CONTROL THEOREMS FOR ELLIPTIC CURVES OVER FUNCTION FIELDS

A. BANDINI, I. LONGHI

Abstract. Let F be a global field of characteristic $p > 0$, $\mathcal{F}/F$ a Galois extension with $Gal(\mathcal{F}/F) \simeq \mathbb{Z}_p^{\mathbb{N}}$ and E/F a non-isotrivial elliptic curve. We study the behaviour of Selmer groups $Sel_E(L)_l$ (l any prime) as L varies through the subextensions of $\mathcal{F}$ via appropriate versions of Mazur's Control Theorem. In the case $l = p$ we let $\mathcal{F} = \bigcup \mathcal{F}_d$ where $\mathcal{F}_d/F$ is a $\mathbb{Z}_p^d$-extension. We prove that $Sel_E(\mathcal{F}_d)_p$ is a cofinitely generated $\mathbb{Z}_p[[Gal(\mathcal{F}_d/F)]]$-module and we associate to its Pontrjagin dual a Fitting ideal. This allows to define an algebraic L-function associated to E in $\mathbb{Z}_p[[Gal(\mathcal{F}/F)]]$, providing an ingredient for a function field analogue of Iwasawa's Main Conjecture for elliptic curves.

Keywords: Function fields; elliptic curves; Selmer groups; Iwasawa theory; Fitting ideals.

MSC2000: 11G05, 11R23, 11R58.

1. Introduction

1.1. **Some motivation.** Iwasawa theory for elliptic curves over number fields is by now an established subject, well developed both in its analytic and algebraic sides. By contrast, its analogue over global function fields is still at its beginnings: as far as the authors know, up to now only analytic aspects have been investigated[1]. Our goal in this paper is to provide some first steps into understanding the algebraic side as well. To relate the two points of view we end by proposing a first version of Iwasawa's Main Conjecture, which we hope to investigate in some future work. We are conscious that our Conjecture 5.11 is too coarsely formulated to be completely satisfactory; however, our point is mainly to show that it is possible to ask questions of this kind also in the characteristic p setting.

We fix F a function field of transcendence degree 1 over its constant field $\mathbb{F}_q$, q a power of a prime p, and an elliptic curve E/F; we assume that E is non-isotrivial (i.e., $j(E) \notin \mathbb{F}_q$). In particular, E has bad

[1]The situation has changed very recently: see forthcoming papers by Ochiai-Trihan and by K.-S. Tan.

reduction at some place of F; replacing, if needed, F by a finite extension, we can (and will) assume that E has good or split multiplicative reduction at any place v of F.

1.2. **Analytic theory.** We briefly review the state of the art.

1.2.1. *The extensions.* Let $\widetilde{\mathcal{F}}/F$ be an infinite Galois extension such that $Gal(\widetilde{\mathcal{F}}/F)$ contains a finite index subgroup Γ isomorphic to $\mathbb{Z}_p^{\mathbb{N}}$ (an infinite product of $\mathbb{Z}_p$'s). The reader is reminded that class field theory provides lots of such extensions, thanks to the fact that if L is a local field in characteristic p and $U_1(L)$ denotes its group of 1-units then $U_1(L) \simeq \mathbb{Z}_p^{\mathbb{N}}$ (see e.g. [19, II.5.7]). Observe that, exactly for this reason, in the function field setting it becomes quite natural to concentrate on such a Γ rather than on a finite dimensional p-adic Lie group.

A good example, which closely parallels the classical cyclotomic $\mathbb{Z}_p$-extension of a number field, is the "cyclotomic extension at $\mathfrak{p}$". In the simplest formulation, we take $F := \mathbb{F}_q(T)$, $A := \mathbb{F}_q[T]$ and let Φ be the Carlitz module (see e.g. [21, Chapter 12]). Choose $\mathfrak{p}$ a prime of A and, for any positive integer n, let $\Phi[\mathfrak{p}^n]$ denote the $\mathfrak{p}^n$-torsion of the Carlitz module. Let $F(\Phi[\mathfrak{p}^n])$ be the extension of F obtained via the $\mathfrak{p}^n$-torsion and let $\widetilde{\mathcal{F}} := F(\Phi[\mathfrak{p}^\infty]) = \bigcup F(\Phi[\mathfrak{p}^n])$. It is well known that $F(\Phi[\mathfrak{p}^n])/F$ is a Galois extension and that

$$Gal(F(\Phi[\mathfrak{p}^n])/F) \simeq (A/\mathfrak{p}^n)^* \ ,$$

$$Gal(\widetilde{\mathcal{F}}/F) \simeq \varprojlim_n (A/\mathfrak{p}^n)^* \simeq \mathbb{Z}_p^{\mathbb{N}} \times (A/\mathfrak{p})^* \ .$$

1.2.2. *The "p-adic L-function".* Here by p-adic L-function we mean an element in the Iwasawa algebra $\mathbb{Z}_p[[Gal(\widetilde{\mathcal{F}}/F)]]$ (identified with the algebra of $\mathbb{Z}_p$-valued measures on $Gal(\widetilde{\mathcal{F}}/F)$): to our knowledge, up to now no satisfactory closer analogue of the usual p-adic L-function arising in characteristic 0 was found. (A key problem seems to be the lack of an adequate theory of Mellin transform, in spite of some attempts by Goss - see [6].)

The first instance of construction of a measure related to E is due to Teitelbaum ([24, pag. 290-292]): the $\widetilde{\mathcal{F}}$ he implicitly considers is exactly the Carlitz cyclotomic extension at $\mathfrak{p}$ described above (where $\mathfrak{p}$ is a prime of split multiplicative reduction for E). Other examples (which can be loosely described as cyclotomic and anticyclotomic at ∞) were given in [14]. For a more detailed discussion see section 5.2.

1.3. **The present work.** Since in this paper we are not going to work out a comparison with the analytic theory, our attention will be focussed only on a $\mathbb{Z}_p^{\mathbb{N}}$-extension $\mathcal{F}/F$, i.e. a Galois extension such that $\Gamma := Gal(\mathcal{F}/F) \simeq \mathbb{Z}_p^{\mathbb{N}}$. For example, in the situation described above, one can take $\mathcal{F}$ to be the subfield of $F(\Phi[\mathfrak{p}^\infty])$ fixed by $(A/\mathfrak{p})^*$: then $\mathcal{F}/F$ is a $\mathbb{Z}_p^{\mathbb{N}}$-extension. We shall consider $\mathbb{Z}_p^d$-extensions $\mathcal{F}_d/F$ such that $\mathcal{F} = \bigcup \mathcal{F}_d$.

Denote by $\Lambda := \mathbb{Z}_p[[\Gamma]]$ and by $\Lambda_d := \mathbb{Z}_p[[Gal(\mathcal{F}_d/F)]]$ the associated Iwasawa algebras.

In section 2 we will define the (p-part of the) Selmer group $Sel_E(L)_p$, L any algebraic extension of F. For any d, let $\mathcal{S}_d$ (resp. $\mathcal{S}$) be the Pontrjagin dual of $Sel_E(\mathcal{F}_d)_p$ (resp. of $Sel_E(\mathcal{F})_p$): it is a Λ_d-module (resp. a Λ-module). The main result of this paper is the following.

Theorem 1.1. *Assume that all ramified primes in $\mathcal{F}_d/F$ are of split multiplicative reduction for E. Then $\mathcal{S}_d$ is a finitely generated Λ_d-module.*

We get Theorem 1.1 as Corollary 4.8 of our Theorem 4.4 which is an analogue of Mazur's classical Control Theorem (for which the reader is referred to [15] or [8]).
The most interesting consequence is that it is possible to define a kind of Fitting ideal $\widetilde{Fitt}_\Lambda(\mathcal{S}) \subset \Lambda$ of $\mathcal{S}$ as the intersection of counterimages of the $Fitt_{\Lambda_d}(\mathcal{S}_d)$'s in Λ (see section 5.1.2, Definition 5.8). The natural next step is the formulation of a Main Conjecture relating this $\widetilde{Fitt}_\Lambda(\mathcal{S})$ and a "p-adic L-function" as described above (Conjecture 5.11).

By the same techniques, and with less effort, we also investigate the variation of the l-part of the Selmer group (l a prime different from p) in subextensions of $\mathcal{F}/F$. Theorem 3.4 shows that also in this case we can control the Selmer groups; however we lack a good theory of modules over the ring $\mathbb{Z}_l[[\Gamma]]$ and thus are unable to say much more.

Remark 1.2. It might be worthwhile to remark that the prime number p is not a place of our field, contrary to the classical situation. In particular we don't have to ask anything about the reduction of E being not supersingular at some place.

1.4. **Structure of this paper.** In section 2 we establish notations and define our Selmer groups by flat cohomology, which, for $l \neq p$, reduces to the usual Galois cohomology. Section 3 is dedicated to the easier case $l \neq p$: here we can establish the control theorem without any assumption on the $\mathbb{Z}_p^{\mathbb{N}}$-extension $\mathcal{F}/F$. On the contrary the control theorems for $l = p$ are proven (in section 4) only for a $\mathbb{Z}_p^d$-extension $\mathcal{F}_d/F$: the technical reasons for this limitation are explained in Remark 4.5. We begin with Theorem 4.4 which regards classical Selmer groups and leads to finitely generated Λ_d-modules in Corollary 4.8. To provide some examples of torsion modules we also present another control theorem for some slightly modified Selmer groups (Theorem 4.12) where we change the local conditions at the ramified primes. In section 5 we go back to $\mathcal{F}/F$. We define the Λ-ideal $\widetilde{Fitt}_\Lambda(\mathcal{S})$, which provides our candidate for an algebraic L-function and by which we formulate our version of Iwasawa's Main Conjecture.

Acknowledgements. We thank Massimo Bertolini, Henri Darmon, Ralph Greenberg, Marc-Hubert Nicole, Tadashi Ochiai, David Vauclair, Stefano Vigni and Christian Wuthrich for useful suggestions and comments on early drafts of this paper.
The first author has been supported by a scientific grant from the University of Pisa. The second author has been supported by a scientific grant from the University of Milano.

2. Selmer groups

2.1. **Notations.** For the convenience of the reader we list some notations that will be used in this paper and describe the basic setting in which the theory will be developed.

2.1.1. *Fields.* Let L be a field: then $\overline{L}$ will denote an algebraic closure and $L^{sep} \subset \overline{L}$ a separable closure; besides, we put $G_L := Gal(L^{sep}/L)$. If L is a global field (or an algebraic extension of such), $\mathcal{M}_L$ will be its set of places. For any place $v \in \mathcal{M}_L$ we let L_v be the completion of L at v, $\mathcal{O}_v$ the ring of integers of L_v , $\mathfrak{m}_v$ the maximal ideal of $\mathcal{O}_v$ and $\mathbb{L}_v := \mathcal{O}_v/\mathfrak{m}_v$ the residue field. Let ord_v be the valuation associated to v.
If L is a local field, the notations above will often be changed to $\mathcal{O}_L$, $\mathfrak{m}_L$, $\mathbb{L}$; besides $U_1(L) \subset \mathcal{O}_L^*$ will be the group of 1-units.

As stated in the introduction, we fix a global field F of characteristic $p > 0$ and an algebraic closure $\overline{F}$. For any place $v \in \mathcal{M}_F$ we choose $\overline{F_v}$ and an embedding $\overline{F} \hookrightarrow \overline{F_v}$, so to get a restriction map $G_{F_v} \hookrightarrow G_F$. All algebraic extensions of F (resp. F_v) will be assumed to be contained in $\overline{F}$ (resp. $\overline{F_v}$).

Script letters will denote infinite extensions of F: more precisely we fix a $\mathbb{Z}_p^{\mathbb{N}}$-extension $\mathcal{F}/F$ with Galois group Γ and for any $d \geq 1$ we will consider $\mathcal{F}_d \subset \mathcal{F}$, a $\mathbb{Z}_p^d$-extension of F.

2.1.2. *Elliptic curves.* We fix an elliptic curve E/F, non-isotrivial and having split multiplicative reduction at all places supporting its conductor. The reader is reminded that then at such places E is isomorphic to a Tate curve, i.e. $E(F_v) \simeq F_v^*/q_{E,v}^{\mathbb{Z}}$ for some $q_{E,v}$.
For any positive integer n let $E[n]$ be the scheme of n-torsion points.

Moreover, for any prime l, let $E[l^\infty] := \lim\limits_{\rightarrow} E[l^n]$.
For any $v \in \mathcal{M}_F$ we choose a minimal Weierstrass equation for E. Let E_v be the reduction of E modulo v and for any point $P \in E$ let P_v be its image in E_v .
Besides $E_{v,ns}(\mathbb{F}_v)$ is the set of nonsingular points of $E_v(\mathbb{F}_v)$, and

$$E_0(F_v) := \{\, P \in E(F_v) \ |\ P_v \in E_{v,ns}(\mathbb{F}_v) \,\} \ .$$

By the theory of Tate curves we know that, in case of bad reduction, $E_0(F_v) \simeq \mathcal{O}_v^*$ (see e.g. [23, V section 4]).
Finally, let $T_v := E(F_v)/E_0(F_v)$. In case of bad reduction T_v is the group of components of the special fibre and our hypothesis implies that its order is $-ord_v(j(E))$ (see e.g. [23, IV.9.2]).
For all basic facts about elliptic curves, the reader is referred to Silverman's books [22] and [23].

2.1.3. *Duals.* For X a topological abelian group, we denote its Pontrjagin dual by $X^\vee := Hom_{cont}(X, \mathbb{C}^*)$. In the cases considered in this paper, X will be a (mostly discrete) topological $\mathbb{Z}_l$-module, so that $X^\vee$ can be identified with $Hom_{cont}(X, \mathbb{Q}_l/\mathbb{Z}_l)$ and it has a natural structure of $\mathbb{Z}_l$-module.
The reader is reminded that to say that an R-module X (R any ring) is cofinitely generated means that $X^\vee$ is a finitely generated R-module.

2.2. **The Selmer groups.** We are interested in torsion subschemes of the elliptic curve E. Since $char\, F = p$, in order to deal with the p-torsion and to define Selmer groups with the usual cohomological techniques, we need to consider flat cohomology of group schemes.
For the basic theory of sites and cohomology on a site see [17, Chapters II, III]. Briefly, for any scheme X we let X_{fl} be the subcategory of $\mathbf{Sch}/X$ (schemes over X) whose structure morphisms are locally of finite type. Moreover X_{fl} is endowed with the flat topology, i.e., if we let $Y \to X$ be an element of X_{fl} , then a covering of Y is a family $\{g_i : U_i \to Y\}$ such that $Y = \bigcup g_i(U_i)$ and each g_i is a flat morphism locally of finite type.
We only consider flat cohomology so when we write a scheme X we always mean X_{fl} .

Definition 2.1. *Let $\mathcal{P}$ be a sheaf on X and consider the global section functor sending $\mathcal{P}$ to $\mathcal{P}(X)$. The i-th flat cohomology group of X with values in $\mathcal{P}$, denoted by $H^i_{fl}(X, \mathcal{P})$, is the value at $\mathcal{P}$ of the i-th right derived functor of the global section functor.*

Let L be an algebraic extension of F and $X_L := Spec\, L$. For any positive integer m the group schemes $E[m]$ and E define sheaves on X_L (see [17, II.1.7]): for example $E[m](X_L) := E[m](L)$. Consider the exact sequence

$$E[m] \hookrightarrow E \xrightarrow{m} \twoheadrightarrow E$$

and take flat cohomology with respect to X_L to get

$$E(L)/mE(L) \hookrightarrow H^1_{fl}(X_L, E[m]) \to H^1_{fl}(X_L, E) \ .$$

In particular let m run through the powers l^n of a prime l. Taking direct limits one gets an injective map (a "Kummer homomorphism")

$$\kappa : E(L) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow \varinjlim_n H^1_{fl}(X_L, E[l^n]) =: H^1_{fl}(X_L, E[l^\infty]) \ .$$

Exactly as above one can build local Kummer maps for any place $v \in \mathcal{M}_L$

$$\kappa_v : E(L_v) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow H^1_{fl}(X_{L_v}, E[l^\infty])$$

where $X_{L_v} := Spec\, L_v$.

Definition 2.2. *The* l-part of the Selmer group *of* E *over* L*, denoted by* $Sel_E(L)_l$ *, is defined to be*

$$Sel_E(L)_l := Ker\{H^1_{fl}(X_L, E[l^\infty]) \to \prod_{v \in \mathcal{M}_L} H^1_{fl}(X_{L_v}, E[l^\infty])/Im\, \kappa_v\}$$

where the map is the product of the natural restrictions between cohomology groups.

The reader is reminded that if L/F is a finite extension then $Sel_E(L)_p$ is a cofinitely generated $\mathbb{Z}_p$-module (see, e.g. [18, III.8 and 9]). Moreover the *Tate-Shafarevich group* Ш(E/L) fits into the exact sequence

$$E(L) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow Sel_E(L)_l \twoheadrightarrow Ш(E/L)[l^\infty] \ .$$

According to the function field version of the Birch and Swinnerton-Dyer conjecture (some evidence for which can be found in [5] and [26]), Ш(E/L) is finite for any finite extension L of F. Applying to this last sequence the exact functor $Hom(\cdot, \mathbb{Q}_l/\mathbb{Z}_l)$, it follows that

$$rank_{\mathbb{Z}_l}(Sel_E(L)_l^\vee) = rank_{\mathbb{Z}}(E(L))$$

(recall that the cohomology groups H^i_{fl} , hence the Selmer groups, are endowed with the discrete topology).

Letting L vary through subextensions of $\mathcal{F}/F$, the groups $Sel_E(L)_l$ admit natural actions by $\mathbb{Z}_l$ (because of $E[l^\infty]$) and by Γ. Hence they are modules over the Iwasawa algebra $\mathbb{Z}_l[[\Gamma]]$.

2.2.1. *The case $l = p$.* We shall consider $\mathbb{Z}_p^d$-extensions $\mathcal{F}_d/F$ such that $\mathcal{F} = \bigcup \mathcal{F}_d$. One of the main reasons for doing this is the fact that $Sel_E(\mathcal{F}_d)_p$ is a $\Lambda_d := \mathbb{Z}_p[[Gal(\mathcal{F}_d/F)]]$-module and, thanks to the (non-canonical) isomorphism $\Lambda_d \simeq \mathbb{Z}_p[[T_1, \dots, T_d]]$, we have a fairly precise description of such modules (see, for example, [3, VII.4]). The first step towards the proof of Theorem 1.1 will be the study of the restriction maps

$$Sel_E(L)_p \longrightarrow Sel_E(\mathcal{F}_d)_p^{Gal(\mathcal{F}_d/L)}$$

as L varies in $\mathcal{F}_d/F$.

2.2.2. *The case $l \neq p$.* Here we deal with the full $\mathbb{Z}_p^{\mathbb{N}}$-extension and again study the maps

$$Sel_E(L)_l \longrightarrow Sel_E(\mathcal{F})_l^{Gal(\mathcal{F}/L)} .$$

Note that to define $Sel_E(L)_l$ we could have used the sequence

$$E[l^n](\overline{F}) \hookrightarrow E(F^{sep}) \xrightarrow{l^n} E(F^{sep})$$

and classical Galois (=étale) cohomology since, in this case,

$$H^1_{fl}(X_L, E[l^n]) \simeq H^1_{et}(X_L, E[l^n]) \simeq H^1(G_L, E[l^n](\overline{F}))$$

(see [17, III.3.9]). In order to lighten notations, each time we work with $l \neq p$ (i.e., in the next chapter) we shall use the classical notation $H^i(L, \cdot)$ instead of $H^i(G_L, \cdot) \simeq H^i_{fl}(X_L, \cdot)$ and write $E[n]$ for $E[n](\overline{F})$, putting $E[l^\infty] := \bigcup E[l^n]$.
In this case the Kummer map

$$\kappa : E(L) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow H^1(G_L, E[l^\infty])$$

has an explicit description as follows. Let $\alpha \in E(L) \otimes \mathbb{Q}_l/\mathbb{Z}_l$ be represented as $\alpha = P \otimes \frac{a}{l^k}$ $(a \in \mathbb{Z})$ and let $Q \in E(L^{sep})$ be such that $aP = l^k Q$. Then $\kappa(\alpha) = \varphi_\alpha$, where $\varphi_\alpha(\sigma) := \sigma(Q) - Q$ for any $\sigma \in G_L$.

3. Control theorem for $l \neq p$

3.1. **The image of κ_v.** We start by giving a more precise description of $Im\, \kappa_v$ (following the path traced by Greenberg in [7] and [8]).

Lemma 3.1. *Let L_w be the completion of an algebraic extension of F_v. If E has split multiplicative reduction at w then there is a sequence*

$$0 \to U_1(L_w) \to E(L_w) \to A \to 0$$

with A a torsion group.

Proof. The hypothesis implies that E is isomorphic to a Tate curve: in particular, $E(L_w) \simeq L_w^*/q_{E,w}^{\mathbb{Z}}$ for some $q_{E,w}$ (the Tate period). Now it suffices to observe that $U_1(L_w)$ embeds into $L_w^*/q_{E,w}^{\mathbb{Z}}$ with torsion quotient. □

Remark 3.2. The previous lemma can be seen as a (partial) function field analog of Lutz's Theorem ([22, VII.6.3]). In the characteristic 0 case for a finite extension $K/\mathbb{Q}_p$ and an elliptic curve E defined over $\mathbb{Q}_p$ one finds that $E(K)$ contains a subgroup isomorphic to the ring of integers of K (taken as an additive group), i.e. a subgroup isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$.
In the function field (characteristic p) case we lack the logarithmic function and we have to deal with the multiplicative group of the ring $\mathcal{O}_v$. For any complete local field like F_v one has $U_1(F_v) \simeq \mathbb{Z}_p^{\mathbb{N}}$, hence, for any finite extension K_w/F_v, one finds both in $E(K_w)$ and in $E(F_v)$ a subgroup of finite index isomorphic to $\mathbb{Z}_p^{\mathbb{N}}$ making it hard to emphasize any kind of relation with the degree $[K_w : F_v]$.

Proposition 3.3. *Let L_w be the completion of an algebraic extension of F_v. Let $l \neq p$: then*

$$E(L_w) \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$$

(i.e. the Kummer map κ_w has trivial image).

Proof. We consider two cases, according to the behaviour of E at w.

Case 1: E has good reduction at w.
In this case $E[l^\infty] \simeq E_w[l^\infty]$ and by the Néron-Ogg-Shafarevich criterion this is an isomorphism of G_{L_w}-modules. Hence one has a sequence of maps

$$H^1(L_w, E[l^\infty]) \xrightarrow{\sim} H^1(L_w, E_w[l^\infty]) \hookrightarrow H^1(L_w, E_w(\overline{\mathbb{L}_w}))$$

where the last map on the right is induced by the natural inclusion $E_w[l^\infty] \hookrightarrow E_w(\overline{\mathbb{L}_w})$. Such map is injective because $E_w(\overline{\mathbb{L}_w})$ is a torsion abelian group and $E_w[l^\infty]$ is its l-primary part. Composing κ_w with this sequence, one gets an injection

$$E(L_w) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow H^1(L_w, E_w(\overline{\mathbb{L}_w})) .$$

By definition $\varphi \in Im\, \kappa_w$ implies $\varphi(\sigma) = \sigma(Q) - Q$ for some $Q \in E(L_w^{sep})$, hence the image of φ in $H^1(L_w, E_w(\overline{\mathbb{L}_w}))$ is φ_w with $\varphi_w(\sigma) = \sigma(Q_w) - Q_w$ ($Q_w \in E_w(\overline{\mathbb{L}_w})$ is the reduction of Q mod w). Thus φ_w is a 1-coboundary; since all the maps involved are injective, one gets $\varphi = 0$ and finally $E(L_w) \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$.

Case 2: E has bad reduction at w, i.e. split multiplicative (according to our hypothesis).
By Lemma 3.1 one has

$$0 \to U_1(L_w) \to E(L_w) \to A \to 0$$

where A is a torsion group. Since $U_1(L_w)$ is a $\mathbb{Z}_p$-module, one gets

$$0 = U_1(L_w) \otimes \mathbb{Q}_l/\mathbb{Z}_l \to E(L_w) \otimes \mathbb{Q}_l/\mathbb{Z}_l \to A \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0 \ . \qquad \square$$

3.2. **The theorem.** Recall our $\mathbb{Z}_p^{\mathbb{N}}$-extension $\mathcal{F}/F$: we choose any sequence of finite extensions of F such that

$$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots \subset \bigcup F_n = \mathcal{F} \ .$$

In this setting we let $\Gamma_n := Gal(\mathcal{F}/F_n)$ and $\Gamma = Gal(\mathcal{F}/F)$ so that

$$\mathbb{Z}_p^{\mathbb{N}} \simeq \Gamma \simeq \varprojlim_n \Gamma/\Gamma_n = \varprojlim_n Gal(F_n/F) \ .$$

For example if $\mathcal{F}$ is the cyclotomic extension at $\mathfrak{p}$ (see section 1.2.1), one can take F_n to be the subfield of $F(\Phi[\mathfrak{p}^n])$ fixed by $(A/\mathfrak{p})^*$.

We will denote by v_n (resp. w) primes of F_n (resp. $\mathcal{F}$) and, to shorten notations, we shall denote by F_{v_n} (resp. $\mathcal{F}_w$) the completion of F_n at v_n (resp. of $\mathcal{F}$ at w). Finally, for any algebraic extension L/F, we put

$$\mathcal{G}(L) := Im\big\{H^1(L, E[l^\infty]) \to \prod_{v\in\mathcal{M}_L} H^1(L_v, E[l^\infty])/Im\,\kappa_v\big\} \ .$$

For any n, the restriction $Sel_E(F_n)_l \to Sel_E(\mathcal{F})_l^{\Gamma_n}$ fits into the following diagram (with exact rows)

$$\begin{array}{ccccc} Sel_E(F_n)_l & \hookrightarrow & H^1(F_n, E[l^\infty]) & \twoheadrightarrow & \mathcal{G}(F_n) \\ \downarrow a_n & & \downarrow b_n & & \downarrow c_n \\ Sel_E(\mathcal{F})_l^{\Gamma_n} & \hookrightarrow & H^1(\mathcal{F}, E[l^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}(\mathcal{F}) \ . \end{array}$$

Theorem 3.4. *For any n, $Sel_E(F_n)_l \simeq Sel_E(\mathcal{F})_l^{\Gamma_n}$.*

Proof. The snake lemma applied to the diagram above shows that it is enough to prove that $Ker\, b_n = Coker\, b_n = Ker\, c_n = 0$ (i.e., to prove that a_n is an isomorphism we shall prove that c_n is injective and that b_n is an isomorphism as well).
The map b_n . By the Hochschild-Serre spectral sequence (see [20, 2.1.5]) one has

$$Ker\, b_n \simeq H^1(\Gamma_n, E[l^\infty]^{G_{\mathcal{F}}}) \ ,$$

and

$$Coker\, b_n \subseteq H^2(\Gamma_n, E[l^\infty]^{G_{\mathcal{F}}}) \ .$$

The group $E[l^\infty]^{G_{\mathcal{F}}} = E[l^\infty](\mathcal{F})$ is l-primary. Moreover

$$\Gamma_n = Gal(\mathcal{F}/F_n) \simeq \varprojlim_m Gal(F_m/F_n)$$

is a pro-p-group for all $n \geq 0$ and

$$H^i(\Gamma_n, E[l^\infty](\mathcal{F})) \simeq \varinjlim_m H^i(Gal(F_m/F_n), E[l^\infty](F_m)) \ .$$

For any $m \geq n \geq 0$, $H^i(Gal(F_m/F_n), E[l^\infty](F_m))$ $(i \geq 1)$ is killed by $|E[l^\infty](F_m)|$, which is a (finite) power of l, and by $[F_m : F_n]$ (by the $cor \circ res$ map, see e.g. [20, 1.6.1]) which is a power of $p \neq l$. Hence, for $i \geq 1$, $H^i(Gal(F_m/F_n), E[l^\infty](F_m)) = 0$ and eventually $H^i(\Gamma_n, E[l^\infty](\mathcal{F})) = 0$ as well.

The map c_n *.* By Proposition 3.3 $Ker\, c_n$ is contained in the kernel of the natural map

$$d_n \,:\, \prod_{v_n \in \mathcal{M}_{F_n}} H^1(F_{v_n}, E[l^\infty]) \to \prod_{w \in \mathcal{M}_{\mathcal{F}}} H^1(\mathcal{F}_w, E[l^\infty]) \ .$$

Considering every component, we find maps

$$d_w \,:\, H^1(F_{v_n}, E[l^\infty]) \to H^1(\mathcal{F}_w, E[l^\infty])$$

and $Ker\, c_n \subseteq \prod_{w \in \mathcal{M}_{\mathcal{F}}} Ker\, d_w$.

As we have seen for $Ker\, b_n$, one has from the inflation restriction sequence

$$Ker\, d_w \simeq H^1(Gal(\mathcal{F}_w/F_{v_n}), E[l^\infty]^{G_{\mathcal{F}_w}})$$

i.e., $Ker\, d_w = 0$ because $Gal(\mathcal{F}_w/F_{v_n})$ is a pro-p-group and $E[l^\infty]^{G_{\mathcal{F}_w}}$ is an l-primary group. □

Remark 3.5. Let $\Gamma_{v_n} := Gal(\mathcal{F}_w/F_{v_n})$: then the image of d_w is Γ_{v_n}-invariant. The Hochschild-Serre spectral sequence

$$H^1(F_{v_n}, E[l^\infty]) \to H^1(\mathcal{F}_w, E[l^\infty])^{\Gamma_{v_n}} \to H^2(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) = 0$$

shows that $Coker\, d_w = 0$ as well.

3.3. **The Selmer dual.** Theorem 3.4 leads to a (partial) description of the Selmer groups (actually of their Pontrjagin duals) as modules over the algebra $\mathbb{Z}_l[[\Gamma]]$. Since $\mathbb{Z}_l[[\Gamma]] = \varprojlim \mathbb{Z}_l[\Gamma/\Gamma_n]$, this ring is compact with respect to the inverse limit topology. The following generalization of Nakayama's Lemma is proved in [1, section 3].

Theorem 3.6. *Let* Λ *be a compact topological ring with 1 and let* J *be an ideal such that* $J^n \to 0$*. Let* X *be a profinite* Λ*-module. If* X/JX *is a finitely generated* (Λ/J)*-module then* X *is a finitely generated* Λ*-module.*

We lack an adequate description of the ideals J of $\mathbb{Z}_l[[\Gamma]]$ such that $J^n \to 0$. As an example consider the classical augmentation ideal I, i.e. the kernel of the map $\mathbb{Z}_l[[\Gamma]] \to \mathbb{Z}_l$ sending each $\sigma \in \Gamma$ to 1. It does not verify this condition since $I = I^2$, as the next lemma shows.

Lemma 3.7. *Let* R *be a compact topological ring where* p *is invertible and* $G = \varprojlim G/U_n$*, where the* G/U_n*'s are finite abelian* p*-groups. Denote by* I *the augmentation ideal of* $R[[G]]$*: then* $I/I^2 = 0$*.*

Proof. Define I_n as the augmentation ideal of $R[G/U_n]$. The augmentation map on $R[[G]]$ is defined via a limit and $I = \varprojlim I_n$. Besides $I^2 = \varprojlim I_n^2$ because of the compactness hypothesis: the claim follows if $I_n/I_n^2 = 0$ for all $n > 0$. Let J_n be the augmentation ideal of $\mathbb{Z}[G/U_n]$: since I_n is the free module generated by the elements $g-1$, we have $I_n = J_n \otimes R$ and $I_n^2 = J_n^2 \otimes R$. For a commutative group H one has $H \simeq J_H/J_H^2$ (where J_H is the augmentation of $\mathbb{Z}[H]$): it follows $I_n/I_n^2 = (J_n/J_n^2) \otimes R = 0$. □

Anyway the ideal lI obviously verifies $(lI)^n \to 0$ and we want to apply Theorem 3.6 with $\Lambda = \mathbb{Z}_l[[\Gamma]]$, $J = lI$ and $X = Sel_E(\mathcal{F})_l^\vee$.

Lemma 3.8. *Let M be a discrete $\mathbb{Z}_l[[\Gamma]]$-module and $m_l : M \to M$ the multiplication by l. Then*

$$M^\vee/lIM^\vee \simeq (m_l^{-1}(M^\Gamma))^\vee = (M^\Gamma + M[l])^\vee$$

(where $M[l]$ is the l-torsion of M).

Proof. Let N be the dual of M: then N is a $\mathbb{Z}_l[[\Gamma]]$-module. Consider the natural projection $\pi : N \twoheadrightarrow N/lIN$ and its dual map $\pi^\vee : (N/lIN)^\vee \hookrightarrow N^\vee$. Let $\phi \in N^\vee$: then

$$\phi \in Im\,\pi^\vee \iff \phi(l(\gamma - 1)\cdot a) = 0$$

for any $\gamma \in \Gamma$ and any $a \in N$. But $\phi(l\gamma \cdot a) = \phi(la)$ if and only if $l\phi$ is Γ-invariant, i.e. $\phi \in Im\,\pi^\vee \iff l\phi \in (N^\vee)^\Gamma$. Therefore

$$(N/lIN)^\vee \simeq m_l^{-1}((N^\vee)^\Gamma) \;.$$

Taking duals one gets

$$M^\vee/lIM^\vee \simeq (m_l^{-1}(M^\Gamma))^\vee \;.$$

Since Γ is pro-p and $M[l]$ is l-torsion, one has $H^1(\Gamma, M[l]) = 0$: therefore

$$m_l(M)^\Gamma \simeq (M/M[l])^\Gamma \simeq M^\Gamma/M[l]^\Gamma \simeq m_l(M^\Gamma) \;.$$

Thus

$$m_l^{-1}(M^\Gamma) = m_l^{-1}(m_l(M)^\Gamma) \simeq m_l^{-1}(m_l(M^\Gamma)) = M^\Gamma + M[l] \;. \qquad \square$$

Corollary 3.9. *Assume that both $Sel_E(F)_l$ and $Sel_E(\mathcal{F})_l[l]$ are finite. Then $Sel_E(\mathcal{F})_l^\vee$ is a finitely generated $\mathbb{Z}_l[[\Gamma]]$-module.*

Proof. By the previous lemma with $M = Sel_E(\mathcal{F})_l$ one has

$$Sel_E(\mathcal{F})_l^\vee/lISel_E(\mathcal{F})_l^\vee \simeq (Sel_E(\mathcal{F})_l^\Gamma + Sel_E(\mathcal{F})_l[l])^\vee \simeq$$
$$\simeq (Sel_E(F)_l + Sel_E(\mathcal{F})_l[l])^\vee$$

(by Theorem 3.4), so this quotient is finite by hypotheses. Then Theorem 3.6 yields the corollary. □

In the corollary it would be enough to assume that $Sel_E(F)_l$ and $Sel_E(\mathcal{F})_l[l]$ are cofinitely generated modules over the mysterious ring

$\mathbb{Z}_l[[\Gamma]]/lI\mathbb{Z}_l[[\Gamma]]$. Unfortunately even with the stronger assumption of finiteness we can't go further (i.e., we are not able to see whether $Sel_E(\mathcal{F})_l^\vee$ is a torsion $\mathbb{Z}_l[[\Gamma]]$-module or not) due to our lack of understanding of the structure of $\mathbb{Z}_l[[\Gamma]]$-modules even for simpler Γ's like for example $\mathbb{Z}_p$.

4. Control theorems for $l = p$

As stated in the introduction, in this section we shall work with a $\mathbb{Z}_p^d$-extension $\mathcal{F}_d/F$, $d \geq 1$. As before, it is convenient to write $\mathcal{F}_d$ as the union of finite extensions F_n's of F with $F_n \subset F_{n+1}$.
Moreover we shall consider the p-torsion of the elliptic curve E: therefore we use flat cohomology as explained in section 2, where we described the Selmer groups for this case. We will mainly follow the notations given there except for the following minor change regarding the Galois groups: in this section we will write $\Gamma := Gal(\mathcal{F}_d/F)$ and $\Gamma_n := Gal(\mathcal{F}_d/F_n)$.

4.1. **Lemmas.** We need some lemmas which will be used in the proof of the main theorems.

Lemma 4.1. *Let $\Gamma \simeq \mathbb{Z}_p^d$ and B a finite p-primary Γ-module. Then*

$$|H^1(\Gamma, B)| \leq |B|^d \text{ and } |H^2(\Gamma, B)| \leq |B|^{\frac{d(d-1)}{2}} .$$

Proof. We use induction on d. The case $d = 1$ is straightforward since, for $\Gamma = \overline{\langle\gamma\rangle} \simeq \mathbb{Z}_p$, $H^1(\Gamma, B) \simeq B/(\gamma - 1)B$, so that $|H^1(\Gamma, B)| \leq |B|$, and $H^2(\Gamma, B) = 0$ because $\mathbb{Z}_p$ has p-cohomological dimension 1 (see [20, 3.5.9]).
For the induction step take γ in a set of independent topological generators of Γ and let $\Gamma' := \Gamma/\overline{\langle\gamma\rangle} \simeq \mathbb{Z}_p^{d-1}$.
From the inflation restriction sequence one has

$$H^1(\Gamma', B^{\overline{\langle\gamma\rangle}}) \hookrightarrow H^1(\Gamma, B) \to H^1(\overline{\langle\gamma\rangle}, B)^{\Gamma'}$$

and, using induction,

$$|H^1(\Gamma, B)| \leq |H^1(\Gamma', B^{\overline{\langle\gamma\rangle}})||H^1(\overline{\langle\gamma\rangle}, B)| \leq |B|^{d-1}|B| .$$

Since $H^i(\overline{\langle\gamma\rangle}, B) = 0$ for all $i \geq 2$, the Hochschild-Serre spectral sequence (see [20, II.1 Exercise 5]) gives an exact sequence

$$H^2(\Gamma', B^{\overline{\langle\gamma\rangle}}) \to H^2(\Gamma, B) \to H^1(\Gamma', H^1(\overline{\langle\gamma\rangle}, B)) .$$

By induction and the result on the H^1 one has

$$|H^2(\Gamma, B)| \leq |H^2(\Gamma', B^{\overline{\langle\gamma\rangle}})||H^1(\Gamma', H^1(\overline{\langle\gamma\rangle}, B))| \leq$$
$$\leq |B|^{\frac{(d-1)(d-2)}{2}}|B|^{d-1} = |B|^{\frac{d(d-1)}{2}} . \qquad \square$$

Lemma 4.2. *Let L/K be a finite Galois extension of local fields and G its Galois group. Let E/K be an elliptic curve with split multiplicative reduction. Then $H^1(G, E_0(L)) \simeq \mathbb{Z}/e\mathbb{Z}$ (where e is the ramification index of L/K and $H^1(G, \cdot)$ denotes Galois cohomology).*

Proof. We recall that Tate parametrization yields an isomorphism of Galois modules $E_0(L) \simeq \mathcal{O}_L^*$. The valuation map gives the sequence

$$\mathcal{O}_L^* \hookrightarrow L^* \twoheadrightarrow \mathbb{Z}$$

and, via G-cohomology,

$$\mathcal{O}_K^* \hookrightarrow K^* \stackrel{\nu}{\longrightarrow} \mathbb{Z} \twoheadrightarrow H^1(G, \mathcal{O}_L^*)$$

(because $H^1(G, L^*) = 0$ by Hilbert 90). The lemma follows from $Im\, \nu = e\mathbb{Z}$. □

Lemma 4.3. *The group $E[p^\infty](\mathcal{F}_d)$ is finite.*

Proof. The following argument actually proves that $E[p^\infty](F^{sep})$ is finite (for a more detailed exposition see [4, Lemma 2.2]).
Factoring the multiplication-by-p^m map via the p^mth power Frobenius one sees that $E[p^m](\overline{F}) \subset E(F)$ implies $j(E) \in (F^*)^{p^m}$. Therefore if $j(E) \in (F^*)^{p^n} - (F^*)^{p^{n+1}}$ one has $E[p^\infty](F^{sep}) \subset E[p^n](\overline{F})$. □

4.2. **The theorem.** We are now ready to prove the main theorem: the proof is divided in several parts and exploits all the techniques which will later lead to similar results like Theorems 4.12 and 5.3.

Theorem 4.4. *Assume that all primes which are ramified in $\mathcal{F}_d/F$ are of split multiplicative reduction for E. Then the canonical maps*

$$Sel_E(F_n)_p \longrightarrow Sel_E(\mathcal{F}_d)_p^{\Gamma_n}$$

have finite kernels all bounded by $|E[p^\infty](\mathcal{F}_d)|^d$ and cofinitely generated cokernels (over $\mathbb{Z}_p$).

Proof. We start by fixing the notations which will be used throughout the proof.
Let $X_n := Spec\, F_n$, $\mathcal{X}_d := Spec\, \mathcal{F}_d$, $X_{v_n} := Spec\, F_{v_n}$ and $\mathcal{X}_w := Spec\, \mathcal{F}_w$ (now $\mathcal{F}_w$ is the completion of $\mathcal{F}_d$ at w).
Finally, to ease notations, let

$$\mathcal{G}(X_n) := Im\big\{H^1_{fl}(X_n, E[p^\infty]) \to \prod_{v_n \in \mathcal{M}_{F_n}} H^1_{fl}(X_{v_n}, E[p^\infty])/Im\, \kappa_{v_n}\big\}$$

(analogous definition for $\mathcal{G}(\mathcal{X}_d)$).
The map $\mathcal{X}_d \to X_n$ is a Galois covering with Galois group Γ_n. In this

context the Hochschild-Serre spectral sequence holds by [17, III.2.21 a),b) and III.1.17 d)]. Therefore one has an exact sequence

$$\begin{array}{l} H^1(\Gamma_n, E[p^\infty](\mathcal{F}_d)) \longrightarrow H^1_{fl}(X_n, E[p^\infty]) \\ \qquad\qquad \downarrow \\ H^1_{fl}(\mathcal{X}_d, E[p^\infty])^{\Gamma_n} \longrightarrow H^2(\Gamma_n, E[p^\infty](\mathcal{F}_d)) \end{array}$$

which fits into the diagram

$$\begin{array}{ccccc} Sel_E(F_n)_p & \hookrightarrow & H^1_{fl}(X_n, E[p^\infty]) & \twoheadrightarrow & \mathcal{G}(X_n) \\ \downarrow a_n & & \downarrow b_n & & \downarrow c_n \\ Sel_E(\mathcal{F}_d)_p^{\Gamma_n} & \hookrightarrow & H^1_{fl}(\mathcal{X}_d, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}(\mathcal{X}_d) \end{array} .$$

As in Theorem 3.4 we shall focus on

$$Ker\, b_n = H^1(\Gamma_n, E[p^\infty](\mathcal{F}_d)) \ , \ Coker\, b_n \subseteq H^2(\Gamma_n, E[p^\infty](\mathcal{F}_d))$$

and $Ker\, c_n$.

4.2.1. *$Ker\, b_n$.* Since $\Gamma_n \simeq \mathbb{Z}_p^d$ and $E[p^\infty](\mathcal{F}_d)$ is finite by Lemma 4.3, we can apply Lemma 4.1 to get $|Ker\, b_n| \leq |E[p^\infty](\mathcal{F}_d)|^d$.

4.2.2. *$Coker\, b_n$.* As above we simply use Lemma 4.1 to get $|Coker\, b_n| \leq |E[p^\infty](\mathcal{F}_d)|^{\frac{d(d-1)}{2}}$.

Remark 4.5. Note that the result on $Ker\, b_n$ already implies the finiteness of $Ker\, a_n$ and gives a bound independent of n. The bounds for $Ker\, b_n$ and $Coker\, b_n$ depend on d and this is one of the reasons we could not consider the full $\mathbb{Z}_p^{\mathbb{N}}$-extension in this setting.

4.2.3. *$Ker\, c_n$.* First of all we note that $Ker\, c_n$ is contained in the kernel of the map

$$d_n : \prod_{v_n} H^1_{fl}(X_{v_n}, E[p^\infty])/Im\, \kappa_{v_n} \longrightarrow \prod_{w} H^1_{fl}(\mathcal{X}_w, E[p^\infty])/Im\, \kappa_w$$

and we consider the maps

$$d_w : H^1_{fl}(X_{v_n}, E[p^\infty])/Im\, \kappa_{v_n} \longrightarrow H^1_{fl}(\mathcal{X}_w, E[p^\infty])/Im\, \kappa_w$$

separately. Note that if $w_1 , w_2 \mid v_n$ then $Ker\, d_{w_1} \simeq Ker\, d_{w_2}$. Moreover, letting $d_{v_n} := \prod_{w|v_n} d_w$, we have

$$Ker\, d_{v_n} = \bigcap_{w|v_n} Ker\, d_w \text{ and } Ker\, c_n \subseteq \prod_{v_n \in \mathcal{M}_{F_n}} Ker\, d_{v_n} \ .$$

4.2.4. *Primes of good reduction.* Let v be the prime of F lying below v_n. Assume that E has good reduction at v. In this setting Ulmer proves that

$$Im(E(F_{v_n})/p^m E(F_{v_n})) \simeq H^1_{fl}(Y_{v_n}, E[p^m])$$

where $Y_{v_n} := Spec\,\mathcal{O}_{v_n}$ and $\mathcal{O}_{v_n}$ is the ring of integers of F_{v_n} (see [25, Lemma 1.2]).
Taking direct limits one finds

$$Im\,\kappa_{v_n} = Im(E(F_{v_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \simeq H^1_{fl}(Y_{v_n}, E[p^\infty]) .$$

To ease notations let, for any local field L,

$$\mathcal{H}(L) := H^1_{fl}(Spec\,L, E[p^\infty])/H^1_{fl}(Spec\,\mathcal{O}_L, E[p^\infty]) .$$

One gets a diagram

$$\begin{array}{ccccc} H^1_{fl}(Y_{v_n}, E[p^\infty]) & \hookrightarrow & H^1_{fl}(X_{v_n}, E[p^\infty]) & \twoheadrightarrow & \mathcal{H}(F_{v_n}) \\ \downarrow{\scriptstyle \lambda_1} & & \downarrow{\scriptstyle \lambda_2} & & \downarrow{\scriptstyle d_w} \\ H^1_{fl}(\mathcal{Y}_w, E[p^\infty])^{\Gamma_{v_n}} & \hookrightarrow & H^1_{fl}(\mathcal{X}_w, E[p^\infty])^{\Gamma_{v_n}} & \longrightarrow & \mathcal{H}(\mathcal{F}_w)^{\Gamma_{v_n}} \end{array}$$

with $\mathcal{Y}_w := Spec\,\mathcal{O}_w$ and $\Gamma_{v_n} := Gal(\mathcal{F}_w/F_{v_n})$(for the injectivity of the horizontal maps on the left see [18, III.7]). Note that the vertical map on the right is exactly d_w because both are induced by the restriction λ_2 and $Im\,d_w$ is Γ_{v_n}-invariant.
The snake lemma yields an exact sequence

$$Ker\,\lambda_1 \to Ker\,\lambda_2 \to Ker\,d_w \to Coker\,\lambda_1 \to Coker\,\lambda_2 .$$

By our hypothesis all primes of good reduction are unramified: so for the two maps λ_i the situation is identical to the one we described for the map b_n, i.e. one has Galois coverings $\mathcal{X}_w \to X_{v_n}$ and $\mathcal{Y}_w \to Y_{v_n}$ both with Galois group Γ_{v_n}, a subgroup of Γ_n (which one depends on the behaviour of the prime v_n in the extension $\mathcal{F}_d/F_n$). Hence

$$\begin{aligned} Ker\,\lambda_1 &= H^1(\Gamma_{v_n}, E[p^\infty](\mathcal{O}_w)) , \\ Ker\,\lambda_2 &= H^1(\Gamma_{v_n}, E[p^\infty](\mathcal{F}_w)) , \\ Coker\,\lambda_1 &\subset H^2(\Gamma_{v_n}, E[p^\infty](\mathcal{O}_w)) , \\ Coker\,\lambda_2 &\subset H^2(\Gamma_{v_n}, E[p^\infty](\mathcal{F}_w)) . \end{aligned}$$

Since E has good reduction at v (hence at w) one has $E(\mathcal{O}_w) = E(\mathcal{F}_w)$, therefore $Ker\,\lambda_1 \simeq Ker\,\lambda_2$. For the same reason

$$H^2(\Gamma_{v_n}, E[p^\infty](\mathcal{O}_w)) \simeq H^2(\Gamma_{v_n}, E[p^\infty](\mathcal{F}_w))$$

and the map $Coker\,\lambda_1 \to Coker\,\lambda_2$ (which is induced by this isomorphism) has to be injective. The snake lemma sequence yields $Ker\,d_w = 0$. Note that this is coherent with the number field case, where one has $Ker\,d_w = 0$ for all primes w dividing a prime $l \neq p$ of good reduction (see e.g. [8, Lemma 4.4]).

4.2.5. *Primes of bad reduction.* Note that if v_n splits completely then $\mathcal{F}_w = F_{v_n}$ and d_w is clearly an isomorphism.
Now let v_n be a prime of bad reduction with nontrivial decomposition group in Γ_n. From the Kummer exact sequence we have a diagram

$$\begin{array}{ccc} H^1_{fl}(X_{v_n}, E[p^\infty])/Im\,\kappa_{v_n} & \hookrightarrow & H^1_{fl}(X_{v_n}, E) \\ \downarrow{\scriptstyle d_w} & & \downarrow{\scriptstyle h_w} \\ H^1_{fl}(\mathcal{X}_w, E[p^\infty])/Im\,\kappa_w & \hookrightarrow & H^1_{fl}(\mathcal{X}_w, E) \end{array}$$

so that

$$Ker\, d_w \hookrightarrow Ker\, h_w \simeq H^1(\Gamma_{v_n}, E(\mathcal{F}_w)) \ .$$

Consider the Tate curve exact sequence

$$q_{E,v}^{\mathbb{Z}} \hookrightarrow \mathcal{F}_w^* \twoheadrightarrow E(\mathcal{F}_w)$$

and take Galois cohomology to get

$$H^1(\Gamma_{v_n}, E(\mathcal{F}_w)) \hookrightarrow H^2(\Gamma_{v_n}, q_{E,v}^{\mathbb{Z}})$$

where the injectivity comes from Hilbert 90.
Since $q_{E,v} \in F_v$ the action of Γ_{v_n} on $q_{E,v}^{\mathbb{Z}}$ is trivial, hence

$$Ker\, d_w \hookrightarrow H^2(\Gamma_{v_n}, q_{E,v}^{\mathbb{Z}}) \simeq H^2(\Gamma_{v_n}, \mathbb{Z}) \simeq (\Gamma_{v_n}^{ab})^\vee \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{d(v_n)}$$

where $d(v_n) = \mathrm{rank}_{\mathbb{Z}_p} \Gamma_{v_n} \leq d$ (see [20, pag. 50]).
Therefore $Ker\, d_w$ and $Ker\, d_{v_n} = \bigcap Ker\, d_w$ are cofinitely generated and, since there are only finitely many v_n's of bad reduction, $Ker\, c_n$ is cofinitely generated as well. □

Remark 4.6. In the main examples we have in mind for $\mathcal{F}/F$ (see sections 1.2.2 and 5.2) there is only one prime which ramifies and it totally ramifies in $\mathcal{F}/F$. Moreover the available constructions for p-adic L-functions require this prime to be of split multiplicative reduction so our Theorem 4.4 applies to these settings.

Remark 4.7. Note that, due to the (possibly) increasing number of primes of bad reduction in the tower of F_n's, the coranks of the $Ker\, c_n$'s are finite but not bounded in general. For example if v is inert unramified in $\mathcal{F}_d/F$ and $d \geq 2$ then there are infinitely many primes in $\mathcal{F}_d$ lying over v.

Recall that Λ_d acts on $Sel_E(\mathcal{F}_d)_p$ and on $\mathcal{S}_d := Sel_E(\mathcal{F}_d)_p^\vee$.

Corollary 4.8. *In the setting of Theorem 4.4, $\mathcal{S}_d$ is a finitely generated Λ_d-module.*

Proof. Let I be the augmentation ideal of Λ_d. One has that $\mathcal{S}_d/I\mathcal{S}_d$ is dual to $Sel_E(\mathcal{F}_d)_p^\Gamma$ which, by Theorem 4.4, is cofinitely generated over $\mathbb{Z}_p$. Therefore $\mathcal{S}_d$ is a finitely generated Λ_d-module by Theorem 3.6 . □

4.3. **Primes of bad reduction.** We can be more precise on $Ker\, d_w$ for the inert primes of bad reduction.

Lemma 4.9. *With the hypothesis and notations of Theorem 4.4, let v_n be a place of bad reduction. One has:*

1. *$Ker\, d_w$ is finite if v_n is unramified in $\mathcal{F}_d/F_n$;*
2. *$Ker\, d_w = 0$ if v_n splits completely in $\mathcal{F}_d/F_n$;*
3. *$corank_{\mathbb{Z}_p} Ker\, d_w \leq d$ if v_n is ramified in $\mathcal{F}_d/F_n$.*

Proof. Part **2** and **3** have been proven in section 4.2.5. For the other primes consider the embedding coming from the Kummer exact sequence

$$Ker\, d_w \hookrightarrow Ker\, h_w \simeq H^1(\Gamma_{v_n}, E(\mathcal{F}_w)) \simeq \varinjlim_m H^1(\Gamma_{v_n}^{v_m}, E(F_{v_m}))$$

where $\Gamma_{v_n}^{v_m} := Gal(F_{v_m}/F_{v_n})$ is a quotient of $\Gamma_{v_n} \subset \mathbb{Z}_p^d$. Consider the exact sequence

$$E_0(F_{v_m}) \hookrightarrow E(F_{v_m}) \twoheadrightarrow T_{v_m}$$

where T_{v_m} is a cyclic group of order $-ord_{v_m}(j(E))$. Our Lemma 4.2 applies here with $L = F_{v_m}$ and $K = F_{v_n}$ and one gets

$$T_{v_m}^{\Gamma_{v_n}^{v_m}}/T_{v_n} \hookrightarrow \mathbb{Z}/e_{v_m/v_n}\mathbb{Z} \to H^1(\Gamma_{v_n}^{v_m}, E(F_{v_m})) \to H^1(\Gamma_{v_n}^{v_m}, T_{v_m})$$

where e_{v_m/v_n} is the ramification index of F_{v_m}/F_{v_n}, hence a power of p. From Tate parametrization one has an isomorphism of Galois modules $T_{v_m} \simeq F_{v_m}^*/\mathcal{O}_{v_m}^* q_{E,v_m}^{\mathbb{Z}}$. Let π_{v_m} be a uniformizer for the prime v_m : then for any $\sigma \in \Gamma_{v_n}^{v_m}$ one has $\sigma(\pi_{v_m}) = u\pi_{v_m}$ for some $u \in \mathcal{O}_{v_m}^*$. Hence $\Gamma_{v_n}^{v_m}$ acts trivially on T_{v_m} and

$$H^1(\Gamma_{v_n}^{v_m}, T_{v_m}) \hookrightarrow (T_{v_m,p})^{d(v_n)}$$

(where $T_{v_m,p}$ is the p-part of the group T_{v_m} and $d(v_n)$ is the number of generators of $\Gamma_{v_n}^{v_m}$). If v_n is unramified then, for any m, $e_{v_m/v_n} = 1$, $d(v_n) \leq 1$ and

$$|T_{v_m}| = |T_{v_n}| = |T_v| = -ord_v(j(E))$$

is finite and constant, so $H^1(\Gamma_{v_n}, E(\mathcal{F}_w)) \hookrightarrow T_{v,p}$. Thus $Ker\, d_w$ is finite and this proves **1** . □

Remark 4.10. With the notations of the previous lemma, if v_n is ramified then

$$|T_{v_m}| = -ord_{v_m}(j(E)) = -ord_{v_n}(j(E))e_{v_m/v_n} = |T_{v_n}|e_{v_m/v_n}\ .$$

Since the T_{v_k}'s are cyclic and the action of $\Gamma_{v_n}^{v_m}$ is trivial one gets

$$T_{v_m}^{\Gamma_{v_n}^{v_m}}/T_{v_n} \simeq \mathbb{Z}/e_{v_m/v_n}\mathbb{Z}$$

and one finds injections

$$H^1(\Gamma_{v_n}^{v_m}, E(F_{v_m})) \hookrightarrow H^1(\Gamma_{v_n}^{v_m}, T_{v_m}) \hookrightarrow (T_{v_m,p})^{d(v_n)}\ .$$

Hence, taking limits, one has

$$H^1(\Gamma_{v_n}, E(\mathcal{F}_w)) \hookrightarrow \varinjlim_{m} (T_{v_m,p})^{d(v_n)} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{d(v_n)}$$

which gives another proof of part **3** of Lemma 4.9.

4.4. **Modified Selmer groups.** In section 5 we are going to consider characteristic and Fitting ideals of $Sel_E(\mathcal{F}_d)_p^\vee$ in order to define some algebraic L-function for E. Those ideals are well defined for the finitely generated modules provided by Corollary 4.8, but they are non-trivial only for torsion modules. In order to reduce to this latter case one needs finite kernels and cokernels for the maps

$$Sel_E(F_n)_p \longrightarrow Sel_E(\mathcal{F}_d)_p^{\Gamma_n}$$

and in Theorem 4.4 and Lemma 4.9 we have seen that the only obstruction comes from the ramified primes. We are going to modify the definition of the Selmer groups in order to give at least two ways in which one could get torsion modules.

Definition 4.11. *With all notations as in section 2.2 let $\Sigma \subset \mathcal{M}_L$ be a set of places of an algebraic extension L of F. We define*

$$Sel_{E,\Sigma}(L)_p := Ker\{H^1_{fl}(X_L, E[p^\infty]) \to \prod_{v \notin \Sigma} H^1_{fl}(X_{L_v}, E[p^\infty])/Im\,\kappa_v\}$$

and

$$Sel_E^{\Sigma}(L)_p := Ker\{H^1_{fl}(X_L, E[p^\infty])$$
$$\to \prod_{v \notin \Sigma} H^1_{fl}(X_{L_v}, E[p^\infty])/Im\,\kappa_v \times \prod_{v \in \Sigma} H^1_{fl}(X_{L_v}, E[p^\infty])\}$$

to be the p-parts of the (lower and upper respectively) Σ-Selmer groups *of E over L.*

Note that

$$Sel_E^{\Sigma}(L)_p \subseteq Sel_E(L)_p \subseteq Sel_{E,\Sigma}(L)_p$$

with equality occurring if $\Sigma = \emptyset$.
In the same setting of Theorem 4.4 we can now prove

Theorem 4.12. *Let $\mathcal{F}_d/F$ be a $\mathbb{Z}_p^d$-extension. Let $\Sigma(d)$ be the set of ramified places in $\mathcal{F}_d$ and, for any n, let Σ_n be the set of primes of F_n lying below $\Sigma(d)$. Assume that E has split multiplicative reduction at all places in Σ_0 (so that, in particular, Σ_0 is finite). Then the maps*

$$\alpha_n \,:\, Sel_{E,\Sigma_n}(F_n)_p \to Sel_{E,\Sigma(d)}(\mathcal{F}_d)_p^{\Gamma_n}$$

and

$$\beta_n \,:\, Sel_E^{\Sigma_n}(F_n)_p \to Sel_E^{\Sigma(d)}(\mathcal{F}_d)_p^{\Gamma_n}$$

have finite kernels and cokernels.

Proof. The structure of the proof is the same as for Theorem 4.4: no changes are needed for the maps b_n and d_w's for all w's of good reduction. We are left with the finitely many places of bad reduction in F_n. For unramified primes Lemma 4.9 shows that $Ker\, d_w$ is finite and this completes the proof for the maps α_n.
For the upper Σ-Selmer groups one has to consider also the maps

$$\tilde{d}_w \,:\, H^1_{fl}(X_{v_n}, E[p^\infty]) \to H^1_{fl}(\mathcal{X}_w, E[p^\infty])$$

for the ramified primes v_n. As seen before one can apply Hochschild-Serre to find $Ker\,\tilde{d}_w = H^1(\Gamma_{v_n}, E[p^\infty](\mathcal{F}_w))$ and, since $E[p^\infty](\mathcal{F}_w)$ is finite (same proof as Lemma 4.3, using $\mathcal{F}_w \bigcap \overline{F} \subseteq F^{sep}$), one gets

$$|Ker\,\tilde{d}_w| \leq |E[p^\infty](\mathcal{F}_w)|^d$$

by Lemma 4.1. □

Corollary 4.13. *In the setting of Theorem 4.12 assume that $Sel_{E,\Sigma_0}(F)_p$ is cofinitely generated over $\mathbb{Z}_p$ (resp. finite). Then $Sel_{E,\Sigma(d)}(\mathcal{F}_d)_p$ is a cofinitely generated (resp. torsion) Λ_d-module. The same statement holds for the upper $\Sigma(d)$-Selmer group.*

Proof. The proof of Corollary 4.8 applies here as well. One only has to note that if M/IM is finite for some finitely generated Λ_d-module M (where I is the augmentation ideal of Λ_d) then M is a torsion module by the final Theorem of [1, section 4]. □

For a $\mathbb{Z}_p$-extension we can therefore give a proof of the following corollary along the lines of [8, Corollary 4.9 and Theorem 1.3].

Corollary 4.14. *In the setting of the previous corollary assume that $Sel_{E,\Sigma_0}(F)_p$ is finite. Then $E(\mathcal{F}_1)$ is finitely generated.*

Proof. Let $\Sigma := \Sigma(1)$ and let $\mathcal{S}_{1,\Sigma}$ be the dual of $Sel_{E,\Sigma}(\mathcal{F}_1)_p$. By Corollary 4.13 $\mathcal{S}_{1,\Sigma}$ is a finitely generated torsion Λ_1-module. By the well-known structure theorem for such modules there is a pseudo-isomorphism (i.e. with finite kernel and cokernel)

$$\mathcal{S}_{1,\Sigma} \sim \bigoplus_{i=1}^{r} \mathbb{Z}_p[[T_1]]/(f_i^{e_i})\,.$$

Let $\lambda = \deg \prod f_i^{e_i}$: then $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{S}_{1,\Sigma} = \lambda$ and, taking duals, one gets

$$(Sel_{E,\Sigma}(\mathcal{F}_1)_p)_{div} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$$

(where $(Sel_{E,\Sigma}(\mathcal{F}_1)_p)_{div}$ is the divisible part of $Sel_{E,\Sigma}(\mathcal{F}_1)_p$). By Theorem 4.12, for any n, one has

$$(Sel_{E,\Sigma_n}(F_n)_p)_{div} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n} \text{ with } t_n \leq \lambda\ .$$

Moreover we know that

$$E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{rank\,E(F_n)}$$

and, obviously,

$$E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow (Sel_{E,\Sigma_n}(F_n)_p)_{div}$$

(which is not true in general for the upper Σ-Selmer groups). Therefore $rank\, E(F_n) \leq t_n \leq \lambda$ for any n, i.e. such ranks are bounded.
Choose m such that $rank\, E(F_m)$ is maximal, then $E(\mathcal{F}_1)/E(F_m)$ is a torsion group. Take $P \in E(\mathcal{F}_1)$ and let s be such that $sP \in E(F_m)$. Then for any $\gamma \in Gal(\mathcal{F}_1/F_m)$ one has $s(\gamma(P)-P) = 0$, i.e. $\gamma(P)-P \in E(\mathcal{F}_1)_{tor}$. Since the torsion points in $E(\mathcal{F}_1)$ are finite (we provide a proof in Lemma 4.15 below) take $t = |E(\mathcal{F}_1)_{tor}|$ to get $t(\gamma(P)-P) = 0$. Thus $tP \in E(F_m)$ for all $P \in E(\mathcal{F}_1)$ and multiplication by t gives a homomorphism $\varphi_t : E(\mathcal{F}_1) \to E(F_m)$ whose image is finitely generated (being a subgroup of $E(F_m)$) and whose kernel is the finite group $E(\mathcal{F}_1)_{tor}$. Hence $E(\mathcal{F}_1)$ is indeed finitely generated. □

Lemma 4.15. *For any $d \geq 1$, the set $E(\mathcal{F}_d)_{tor}$ is finite.*

Proof. For any l, let K_l be the minimal extension of F such that $E[l](K_l) = E[l](\overline{F})$. By Igusa's work [12], it is known that for almost all primes $l \neq p$ the Galois group $Gal(K_l/F)$ contains a subgroup isomorphic to $SL_2(\mathbb{F}_l)$. This implies that the subgroup generated by the Galois orbit of any $P \in E[l](\overline{F}) - \{0\}$ is all of $E[l](\overline{F})$. In particular, since $\mathcal{F}_d/F$ is Galois, $E[l](\mathcal{F}_d) \neq \{0\}$ would imply $K_l \subset \mathcal{F}_d$, contradicting the fact that $\mathcal{F}_d/F$ is abelian.
We are left with the possibility that $E[l^\infty](\mathcal{F}_d)$ is infinite for some prime l. Assume that this happens: then one can choose an infinite sequence $P_n \in E[l^n]$ so that $lP_{n+1} = P_n$. Let $\mathcal{F}' \subset \mathcal{F}_d$ be the minimal extension of F such that $\{P_n\}_{n\in\mathbb{N}} \subset E(\mathcal{F}')$ and put $\Gamma' := Gal(\mathcal{F}'/F)$. Then Γ' is both an infinite subgroup of $\mathbb{Z}_l^*$ (the automorphisms of the group generated by the P_n's) and a quotient of $\Gamma \simeq \mathbb{Z}_p^d$: this is impossible for $l \neq p$. We already proved that $E[p^\infty](F^{sep})$ is finite in Lemma 4.3. □

5. The algebraic L-function and the main conjecture

5.1. **The characteristic and Fitting ideals.** In this section, we work again with a $\mathbb{Z}_p^{\mathbb{N}}$-extension $\mathcal{F}/F$. In order to apply results from section 4, we consider $\mathbb{Z}_p^d$-subextensions $\mathcal{F}_d \subset \mathcal{F}$, naturally ordered by inclusion; we call such fields *$\mathbb{Z}_p$-finite extensions* (of F). We will let $\mathcal{F}_d$ vary among all $\mathbb{Z}_p$-finite subextensions of $\mathcal{F}$: therefore we need to refine our notations.
Let $\Lambda(\mathcal{F}_d) := \mathbb{Z}_p[[Gal(\mathcal{F}_d/F)]]$ and $\mathcal{S}(\mathcal{F}_d) := Sel_E(\mathcal{F}_d)_p^\vee$ (shortened into Λ_d and $\mathcal{S}_d$ when it is clear to which extension they refer).

It is assumed throughout that all places which ramify in $\mathcal{F}/F$ are of split multiplicative reduction for E.

For any fixed $\mathcal{F}_d$, Corollary 4.8 states that $\mathcal{S}_d$ is a finitely generated Λ_d-module. Recall that Λ_d is (noncanonically) isomorphic to $\mathbb{Z}_p[[T_1, \dots, T_d]]$. A finitely generated torsion Λ_d-module is said to be *pseudo-null* if it has at least two relatively prime annihilators (or, equivalently, if its annihilator ideal has height at least 2). For example if $d = 1$ pseudo-null is equivalent to finite. A *pseudo-isomorphism* between finitely generated Λ_d-modules M and N (i.e. a morphism with pseudo-null kernel and cokernel) will be denoted by $M \sim_{\Lambda_d} N$. If M is a finitely generated Λ_d-module then there is a pseudo-isomorphism

$$M \sim_{\Lambda_d} \Lambda_d^r \oplus \left(\bigoplus_{i=1}^{n(M)} \Lambda_d/(g_i^{e_i})\Lambda_d \right)$$

where the g_i's are irreducible elements of Λ_d (determined up to an element of Λ_d^*) and r, $n(M)$ and the e_i's are uniquely determined (see e.g. the structure theorem [3, VII.4.4 Theorem 5]).

Definition 5.1. *In the above setting the* characteristic ideal *of M is*

$$Char_{\Lambda_d}(M) := \begin{cases} 0 & \text{if } M \text{ is not torsion} \\ \left(\prod_{i=1}^{n(M)} g_i^{e_i}\right) & \text{otherwise} \end{cases} .$$

Let Z be a finitely generated Λ_d-module and let

$$\Lambda_d^a \xrightarrow{\varphi} \Lambda_d^b \twoheadrightarrow Z$$

be a presentation where the map φ can be represented by an $a \times b$ matrix Φ with entries in Λ_d.

Definition 5.2. *In the above setting the* Fitting ideal *of Z is*

$$Fitt_{\Lambda_d}(Z) := \begin{cases} 0 & \text{if } a < b \\ \text{the ideal generated by all the} & \\ \text{determinants of the } b \times b & \text{if } a \geq b \\ \text{minors of the matrix } \Phi & \end{cases} .$$

For the basic theory and properties of Fitting ideals the reader is referred to the Appendix in [16]. Here we only mention the fact that $Fitt_{\Lambda_d}(Z)$ is independent from the presentation and that if Z is an elementary module, i.e. if

$$Z = \Lambda_d^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda_d/(g_i^{e_i})\Lambda_d \right)$$

then $Fitt_{\Lambda_d}(Z) = Char_{\Lambda_d}(Z)$.

5.1.1. *$\mathbb{Z}_p$-finite extensions.* We can extend our control theorem to a relation between Selmer groups of $\mathbb{Z}_p$-finite extensions of F.

Theorem 5.3. *For any inclusion of $\mathbb{Z}_p$-finite extensions $\mathcal{F}_d \subset \mathcal{F}_e$, $e > d \geq 2$, one has*

$$Sel_E(\mathcal{F}_d)_p^\vee \sim_{\Lambda_d} (Sel_E(\mathcal{F}_e)_p^{\Gamma_d^e})^\vee$$

(where $\Gamma_d^e = Gal(\mathcal{F}_e/\mathcal{F}_d)$).

Proof. We look for annihilators of the kernel and cokernel of the natural map between $Sel_E(\mathcal{F}_d)_p$ and $Sel_E(\mathcal{F}_e)_p^{\Gamma_d^e}$ because they annihilate the duals as well. As in the proof of Theorem 4.4, consider the diagram

$$\begin{array}{ccccc} Sel_E(\mathcal{F}_d)_p & \hookrightarrow & H^1_{fl}(\mathcal{X}_d, E[p^\infty]) & \twoheadrightarrow & \mathcal{G}(\mathcal{X}_d) \\ \downarrow a & & \downarrow b & & \downarrow c \\ Sel_E(\mathcal{F}_e)_p^{\Gamma_d^e} & \hookrightarrow & H^1_{fl}(\mathcal{X}_e, E[p^\infty])^{\Gamma_d^e} & \longrightarrow & \mathcal{G}(\mathcal{X}_e)\ . \end{array}$$

By Corollary 4.8 we know that $Ker\, a$ and $Coker\, a$ are cofinitely generated Λ_d-modules. Moreover $Ker\, a$, $Ker\, b$ and $Coker\, b$ are finite. Therefore it is enough to find two relatively prime annihilators for $Ker\, c$. We consider the maps

$$d_{w_e} : H^1_{fl}(\mathcal{X}_{w_d}, E[p^\infty])/Im\, \kappa_{w_d} \to H^1_{fl}(\mathcal{X}_{w_e}, E[p^\infty])/Im\, \kappa_{w_e}$$

(for any $w_e \in \mathcal{M}_{\mathcal{F}_e}$ dividing $w_d \in \mathcal{M}_{\mathcal{F}_d}$). As in section 4.2.4 one sees that $Ker\, d_{w_e} = 0$ for primes of good reduction and for primes which split completely in $\mathcal{F}_e/\mathcal{F}_d$.
For primes w_d of bad reduction which do not split completely, working as in Theorem 4.4, one finds injections

$$Ker\, d_{w_e} \hookrightarrow H^1(\Gamma_{w_d}^{w_e}, E(\mathcal{F}_{w_e})) \hookrightarrow H^2(\Gamma_{w_d}^{w_e}, q_{E,v}^{\mathbb{Z}})$$

(where $\Gamma_{w_d}^{w_e}$ is the local Galois group).
The group $Gal(\mathcal{F}_d/F)$ acts trivially both on $q_{E,v} \in F_v$ and on $\Gamma_{w_d}^{w_e}$ (because Γ is abelian). Since $d \geq 2$ there are two topologically independent elements γ_1, γ_2 of $Gal(\mathcal{F}_d/F)$. Hence

$$H^2(\Gamma_{w_d}^{w_e}, q_{E,v}^{\mathbb{Z}}) \sim_{\Lambda_d} 0$$

because its annihilator ideal contains at least $\gamma_1 - 1$ and $\gamma_2 - 1$. Therefore all $Ker\, d_{w_e}$'s are "pseudo-null" Λ_d-modules and have common annihilators which then annihilate $Ker\, c$ as well. □

Corollary 5.4. *In the same setting of Theorem 5.3 let $\pi_d^e : \Lambda_e \to \Lambda_d$ be the canonical projection and $I_{e/d}$ its kernel. Then*

$$Char_{\Lambda_d}(\mathcal{S}_d) = Char_{\Lambda_d}(\mathcal{S}_e/I_{e/d}\mathcal{S}_e)\ .$$

Proof. Just take duals in the pseudo-isomorphism given by Theorem 5.3. □

Lemma 5.5. *Let $\mathcal{F}_d \subset \mathcal{F}_e$ be an inclusion of $\mathbb{Z}_p$-finite extensions, $e > d$. Assume that $E[p^\infty](\mathcal{F}) = 0$ or that $Fitt_{\Lambda_d}(\mathcal{S}_d)$ is principal. Then*

$$\pi_d^e(Fitt_{\Lambda_e}(\mathcal{S}_e)) \subseteq Fitt_{\Lambda_d}(\mathcal{S}_d) \ .$$

Proof. Dualising the left hand side of the diagram in Theorem 5.3 one finds a sequence

$$\mathcal{S}_e/I_{e/d}\mathcal{S}_e \to \mathcal{S}_d \twoheadrightarrow (Ker\, a)^\vee$$

where

$$Ker\, a \hookrightarrow H^1(\Gamma_d^e, E[p^\infty](\mathcal{F}_e))$$

is finite (by Lemmas 4.3 and 4.1). If $E[p^\infty](\mathcal{F}) = 0$ then $(Ker\, a)^\vee = 0$ and

$$\pi_d^e(Fitt_{\Lambda_e}(\mathcal{S}_e)) = Fitt_{\Lambda_d}(\mathcal{S}_e/I_{e/d}\mathcal{S}_e) \subseteq Fitt_{\Lambda_d}(\mathcal{S}_d)$$

by [16, properties 1 and 4].
If $E[p^\infty](\mathcal{F}) \neq 0$, by [16, property 9] one gets

$$Fitt_{\Lambda_d}(\mathcal{S}_e/I_{e/d}\mathcal{S}_e) Fitt_{\Lambda_d}((Ker\, a)^\vee) \subseteq Fitt_{\Lambda_d}(\mathcal{S}_d) \ .$$

The Fitting ideal of a finitely generated torsion module contains a power of its annihilator ([16, property 8]) so let σ_1, σ_2 be two relatively prime elements of $Fitt_{\Lambda_d}((Ker\, a)^\vee)$. (Recall that Λ_d is a unique factorization domain and relatively prime means that they have no common factor.) Let θ_d be a generator of $Fitt_{\Lambda_d}(\mathcal{S}_d)$. Then for any $\alpha \in Fitt_{\Lambda_d}(\mathcal{S}_e/I_{e/d}\mathcal{S}_e)$ one finds that $\sigma_1\alpha$ and $\sigma_2\alpha$ are divisible by θ_d (or $\sigma_1\alpha = \sigma_2\alpha = 0$ if $\theta_d = 0$). Hence θ_d divides α (or $\alpha = 0$) and

$$\pi_d^e(Fitt_{\Lambda_e}(\mathcal{S}_e)) = Fitt_{\Lambda_d}(\mathcal{S}_e/I_{e/d}\mathcal{S}_e) \subseteq Fitt_{\Lambda_d}(\mathcal{S}_d) \ . \qquad \square$$

Remark 5.6. The hypothesis on $Fitt_{\Lambda_d}(\mathcal{S}_d)$ is verified, for example, if $\mathcal{S}_d$ is an elementary module or if one can find a presentation with the same number of generators and relations. Also $E[p^\infty](\mathcal{F}) = 0$ if $j(E) \notin (F^*)^p$ (see Lemma 4.3).

5.1.2. *Going to the limit.* For $\mathcal{F}_d \subset \mathcal{F}$ a $\mathbb{Z}_p$-finite extension of F we let $\pi_{\mathcal{F}_d} : \Lambda \to \Lambda(\mathcal{F}_d)$ be the canonical projection. All $\Lambda(\mathcal{F}_d)$-modules can be thought of as modules over the ring Λ with trivial action of $Gal(\mathcal{F}/\mathcal{F}_d)$.
Define

$$\widetilde{Fitt}_\Lambda(\mathcal{S}(\mathcal{F}_d)) := \pi_{\mathcal{F}_d}^{-1}(Fitt_{\Lambda(\mathcal{F}_d)}(\mathcal{S}(\mathcal{F}_d))) \ .$$

Lemma 5.7. *Under the same assumptions of Lemma 5.5 one has*

$$\widetilde{Fitt}_\Lambda(\mathcal{S}_e) \subseteq \widetilde{Fitt}_\Lambda(\mathcal{S}_d) \ .$$

Proof. By Lemma 5.5

$$\pi_d^e(Fitt_{\Lambda_e}(\mathcal{S}_e)) \subseteq Fitt_{\Lambda_d}(\mathcal{S}_d) \ .$$

The claim follows observing that $\pi_{\mathcal{F}_d} = \pi_d^e \circ \pi_{\mathcal{F}_e}$. $\square$

Definition 5.8. *With the assumptions of Lemma 5.5, let* $\mathcal{S} := Sel_E(\mathcal{F})_p^\vee$ *. Its* pro-Fitting ideal *is*

$$\widetilde{Fitt}_\Lambda(\mathcal{S}) := \bigcap \widetilde{Fitt}_\Lambda(\mathcal{S}(\mathcal{F}_d))$$

where the intersection is taken over all $\mathbb{Z}_p$*-finite subextensions.*

Remark 5.9. *1.* By Corollary 4.8 the Λ-modules $\mathcal{S}(\mathcal{F}_d)$ are finitely generated: hence one can define their Fitting ideals $Fitt_\Lambda(\mathcal{S}(\mathcal{F}_d))$ in the usual way, as the ideals generated by maximal minors of the matrix expressing relations between a (finite) chosen set of generators. Then, by [16, property 4],

$$\widetilde{Fitt}_\Lambda(\mathcal{S}(\mathcal{F}_d)) = Fitt_\Lambda(\mathcal{S}(\mathcal{F}_d)) + Ker(\pi_{\mathcal{F}_d}) \ .$$

When also $\mathcal{S}$ is finitely generated one constructs $Fitt_\Lambda(\mathcal{S})$ in the same way. Moreover if $E[p^\infty](\mathcal{F}) = 0$, then the natural maps $\mathcal{S} \to \mathcal{S}(\mathcal{F}_d)$ are surjective and

$$Fitt_\Lambda(\mathcal{S}) = \widetilde{Fitt}_\Lambda(\mathcal{S})$$

by [16, property 10] (the result is true also without the noetherian hypothesis in the reference).
2. Since $\Lambda = \varprojlim \Lambda(\mathcal{F}_d)$, one has an equivalent definition using projective limits. Indeed

$$\widetilde{Fitt}_\Lambda(\mathcal{S}) = \bigcap_{\mathcal{F}_d} \pi_{\mathcal{F}_d}^{-1}(Fitt_{\Lambda(\mathcal{F}_d)}(\mathcal{S}(\mathcal{F}_d))) = \\ = \varprojlim_{\mathcal{F}_d} Fitt_{\Lambda(\mathcal{F}_d)}(\mathcal{S}(\mathcal{F}_d)) \ .$$

In particular if $\mathcal{S}$ is finitely generated and $E[p^\infty](\mathcal{F}) = 0$, then

$$Fitt_\Lambda(\mathcal{S}) = \widetilde{Fitt}_\Lambda(\mathcal{S}) = \varprojlim_{\mathcal{F}_d} Fitt_{\Lambda(\mathcal{F}_d)}(\mathcal{S}(\mathcal{F}_d))$$

(for a similar result on the behaviour of Fitting ideals with respect to projective limits see [10, Theorem 2.1]).

The use of Fitting ideals instead of characteristic ideals is justified exactly by their behaviour with respect to limits and some reformulations of the Main Conjectures of Iwasawa theory in terms of Fitting ideals have already been given in [9], [10] and [13]. Anyway the two ideals are strictly connected as the following lemma shows. The ideal $\widetilde{Fitt}_\Lambda(\mathcal{S})$ (or, if it is principal, a generator of such an ideal) might be a good candidate for our algebraic L-function.

Lemma 5.10. *Let* $\mathcal{F}_d/F$ *be a* $\mathbb{Z}_p^d$*-extension and* $\Lambda_d := \Lambda(\mathcal{F}_d)$*. Let* M *be a finitely generated* Λ_d*-module. Then*

$$Fitt_{\Lambda_d}(M) \subseteq Char_{\Lambda_d}(M) \ .$$

Moreover if $Fitt_{\Lambda_d}(M)$ *is principal then* $Fitt_{\Lambda_d}(M) = Char_{\Lambda_d}(M)$.

Proof. If M is not torsion then $Fitt_{\Lambda_d}(M) = Char_{\Lambda_d}(M) = 0$ so we can assume that M is a torsion Λ_d-module.
Let E be the elementary module which is pseudo-isomorphic to M by the structure theorem stated before Definition 5.1. Being pseudo-isomorphic is an equivalence relation between finitely generated torsion Λ_d-modules so the structure theorem gives rise to two exact sequences

$$A_1 \hookrightarrow M \to E \twoheadrightarrow A_2$$

and

$$B_1 \hookrightarrow E \to M \twoheadrightarrow B_2$$

where A_1 , A_2 , B_1 , B_2 are pseudo-null. From these sequences one gets

$$Fitt_{\Lambda_d}(M)Fitt_{\Lambda_d}(A_2) \subseteq Fitt_{\Lambda_d}(E) = Char_{\Lambda_d}(E) = Char_{\Lambda_d}(M)$$

(by [16, property 9], using $Fitt_{\Lambda_d}(M) \subseteq Fitt_{\Lambda_d}(M/A_1)$) and

$$Char_{\Lambda_d}(M)Fitt_{\Lambda_d}(B_2) = Fitt_{\Lambda_d}(E)Fitt_{\Lambda_d}(B_2) \subseteq Fitt_{\Lambda_d}(M) \ .$$

As seen in Lemma 5.5 let σ_1 , σ_2 be two relatively prime elements of $Fitt_{\Lambda_d}(B_2)$ and τ_1 , τ_2 two relatively prime elements of $Fitt_{\Lambda_d}(A_2)$. Let θ be a generator of $Char_{\Lambda_d}(M)$: then, for any $\alpha \in Fitt_{\Lambda_d}(M)$, $\alpha\tau_1$ and $\alpha\tau_2$ are divisible by θ . Hence θ divides α and $Fitt_{\Lambda_d}(M) \subseteq Char_{\Lambda_d}(M)$.
If $Fitt_{\Lambda_d}(M)$ is principal we can use the same proof with the σ_i's in the place of the τ_i's to get the reverse inclusion and eventually the equality $Fitt_{\Lambda_d}(M) = Char_{\Lambda_d}(M)$. □

5.2. **The analytic side.** We briefly describe how to associate p-adic L-functions (in the sense of 1.2.2) to E and to certain Galois extensions $\widetilde{\mathcal{F}}/F$. Since our goal is just to provide an introduction to a main conjecture, the angel of brevity compels us to be very sketchy; for the missing details the reader is referred to the original papers and to [2].

All examples we know can be seen as applications of the following general ideas.
To begin with, we fix a place ∞ such that E has conductor $\mathfrak{n}\infty$ (in particular, because of our initial assumption, E has split multiplicative reduction at ∞). Then, thanks to the analytic uniformization of elliptic curves by Drinfeld modular curves, one can associate to E a $\mathbb{Z}$-valued measure $\mu_{E,\infty}$ on $\mathbb{P}^1(F_\infty)$ ([14, page 386]). The next ingredients are a quadratic algebra K/F (the case $K = F \times F$ is allowed) and an embedding $\Psi : K \to M_2(F)$. The algebra K and the map Ψ are required to satisfy certain conditions which it would be too long to discuss here.
At this point there are essentially two constructions. One (carried out in [14]) consists in taking a fundamental domain X for the action on $\mathbb{P}^1(F_\infty)$ of a certain quotient of the group $(K \otimes F_\infty)^*$ via Ψ.
In the second approach, developed in [11], one chooses a second place

$\mathfrak{p}$ dividing $\mathfrak{n}$. Then, by a construction reminiscent of modular symbols, the fixed points x, y of $\Psi(K^*)$ and the measure $\mu_{E,\infty}$ (or rather the harmonic cocycle attached to it) are employed to define a measure $\mu_E\{x \to y\}$ on $\mathbb{P}^1(F_{\mathfrak{p}})$.
In both cases, class field theory allows to identify the set X (respectively $\mathcal{O}_{\mathfrak{p}}^* \subset \mathbb{P}^1(F_{\mathfrak{p}})$) with a Galois group $G := Gal(\widetilde{\mathcal{F}}/H)$, where $\widetilde{\mathcal{F}}$ is either an anticyclotomic extension of K (if K is a field) or a cyclotomic extension of F and H/F is a finite extension. We skip precise definitions, just remarking that G contains a finite index subgroup isomorphic to $\mathbb{Z}_p^{\mathbb{N}}$.
The restriction of $\mu_{E,\infty}$ to X (resp. of $\mu_E\{x \to y\}$ to $\mathcal{O}_{\mathfrak{p}}^*$) can be thought of as a measure on G, that is, an element $L(E) \in \mathbb{Z}[[G]] \subset \mathbb{Z}_p[[G]]$. Teitelbaum's measure referred to in paragraph 1.2.2 appears as a special instance of $\mu_E\{x \to y\}$ ([11, Lemma 3.10]).

5.3. **Main Conjecture.** From classical Iwasawa theory, one would expect that an analytic p-adic L-function should annihilate the dual Selmer group $\mathcal{S}$ of the corresponding extension $\mathcal{F}/F$.

Notations are as in section 5.2. We let $\widetilde{\mathcal{F}}$ be either an anticyclotomic extension as in [14, Section 2.3] or a cyclotomic one as in [14, Section 3] or in 1.2.1 above. The torsion of $G = Gal(\widetilde{\mathcal{F}}/H)$ is a finite subgroup and, unless possibly when K is a quadratic field where the place ∞ splits, $\Gamma := G/G_{tor}$ is the Galois group of a $\mathbb{Z}_p^{\mathbb{N}}$-subextension $\mathcal{F}/H$. Let $\pi : \mathbb{Z}[[G]] \to \mathbb{Z}[[\Gamma]]$ be the natural projection.

Conjecture 5.11. *Assume that $E[p^\infty](\mathcal{F}) = 0$ or that $Fitt_{\Lambda_d}(\mathcal{S}_d)$ is principal for all d. For all the $L(E)$'s as described above one has*

$$\widetilde{Fitt}_\Lambda(\mathcal{S}) = (\pi(L(E))) \ .$$

Remark 5.12. 1. The interesting cases are when the Fitting ideal is not zero. By analogy with the classical situation one expects that then the group $E(\mathcal{F})$ should be finitely generated. The only case we are aware of where the behaviour of Mordell-Weil has been studied in a $\mathbb{Z}_p^{\mathbb{N}}$-tower of function fields is [4]: Breuer proves that $E(H[\mathfrak{p}^\infty])$ has infinite rank. Observe that no analytic L-function has been defined in his setting.
2. The available (partial) proofs of Main Conjecures over number fields often require to modify local conditions defining Selmer groups. We made a first attempt in Definition 4.11 in order to get torsion Λ_d-modules. To tackle Conjecture 5.11 one might have to further refine local conditions at places of bad reduction.
3. The analytic p-adic L-function is an element $L(E) \in \mathbb{Z}[[\Gamma]]$. In the prospect of Iwasawa theory, it seems natural to extend scalars to $\mathbb{Z}_p$; however, $L(E)$ may be seen as belonging to $\mathbb{Z}_l[[\Gamma]]$ as well and one can

wonder if it also annihilates the Selmer dual arising from the l-torsion. In absence of any support or clue, this is just a speculation.

References

[1] P.N. Balister - S. Howson *Note on Nakayama's lemma for compact* Λ-*modules*, Asian J. Math. **1** (1997), no. 2, 224–229.

[2] A. Bandini - I. Longhi *p-adic L-functions for elliptic curves over function fields*, in preparation.

[3] N. Bourbaki, *Commutative algebra. Chapters 1-7*, Elements of Mathematics, Springer-Verlag, Berlin, 1998.

[4] F. Breuer *Higher Heegner points on elliptic curves over function fields*, J. Number Theory **104** (2004), no. 2, 315–326.

[5] M.L. Brown *Heegner modules and elliptic curves*, Lecture Notes in Math., 1849, Springer, Berlin, 2004.

[6] D. Goss *Some integrals attached to modular forms in the theory of function fields*, in The arithmetic of function fields (Columbus, OH, 1991), 227–251, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.

[7] R. Greenberg *Iwasawa theory for elliptic curves*, in Arithmetic theory of elliptic curves (Cetraro, 1997), 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[8] R. Greenberg *Introduction to Iwasawa theory for elliptic curves*, in Arithmetic algebraic geometry (Park City, UT, 1999), 407–464, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001.

[9] C. Greither *Computing Fitting ideals of Iwasawa modules*, Math. Zeitschrift **246** (2004), 733–767.

[10] C. Greither - M. Kurihara *Stickelberger elements, Fitting ideals of class groups of CM fields and dualisation*, Math. Z. **260** (4) (2008), 905–930.

[11] H. Hauer - I. Longhi *Teitelbaum's exceptional zero conjecture in the function field case*, J. Reine Angew. Math. **591** (2006), 149–175.

[12] J. Igusa *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959) 453–476.

[13] M. Kurihara *Iwasawa theory and Fitting ideals*, J. Reine Angew. Math. **561** (2003), 39–86.

[14] I. Longhi *Non-archimedean integration and elliptic curves over function fields*, J. Number Theory **94** (2002),no. 2, 375–404.

[15] B. Mazur *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[16] B. Mazur - A- Wiles *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179–330.

[17] J.S. Milne *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, Princeton, N.J., 1980.

[18] J.S. Milne *Arithmetic duality theorems*, Perspectives in Mathematics **1**, Academic Press Inc., Boston, MA, 1986.

[19] J. Neukirch *Algebraic number theory*, translated from German by Norbert Schappacher, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999.

[20] J. Neukirch - A. Schmidt - K. Wingberg *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2000.

[21] M. Rosen *Number theory in function fields*, **GTM 210**, Springer-Verlag, New York, 2002.

[22] J.H. Silverman *The arithmetic of elliptic curves*, **GTM 106**, Springer-Verlag, New York, 1986.
[23] J.H. Silverman *Advanced topics in the arithmetic of elliptic curves*, **GTM 151**, Springer-Verlag, New York, 1994.
[24] J. Teitelbaum *Modular symbols for* $\mathbb{F}_q[T]$, Duke Math. J. **68** (1992), no. 2, 271–295.
[25] D.L. Ulmer *p-descent in characteristic* p, Duke Math. J. **62** (1991), no. 2, 237–265.
[26] D.L. Ulmer *Geometric non-vanishing*, Invent. Math. **159** (2005), no. 1, 133–186.

A. Bandini
Università della Calabria - Dipartimento di Matematica
via P. Bucci - Cubo 30B - 87036 Arcavacata di Rende (CS) - Italy
bandini@mat.unical.it

I. Longhi
Department of Mathematics - National Taiwan University
No. 1, section 4 Roosevelt Road
Taipei 106 - Taiwan
longhi@math.ntu.edu.tw