)$; by definition, for every $i = 1,\dots,n$ there exists $\varphi_i \in (x_iN)^\vee$ such that $\varphi = \xi^\vee\bigl((\varphi_1,\dots,\varphi_n)\bigr)$. For every i, the inclusion $x_iN \hookrightarrow N$ gives a surjection $N^\vee \twoheadrightarrow (x_iN)^\vee$. Now for each $i = 1,\dots,n$ choose a lift $\psi_i \in N^\vee$ of φ_i. It follows that $\varphi = \sum_{i=1}^n x_i\psi_i \in IN^\vee$, and the proof is complete. □

The vanishing of S_Γ will be a consequence of the following result.

Proposition 5.18. $H^1(F_\Sigma/F_\infty, A)_\Gamma = 0$.

Proof. By Proposition 5.15, it suffices to show that $H^1(F_\Sigma/F_\infty, A)_\Gamma$ is finite. Let $H^1(F_\Sigma/F_\infty, A)_{\Lambda\text{-div}}$ be the maximal Λ-divisible submodule of $H^1(F_\Sigma/F_\infty, A)$ and define the Λ-module Q via the short exact sequence

$$0 \longrightarrow H^1(F_\Sigma/F_\infty, A)_{\Lambda\text{-div}} \longrightarrow H^1(F_\Sigma/F_\infty, A) \longrightarrow Q \longrightarrow 0. \tag{5.20}$$

The Pontryagin dual $Q^\vee$ of Q is the torsion Λ-submodule of the Pontryagin dual Y of $H^1(F_\Sigma/F_\infty, A)$; it follows from Proposition 5.15 that there is a pseudoisomorphism

$$Y \sim \Lambda^{r^-\cdot[F:\mathbb{Q}]} \oplus Q^\vee, \tag{5.21}$$

and Q is a cofinitely generated cotorsion Λ-module. Set $M := H^1(F_\Sigma/F_\infty, A)$ and fix, as before, a topological generator γ of Γ. Combining the vanishing of $H^2(\Gamma, N)$ for all torsion discrete Γ-modules N (see, *e.g.*, [11, Corollary 4.27]) with the identifications $H^1(\Gamma, N) = N/(\gamma-1)N = N_\Gamma$ for every Γ-module N, exact sequence (5.20) yields an exact sequence

$$0 \longrightarrow M^\Gamma_{\Lambda\text{-div}} \longrightarrow M^\Gamma \longrightarrow Q^\Gamma \longrightarrow (M_{\Lambda\text{-div}})_\Gamma \longrightarrow M_\Gamma \longrightarrow Q_\Gamma \longrightarrow 0 \tag{5.22}$$

in Galois cohomology. Since $(M_{\Lambda\text{-div}})_\Gamma = 0$ because $M_{\Lambda\text{-div}}$ is Λ-divisible, it follows from (5.22) that $M_\Gamma \simeq Q_\Gamma$. Therefore, it is enough to show that Q_Γ is finite. Furthermore, since Q is a finitely generated cotorsion Λ-module, the exact sequence

$$0 \longrightarrow Q^\Gamma \longrightarrow Q \xrightarrow{(\gamma-1)\cdot} Q \longrightarrow Q_\Gamma \longrightarrow 0 \tag{5.23}$$

shows that Q^Γ and Q_Γ have the same $\mathcal{O}$-corank. Thus, we are reduced to proving that the $\mathcal{O}$-corank of Q^Γ is 0.

Lemma 5.14 implies that the $\mathcal{O}$-corank of $\mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty)^{\Gamma}$ is $r^- \cdot [F:\mathbb{Q}]$. By Lemma 5.11 and the finiteness of $\ker(g)$, the $\mathcal{O}$-corank of $\mathcal{P}^{\Sigma}_{\mathrm{BK}}(A/F)$ is $r^- \cdot [F:\mathbb{Q}]$ as well. In addition, the map $\delta_\Sigma : H^1(F_\Sigma/F, A) \twoheadrightarrow \mathcal{P}^{\Sigma}_{\mathrm{BK}}(A/F)$ is, by Lemma 5.7, surjective and has the finite group $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ as its kernel, hence

$$\mathrm{corank}_{\mathcal{O}}\big(H^1(F_\Sigma/F, A)\big) = r^- \cdot [F:\mathbb{Q}]. \tag{5.24}$$

Now consider the inflation-restriction exact sequence

$$\begin{aligned} 0 \longrightarrow H^1\big(\Gamma, A(F_\infty)\big) &\longrightarrow H^1(F_\Sigma/F, A) \\ &\xrightarrow{\theta} H^1(F_\Sigma/F_\infty, A)^{\Gamma} \longrightarrow H^2\big(\Gamma, A(F_\infty)\big). \end{aligned}$$

The map θ is an isomorphism because, by Lemma 5.5, $A(F_\infty) = 0$. Thus, in particular, we get an equality

$$\mathrm{corank}_{\mathcal{O}}\big(H^1(F_\Sigma/F, A)\big) = \mathrm{corank}_{\mathcal{O}}\big(H^1(F_\Sigma/F_\infty, A)^{\Gamma}\big). \tag{5.25}$$

Taking $I = (\gamma - 1)$ and $N = Q$ in Lemma 5.17, we obtain an isomorphism of Λ-modules $(Q^\vee)_\Gamma \simeq \big(Q^\Gamma\big)^\vee$. On the other hand, exact sequence (5.23) with $Q^\vee$ in place of Q shows that $(Q^\vee)^\Gamma$ and $(Q^\vee)_\Gamma$ have the same $\mathcal{O}$-rank. We surmise that

$$\mathrm{rank}_{\mathcal{O}}\big((Q^\vee)^\Gamma\big) = \mathrm{rank}_{\mathcal{O}}\big((Q^\vee)_\Gamma\big) = \mathrm{rank}_{\mathcal{O}}\big((Q^\Gamma)^\vee\big) = \mathrm{corank}_{\mathcal{O}}\big(Q^\Gamma\big). \tag{5.26}$$

Analogously, since $Y = H^1(F_\Sigma/F_\infty, A)^\vee$, we get an equality

$$\mathrm{rank}_{\mathcal{O}}\big(Y^\Gamma\big) = \mathrm{corank}_{\mathcal{O}}\big(H^1(F_\Sigma/F_\infty, A)^\Gamma\big). \tag{5.27}$$

In light of (5.26) and (5.27), pseudoisomorphism (5.21) ensures that

$$\mathrm{corank}_{\mathcal{O}}\big(H^1(F_\Sigma/F_\infty, A)^\Gamma\big) = r^- \cdot [F:\mathbb{Q}] + \mathrm{corank}_{\mathcal{O}}\big(Q^\Gamma\big). \tag{5.28}$$

Finally, combining (5.24), (5.25) and (5.28) gives $\mathrm{corank}_{\mathcal{O}}\big(Q^\Gamma\big) = 0$, as was to be shown. □

Now we can turn to the vanishing result that will play a crucial role in the proof of our main theorem.

Corollary 5.19. $S_\Gamma = 0$.

Proof. With notation as in §5.2, set

$$\tilde{\mathcal{P}}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty) := \mathrm{im}(\delta_{\Sigma,\infty}) \subset \mathcal{P}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty),$$

so that there is a short exact sequence

$$0 \longrightarrow S \longrightarrow H^1(F_\Sigma/F_\infty, A) \xrightarrow{\delta_{\Sigma,\infty}} \tilde{\mathcal{P}}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty) \longrightarrow 0 \tag{5.29}$$

of Γ-modules. Diagram (5.15) and Lemma 5.11 imply that $\delta^{\Gamma}_{\infty,\Sigma}$ is surjective. It follows that $\delta^{\Gamma}_{\infty,\Sigma}$ induces a surjection

$$\delta^{\Gamma}_{\infty,\Sigma} : H^1(F_\Sigma/F_\infty, A)^\Gamma \twoheadrightarrow \tilde{\mathcal{P}}^{\Sigma}_{\mathrm{Gr}}(A/F_\infty)^\Gamma,$$

which we denote by the same symbol. We can extract from the long exact sequence in cohomology associated with (5.29) an exact sequence

$$H^1(F_\Sigma/F_\infty, A)^\Gamma \xrightarrow{\delta^\Gamma_{\infty,\Sigma}} \tilde{\mathcal{P}}^\Sigma_{\mathrm{Gr}}(A/F_\infty)^\Gamma \longrightarrow S_\Gamma \longrightarrow H^1(F_\Sigma/F_\infty, A)_\Gamma.$$

Since $\delta^\Gamma_{\infty,\Sigma}$ is surjective, we deduce that S_Γ embeds into $H^1(F_\Sigma/F_\infty, A)_\Gamma$, and the triviality of S_Γ follows from Proposition 5.18. □

Remark 5.20. A result analogous to Corollary 5.19 in an anticyclotomic imaginary quadratic setting can be found in [13, Lemma 3.3.5].

6. Main result

Putting together the results we have collected so far, we obtain the main theorem of this paper. For the convenience of the reader, we recall our setting.

Let F be a number field, let $\mathcal{O}$ be the valuation ring of a finite field extension K of $\mathbb{Q}_p$ and let T be a free $\mathcal{O}$-module that is equipped with a continuous action of the absolute Galois group of F satisfying Assumption 2.1. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension of F and let $\Lambda := \mathcal{O}[\![\Gamma]\!]$ be the associated Iwasawa algebra, where $\Gamma := \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$. Let $A := T \otimes_{\mathcal{O}} (K/\mathcal{O})$, let $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ be the Greenberg Selmer group of A over F_∞ and let $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ the Bloch–Kato Selmer group of A over F. Finally, let $c_v(A)$ be the p-part of the Tamagawa number of A at a prime v of F and denote by Σ the (finite) set of primes v of F such that either v is archimedean or v lies above p or A is ramified at v. Notice that the finiteness of $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ in the statement below is Assumption 4.5.

Theorem 6.1. *Suppose that* $\mathrm{Sel}_{\mathrm{BK}}(A/F)$ *is finite. Then*

(1) $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$ *is* Λ*-cotorsion;*
(2) *if* $\mathcal{F}$ *is the characteristic power series of the Pontryagin dual of* $\mathrm{Sel}_{\mathrm{Gr}}(A/F_\infty)$*, then* $\mathcal{F}(0) \neq 0$*;*
(3) *there is an equality*

$$\#\big(\mathcal{O}/\mathcal{F}(0)\cdot\mathcal{O}\big) = \#\,\mathrm{Sel}_{\mathrm{BK}}(A/F)\cdot \prod_{\substack{v\in\Sigma\\ v\nmid p}} c_v(A).$$

Proof. Parts (1) and (2) are (4.1), while part (3) follows by combining (4.2), Proposition 5.10 and Corollary 5.19. □

Remark 6.2. Recall that π is a uniformizer of $\mathcal{O}$. The equality in part (3) of Theorem 6.1 can be equivalently formulated as

$$\mathrm{length}_{\mathcal{O}}\big(\mathcal{O}/\mathcal{F}(0)\cdot\mathcal{O}\big) = \mathrm{length}_{\mathcal{O}}\big(\mathrm{Sel}_{\mathrm{BK}}(A/F)\big)\cdot \mathrm{ord}_\pi\Bigg(\prod_{\substack{v\in\Sigma\\ v\nmid p}} c_v(A)\Bigg),$$

where $\mathrm{length}_{\mathcal{O}}(\star)$ denotes the length of the $\mathcal{O}$-module $\star$ and ord_π is the π-adic valuation.

Remark 6.3. An analogue of part (3) of Theorem 6.1 when F is an imaginary quadratic field and F_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of F is provided by Jetchev–Skinner–Wan in [13, Theorem 3.3.1].

References

[1] Balister, Paul N; Howson, Susan. Note on Nakayama's lemma for compact Λ-modules. *Asian J. Math.* **1** (1997), no. 2, 224–229. MR1491983, Zbl 0904.16019, doi: 10.4310/AJM.1997.v1.n2.a2. 449

[2] Bertolini, Massimo; Darmon, Henri. Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions. *Ann. of Math. (2)* **162** (2005), no. 1, 1–64. MR2178960, Zbl 1093.11037, doi: 10.4007/annals.2005.162.1. 440

[3] Bloch, Spencer; Kato, Kazuya. L-functions and Tamagawa numbers of motives. *The Grothendieck Festschrift, I,* 333–400, Progr. Math., 86. *Birkhäuser Boston, Boston, MA*, 1990. MR1086888, Zbl 0768.14001, doi: 10.1007/978-0-8176-4574-8. 457

[4] Deligne, Pierre. Formes modulaires et représentations ℓ-adiques. *Séminaire Bourbaki. 1968/69: Exposés 347–363*, Exp. No. 355, 139–172. Lecture Notes in Math., 175, *Springer, Berlin*, 1971. MR3077124, Zbl 0206.49901, doi: 10.1007/BFb0058810. 444

[5] Fischman, Ami. On the image of Λ-adic Galois representations. *Ann. Inst. Fourier* (Grenoble) **52** (2002), no. 2, 351–378. MR1906479, Zbl 1020.11037, doi: 10.5802/aif.1890. 443

[6] Flach, Matthias. A generalisation of the Cassels–Tate pairing. *J. Reine Angew. Math* **412** (1990), 113–127. MR1079004, Zbl 0711.14001, doi: 10.1515/crll.1990.412.113. 447, 449, 454

[7] Greenberg, Ralph. Iwasawa theory for p-adic representations. *Algebraic number theory*, 97–137, Adv. Stud. Pure Math., 17. *Academic Press, Boston, MA*, 1989. MR1097613, Zbl 0739.11045, doi: 10.2969/aspm/01710097. 438, 441, 460, 461

[8] Greenberg, Ralph. The structure of Selmer groups. *Proc. Nat. Acad. Sci. U.S.A.* **94** (1997), no. 21, 11125–11128. MR1491971, Zbl 0918.11058, doi: 10.1073/pnas.94.21.11125. 461

[9] Greenberg, Ralph. Iwasawa theory for elliptic curves. *Arithmetic theory of elliptic curves* (Cetraro, 1997), 51–144, Lecture Notes in Math., 1716. *Springer, Berlin*, 1999. MR1754686, Zbl 0946.11027, doi: 10.1007/BFb0093451. 437, 438, 439, 449, 456, 457, 458, 460

[10] Greenberg, Ralph. On the structure of Selmer groups. *Elliptic curves, modular forms and Iwasawa theory*, 225–252, Springer Proc. Math. Stat., 188. *Springer, Cham*, 2016. MR3629652, Zbl 1414.11140, doi: 10.1007/978-3-319-45032-2_6. 458

[11] Hida, Haruzo. Modular forms and Galois cohomology. Cambridge Studies in Advanced Mathematics, 69. *Cambridge University Press, Cambridge*, 2000. x+343 pp. ISBN: 0-521-77036-X. MR1779182, Zbl 0952.11014, doi: 10.1017/CBO9780511526046. 462

[12] Howard, Benjamin. Variation of Heegner points in Hida families. *Invent. Math.* **167** (2007), no. 1, 91–128. MR2264805, Zbl 1171.11033, arXiv:1202.6358, doi: 10.1007/s00222-006-0007-0. 448

[13] Jetchev, Dimitar; Skinner, Christopher; Wan, Xin. The Birch and Swinnerton–Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.* **5** (2017), no. 3, 369–434. MR3684675, Zbl 1401.11103, arXiv:1512.06894, doi: 10.4310/CJM.2017.v5.n3.a2. 438, 440, 464, 465

[14] Lang, Serge. Algebraic number theory. Second edition. Graduate Texts in Mathematics, 110. *Springer-Verlag, New York*, 1994. xiv+357 pp. ISBN: 0-387-94225-4. MR1282723, Zbl 0811.11001, doi: 10.1007/978-1-4612-0853-2. 461

[15] Longo, Matteo; Vigni, Stefano. A refined Beilinson–Bloch conjecture for motives of modular forms. *Trans. Amer. Math. Soc.* **369** (2017), no. 10, 7301–7342. MR3683110, Zbl 1432.14008, arXiv:1303.4335, doi: 10.1090/tran/6947. 456

[16] Longo, Matteo; Vigni, Stefano. Kolyvagin systems and Iwasawa theory of generalized Heegner cycles. *Kyoto J. Math.* **59** (2019), no. 3, 717–746. MR3990184, Zbl 1450.11116, arXiv:1605.03168, doi: 10.1215/21562261-2019-0005. 456

[17] Longo, Matteo; Vigni, Stefano. The equivariant Tamagawa number conjecture and Kolyvagin's conjecture for motives of modular forms. Preprint, 2021. 438, 440

[18] Nekovář, Jan. Kolyvagin's method for Chow groups of Kuga–Sato varieties. *Invent. Math.* **107** (1992), no. 1, 99–125. MR1135466, Zbl 0729.14004, doi: 10.1007/BF01231883. 444

[19] Nekovář, Jan. Selmer complexes. *Astérisque* **310** (2006), viii+559 pp. ISBN: 978-2-85629-226-6. MR2333680, Zbl 1211.11120, 447, 449

[20] Nekovář, Jan; Plater, Andrew. On the parity of ranks of Selmer groups. *Asian J. Math.* **4** (2000), no. 2, 437–497. MR1797592, Zbl 0973.11066, doi: 10.4310/AJM.2000.v4.n2.a11. 444

[21] Ochiai, Tadashi. Control theorem for Bloch–Kato's Selmer groups of p-adic representations. *J. Number Theory* **82** (2000), no. 1, 69–90. MR1755154, Zbl 0989.11029, doi: 10.1006/jnth.1999.2483. 439, 440, 442, 444, 447, 449, 454

[22] Panchishkin, Alexei A. Motives over totally real fields and p-adic L-functions. *Ann. Inst. Fourier (Grenoble)* **44** (1994), no. 4, 989–1023. MR1306547, Zbl 0808.11034, doi: 10.5802/aif.1424. 442

[23] Perrin-Riou, Bernadette. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Mém. Soc. Math. France (N.S.)* **17** (1984), 130 pp. MR0799673, Zbl 0599.14020, doi: 10.24033/msmf.318. 438

[24] Ribet, Kenneth A. On l-adic representations attached to modular forms II. *Glasgow Math. J.* **27** (1985), 185–194. MR0819838, Zbl 0596.10027, doi: 10.1017/S0017089500006170. 456

[25] Rubin, Karl. Euler systems. Annals of Mathematics Studies, 147. *Princeton University Press, Princeton, NJ*, 2000. xii+227 pp. ISBN: 0-691-05075-9; 0-691-05076-7. MR1749177, Zbl 0977.11001, doi: 10.1515/9781400865208. 446, 447

[26] Rubin, Karl. Euler systems and Kolyvagin systems. *Arithmetic of L-functions*, 449–499, IAS/Park City Math. Ser., 18. *Amer. Math. Soc., Providence, RI,* 2011. MR2882697, doi: 10.1090/pcms/018. 453, 455

[27] Schneider, Peter. Iwasawa L-functions of varieties over algebraic number fields. A first approach. *Invent. Math.* **71** (1983), no. 2, 251–293. MR0689645, Zbl 0511.14010, doi: 10.1007/BF01389099. 438

[28] Scholl, Anthony J. Motives for modular forms. *Invent. Math.* **100** (1990), no. 2, 419–430. MR1047142, Zbl 0760.14002, doi: 10.1007/BF01231194. 438

[29] Serre, Jean-Pierre. Linear representations of finite groups. Graduate Texts in Mathematics, 42. *Springer-Verlag, New York-Heidelberg*, 1977. x+170 pp. ISBN: 0-387-90190-6. MR0450380, Zbl 0355.20006, doi: 10.1007/978-1-4684-9458-7. 456

[30] Serre, Jean-Pierre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR0644559, Zbl 0496.12011, doi: 10.1007/BF02698692. 443

[31] Skinner, Christopher; Urban, Eric. The Iwasawa main conjectures for GL_2. *Invent. Math.* **195** (2014), no. 1, 1–277. MR3148103, Zbl 1301.11074, doi: 10.1007/s00222-013-0448-1. 440, 448

[32] Tate, John. Relations between K_2 and Galois cohomology. *Invent. Math.* **36** (1976), 257–274. MR0429837, Zbl 0359.12011, doi: 10.1007/BF01390012. 459

(Matteo Longo) Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy
mlongo@math.unipd.it

(Stefano Vigni) Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, 16146 Genova, Italy
stefano.vigni@unige.it

This paper is available via http://nyjm.albany.edu/j/2021/27-17.html.