TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 3, March 2018, Pages 1925–1958
http://dx.doi.org/10.1090/tran/7016
Article electronically published on August 15, 2017

PONTRYAGIN DUALITY FOR IWASAWA MODULES AND ABELIAN VARIETIES

KING FAI LAI, IGNAZIO LONGHI, KI-SENG TAN, AND FABIEN TRIHAN

Abstract. We prove a functional equation for two projective systems of finite abelian p-groups, $\{\mathfrak{a}_n\}$ and $\{\mathfrak{b}_n\}$, endowed with an action of $\mathbb{Z}_p^d$ such that $\mathfrak{a}_n$ can be identified with the Pontryagin dual of $\mathfrak{b}_n$ for all n.

Let K be a global field. Let L be a $\mathbb{Z}_p^d$-extension of K ($d \geq 1$), unramified outside a finite set of places. Let A be an abelian variety over K. We prove an algebraic functional equation for the Pontryagin dual of the Selmer group of A.

1. Introduction

Let Γ be an abelian p-adic Lie group isomorphic to $\mathbb{Z}_p^d$ where $\mathbb{Z}_p$ is the ring of p-adic integers and d is a positive integer. The Iwasawa algebra is the complete group ring $\mathbb{Z}_p[[\Gamma]]$ which we denote by Λ. An Iwasawa module is a topological Λ-module.

We study a Pontryagin duality for Iwasawa modules which are inverse limits of finite Iwasawa modules with Λ acting through Γ_n, where Γ_n denotes Γ/Γ^{p^n}. Our result leads to a functional equation for the characteristic ideals of these Iwasawa modules. We then apply these results to Selmer groups of abelian varieties over $\mathbb{Z}_p^d$-extensions of global fields.

Before we describe our Pontryagin duality we recall a few simple notions concerning Iwasawa modules. A finitely generated Λ-module M is said to be *pseudo-null* if no height one prime ideal contains its annihilator ([Bou65, §4]). A *pseudo-isomorphism* of Λ-modules is a homomorphism with pseudo-null kernel and cokernel. We write $M \sim N$ to mean that there exists a pseudo-isomorphism from M to N.

The inversion $\Gamma \to \Gamma$, $\gamma \mapsto \gamma^{-1}$, gives rise to an isomorphism from Λ to Λ which we denote as sending an element λ to $\lambda^\sharp$. This allows us to twist a Λ-module M to ${}_\sharp\Lambda \otimes_\Lambda M$, which we denote by $M^\sharp$ (see §2.2.2).

Now let us describe the formal structure we need for the Pontryagin duality.

Consider a collection

$$\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n \ \mid\ n, m \in \mathbb{N} \cup \{0\},\ n \geq m\}$$

Received by the editors February 4, 2016 and, in revised form, June 27, 2016.

2010 *Mathematics Subject Classification.* Primary 11S40; Secondary 11R23, 11R34, 11R42, 11R58, 11G05, 11G10.

Key words and phrases. Pontryagin duality, abelian variety, Selmer group, Iwasawa theory.

The first, second, and third authors were partially supported by the National Science Council of Taiwan, grants NSC98-2115-M-110-008-MY2, NSC100-2811-M-002-079, and NSC99-2115-M-002-002-MY3, respectively.

The fourth author was supported by EPSRC.

where

(Γ-1) $\mathfrak{a}_n, \mathfrak{b}_n$ are finite abelian groups, with an action of Λ factoring through $\mathbb{Z}_p[\Gamma_n]$.

(Γ-2) For $n \geq m$,

$$\mathfrak{r}_m^n \colon \mathfrak{a}_m \times \mathfrak{b}_m \longrightarrow \mathfrak{a}_n \times \mathfrak{b}_n\,,$$
$$\mathfrak{k}_m^n \colon \mathfrak{a}_n \times \mathfrak{b}_n \longrightarrow \mathfrak{a}_m \times \mathfrak{b}_m$$

are Γ-morphisms such that $\mathfrak{r}_m^n(\mathfrak{a}_m) \subset \mathfrak{a}_n$, $\mathfrak{r}_m^n(\mathfrak{b}_m) \subset \mathfrak{b}_n$, $\mathfrak{k}_m^n(\mathfrak{a}_n) \subset \mathfrak{a}_m$, $\mathfrak{k}_m^n(\mathfrak{b}_n) \subset \mathfrak{b}_m$ and $\mathfrak{r}_n^n = \mathfrak{k}_n^n = \mathrm{id}$. Also, $\{\mathfrak{a}_n \times \mathfrak{b}_n, \mathfrak{r}_m^n\}_n$ form an inductive system and $\{\mathfrak{a}_n \times \mathfrak{b}_n, \mathfrak{k}_m^n\}_n$ form a projective system.

(Γ-3) We have

$$\mathfrak{r}_m^n \circ \mathfrak{k}_m^n = \mathrm{N}_{\Gamma_n/\Gamma_m} \colon \mathfrak{a}_n \times \mathfrak{b}_n \longrightarrow \mathfrak{a}_n \times \mathfrak{b}_n$$

(where $\mathrm{N}_{\Gamma_n/\Gamma_m} := \sum_{\sigma \in \mathrm{Ker}(\Gamma_n \twoheadrightarrow \Gamma_m)} \sigma$ is the norm associated with $\Gamma_n \twoheadrightarrow \Gamma_m$) and

$$\mathfrak{k}_m^n \circ \mathfrak{r}_m^n = p^{d(n-m)} \cdot \mathrm{id} \colon \mathfrak{a}_m \times \mathfrak{b}_m \longrightarrow \mathfrak{a}_m \times \mathfrak{b}_m.$$

(Γ-4) For each n, $\langle\ ,\ \rangle_n \colon \mathfrak{a}_n \times \mathfrak{b}_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ is a perfect pairing (and hence $\mathfrak{a}_n$ and $\mathfrak{b}_n$ are dual p-groups) respecting Γ-action as well as the morphisms $\mathfrak{r}_m^n$ and $\mathfrak{k}_m^n$ in the sense that

$$\langle \gamma \cdot a, \gamma \cdot b \rangle_n = \langle a, b \rangle_n \ \forall\, \gamma \in \Gamma,$$

$$\langle a, \mathfrak{r}_m^n(b) \rangle_n = \langle \mathfrak{k}_m^n(a), b \rangle_m, \tag{1}$$

and

$$\langle \mathfrak{r}_m^n(a), b \rangle_n = \langle a, \mathfrak{k}_m^n(b) \rangle_m.$$

Write

$$\mathfrak{a} := \varprojlim_n \mathfrak{a}_n \ \text{ and } \ \mathfrak{b} := \varprojlim_n \mathfrak{b}_n\,.$$

Definition 1.0.1. We say $\mathfrak{A}$ as above is a Γ-system if both $\mathfrak{a}$ and $\mathfrak{b}$ are finitely generated torsion Λ-modules.[1] We say that a Γ-system $\mathfrak{A}$ is *pseudo-controlled* if

$$\mathfrak{a}^0 \times \mathfrak{b}^0 := \varprojlim_m \bigcup_{n \geq m} \mathrm{Ker}(\mathfrak{r}_m^n)$$

is a pseudo-null Λ-module.

The following Pontryagin duality theorem is proved in §3.3. The technical hypotheses in cases (1), (2) and (3) will be explained later.

Theorem 1. *Let*

$$\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n \ \mid\ n, m \in \mathbb{N},\ n \geq m\}$$

be a pseudo-controlled Γ-system. Then there is a pseudo-isomorphism

$$\mathfrak{a}^\sharp \sim \mathfrak{b}$$

in the following three cases:

(1) *there exists $\xi \in \Lambda$ not divisible by any simple element and such that $\xi\mathfrak{b}$ is pseudo-null;*

(2) *$\mathfrak{A}$ is pseudo-isomorphic to a twistable pseudo-controlled Γ-system;*

(3) *$\mathfrak{A}$ is part of a $\mathbf{T}$-system.*

[1] As we learned only after this paper had been essentially completed, our definition of Γ-system is very similar to the notion of "normic system" introduced in [Vau09, Définition 2.1]. The main difference is that Vauclair does not include a duality in his definition.

A *simple element* is the evaluation at $\gamma \in \Gamma - \Gamma^p$ of a cyclotomic polynomial: the precise definition will be given in §2.1.3. We say that the Γ-system $\mathfrak{A}$ is *twistable* if there exists an integer k such that $p^{n+k}\mathfrak{a}_n = 0$ for every n. For the definition of $\mathbf{T}$-system and of pseudo-isomorphism of Γ-systems, see respectively §3.1.1 and §3.1.2.

In §4.3 we apply our results on Pontryagin duality to prove the following.

Theorem 2. *Let K be a global field. Let L/K be a $\mathbb{Z}_p^d$-extension with a finite ramification locus S and $d \geq 1$. Let A/K be an abelian variety having potentially ordinary reduction at each place of S. Then the characteristic ideals of $X_p(A/L)$ and of $X_p(A^t/L)$ (the Pontryagin duals of the Selmer groups of A and of its dual abelian variety A^t) satisfy the following equation:*

$$\chi(X_p(A/L))^\sharp = \chi(X_p(A^t/L)) = \chi(X_p(A/L)) = \chi(X_p(A^t/L))^\sharp.$$

The characteristic ideal χ is explained in §2.1.2 and $X_p(A/L)$ is defined in §4.1.

One key tool in the proof of Theorem 2 will be the notion of the Cassels-Tate system, introduced in §4. We take $\mathrm{Gal}(L/K)$ as Γ. Then, roughly, the Cassels-Tate system attached to $(A, L/K)$ is a collection $\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n\}$ as before, where $\mathfrak{a}_n$ and $\mathfrak{b}_n$ are respectively the co-torsion part of the p-primary Selmer groups of A and A^t over $K_n := L^{\Gamma^{p^n}}$ (see §4.2.2).

In §4.4 we prove the following theorem.

Theorem 3. *Let A, L/K be as before and let $\mathfrak{A}$ be the Cassels-Tate system attached to $(A, L/K)$. Then $\mathfrak{A}$ is a Γ-system, and hence $\mathfrak{a}$ and $\mathfrak{b}$ are torsion Λ-modules. If furthermore $X_p(A/L)$ is torsion, then they satisfy the functional equation:*

$$\mathfrak{a}^\sharp \sim \mathfrak{b}.$$

In §5, we prove functional equations for characteristic ideals of Pontryagin duals of the projections of Selmer groups by central idempotents. This provides a powerful tool for solving the Iwasawa Main Conjecture in the constant ordinary case ([LLTT]).

Theorem 1 and Theorem 3 imply equality of the corresponding characteristic ideals. Using Fitting ideals Mazur and Wiles [MW84] proved such a functional equation in the $d = 1$ case, in which $\mathfrak{A}$ is automatically a $\mathbf{T}$-system. For $d \geq 2$, Fitting ideals do not seem to yield a promising approach for a proof. Theorem 1 seems to lie quite deep. Even in the case of Cassels-Tate systems, our result is not a straightforward consequence of the control theorems in the number field ([Gr03]) or function field case ([BL09], [Tan10]) as one might have expected. See in particular our use of an old result of Monsky (Theorem 3.2.5).

In the number field case, results in the direction of Theorem 2 were obtained (for $d \leq 2$) in [Maz72, §7], [Gr89, §8] and [P03] (see also [Zab10] for a non-commutative generalization). Also (in the number field case), a functional equation similar to that in Theorem 2 is proved by Nekovář for some Iwasawa cohomology (see [Nek06, §0.13]) under some technical hypothesis (no place of bad reduction and not above p splits completely in L/K). The difference between the Iwasawa cohomology of Nekovář and the classical Selmer group is studied in [Nek06, §9.6]. These two Iwasawa modules are not pseudo-isomorphic in general and no functional equation for one is (apparently) deduced from that for the other. We do not exclude however the possibility that this can be achieved. It is also worthwhile to mention that although Nekovář's technical assumption is satisfied by any L containing the

cyclotomic $\mathbb{Z}_p$-extension, sometimes it can be restrictive. For instance, if A is an elliptic curve defined over $\mathbb{Q}$ having multiplicative reduction at some $q \neq p$, K is an imaginary quadratic field over which q does not split, and L/K is the anticyclotomic $\mathbb{Z}_p$-extension, then the assumption is not satisfied.

2. Preparations

In this section we set up notation for later use.

2.1. **Iwasawa modules.** A comprehensive reference is [Bou65, §4].

2.1.1. Let M be a finitely generated Λ-module. By definition, M is pseudo-null if and only if no height one prime ideal contains its annihilator (i.e., if for any height one prime $\mathfrak{p}$ the localization $M_{\mathfrak{p}} = 0$ is trivial).

Lemma 2.1.1. *A finitely generated Λ-module M is pseudo-null if and only if there exist relatively prime $f_1, ..., f_k \in \Lambda$, $k \geq 2$, such that $f_i M = 0$ for every i.*

Proof. From $\Gamma \simeq \mathbb{Z}_p^d$ we get $\Lambda(\Gamma) \simeq \mathbb{Z}_p[[T_1, ..., T_d]]$. Thus Λ is a unique factorization domain, hence all height one prime ideals are principal and the claim follows. □

Lemma 2.1.2. *A composition of pseudo-injections (resp. pseudo-surjections, resp. pseudo-isomorphisms) is a pseudo-injection (resp. pseudo-surjection, resp. pseudo-isomorphism). Pseudo-isomorphism is an equivalence relation in the category of finitely generated torsion Λ-modules.*

Proof. Let $\alpha\colon M \to N$ and $\beta\colon N \to P$ be two morphisms of Λ-modules. The first claim follows observing that there are exact sequences

$$0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow \mathrm{Ker}(\beta \circ \alpha) \longrightarrow \mathrm{Im}(\alpha) \cap \mathrm{Ker}(\beta) \longrightarrow 0$$

and

$$\mathrm{Coker}(\alpha) \longrightarrow \mathrm{Coker}(\beta \circ \alpha) \longrightarrow \mathrm{Coker}(\beta) \longrightarrow 0. \tag{2}$$

For the second statement, the only thing left to prove is symmetry. Let $\alpha\colon M \to N$ be a pseudo-isomorphism. Let T be the set of height one primes containing $Ann_\Lambda(M)$ and put $S := (\Lambda - \bigcup_{\mathfrak{p} \in T} \mathfrak{p})$. The map α induces an isomorphism of $S^{-1}\Lambda$-modules $S^{-1}M \to S^{-1}N$: let β be its inverse. Then

$$\mathrm{Hom}_{S^{-1}\Lambda}(S^{-1}N, S^{-1}M) \simeq S^{-1}\,\mathrm{Hom}_\Lambda(N, M)$$

implies $s\beta \in \mathrm{Hom}_\Lambda(N, M)$ for some $s \in S$ and $s\beta$ is the required pseudo-isomorphism. For more details, the reader is referred to the proof of [Bou65, §4, no. 4, Th. 5]. □

2.1.2. As before, let M be a finitely generated Λ-module. We write $\chi(M) = \chi_\Gamma(M) \subset \Lambda$ for its *characteristic ideal*. Thus, $\chi(M) = 0$ if and only if M is non-torsion. Suppose M is torsion. Combining [Bou65, §4, no. 4, Th. 5] with Lemma 2.1.2, there is a pseudo-isomorphism

$$\Phi\colon \bigoplus_{i=1}^{m} \Lambda/\xi_i^{r_i}\Lambda \longrightarrow M, \tag{3}$$

where each ξ_i is irreducible. In this situation, we have

$$\chi(M) := \prod_{i=1}^{m} (\xi_i^{r_i}).$$

It follows that $\chi(M) = \Lambda$ if and only if M is pseudo-null.

Denote

$$[M] := \bigoplus_{i=1}^{m} \Lambda/\xi_i^{r_i}\Lambda\ .$$

Since a non-zero element in $[M]$ cannot be simultaneously annihilated by relatively prime elements of Λ, there is no non-trivial pseudo-null submodule of $[M]$, and hence Φ in (3) is an embedding. The module $[M]$ is uniquely determined by M up to isomorphism, while Φ is not. However, we shall fix one such Φ and view $[M]$ as a submodule of M.

Lemma 2.1.3. *Let $\alpha\colon M \to N$ and $\beta\colon N \to M$ be two pseudo-injections of finitely generated torsion Λ-modules. Then α and β are pseudo-isomorphisms.*

Proof. We have $\chi(\mathrm{Ker}(\beta\circ\alpha))\cdot\chi(M) = \chi(M)\cdot\chi(\mathrm{Coker}(\beta\circ\alpha))$ deduced from the sequence

$$0 \longrightarrow \mathrm{Ker}(\beta\circ\alpha) \longrightarrow M \longrightarrow M \longrightarrow \mathrm{Coker}(\beta\circ\alpha) \longrightarrow 0\ .$$

By Lemma 2.1.2, $\chi(\mathrm{Ker}(\beta\circ\alpha)) = \Lambda$, whence $\chi(\mathrm{Coker}(\beta\circ\alpha)) = \Lambda$. By (2), this implies that $\mathrm{Coker}(\beta)$ is pseudo-null: thus β is a pseudo-isomorphism. The same reasoning applied to $\alpha\circ\beta$ shows that α is a pseudo-isomorphism. □

2.1.3. *The simple part.* The group of roots of unity is denoted $\boldsymbol{\mu}_{p^\infty} := \bigcup_m \boldsymbol{\mu}_{p^m}$. We say that $f \in \Lambda$ is a *simple element* if there exist $\gamma \in \Gamma - \Gamma^p$ and $\zeta \in \boldsymbol{\mu}_{p^\infty}$ such that $f = f_{\gamma,\zeta}$, where

$$f_{\gamma,\zeta} := \prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} (\gamma - \sigma(\zeta)).$$

(Thus $f_{\gamma,\zeta}$ is the evaluation at γ of the cyclotomic polynomial of which ζ is a primitive root.) It is easy to check that simple elements are irreducible in Λ and that

$$f_{\gamma',\zeta'}\cdot\Lambda = f_{\gamma,\zeta}\cdot\Lambda \Longleftrightarrow (\gamma')^{\mathbb{Z}_p} = \gamma^{\mathbb{Z}_p} \text{ and } \zeta' \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\cdot\zeta\ . \tag{4}$$

For any finitely generated torsion Λ-module M, we get a decomposition in *simple part* and *non-simple part*

$$[M] = [M]_{si} \oplus [M]_{ns},$$

in the following way: recalling that $[M]$ is a direct sum of components $\Lambda/\xi_i^{r_i}\Lambda$, we define $[M]_{si}$ as the sum over those ξ_i which are simple and $[M]_{ns}$ as its complement.

2.2. **Twists.** Any continuous group homomorphism $\Gamma \to \Lambda^\times$ gives rise by linearity to an endomorphism $\Lambda \to \Lambda$.

2.2.1. An example is the map $^\sharp\colon \Lambda \longrightarrow \Lambda$ which we have defined by using $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$. The particular importance of this map for us stems from the fact that if $\langle\ ,\ \rangle$ is a Γ-invariant pairing between Λ-modules, then

$$\langle \lambda \cdot a, b\rangle = \langle a, \lambda^\sharp \cdot b\rangle \tag{5}$$

for any $\lambda \in \Lambda$.

Suppose $\phi\colon \Gamma \to \mathbb{Z}_p^\times$ is a continuous homomorphism. Define $\phi^*\colon \Lambda \to \Lambda$ to be the ring homomorphism determined by $\phi^*(\gamma) := \phi(\gamma)^{-1} \cdot \gamma$ for $\gamma \in \Gamma$. Since on Γ the composition $\phi^* \circ (1/\phi)^*$ is the identity map, we see that ϕ^* is an isomorphism on Λ.

2.2.2. Let M be a Λ-module. Any endomorphism $\alpha\colon \Lambda \to \Lambda$ defines a twisted Λ-module $\Lambda\ {}_\alpha\otimes_\Lambda M$, where the action on the copy of Λ on the left is via α (i.e., we have $(\alpha(\lambda)\mu) \otimes m = \mu \otimes \lambda m$ for λ, $\mu \in \Lambda$ and $m \in M$) and the module structure is given by

$$\lambda \cdot (\mu \otimes m) := (\lambda\mu) \otimes m \tag{6}$$

(where $\lambda\mu$ is the product in Λ). If moreover α is an isomorphism, $\Lambda\ {}_\alpha\otimes_\Lambda M$ can be identified with M with the $\Lambda(\Gamma)$-action twisted by α^{-1}, since in this case (6) becomes

$$\lambda \cdot (1 \otimes m) = 1 \otimes \alpha^{-1}(\lambda)m\,. \tag{7}$$

Following the above we shall write

$$M^\sharp := \Lambda\ {}_\sharp\otimes_\Lambda M.$$

Since $.^\sharp$ is an involution, (7) shows that the action of Λ becomes $\lambda \cdot m = \lambda^\sharp m$.

Let $f_{\gamma,\zeta} \in \Lambda$ be simple, as in §2.1.3. From (4) we obtain the equalities of ideals

$$(f_{\gamma,\zeta})^\sharp = (f_{\gamma^{-1},\zeta}) = (f_{\gamma,\zeta}). \tag{8}$$

It follows that

$$[M]^\sharp_{si} = [M]_{si}\,. \tag{9}$$

2.2.3. Let ϕ be as in §2.2.1. Set

$$M(\phi) := \Lambda\ {}_{\phi^*}\otimes_\Lambda M. \tag{10}$$

Note that, if we endow $\mathbb{Z}_p$ with the trivial action of Γ, then the Λ-module $\mathbb{Z}_p(\phi)$ can be viewed as the free rank one $\mathbb{Z}_p$-module with the action of Γ through multiplication by ϕ, in the sense that

$$\gamma \cdot a = \phi(\gamma)a \quad \text{ for all } \gamma \in \Gamma, a \in \mathbb{Z}_p(\phi)\,.$$

Then for a Λ-module M we have

$$M(\phi) = \mathbb{Z}_p(\phi) \otimes_{\mathbb{Z}_p} M,$$

where Γ acts by

$$\gamma \cdot (a \otimes x) := (\gamma \cdot a) \otimes (\gamma \cdot x) = \phi(\gamma) \cdot (a \otimes \gamma x)\,.$$

The proof of the following is straightforward and can be found in [LLTT, Lemma 2.4.1].

Lemma 2.2.1. *Let α be an automorphism of Λ. Suppose M is a finitely generated torsion Λ-module with*

$$[M] = \bigoplus_{i=1}^{m} \Lambda/\xi_i^{r_i}\Lambda.$$

Then

$$[\Lambda\ {}_{\alpha}\otimes_{\Lambda} M] = \Lambda\ {}_{\alpha}\otimes_{\Lambda}[M] = \bigoplus_{i=1}^{m} \Lambda/\alpha(\xi_i)^{r_i}\Lambda,$$

and hence

$$\chi\big(\Lambda\ {}_{\alpha}\otimes_{\Lambda} M\big) = \alpha(\chi(M)).$$

2.3. **Some more notation.** The Pontryagin dual of an abelian group B will be denoted $B^\vee$. Since we are going to deal mostly with finite p-groups and their inductive and projective limits, we generally won't distinguish between the Pontryagin dual and the set of continuous homomorphisms into the group of roots of unity $\boldsymbol{\mu}_{p^\infty}$. Note that we shall usually think of $\boldsymbol{\mu}_{p^\infty}$ as a subset of $\bar{\mathbb{Q}}_p$ (hence with the discrete topology), so that for a Λ-module M homomorphisms in $M^\vee$ will often take values in $\bar{\mathbb{Q}}_p$.

We shall denote the ψ-part of a G-module M (for G a group and $\psi \in G^\vee$) by

$$M^{(\psi)} := \{x \in M \mid g\cdot x = \psi(g)x \text{ for all } g \in G\}. \tag{11}$$

3. Controlled Γ-systems and the algebraic functional equation

Until §4, we do not need our group Γ to be a Galois group. However, to simplify the notation, we shall identify Γ as $\mathrm{Gal}(L/K)$ for some L/K so that each open subgroup can be written as $\mathrm{Gal}(L/F)$ for some finite intermediate extension F. Let K_n denote the nth layer of L/K, so that $\Gamma_n = \mathrm{Gal}(K_n/K)$ and $\mathrm{Gal}(L/K_n) = \Gamma^{p^n} =: \Gamma^{(n)}$.

3.1. Γ-systems.

3.1.1. **T**-*system.* The definition of Γ-systems can be extended to the notion of a *complete* Γ-*system*, for which we stipulate that for each finite intermediate extension F of L/K there are $\mathrm{Gal}(F/K)$-modules $\mathfrak{a}_F$ and $\mathfrak{b}_F$ with a pairing $\langle\ ,\ \rangle_F$, and for any pair F, F' of finite intermediate extensions with $F \subset F'$, there are Γ-morphisms $\mathfrak{r}_F^{F'}$ and $\mathfrak{k}_F^{F'}$ satisfying the obvious analogues of (Γ-1)-(Γ-4).

We say that $\mathfrak{A}$ is part of a complete Γ-system $\{\mathfrak{a}_F, \mathfrak{b}_F, \langle\ ,\ \rangle_F, \mathfrak{r}_F^{F'}, \mathfrak{k}_F^{F'}\}$ if $\mathfrak{a}_n = \mathfrak{a}_{K_n}$, $\mathfrak{b}_n = \mathfrak{b}_{K_n}$, $\mathfrak{r}_n^m = \mathfrak{r}_{K_n}^{K_m}$ and $\mathfrak{k}_n^m = \mathfrak{k}_{K_n}^{K_m}$. Obviously this implies $\mathfrak{a} = \varprojlim_F \mathfrak{a}_F$ and $\mathfrak{b} = \varprojlim_F \mathfrak{b}_F$.

Assume that $\mathfrak{A}$ is a complete Γ-system. Let F be a finite intermediate extension and let L'/F be an intermediate $\mathbb{Z}_p^e$-extension of L/F. Write

$$\mathfrak{a}_{L'/F} = \varprojlim_{F\subset F'\subset L'} \mathfrak{a}_{F'} \quad \text{and} \quad \mathfrak{b}_{L'/F} = \varprojlim_{F\subset F'\subset L'} \mathfrak{b}_{F'}.$$

They are modules over $\Lambda_{L'/F} := \mathbb{Z}_p[[\mathrm{Gal}(L'/F)]]$. Set the condition

- (**T**) For every finite intermediate extension F and every intermediate $\mathbb{Z}_p^{d-1}$-extension L'/F of L/F, $\mathfrak{a}_{L'/F}$ and $\mathfrak{b}_{L'/F}$ are finitely generated and torsion over $\Lambda_{L'/F}$.

By a **T**-system we mean a complete Γ-system enjoying the property **T**.

3.1.2. *Morphisms.* We shall always assume that a Γ-system $\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n\}$ is *oriented* in the sense that we have fixed an order of the pairs $(\mathfrak{a}_n, \mathfrak{b}_n)$. We define a morphism of Γ-systems

$$\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n^{\mathfrak{A}}, \mathfrak{r}(\mathfrak{A})_m^n, \mathfrak{k}(\mathfrak{A})_m^n\} \longrightarrow \mathfrak{C} = \{\mathfrak{c}_n, \mathfrak{d}_n, \langle\ ,\ \rangle_n^{\mathfrak{C}}, \mathfrak{r}(\mathfrak{C})_m^n, \mathfrak{k}(\mathfrak{C})_m^n\}$$

to be a collection of morphisms of Γ-modules $f_n \colon \mathfrak{a}_n \to \mathfrak{c}_n$, $g_n \colon \mathfrak{d}_n \to \mathfrak{b}_n$ commuting with the structure maps and such that $\langle f_n(a), d\rangle_n^{\mathfrak{C}} = \langle a, g_n(d)\rangle_n^{\mathfrak{A}}$ for all n.

A pseudo-isomorphism of Γ-systems is a morphism $\mathfrak{A} \to \mathfrak{C}$ such that the induced maps $\mathfrak{a} \to \mathfrak{c}$, $\mathfrak{d} \to \mathfrak{b}$ are pseudo-isomorphisms of Γ-modules.

Example 3.1.1. *Given a Γ-system $\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n\}$ and $\lambda \in \Lambda$, let us write $\mathfrak{a}_n[\lambda]$ for the λ-torsion of $\mathfrak{a}_n$, namely, consisting of those elements in $\mathfrak{a}_n$ killed by λ. We can then define $\lambda \cdot \mathfrak{A} := \{\lambda\mathfrak{a}_n, \lambda^\sharp\mathfrak{b}_n\}$ and $\mathfrak{A}[\lambda] := \{\mathfrak{a}_n[\lambda], \mathfrak{b}_n/\lambda^\sharp\mathfrak{b}_n\}$, with the pairing and the transition maps induced by those of $\mathfrak{A}$. It is easy to check that $\lambda \cdot \mathfrak{A}$ and $\mathfrak{A}[\lambda]$ are Γ-systems and that the exact sequences $\mathfrak{a}_n[\lambda] \hookrightarrow \mathfrak{a}_n \twoheadrightarrow \lambda\mathfrak{a}_n$ and $\lambda^\sharp\mathfrak{b}_n \hookrightarrow \mathfrak{b}_n \twoheadrightarrow \mathfrak{b}_n/\lambda^\sharp\mathfrak{b}_n$ provide morphisms of oriented Γ-systems $\mathfrak{A}[\lambda] \to \mathfrak{A}$ and $\mathfrak{A} \to \lambda \cdot \mathfrak{A}$.*

3.1.3. *Derived systems.* Let $\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n\}$ be a Γ-system. In the following, we let $\mathfrak{k}_n$ denote the natural map

$$\mathfrak{a} \times \mathfrak{b} \longrightarrow \mathfrak{a}_n \times \mathfrak{b}_n\,.$$

Suppose for each n we are given a Γ-submodule $\mathfrak{c}_n \subset \mathfrak{a}_n$ such that $\mathfrak{r}_m^n(\mathfrak{c}_m) \subset \mathfrak{c}_n$ and $\mathfrak{k}_m^n(\mathfrak{c}_n) \subset \mathfrak{c}_m$. Using these, we can obtain two derived Γ-systems from $\mathfrak{A}$. Let $\mathfrak{f}_n \subset \mathfrak{b}_n$ be the annihilator of $\mathfrak{c}_n$, via the duality induced from $\langle\ ,\ \rangle_n$, and let $\mathfrak{d}_n := \mathfrak{b}_n/\mathfrak{f}_n$. Then we also have $\mathfrak{r}_m^n(\mathfrak{f}_m) \subset \mathfrak{f}_n$ and $\mathfrak{k}_m^n(\mathfrak{f}_n) \subset \mathfrak{f}_m$. Hence $\mathfrak{r}_m^n$ induces a morphism $\mathfrak{c}_m \times \mathfrak{d}_m \to \mathfrak{c}_n \times \mathfrak{d}_n$, which, by abuse of notation, we also denote as $\mathfrak{r}_m^n$. Similarly, we have the morphism $\mathfrak{k}_m^n \colon \mathfrak{c}_n \times \mathfrak{d}_n \to \mathfrak{c}_m \times \mathfrak{d}_m$ and the pairing $\langle\ ,\ \rangle_n$ on $\mathfrak{c}_n \times \mathfrak{d}_n$. Let $\mathfrak{C}$ denote the Γ-system

$$\{\mathfrak{c}_n, \mathfrak{d}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n \ \mid\ m, n \in \mathbb{N}, n \geq m\}.$$

We also write $\mathfrak{e}_n := \mathfrak{a}_n/\mathfrak{c}_n$ and let $\mathfrak{E}$ denote the Γ-system

$$\{\mathfrak{e}_n, \mathfrak{f}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n \ \mid\ m, n \in \mathbb{N}, n \geq m\}.$$

Then we have the sequences

$$0 \longrightarrow \mathfrak{c} \longrightarrow \mathfrak{a} \longrightarrow \mathfrak{e} \longrightarrow 0 \tag{12}$$

and

$$0 \longrightarrow \mathfrak{f} \longrightarrow \mathfrak{b} \longrightarrow \mathfrak{d} \longrightarrow 0. \tag{13}$$

Here $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{e}$ and $\mathfrak{f}$ are the obvious projective limits; the systems $\{\mathfrak{c}_n\}$ and $\{\mathfrak{f}_n\}$ satisfy the Mittag-Leffler condition (because all groups are finite), so (12) and (13) are exact.

Lemma 3.1.2. *Assume $\mathfrak{a}_n = \mathfrak{k}_n(\mathfrak{a})$ for all n. Then $\mathfrak{e} \sim 0$ implies $\mathfrak{f} \sim 0$.*

Proof. The assumption implies $\mathfrak{k}_n(\mathfrak{e}) = \mathfrak{e}_n$. Thus $f \cdot \mathfrak{e} = 0$ implies $f \cdot \mathfrak{e}_n = 0$, and consequently, by the duality, $f^\sharp \cdot \mathfrak{f}_n = 0$ for all n, yielding $f^\sharp \cdot \mathfrak{f} = 0$. Now apply Lemma 2.1.1. □

3.1.4. *The system* $\mathfrak{A}'$. In the following case, we apply the above two methods together. We first get a system $\{\mathfrak{a}_n/\mathfrak{a}_n^0\,,\mathfrak{b}_n^1\}$ by putting

$$\mathfrak{a}_n^0\times\mathfrak{b}_n^0:=\bigcup_{n'\geq n}\mathrm{Ker}(\mathfrak{r}_n^{n'})=\mathrm{Ker}\big(\mathfrak{a}_n\times\mathfrak{b}_n\longrightarrow\varinjlim_m\mathfrak{a}_m\times\mathfrak{b}_m\big)\tag{14}$$

and letting $\mathfrak{a}_n^1$, $\mathfrak{b}_n^1$ be respectively the annihilators of $\mathfrak{b}_n^0$, $\mathfrak{a}_n^0$, via $\langle\ ,\ \rangle_n$. Then we apply the $\mathfrak{C}$-construction to $\{\mathfrak{a}_n/\mathfrak{a}_n^0\,,\mathfrak{b}_n^1\}$ defining $\mathfrak{a}_n'\subset\mathfrak{a}_n/\mathfrak{a}_n^0$ via

$$\mathfrak{a}_n'\times\mathfrak{b}_n':=\mathrm{Im}\big(\mathfrak{a}_n^1\times\mathfrak{b}_n^1\longrightarrow(\mathfrak{a}_n/\mathfrak{a}_n^0)\times(\mathfrak{b}_n/\mathfrak{b}_n^0)\big)\,.$$

Notice that $\mathfrak{b}_n'$ is dual to $\mathfrak{a}_n'$, as can be seen by dualizing the diagram

$$\begin{array}{ccccc}0&\longrightarrow&\mathfrak{a}_n^1&\longrightarrow&\mathfrak{a}_n\\&&\downarrow&&\downarrow\\0&\longrightarrow&\mathfrak{a}_n'&\longrightarrow&\mathfrak{a}_n/\mathfrak{a}_n^0\end{array}$$

(recall that the duals of $\mathfrak{a}_n^1$ and $\mathfrak{a}_n/\mathfrak{a}_n^0$ are respectively $\mathfrak{b}_n/\mathfrak{b}_n^0$ and $\mathfrak{b}_n^1$). Thus we get a Γ-system

$$\mathfrak{A}':=\{\mathfrak{a}_n',\mathfrak{b}_n',\langle\ ,\ \rangle_n,\mathfrak{r}_m^n,\mathfrak{k}_m^n\ \mid\ m,n\in\mathbb{N},n\geq m\}.$$

Denote, for $i=0,1$,

$$\mathfrak{a}^i\times\mathfrak{b}^i:=\varprojlim_n\mathfrak{a}_n^i\times\mathfrak{b}_n^i$$

and

$$\mathfrak{a}'\times\mathfrak{b}':=\varprojlim_n\mathfrak{a}_n'\times\mathfrak{b}_n'=\mathrm{Im}\big(\mathfrak{a}^1\times\mathfrak{b}^1\longrightarrow(\mathfrak{a}/\mathfrak{a}^0)\times(\mathfrak{b}/\mathfrak{b}^0)\big).$$

The pairings $\langle\ ,\ \rangle_n$ allow identifying each $\mathfrak{a}_n\times\mathfrak{b}_n$ with its own Pontryagin dual and this identification is compatible with the maps $\mathfrak{r}_m^n$, $\mathfrak{k}_m^n$. Then $\mathfrak{a}\times\mathfrak{b}$ is the dual of $\varinjlim\mathfrak{a}_n\times\mathfrak{b}_n$. Consider the exact sequence

$$0\longrightarrow\mathfrak{a}_n^0\times\mathfrak{b}_n^0\longrightarrow\mathfrak{a}_n\times\mathfrak{b}_n\longrightarrow(\mathfrak{a}_n\times\mathfrak{b}_n)/(\mathfrak{a}_n^0\times\mathfrak{b}_n^0)\longrightarrow 0.\tag{15}$$

By construction, $\mathfrak{a}_n^1\times\mathfrak{b}_n^1$ is the dual of $(\mathfrak{a}_n\times\mathfrak{b}_n)/(\mathfrak{a}_n^0\times\mathfrak{b}_n^0)$. The inductive limit of (15) gets the identity

$$\varinjlim\mathfrak{a}_n\times\mathfrak{b}_n=\varinjlim(\mathfrak{a}_n\times\mathfrak{b}_n)/(\mathfrak{a}_n^0\times\mathfrak{b}_n^0)$$

($\varinjlim\mathfrak{a}_n^0\times\mathfrak{b}_n^0=0$ is immediate from (14)) and hence, taking duals,

$$\mathfrak{a}^1\times\mathfrak{b}^1=\mathfrak{a}\times\mathfrak{b}.$$

Thus we have an exact sequence

$$0\longrightarrow\mathfrak{a}^0\times\mathfrak{b}^0\longrightarrow\mathfrak{a}\times\mathfrak{b}\longrightarrow\mathfrak{a}'\times\mathfrak{b}'\longrightarrow 0.\tag{16}$$

3.1.5. *Strongly-controlled* Γ*-systems.* In the previous section we saw that, since $\mathfrak{b}=\mathfrak{b}^1$ and $\mathfrak{a}=\mathfrak{a}^1$, the information carried by $\mathfrak{a}^0$ and $\mathfrak{b}^0$ does not pass to, respectively, $\mathfrak{b}$ and $\mathfrak{a}$: this is why in Theorem 1 we have the condition $\mathfrak{a}^0\times\mathfrak{b}^0\sim 0$, i.e., $\mathfrak{A}$ is pseudo-controlled (Definition 1.0.1). Now we consider a stronger condition.

Definition 3.1.3. A Γ-system $\mathfrak{A}$ is strongly controlled if $\mathfrak{a}_n^0\times\mathfrak{b}_n^0=0$ for every n.

Lemma 3.1.4. *A* Γ*-system* $\mathfrak{A}$ *is strongly controlled if and only if* $\mathfrak{r}_m^n$ *is injective* (*resp.* $\mathfrak{k}_m^n$ *is surjective*) *for* $n\geq m$.

Proof. The definition and the duality. □

Lemma 3.1.5. *Suppose $\mathfrak{A}$ is a Γ-system. Then the following hold:*

(1) *the system $\mathfrak{A}'$ is strongly controlled;*
(2) *if $\mathfrak{A}$ is pseudo-controlled, then $\mathfrak{a} \sim \mathfrak{a}'$ and $\mathfrak{b} \sim \mathfrak{b}'$.*

Proof. Statement (1) follows from the definition of $\mathfrak{A}'$ and (2) is immediate from the exact sequence (16). □

Lemma 3.1.6. *Suppose $\mathfrak{A}$ is strongly controlled. Then $\xi \cdot \mathfrak{b} = 0$, for some $\xi \in \Lambda$, if and only if $\xi^\sharp \cdot \mathfrak{a} = 0$.*

Proof. By Lemma 3.1.4, we have $\mathfrak{b}_n = \mathfrak{k}_n(\mathfrak{b})$. Thus $\xi \cdot \mathfrak{b} = 0$ implies $\xi \cdot \mathfrak{b}_n = 0$, and consequently, by the duality, $\xi^\sharp \cdot \mathfrak{a}_n = 0$ for all n, yielding $\xi^\sharp \cdot \mathfrak{a} = 0$. □

3.2. **Two maps.** In this subsection we introduce the maps Φ and Ψ, which play a key role in our constructions.

For simplicity, in the following we shall use the notation $Q_n := \mathbb{Q}_p[\Gamma_n]$ and $\Lambda_n := \mathbb{Z}_p[\Gamma_n]$. The projections $\pi^n_m \colon \Gamma_n \to \Gamma_m$ are canonically extended to ring morphisms : $\Lambda_n \to \Lambda_m$. Let

$$Q_\infty := \varprojlim Q_n = \mathbb{Q}_p[[\Gamma]]\,.$$

Thanks to the inclusions $\Lambda_n \hookrightarrow Q_n$ we can see Λ as a subring of Q_∞.

3.2.1. *The Fourier map.* Let $\mathfrak{A}$ be a Γ-system as above. In this section, we construct a Λ-linear map

$$\Phi \colon \mathfrak{a}^\sharp \longrightarrow \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\,\Lambda)\,.$$

First recall that the pairing in (Γ-4) induces for any n an isomorphism of Λ-modules

$$\mathfrak{a}_n^\sharp \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{b}_n, \mathbb{Q}_p/\mathbb{Z}_p),$$

the twist by the involution $\cdot^\sharp$ being due to (5). Equality (1) shows that these isomorphisms form an isomorphism of projective systems, where the right-hand side is endowed with the transition maps induced by the direct system $(\mathfrak{b}_n, \mathfrak{r}^n_m)$. Passing to the projective limit, we deduce a Λ-isomorphism

$$\mathfrak{a}^\sharp \simeq \varprojlim_n \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{b}_n, \mathbb{Q}_p/\mathbb{Z}_p).$$

Now the map Φ is obtained as the composition of this isomorphism and the following Λ-linear maps:

(Φ-1) the homomorphism

$$\varprojlim_n \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{b}_n, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \varprojlim_n \mathrm{Hom}_\Lambda(\mathfrak{b}_n, Q_n/\,\Lambda_n)$$

obtained by sending $(f_n)_n$ to $\big(\hat{f}_n \colon x \mapsto \sum_{\gamma \in \Gamma_n} f_n(\gamma^{-1}x)\gamma\big)_n$;

(Φ-2) the homomorphism

$$\varprojlim \mathrm{Hom}_\Lambda(\mathfrak{b}_n, Q_n/\,\Lambda_n) \longrightarrow \varprojlim \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_n/\,\Lambda_n)$$

induced by $\mathfrak{k}_n \colon \mathfrak{b} \to \mathfrak{b}_n$;

(Φ-3) the canonical isomorphism

$$\varprojlim_n \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_n/\,\Lambda_n) \simeq \mathrm{Hom}_\Lambda(\mathfrak{b}, \varprojlim_n Q_n/\,\Lambda_n)$$

and the identification $\varprojlim Q_n/\,\Lambda_n = Q_\infty/\,\Lambda$ (since the maps $\Lambda_n \to \Lambda_m$ are surjective).

Here as transition maps in $\varprojlim \mathrm{Hom}_\Lambda(\mathfrak{b}_n, Q_n/\Lambda_n)$ we take (for $n \geq m$)

$$\mathrm{Hom}_\Lambda(\mathfrak{b}_n, Q_n/\Lambda_n) \longrightarrow \mathrm{Hom}_\Lambda(\mathfrak{b}_m, Q_m/\Lambda_m)$$

$$\varphi \mapsto p^{-d(n-m)}(\pi_m^n \circ \varphi \circ \mathfrak{r}_m^n)\,. \tag{17}$$

We have to check that (Φ-1) and (Φ-2) define maps of projective systems. For (Φ-1), this means to verify that for any $n \geq m$ we have

$$\hat{f_m} = p^{-d(n-m)}(\pi_m^n \circ \hat{f}_n \circ \mathfrak{r}_m^n)\,, \tag{18}$$

where, by definition, $f_m = f_n \circ \mathfrak{r}_m^n$. For $x \in \mathfrak{b}_m$,

$$\pi_m^n(\hat{f}_n(\mathfrak{r}_m^n x)) = \pi_m^n\Big(\sum_{\gamma\in\Gamma_n} f_n(\gamma^{-1}(\mathfrak{r}_m^n x))\gamma\Big) = \sum_{\gamma\in\Gamma_n} f_n(\gamma^{-1}\mathfrak{r}_m^n x)\pi_m^n(\gamma)$$

(using the fact that, by (Γ-2), $\mathfrak{r}_m^n$ is a Γ-morphism)

$$= \sum_{\gamma\in\Gamma_n} f_n(\mathfrak{r}_m^n(\gamma^{-1}x))\pi_m^n(\gamma) = \frac{|\Gamma_n|}{|\Gamma_m|}\sum_{\gamma\in\Gamma_m} f_n(\mathfrak{r}_m^n(\gamma^{-1}x))\gamma = p^{d(n-m)}\hat{f}_m(x)\,,$$

so (18) holds. As for (Φ-2), the transition map

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, Q_n/\Lambda_n) \longrightarrow \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_m/\Lambda_m)$$

is $\psi \mapsto \pi_m^n \circ \psi$ and the map defined in (Φ-2) is $(\varphi_n)_n \mapsto (\varphi_n \circ \mathfrak{k}_n)_n$. By (17),

$$\varphi_m \circ \mathfrak{k}_m = p^{-d(n-m)}(\pi_m^n \circ \varphi_n \circ \mathfrak{r}_m^n) \circ \mathfrak{k}_m = p^{-d(n-m)}(\pi_m^n \circ \varphi_n \circ \mathfrak{r}_m^n \circ \mathfrak{k}_m^n \circ \mathfrak{k}_n)$$

(by property (Γ-3) of Γ-systems)

$$= p^{-d(n-m)}(\pi_m^n \circ \varphi_n \circ \mathrm{N}_{\Gamma_n/\Gamma_m} \circ \mathfrak{k}_n) = \pi_m^n \circ \varphi_n \circ \mathfrak{k}_n$$

(since φ_n, being a Λ-morphism, commutes with $\mathrm{N}_{\Gamma_n/\Gamma_m}$ and $\pi_m^n \circ \mathrm{N}_{\Gamma_n/\Gamma_m} = p^{d(n-m)}\pi_m^n$). So also (Φ-2) is a map of projective systems.

Remark 3.2.1. Actually, one can also check that the maps $f_n \mapsto \hat{f}_n$ used in (Φ-1) are isomorphisms. The inverse is $f \mapsto \delta_e \circ f$, where $\delta_e \colon Q_n/\Lambda_n \to \mathbb{Q}_p/\mathbb{Z}_p$ is the function sending $\sum_{\Gamma_n} a_\gamma \gamma$ to a_e (e being the neutral element in Γ_n).

If the Γ-system $\mathfrak{A}$ is strongly controlled, then the map Φ is clearly injective (since $\mathfrak{b}$ maps onto $\mathfrak{b}_n$ for all n). In general, we have the following.

Lemma 3.2.2. *The kernel of* Φ *equals* $(\mathfrak{a}^0)^\sharp$.

Proof. The image of $a = (a_n)_n \in \mathfrak{a}$ in $\varprojlim \mathrm{Hom}_\Lambda(\mathfrak{b}_n, Q_n/\Lambda_n)$ is the map

$$b = (b_n)_n \mapsto \Big(\sum_{\gamma\in\Gamma_n} \langle a_n, \gamma^{-1}b_n\rangle_n \gamma\Big)_n\,.$$

To conclude, observe that $\mathfrak{a}_n \to \varinjlim \mathfrak{a}_m$ is dual to $\mathfrak{b} \to \mathfrak{b}_n$. Hence $\langle a_n, b_n\rangle_n = 0$, for every b_n contained in the image of $\mathfrak{b} \to \mathfrak{b}_n$, if and only if $a_n \in \mathfrak{a}_n^0$. □

3.2.2. Let $\mathfrak{b}$ be a finitely generated torsion Λ-module. In §3.2.5 below we shall construct a map

$$\Psi\colon \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\Lambda) \to \mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda),$$

where $Q(\Lambda)$ is the field of fractions of Λ. The interest of having such a Ψ comes from the following lemma.

Lemma 3.2.3. *For $\mathfrak{b}$ a finitely generated torsion Λ-module, we have a pseudo-isomorphism*

$$\mathfrak{b} \sim \mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda).$$

Proof. From the exact sequence

$$0 \longrightarrow [\mathfrak{b}] \longrightarrow \mathfrak{b} \longrightarrow \mathfrak{n} \longrightarrow 0,$$

where $\mathfrak{n}$ is pseudo-null, we deduce the exact sequence

$$\begin{aligned}\mathrm{Hom}_\Lambda(\mathfrak{n}, Q(\Lambda)/\Lambda) \hookrightarrow \mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda) \\ \to \mathrm{Hom}_\Lambda([\mathfrak{b}], Q(\Lambda)/\,\Lambda) \to \mathrm{Ext}^1_\Lambda(\mathfrak{n}, Q(\Lambda)/\Lambda).\end{aligned}$$

The annihilator of $\mathfrak{n}$ also kills $\mathrm{Hom}_\Lambda(\mathfrak{n},\ )$ and its derived functors, so by Lemma 2.1.1, it follows $\mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda) \sim \mathrm{Hom}_\Lambda([\mathfrak{b}], Q(\Lambda)/\Lambda)$, and we can assume that $\mathfrak{b} = [\mathfrak{b}]$. Write

$$\mathfrak{b} = \Lambda/(\xi_1) \oplus \cdots \oplus \Lambda/(\xi_n)\,.$$

Then

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda) = \bigoplus \mathrm{Hom}_\Lambda(\Lambda\,/(\xi_i), Q(\Lambda)/\Lambda) = \bigoplus \mathrm{Hom}_\Lambda(\Lambda/(\xi_i), \xi_i^{-1}\Lambda/\Lambda)$$

because $(Q(\Lambda)/\Lambda)[\xi_i] = \xi_i^{-1}\,\Lambda\,/\Lambda\,$. Since

$$\mathrm{Hom}_\Lambda(\Lambda/(\xi_i), \xi_i^{-1}\Lambda/\Lambda) \simeq \Lambda/(\xi_i)\,,$$

we conclude that in this situation $\mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda) = \mathfrak{b}\,$. □

3.2.3. *A theorem of Monsky.* Let $\Gamma^\vee$ (resp. $\Gamma_n^\vee$) denote the group of continuous characters $\Gamma \to \boldsymbol{\mu}_{p^\infty}$ (resp. $\Gamma_n \to \boldsymbol{\mu}_{p^\infty}$); we view $\Gamma_n^\vee$ as a subgroup of $\Gamma^\vee$. For each $\omega \in \Gamma^\vee$, let $E_\omega := \mathbb{Q}_p(\boldsymbol{\mu}_{p^m}) \subset \bar{\mathbb{Q}}_p$ be the subfield generated by the image $\omega(\Gamma) = \boldsymbol{\mu}_{p^m}$, and write $\mathcal{O}_\omega := \mathbb{Z}_p[\boldsymbol{\mu}_{p^m}]$. Then ω induces a continuous ring homomorphism $\omega\colon \Lambda \to \mathcal{O}_\omega \subset E_\omega$. More generally, if $\mathcal{O}$ is a $\mathbb{Z}_p$-algebra, ω induces a homomorphism on $\mathcal{O}[[\Gamma]]$.

Let $\mathcal{O}$ be a $\mathbb{Z}_p$-algebra and $\xi \in \mathcal{O}[[\Gamma]]$: we say that ω is a zero of ξ if and only if $\omega(\xi) = 0$, and denote the zero set

$$\triangle_\xi := \{\omega \in \Gamma^\vee \ \mid\ \omega(\xi) = 0\}. \tag{19}$$

Then we recall a theorem of Monsky ([Mon81, Lemma 1.5 and Theorem 2.6]).

Definition 3.2.4. A subset $\Xi \subset \Gamma^\vee$ is called a $\mathbb{Z}_p$-flat of codimension k, if there exists $\{\gamma_1, ..., \gamma_k\} \subset \Gamma$ expandable to a $\mathbb{Z}_p$-basis of Γ and $\zeta_1, ..., \zeta_k \in \boldsymbol{\mu}_{p^\infty}$ such that

$$\Xi = \{\omega \in \Gamma^\vee \ \mid\ \omega(\gamma_i) = \zeta_i, i = 1, ..., k\}.$$

This definition is due to Monsky: in [Mon81, §1], he proves that $\mathbb{Z}_p$-flats generate the closed sets of a certain (Noetherian) topology on $\Gamma^\vee$. It turns out that in this topology the sets $\triangle_\xi$ are closed, and they are proper subsets (possibly empty) if $\xi \neq 0$ ([Mon81, Theorem 2.6]). Hence

Theorem 3.2.5 (Monsky)**.** *Suppose $\mathcal{O} \subset \bar{\mathbb{Q}}_p$ is a discrete valuation ring finite over $\mathbb{Z}_p$ and $\xi \in \mathcal{O}[[\Gamma]]$ is non-zero. Then the zero set $\triangle_\xi$ is a proper subset of $\Gamma^\vee$ and is a finite union of $\mathbb{Z}_p$-flats.*

3.2.4. *Structure of Q_∞.* The group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $\Gamma^\vee$ by $(\sigma\cdot\omega)(\gamma) := \sigma(\omega(\gamma))$. Let $[\omega]$ denote the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of ω. Attached to any character $\omega \in \Gamma_n^\vee$ there is an idempotent

$$e_\omega := \frac{1}{|\Gamma_n|}\sum_{\gamma\in\Gamma_n} \omega(\gamma^{-1})\gamma \in \bar{\mathbb{Q}}_p[\Gamma_n]\,. \tag{20}$$

The group ring $\bar{\mathbb{Q}}_p[\Gamma_n]$ is a $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-module via the action on coefficients. Accordingly, we get the decomposition

$$\mathbb{Q}_p[\Gamma_n] = \bar{\mathbb{Q}}_p[\Gamma_n]^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)} = \big(\prod_{\omega\in\Gamma_n^\vee} e_\omega \bar{\mathbb{Q}}_p[\Gamma_n]\big)^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)} = \prod_{[\omega]\subset\Gamma_n^\vee} E_{[\omega]},$$

where $[\omega]$ runs through all the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbits of $\Gamma_n^\vee$ and

$$E_{[\omega]} := \big(\prod_{\chi\in[\omega]} e_\chi \bar{\mathbb{Q}}_p[\Gamma_n]\big)^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)}.$$

Observe that the homomorphism $\omega\colon \mathbb{Q}_p[\Gamma_n] \to \bar{\mathbb{Q}}_p$ induces an isomorphism $E_{[\omega]} \simeq E_\omega$ (the inverse being given by $1 \mapsto \sum_{\sigma\in\mathrm{Gal}(E_\omega/\mathbb{Q}_p)} \sigma(e_\omega) = (e_\chi)_{\chi\in[\omega]}$).

Since $\pi_m^n(e_\omega)$ equals $e_{\omega'}$ if $\omega = \omega'\circ\pi_m^n$ and is 0 otherwise, we have the commutative diagram

$$\begin{array}{ccc} \mathbb{Q}_p[\Gamma_n] & \longrightarrow & \prod_{[\omega]\subset\Gamma_n^\vee} E_{[\omega]} \\ \big\downarrow{\scriptstyle \pi_m^n} & & \big\downarrow \\ \mathbb{Q}_p[\Gamma_m] & \longrightarrow & \prod_{[\omega]\subset\Gamma_m^\vee} E_{[\omega]} \end{array}$$

where the right vertical arrow is the natural projection by the inclusion $\Gamma_n^\vee \hookrightarrow \Gamma_m^\vee$. It follows that we have identities

$$Q_\infty = \varprojlim_n Q_n \simeq \prod_{[\omega]\subset\Gamma^\vee} E_{[\omega]} \tag{21}$$

so that

$$Q_\infty[\lambda] = \prod_{[\omega]\subset\triangle_\lambda} E_{[\omega]} \tag{22}$$

for all $\lambda \in \Lambda$ (here $Q_\infty[\lambda]$ denotes the λ-torsion subgroup).

3.2.5. *The map Ψ.* Let $\mathfrak{b}$ be a finitely generated torsion Λ-module. We assume that $\xi\cdot\mathfrak{b} = 0$, for some non-zero $\xi \in \Lambda$. Let $\triangle_\xi^c := \Gamma^\vee - \triangle_\xi$ denote the complement of $\triangle_\xi$. From (21) and (22) one deduces the direct sum decomposition

$$Q_\infty = Q_\infty[\xi] \oplus Q_\infty^c\,, \tag{23}$$

where $Q_\infty^c = \prod_{[\omega]\subset\triangle_\xi^c} E_{[\omega]}$. Let $\varpi\colon Q_\infty \to Q_\infty^c$ be the natural projection and put $\Lambda^c := \varpi(\Lambda)$ (here Λ is thought of as a subset of Q_∞ via the maps $\mathbb{Z}_p[\Gamma_n] \hookrightarrow \mathbb{Q}_p[\Gamma_n]$).

Lemma 3.2.6. *We have a* Λ*-isomorphism*

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty^c/\,\Lambda^c) \simeq \mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda).$$

Proof. Since $\mathfrak{b}$ is annihilated by ξ, the image of each $\eta \in \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty^c/\,\Lambda^c)$ is contained in $(Q_\infty^c/\,\Lambda^c)[\xi]$. Note that, since $\omega(\xi) \neq 0$ for every $\omega \in \triangle_\xi^c$, the element $\varpi(\xi)$ is a unit in Q_∞^c. Denote

$$\xi^{-1}\,\Lambda^c := \{x \in Q_\infty^c \;\mid\; \xi \cdot x \in \Lambda^c\}.$$

Then

$$(Q_\infty^c/\,\Lambda^c)[\xi] = \xi^{-1}\,\Lambda^c\,/\,\Lambda^c$$

and hence

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty^c/\,\Lambda^c) = \mathrm{Hom}_\Lambda(\mathfrak{b}, \xi^{-1}\,\Lambda^c\,/\,\Lambda^c).$$

Similarly,

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\,\Lambda) = \mathrm{Hom}_\Lambda(\mathfrak{b}, \xi^{-1}\,\Lambda\,/\,\Lambda).$$

To conclude the proof, it suffices to show that $\varpi\colon\ \Lambda \to \Lambda^c$ is an isomorphism, because then so is the induced map

$$\xi^{-1}\Lambda/\Lambda \longrightarrow \xi^{-1}\,\Lambda^c\,/\,\Lambda^c\,.$$

Since $\Lambda^c = \varpi(\Lambda)$ by definition, we just need to check injectivity. Suppose $\varpi(\epsilon) = 0$ for some $\epsilon \in \Lambda$. Then $\omega(\epsilon) = 0$ for every $\omega \notin \triangle_\xi$, and hence $\omega(\xi\epsilon) = 0$ for every $\omega \in \Gamma^\vee$. Monsky's theorem (or, alternatively, the isomorphism (21)) implies that $\xi\epsilon = 0$ and hence $\epsilon = 0$. □

Let

$$\Upsilon\colon\ \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\,\Lambda) \longrightarrow\ \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty^c/\,\Lambda^c) \tag{24}$$

be the morphism induced from ϖ. By composition of the isomorphism of Lemma 3.2.6 with Υ, we deduce the Λ-morphism

$$\Psi\colon\ \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\,\Lambda) \longrightarrow\ \mathrm{Hom}_\Lambda(\mathfrak{b}, Q(\Lambda)/\Lambda).$$

By construction, the map Ψ depends on ξ only via (23) (that is, it depends only on Δ_ξ).

3.3. **Proof of the algebraic functional equation.** In this section, we complete the proof of Theorem 1 by proving each of (1), (2), (3), separately. To prove (3) we use (2) and (3) is used in the proof of Theorem 5.1.3.

3.3.1. *Non-simple annihilator.* In case (1) of Theorem 1 we assume $\xi\mathfrak{b} \sim 0$ for some $\xi \in \Lambda$ such that

(**NS**): ξ *is not divisible by any simple element.*

Lemma 3.3.1. *Hypothesis* (**NS**) *holds if and only if* $\triangle_\xi$ *contains no codimension one* $\mathbb{Z}_p$*-flat.*

Proof. If ξ is divisible by a simple element $f = f_{\gamma,\zeta}$, then $\triangle_\xi$ contains $\triangle_f$ which is a union of the codimension one $\mathbb{Z}_p$-flats

$$\{\omega \in \Gamma^\vee \;\mid\; \omega(\gamma) = \sigma(\zeta)\},\ \ \sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p).$$

Conversely, assume that $\triangle_\xi$ contains the codimension one $\mathbb{Z}_p$-flat

$$\Xi = \{\omega \in \Gamma^\vee \;\mid\; \omega(\gamma) = \zeta\}.$$

Each $\omega \in \Xi$ factors through

$$\pi\colon \Lambda \longrightarrow \mathbb{Z}_p[\zeta][[\Gamma]]/(\gamma-\zeta) = \mathbb{Z}_p[\zeta][[\Gamma']]\,,$$

where Γ' is the quotient $\Gamma/\gamma^{\mathbb{Z}_p}$, and vice versa every continuous character of Γ' can be uniquely lifted to a character in Ξ. Thus the zero set of $\pi(\xi) \in \mathbb{Z}_p[\zeta][[\Gamma']]$ equals $(\Gamma')^\vee$. Then Monsky's theorem implies that $\pi(\xi) = 0$ and hence is divisible by $\gamma-\zeta$ in $\mathbb{Z}_p[\zeta][[\Gamma]]$. This implies that ξ is divisible by $f_{\gamma,\zeta}$ in Λ. □

By Monsky's theorem, we have either $\triangle_\xi = \emptyset$ or $\triangle_\xi = \bigcup_j \Xi_j$, with

$$\Xi_j = \{\omega \in \Gamma^\vee \;\mid\; \omega(\gamma_i^{(j)}) = \zeta_i^{(j)}, i = 1, ..., k^{(j)}\}.$$

In the second case, for all j let G_j be the $\mathbb{Z}_p$-submodule of Γ generated by the $\gamma_i^{(j)}$'s, $i = 1, ..., k^{(j)}$: if (**NS**) holds, each G_j has rank at least 2. Hence, since there is just a finite number of j, it is possible to choose $\{\sigma_1^{(j)}, \sigma_2^{(j)}\}_j$ such that $\sigma_i^{(j)} \in G_j - \Gamma^p$ and each pair $(\sigma_i^{(j)}, \sigma_{i'}^{(j')})$ consists of $\mathbb{Z}_p$-independent elements unless $(i,j) = (i',j')$. Let $\varepsilon_i^{(j)}$ denote the common value that all characters in Ξ_j take on $\sigma_i^{(j)}$ and write

$$\varphi_1 := \prod_j f_{\sigma_1^{(j)},\varepsilon_1^{(j)}}, \qquad \varphi_2 := \prod_j f_{\sigma_2^{(j)},\varepsilon_2^{(j)}}. \tag{25}$$

Then the coprimality criterion (4) ensures that φ_1 and φ_2 are relatively prime. Moreover $\omega(\varphi_i) = 0$ for all $\omega \in \triangle_\xi$, that is, $\triangle_\xi \subseteq \triangle_{\varphi_i}$. By (22) it follows that

$$\varphi_i \cdot Q_\infty[\xi] = 0 \quad \text{for both } i. \tag{26}$$

Remark 3.3.2. The case $\Delta_\xi \neq \emptyset$ can actually occur. For example, let γ_1, γ_2 be two distinct elements of a $\mathbb{Z}_p$-basis of Γ and consider

$$\xi = \gamma_1 - 1 + p(\gamma_2 - 1) + p^2(\gamma_1 - 1)(\gamma_2 - 1).$$

Then $\Delta_\xi = \{\omega \mid \omega(\gamma_1) = \omega(\gamma_2) = 1\}$ as one easily sees comparing p-adic valuations of the three summands $\omega(\gamma_1 - 1)$, $\omega(p(\gamma_2 - 1))$ and $\omega(p^2(\gamma_1 - 1)(\gamma_2 - 1))$.

Lemma 3.3.3. *Assume $\xi\mathfrak{b} = 0$ for some $\xi \in \Lambda$ satisfying hypothesis* (**NS**). *Then the restriction of Ψ to $\Phi(\mathfrak{a}^\sharp)$ is pseudo-injective.*

Proof. We just need to control the kernel of the map Υ of (24). If Δ_ξ is empty, then Υ is the identity and we are done. If not, we show that the kernel and the cokernel of Υ are annihilated by both φ_1 and φ_2 (see (25)). Consider the exact sequence

$$0 \longrightarrow \mathrm{Ker}(\varpi) \longrightarrow Q_\infty/\,\Lambda \longrightarrow Q_\infty^c/\,\Lambda^c \longrightarrow 0$$

(where by abuse of notation we denote the map induced by ϖ with the same symbol). This induces the exact sequence

$$\mathrm{Hom}_\Lambda(\mathfrak{b}, \mathrm{Ker}(\varpi)) \hookrightarrow \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\,\Lambda) \to \mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty^c/\,\Lambda^c) \to \mathrm{Ext}^1_\Lambda(\mathfrak{b}, \mathrm{Ker}(\varpi)).$$

Since $\mathrm{Ker}(\varpi)$ is a quotient of $Q_\infty[\xi]$, (26) yields $\varphi_i \cdot \mathrm{Ker}(\varpi) = 0$. Therefore both $\mathrm{Ker}(\Upsilon)$ and $\mathrm{Coker}(\Upsilon)$ are annihilated by φ_1 and φ_2. (Note that we cannot say that Υ is a pseudo-isomorphism, because $\mathrm{Hom}_\Lambda(\mathfrak{b}, Q_\infty/\,\Lambda)$ is not a finitely generated Λ-module: e.g., any group homomorphism $\mathfrak{b} \mapsto E_\omega$ for $\omega \in \Delta_\xi$ is also a Λ-homomorphism.) □

Now we can complete the proof of Theorem 1(1).

Proof of Theorem 1(1). To start with, assume $\xi\mathfrak{b} = 0$. Then, by Lemmas 3.2.2, 3.3.3 and 3.2.3, we get a pseudo-injection $\mathfrak{a}^\sharp \to \mathfrak{b}$. Moreover, thanks to Lemma 3.1.5, we may assume that $\mathfrak{A}$ is strongly controlled. By Lemma 3.1.6 this implies that $\mathfrak{a}$ is killed by $\xi^\sharp$, which is also not divisible by simple elements. Exchanging the role of $\mathfrak{a}$ and $\mathfrak{b}$, we deduce a pseudo-injection $\mathfrak{b}^\sharp \to \mathfrak{a}$ and therefore a pseudo-injection $\mathfrak{b} \to \mathfrak{a}^\sharp$. The theorem now follows from Lemma 2.1.3.

In the general case when $\xi\mathfrak{b}$ is pseudo-null but not 0, we can still assume that $\mathfrak{A}$ is strongly controlled. Let $\mathfrak{f}_n$ be the kernel of the morphism $\mathfrak{b}_n \to \mathfrak{b}_n$, $b \mapsto \xi b$, and construct two derived systems as in §3.1.3 (but with $\mathfrak{f}_n$ playing the role of $\mathfrak{c}_n$). We get again the two exact sequences (12) and (13). By hypothesis $\mathfrak{d} = \xi\mathfrak{b} \sim 0$ and then Lemma 3.1.2 implies $\mathfrak{c} \sim 0$. Hence

$$\mathfrak{b} \sim \mathfrak{f} \sim \mathfrak{e}^\sharp \sim \mathfrak{a}^\sharp$$

(where the central pseudo-isomorphism holds because $\xi\mathfrak{f} = 0$). □

3.3.2. *The non-simple part.* Let $\mathfrak{A}'$ be the derived system in §3.1.4.

Corollary 3.3.4. *For any* Γ*-system* $\mathfrak{A}$*, we have*

$$[\mathfrak{a}']^\sharp_{ns} = [\mathfrak{b}']_{ns}.$$

Proof. By Lemma 3.1.5(1) we can lighten notation and assume that $\mathfrak{A}$ is strongly controlled (replacing $\mathfrak{A}$ by $\mathfrak{A}'$ if necessary). Write $\chi(\mathfrak{b}) = (\lambda\mu)$, with $\chi([\mathfrak{b}]_{ns}) = (\lambda)$ and $\chi([\mathfrak{b}]_{si}) = (\mu)$. Since $\mathfrak{b}/[\mathfrak{b}]$ is pseudo-null, there are $\eta_1, \eta_2 \in \Lambda$, coprime to each other and both coprime to $\chi(\mathfrak{b})$, such that $\eta_1 \cdot (\mathfrak{b}/[\mathfrak{b}]) = \eta_2 \cdot (\mathfrak{b}/[\mathfrak{b}]) = 0$. Then $\lambda\mu\eta_1 \cdot \mathfrak{b} = \lambda\mu\eta_2 \cdot \mathfrak{b} = 0$. By Lemma 3.1.6

$$(\lambda\mu\eta_1)^\sharp \cdot \mathfrak{a} = (\lambda\mu\eta_2)^\sharp \cdot \mathfrak{a} = 0. \tag{27}$$

This shows that $\chi(\mathfrak{a})$ divides sufficiently high powers of both $(\lambda\mu\eta_1)^\sharp$ and $(\lambda\mu\eta_2)^\sharp$. But since $\eta_1^\sharp$ and $\eta_2^\sharp$ are coprime, they must be both coprime to $\chi(\mathfrak{a})$.

Set $\mathfrak{c} = (\mu\eta_1)^\sharp \cdot \mathfrak{a}$, $\mathfrak{c}_n = \mathfrak{k}_n(\mathfrak{c})$ for each n, and form the Γ-systems $\mathfrak{C}$, $\mathfrak{E}$ by the construction in §3.1.3. Let $\mathfrak{d}$, $\mathfrak{e}$, and $\mathfrak{f}$ be as in (12) and (13). Since $\mathfrak{k}_n(\mathfrak{b}) = \mathfrak{b}_n$, we have $\mathfrak{k}_n(\mathfrak{d}) = \mathfrak{d}_n$, and hence, by Lemma 3.1.4, $\mathfrak{C}$ is also strongly controlled. By (27), $\lambda^\sharp \cdot \mathfrak{c} = 0$, whence $\lambda \cdot \mathfrak{d} = 0$ thanks to Lemma 3.1.6. Then case (1) of Theorem 1 says $\mathfrak{c}^\sharp \sim \mathfrak{d}$. To complete the proof it is sufficient to show that

$$[\mathfrak{b}]_{ns} \times [\mathfrak{a}]_{ns} \xrightarrow{\varphi\times\psi} \mathfrak{d} \times \mathfrak{c}$$

(where φ and ψ are respectively the restrictions to $[\mathfrak{b}]_{ns}$ and $[\mathfrak{a}]_{ns}$ of the projection $\mathfrak{b} \to \mathfrak{d} = \mathfrak{b}/\mathfrak{f}$ and of the multiplication by $(\mu\eta_1)^\sharp$ on $\mathfrak{a}$) is a pseudo-isomorphism.

The inclusion $\mu\eta_1 \cdot \mathfrak{b} \subset \mu \cdot [\mathfrak{b}] \subset [\mathfrak{b}]_{ns}$ implies $\mu\eta_1 \cdot \mathrm{Coker}(\varphi) = 0$. Furthermore, since $\lambda \cdot \mathrm{Coker}(\varphi)$ is a quotient of $\lambda \cdot \mathfrak{d} = 0$, it must be trivial. Thus, by Lemma 2.1.1, $\mathrm{Coker}(\varphi)$, being annihilated by coprime λ and $\mu\eta_1$, is pseudo-null. Next, we observe that $(\mu\eta_1)^\sharp \cdot \mathfrak{e} = (\mu\eta_1)^\sharp \cdot \mathfrak{a}/\mathfrak{c} = 0$ yields $(\mu\eta_1)^\sharp \cdot \mathfrak{e}_n = 0$. The duality implies that each $\mathfrak{f}_n$ is annihilated by $\mu\eta_1$, and by taking the projective limit we see that $\mathfrak{f}$ is also annihilated by $\mu\eta_1$. It follows that $\mathrm{Ker}(\varphi) = [\mathfrak{b}]_{ns} \cap \mathfrak{f} = 0$ since no non-trivial element of $[\mathfrak{b}]_{ns}$ is annihilated by $\mu\eta_1$ (because η_1 is coprime to $\chi(\mathfrak{b})$ while μ is a product of simple elements). Similarly, $\mathrm{Ker}(\psi) = 0$ since no non-trivial element of $[\mathfrak{a}]_{ns}$ is annihilated by $(\mu\eta_1)^\sharp$. To show that $\mathrm{Coker}(\psi)$ is pseudo-null, we choose an $\eta_3 \in \Lambda$, coprime to $\lambda\eta_1$, such that $\eta_3^\sharp \cdot \mathfrak{a} \subset [\mathfrak{a}]$. Then (27) together with the fact

that λ is non-simple imply that $(\mu\eta_1\eta_3)^\sharp \cdot \mathfrak{a} \subset (\mu\eta_1)^\sharp \cdot [\mathfrak{a}] \subset [\mathfrak{a}]_{ns}$. This implies $(\mu\eta_1\eta_3)^\sharp \cdot \mathrm{Coker}(\psi) = 0$. Since $\lambda^\sharp \cdot \mathrm{Coker}(\psi)$, being a quotient of $\lambda^\sharp \cdot \mathfrak{c} = 0$, is trivial and $\lambda^\sharp$, $(\mu\eta_1\eta_3)^\sharp$ are coprime, the proof is completed. □

3.3.3. *Twists of* Γ*-systems.* We say that the Γ-system $\mathfrak{A}$ is *twistable* of order k if there exists an integer k such that $p^{n+k}\mathfrak{a}_n = 0$ for every n.

Recall that associated to a continuous group homomorphism $\phi\colon \Gamma \to \mathbb{Z}_p^\times$, there is the ring isomorphism $\phi^*\colon \Lambda \to \Lambda$ defined in §2.2.1. Given such a ϕ and a Γ-system $\mathfrak{A}$, we can form

$$\mathfrak{A}(\phi) := \{\mathfrak{a}_n(\phi^{-1}), \mathfrak{b}_n(\phi), \langle\ ,\ \rangle_n^\phi, \mathfrak{r}(\phi)_m^n, \mathfrak{k}(\phi)_m^n \ \mid\ n, m \in \mathbb{N}\cup\{0\},\ n \geq m\},$$

where $\mathfrak{a}_n(\phi^{-1})$ and $\mathfrak{b}_n(\phi)$ are twists as defined in (10),

$$\langle x \otimes a_n, y \otimes b_n\rangle_n^\phi := \langle \phi^*(x)a_n, (\phi^{-1})^*(y)b_n\rangle_n$$

and $\mathfrak{r}(\phi)_m^n$, $\mathfrak{k}(\phi)_m^n$ are respectively the maps induced by $1 \otimes \mathfrak{r}_m^n$ and, $1 \otimes \mathfrak{k}_m^n$. In general $\mathfrak{A}(\phi)$ won't be a Γ-system, because the action of Γ on $\mathfrak{a}_n(\phi^{-1})$, $\mathfrak{b}_n(\phi)$ does not factor through Γ_n. However if we take $\mathfrak{A}$ twistable of order k and ϕ such that

$$\phi(\Gamma) \subseteq 1 + p^k\mathbb{Z}_p, \tag{28}$$

then both $\mathfrak{a}_n(\phi^{-1})$ and $\mathfrak{b}_n(\phi)$ are still Γ_n-modules, because $\phi(\Gamma^{(n)}) \subset 1 + p^{n+k}\mathbb{Z}_p$ by (28) and $p^{n+k}\mathfrak{a}_n = 0$.

Lemma 3.3.5. *For any $k \in \mathbb{N}$ and $\xi \in \Lambda - \{0\}$, there exists a continuous group homomorphism $\phi\colon \Gamma \to \mathbb{Z}_p^\times$ such that* (28) *holds and both $\phi^*(\xi)$ and $(\phi^{-1})^*(\xi)$ are not divisible by simple elements.*

Proof. First of all, note that $(\phi^{-1})^*(\xi)$ is not divisible by any simple element if and only if the same holds for $(\phi^{-1})^*(\xi)^\sharp = \phi^*(\xi^\sharp)$. So we just need to find ϕ such that $\phi^*(\xi\xi^\sharp)$ has no simple factor. An abstract proof of the existence of such ϕ can be obtained by the Baire category theorem, observing that if $\lambda \in \Lambda - \{0\}$, then $\mathrm{Hom}(\Gamma, \mathbb{Z}_p^\times)$ cannot be contained in $\cup_\omega \mathrm{Ker}\left(\phi \mapsto \omega(\phi^*(\lambda))\right)$, since all these kernels have empty interior. A more concrete approach is the following.

Call an element $\lambda \in \Lambda$ a simploid if it has the form $\lambda = u \cdot f_{\gamma,\beta}$ where $u \in \Lambda^\times$ and

$$f_{\gamma,\beta} := \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\beta)/\mathbb{Q}_p)} (\gamma - \sigma(\beta))$$

with $\gamma \in \Gamma - \Gamma^p$ and β a unit in some finite Galois extension of $\mathbb{Q}_p$. Simploids are easily seen to be irreducible, so by unique factorization any principal ideal $(\lambda) \subset \Lambda$ can be written as $(\lambda) = (\lambda)_s(\lambda)_n$ with no simploid dividing $(\lambda)_n$. Moreover, given any $\phi\colon \Gamma \to \mathbb{Z}_p^\times$, the equality

$$\phi^*(f_{\gamma,\beta}) = \phi(\gamma)^{-[\mathbb{Q}_p(\beta):\mathbb{Q}_p]} \cdot f_{\gamma,\phi(\gamma)\beta}$$

shows that the set of simploids is stable under the action of ϕ and $(\phi^*(\lambda))_s = \phi^*((\lambda)_s)$. Thus, if $f_{\gamma_1,\beta_1}, ..., f_{\gamma_l,\beta_l}$ is a maximal set of coprime simploid factors of $\xi\xi^\sharp$ and if ϕ is chosen such that no $\phi(\gamma_i)\beta_i$, $i = 1, ..., l$, is a root of unit, then $\phi^*(\xi\xi^\sharp)$ is not divisible by any simple element. □

Proof of Theorem 1(2). Let ξ be a generator of $\chi(\mathfrak{a})\chi(\mathfrak{b})$ and let ϕ be as in Lemma 3.3.5. Then $\mathfrak{A}(\phi)$ also form a pseudo-controlled Γ-system with $\mathfrak{a}(\phi^{-1}) = \varprojlim_n \mathfrak{a}_n(\phi^{-1})$

and $\mathfrak{b}(\phi) = \varprojlim_n \mathfrak{b}_n(\phi)$. By Lemma 2.2.1, both $\chi(\mathfrak{a}(\phi^{-1}))$ and $\chi(\mathfrak{b}(\phi))$ are not divisible by simple elements, and hence $[\mathfrak{a}(\phi^{-1})]^\sharp = [\mathfrak{a}(\phi^{-1})]^\sharp_{ns}$ and $[\mathfrak{b}(\phi)] = [\mathfrak{b}(\phi)]_{ns}$. Therefore,

$$[\mathfrak{a}]^\sharp = [\mathfrak{a}(\phi^{-1})](\phi)^\sharp = [\mathfrak{a}(\phi^{-1})]^\sharp(\phi^{-1}) = [\mathfrak{b}(\phi)](\phi^{-1}) = [\mathfrak{b}],$$

where the first and the last equality are a consequence of Lemma 2.2.1 and the third follows from Theorem 1(1) applied to $\mathfrak{A}(\phi)$. □

3.3.4. *Complete* Γ*-systems.* Now we assume that our original $\mathfrak{A}$ is just a part of a complete Γ-system which we still denote by $\mathfrak{A}$. The original $\mathfrak{A}$ is pseudo-controlled if and only if so is its complete system. Also, if the original $\mathfrak{A}$ is strongly controlled, then by replacing $\mathfrak{a}_F \times \mathfrak{b}_F$ by $\mathfrak{k}_F(\mathfrak{a} \times \mathfrak{b})$ we can make the complete system strongly controlled without altering $\mathfrak{a}$ and $\mathfrak{b}$. So we shall assume that $\mathfrak{A}$ is strongly controlled.

First we assume that $\mathfrak{a}$ is annihilated by a simple element $\xi = f_{\gamma_1,\zeta}$ and extend γ_1 to a basis $\gamma_1, ..., \gamma_d$ of Γ over $\mathbb{Z}_p$. Let Ψ and Γ' be the subgroups of Γ with topological generators respectively γ_1 and $\{\gamma_2, ..., \gamma_d\}$. Note that for $H \subset \Gamma$ a closed subgroup we shall write $H^{(n)}$ for H^{p^n}. Let $K_{n',n}$ denote the fixed field of the subgroup $\Psi^{(n)} \oplus (\Gamma')^{(n')}$ and write $\mathfrak{a}_{\infty,n} := \varprojlim_{n'} \mathfrak{a}_{n',n}$, $\mathfrak{b}_{\infty,n} := \varprojlim_{n'} \mathfrak{b}_{n',n}$ with the obvious meaning of indexes. They are Λ-modules. Let $K_{\infty,n}$ denote the subfield of L fixed by $\Psi^{(n)}$. Then the restriction of Galois action gives rise to a natural isomorphism $\Gamma' \simeq \mathrm{Gal}(K_{\infty,n}/K_{0,n})$. Write $\Lambda' := \Lambda(\Gamma')$. We shall view Λ' as a subring of Λ.

Since $\mathfrak{A}$ is strongly controlled, $\mathfrak{a}_{\infty,n} = \mathfrak{k}_{\infty,n}(\mathfrak{a})$ and $\mathfrak{b}_{\infty,n} = \mathfrak{k}_{\infty,n}(\mathfrak{b})$ are finitely generated over Λ, and hence finitely generated over Λ', because they are fixed by $\Psi^{(n)}$.

Proposition 3.3.6. *Suppose* $\mathfrak{A}$ *is a strongly-controlled complete* Γ*-system such that*

(1) $\mathfrak{a}$ *and* $\mathfrak{b}$ *are annihilated by the simple element* $\xi = f_{\gamma_1,\zeta}$ *defined above, with* ζ *of order* p^l*;*
(2) $\mathfrak{a}_{\infty,m}$ *and* $\mathfrak{b}_{\infty,m}$ *are torsion over* Λ' *for some* $m \geq l$.

Then there exists some non-trivial $\eta \in \Lambda'$ *such that* $\eta \cdot \mathfrak{A}$ *is twistable.*

Here $\eta \cdot \mathfrak{A}$ is the complete Γ-system as defined in Example 3.1.1. It is also strongly controlled if so is $\mathfrak{A}$.

Proof. Since ζ is of order p^l, the action of $\gamma_1^{p^l}$ is trivial on both $\mathfrak{a}_{\infty,n}$ and $\mathfrak{b}_{\infty,n}$ for all n. Assume that $m \geq l$ and suppose both $\mathfrak{a}_{\infty,m}$ and $\mathfrak{b}_{\infty,m}$ are annihilated by some non-zero $\eta \in \Lambda'$. Then $\eta \cdot \mathfrak{a}_{n',m} = 0$ and $\eta \cdot \mathfrak{b}_{n',m} = 0$ for all n'. Hence for $n \geq m$,

$$p^{n-m}\eta\mathfrak{a}_{n',n} = \mathfrak{r}^{n',n}_{n',m}(\mathfrak{k}^{n',n}_{n',m}(\eta\mathfrak{a}_{n',n})) = 0$$

since $\gamma_1^{p^n}$ acts trivially on $\mathfrak{a}_{n',n}$. In particular, $p^{n-m}\eta \cdot \mathfrak{a}_n = 0$ and by similar argument $p^{n-m}\eta \cdot \mathfrak{b}_n = 0$. Then choose k such that $p^k\mathfrak{a}_i = p^k\mathfrak{b}_i = 0$ for each $1 \leq i < m$. □

Corollary 3.3.7. *Suppose* $\mathfrak{A}$ *satisfies the condition of* Proposition 3.3.6. *Then*

$$\mathfrak{a}^\sharp \sim \mathfrak{b}.$$

Proof. The morphism $\mathfrak{A} \to \eta \cdot \mathfrak{A}$ of Example 3.1.1 in this case is a pseudo-isomorphism, because $\mathfrak{a}[\eta]$ and $\mathfrak{b}/\eta^\sharp\mathfrak{b}$ are both killed by $f_{\gamma_1,\zeta}$ and either η or $\eta^\sharp$. Now apply Theorem 1(2). □

Proof of Theorem 1(3). We may assume that $\mathfrak{A}$ is strongly controlled. Suppose $\mathfrak{a}$ is annihilated by $\xi \in \Lambda$, and hence $\mathfrak{b}$ is annihilated by $\xi^\sharp$. Write $\xi = \xi_1^{s_1} \cdots \xi_k^{s_k}$, where each ξ_i is irreducible and s_i is a positive integer. The proof is by induction on k.

First assume $k = 1$. If ξ is non-simple, then the theorem has been proved. Thus, we may assume that ξ_1 is simple and we proceed by induction on s_1. The case $s_1 = 1$ is Corollary 3.3.7. If $s_1 > 1$ let $\mathfrak{c}_F := \xi_1 \cdot \mathfrak{a}_F$ and form the derived systems $\mathfrak{C}$ and $\mathfrak{E}$ as in §3.1.3. Note that both enjoy property (**T**), as immediate from the sequences (12) and (13). Besides $\mathfrak{C}$ is strongly controlled and $\mathfrak{c}$ is annihilated by $\xi_1^{s_1-1}$, whence (as ξ_1 is simple) $[\mathfrak{c}] = [\mathfrak{c}]^\sharp = [\mathfrak{d}]$ by the induction hypothesis. We still have $\mathfrak{f}^0 = 0$, but we don't know if $\mathfrak{e}^0 = 0$. However, induction tells us that $[\mathfrak{e}/\mathfrak{e}^0] = [\mathfrak{f}]$, or equivalently, there is an injection $[\mathfrak{f}] \hookrightarrow [\mathfrak{e}]$. This actually implies an inclusion $[\mathfrak{b}] \hookrightarrow [\mathfrak{a}]$: to see it, write

$$[\mathfrak{a}] = (\Lambda/\xi_1\Lambda)^{a_1} \oplus (\Lambda/\xi_1^2\Lambda)^{a_2} \oplus \cdots \oplus (\Lambda/\xi_1^{s_1}\Lambda)^{a_{s_1}}$$

and

$$[\mathfrak{b}] = (\Lambda/\xi_1\Lambda)^{b_1} \oplus (\Lambda/\xi_1^2\Lambda)^{b_2} \oplus \cdots \oplus (\Lambda/\xi_1^{s_1}\Lambda)^{b_{s_1}}.$$

Then

$$[\mathfrak{c}] = (\Lambda/\xi_1\Lambda)^{a_2} \oplus \cdots \oplus (\Lambda/\xi_1^{s_1-1}\Lambda)^{a_{s_1}}$$

and

$$[\mathfrak{d}] = (\Lambda/\xi_1\Lambda)^{b_2} \oplus \cdots \oplus (\Lambda/\xi_1^{s_1-1}\Lambda)^{b_{s_1}},$$

while

$$[\mathfrak{e}] = (\Lambda/\xi_1\Lambda)^{a_1+a_2+\cdots+a_{s_1}}, \quad [\mathfrak{f}] = (\Lambda/\xi_1\Lambda)^{b_1+b_2+\cdots+b_{s_1}}.$$

Thus, we have $a_1 \geq b_1$ and $a_i = b_i$ for $1 < i \leq s_1$. Then by symmetry, we also have $[\mathfrak{a}] \hookrightarrow [\mathfrak{b}]$, whence $[\mathfrak{a}] = [\mathfrak{b}]$ as desired. This proves the $k = 1$ case.

For $k > 1$, form again $\mathfrak{C}$ and $\mathfrak{E}$, this time setting $\mathfrak{c}_F := \xi_1^{s_1}\mathfrak{a}_F$. Then induction yields $[\mathfrak{c}]^\sharp = [\mathfrak{d}]$ and $[\mathfrak{e}]^\sharp = [\mathfrak{f}]$. To conclude, use the decompositions $[\mathfrak{a}] = [\mathfrak{c}] \oplus [\mathfrak{e}]$, $[\mathfrak{b}] = [\mathfrak{d}] \oplus [\mathfrak{f}]$ which hold because in the sequences (12), (13) the extremes have coprime annihilators. □

4. Cassels-Tate systems of abelian varieties

From now on, K will be a global field, L/K a $\mathbb{Z}_p^d$-extension with a finite ramification locus denoted by S, and $\Gamma = \mathrm{Gal}(L/K)$. Let A/K be an abelian variety which has *potentially ordinary* reduction at every place in S.

In this section we consider Selmer groups of abelian varieties over global fields to construct Cassels-Tate systems, to which we apply the theory of Pontryagin duality for the Iwasawa modules given earlier.

4.1. **The Selmer groups.** Let $i\colon A_{p^n} \hookrightarrow A$ be the group scheme of p^n-torsion of A. The p^n-Selmer group $\mathrm{Sel}_{p^n}(A/K)$ is defined to be the kernel of the composition

$$\mathrm{H}^1_{\mathrm{fl}}(K, A_{p^n}) \xrightarrow{\ i^*\ } \mathrm{H}^1_{\mathrm{fl}}(K, A) \xrightarrow{\ loc_K\ } \bigoplus\nolimits_v \mathrm{H}^1_{\mathrm{fl}}(K_v, A), \tag{29}$$

where $\mathrm{H}^\bullet_{\mathrm{fl}}$ denotes the flat cohomology and loc_K is the localization map to the direct sum of local cohomology groups over all places of K. The same definition works over any finite extension F/K. Taking the direct limit as $n \to \infty$, we get

$$\mathrm{Sel}_{p^\infty}(A/F) := \mathrm{Ker}\Big(\mathrm{H}^1_{\mathrm{fl}}(F, A_{p^\infty}) \longrightarrow \bigoplus_{\text{all } v} \mathrm{H}^1_{\mathrm{fl}}(F_v, A)\Big), \tag{30}$$

where A_{p^∞} is the p-divisible group associated with A. The Selmer group sits in an exact sequence

$$0 \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F) \longrightarrow \mathrm{Sel}_{p^\infty}(A/F) \longrightarrow Ш_{p^\infty}(A/F) \longrightarrow 0, \tag{31}$$

where $Ш_{p^\infty}(A/F)$ denote the p-primary part of the Tate-Shafarevich group

$$Ш(A/F) := \mathrm{Ker}\left(\mathrm{H}^1_{\mathrm{fl}}(F, A) \longrightarrow \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(F_v, A)\right).$$

Also, let $\mathrm{Sel}_{p^\infty}(A/F)_{div}$ denote the p-divisible part of $\mathrm{Sel}_{p^\infty}(A/F)$ and write $\mathcal{M}(A/F)$ for $\mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)$. We have $\mathcal{M}(A/F) \subset \mathrm{Sel}_{p^\infty}(A/F)_{div} \subset \mathrm{Sel}_{p^\infty}(A/F)$.

Definition 4.1.1. Define

$$\mathrm{Sel}_{p^\infty}(A/L) := \varinjlim_F \mathrm{Sel}_{p^\infty}(A/F)$$

and

$$\mathrm{Sel}_{div}(A/L) := \varinjlim_F \mathrm{Sel}_{p^\infty}(A/F)_{div}$$

(where F varies among all finite subextensions of L/K). Let $X_p(A/L)$ and $Y_p(A/L)$ denote the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(A/L)$ and $\mathrm{Sel}_{div}(A/L)$.

The Galois group Γ acts on the above modules turning them into Λ-modules. We point out that $X_p(A/L)$ is finitely generated over Λ, and hence so is $Y_p(A/L)$. In the case where A has ordinary reduction at all places in S, this is [Tan14, Proposition 1.1 and Corollary 2.14]. To pass from potentially ordinary reduction to ordinary reduction, one can argue as in [OT09, Lemma 2.1].

4.1.1. *$Y_p(A/L)$.* The following theorem was originally proved in [Tan14] under the assumption of ordinary reduction. Here we prove a much more general version in Theorem 4.1.3.

Theorem 4.1.2 (Tan)**.** *Suppose $X_p(A/L)$ is a torsion Λ-module. Then there exist relatively prime simple elements $f_1, ..., f_m$ $(m \geq 1)$ such that*

$$f_1 \cdots f_m \cdot \mathrm{Sel}_{div}(A/L) = 0.$$

Theorem 4.1.3. *Let M be a cofinitely generated torsion Λ-module. Then there exist relatively prime simple elements $f_1, ..., f_m$ $(m \geq 1)$ such that*

$$f_1 \cdots f_m \cdot (M^{\mathrm{Gal}(L/F)})_{div} = 0$$

for any finite intermediate extension $K \subset F \subset L$.

Proof. By hypothesis, there is some $\xi \in \Lambda - \{0\}$ annihilating M. Let $f \in \Lambda$ be such that $\omega(f) = 0$ for all $\omega \in \Delta_\xi$. Fix a finite intermediate extensions F/K and, to lighten notation, put $G := \mathrm{Gal}(F/K)$ and $\mathcal{O}$ the ring of integers of $\mathbb{Q}(\boldsymbol{\mu}_{p^d})$, where p^d is the exponent of G. Also, let $N := \mathcal{O} \otimes_{\mathbb{Z}_p} M^{\mathrm{Gal}(L/F)}$. Then defining, as in (20), $e'_\omega := \sum_{g \in G} \omega(g^{-1})g$ for each $\omega \in G^\vee$, one finds $|G| \cdot N = \sum e'_\omega N$ and Λ acts on $e'_\omega N$ by $\lambda \cdot n = \omega(\lambda)n$. In particular, one has $f \cdot e'_\omega N = 0$ for all $\omega \in \Delta_\xi$. On the other hand, if $\omega \notin \Delta_\xi$, then $e'_\omega N$ is finite because it is a cofinitely generated module over the finite ring $\omega(\Lambda)/(\omega(\xi))$. It follows that $f \cdot N$ is finite. Since a finite divisible group must be trivial, this proves that $f \cdot N_{div} = 0$, and hence $f \cdot (M^{\mathrm{Gal}(L/F)})_{div} = 0$.

It remains to prove that one can find a product of distinct simple elements which is killed by Δ_ξ. This is a consequence of Monsky's theorem: one has $\Delta_\xi = \bigcup T_j$

where the T_j's are $\mathbb{Z}_p$-flats, and by definition for each T_j there is at least one simple element vanishing on it. □

Corollary 4.1.4. *If $X_p(A/L)$ is torsion, then there is a pseudo-isomorphism*

$$Y_p(A/L) \sim \bigoplus_{i=1}^{m} (\Lambda / f_i \Lambda)^{r_i},$$

for some non-negative integers r_i, and hence

$$[Y_p(A/L)] = [Y_p(A/L)]_{si} = [Y_p(A/L)]^{\sharp}_{si} = [Y_p(A/L)]^{\sharp}.$$

Proof. The second equality is by (9). □

4.2. **The Cassels-Tate system.**

4.2.1. *The Cassels-Tate pairing.* For an abelian variety A defined over the global field K, let A^t be its dual abelian variety. Let

$$\langle\ ,\ \rangle_{A/K} \colon Ш(A/K) \times Ш(A^t/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

denote the Cassels-Tate pairing ([Mil86, II.5.7(a)]).

The next proposition is used in the proof of [Mil86, I, Theorem 7.3].

Proposition 4.2.1. *Let A, B be abelian varieties defined over the global field K. Suppose $\phi \colon A \to B$ is an isogeny and $\phi^t \colon B^t \to A^t$ is its dual. Then we have the commutative diagram:*

$$\begin{array}{ccccc} \langle\ ,\ \rangle_{A/K} \colon Ш(A/K) \times Ш(A^t/K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow \phi_* \qquad\qquad \big\uparrow \phi_*^t & & \big\| \\ \langle\ ,\ \rangle_{B/K} \colon Ш(B/K) \times Ш(B^t/K) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

4.2.2. *The Cassels-Tate system.* Let A be an abelian variety defined over the global field K. Put

$$\mathfrak{a}_n := Ш_{p^\infty}(A^t/K_n)/Ш_{p^\infty}(A^t/K_n)_{div} = \mathrm{Sel}_{p^\infty}(A^t/K_n)/\mathrm{Sel}_{p^\infty}(A^t/K_n)_{div}\,, \tag{32}$$

$$\mathfrak{b}_n := Ш_{p^\infty}(A/K_n)/Ш_{p^\infty}(A/K_n)_{div} = \mathrm{Sel}_{p^\infty}(A/K_n)/\mathrm{Sel}_{p^\infty}(A/K_n)_{div}. \tag{33}$$

Let

$$\langle\ ,\ \rangle_n \colon \mathfrak{a}_n \times \mathfrak{b}_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \tag{34}$$

be the perfect pairing induced from the Cassels-Tate pairing on $Ш(A^t/K_n) \times Ш(A/K_n)$. Let $\mathfrak{r}_m^n$ and $\mathfrak{k}_m^n$ be the morphisms induced respectively from the restriction

$$\mathrm{H}^1(K_m, A^t \times A) \longrightarrow \mathrm{H}^1(K_n, A^t \times A)$$

and the co-restriction

$$\mathrm{H}^1(K_n, A^t \times A) \longrightarrow \mathrm{H}^1(K_m, A^t \times A).$$

Let

$$\mathfrak{A} = \{\mathfrak{a}_n, \mathfrak{b}_n, \langle\ ,\ \rangle_n, \mathfrak{r}_m^n, \mathfrak{k}_m^n\}.$$

We call $\mathfrak{A}$ the *Cassels-Tate* system of A. As before, we write

$$\mathfrak{a} := \varprojlim_n \mathfrak{a}_n \quad \text{and} \quad \mathfrak{b} := \varprojlim_n \mathfrak{b}_n\,.$$

It is clear that $\mathfrak{A}$ satisfies axioms (Γ-1)-(Γ-4). For the rest of this paper we shall use the above notation.

Theorem 4.4.4 will show that $\mathfrak{A}$ is a Γ-system, but for now we do not need it. As in §3, write $\mathfrak{a}$ and $\mathfrak{b}$ for the projective limits of $\{\mathfrak{a}_n\}_n$ and $\{\mathfrak{b}_n\}_n$. We have the exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow X_p(A/L) \longrightarrow Y_p(A/L) \longrightarrow 0. \tag{35}$$

Lemma 4.2.2. *If $X_p(A/L)$ is torsion, then $[X_p(A/L)]_{ns} = [\mathfrak{a}]_{ns}$.*

Proof. Corollary 4.1.4 and the exact sequence (35). □

4.2.3. *The module $\mathfrak{a}^{00}$.* To study $\mathfrak{a}_n^0$, we first consider the small piece $\mathfrak{a}_n^{00}$ which is the image of

$$\mathfrak{s}_n^{00} := \mathrm{Ker}\big(\mathrm{Sel}_{p^\infty}(A^t/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}(A^t/L)\big)$$

under the projection $\mathrm{Sel}_{p^\infty}(A^t/K_n) \twoheadrightarrow \mathfrak{a}_n$. Obviously, $\mathfrak{s}_n^{00}$ is a Γ_n-submodule of

$$\mathfrak{s}_n^0 := \mathrm{Ker}\left(\mathrm{H}^1_{\mathrm{fl}}(K_n, A^t_{p^\infty}) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(L, A^t_{p^\infty})\right) = \mathrm{H}^1(\Gamma^{(n)}, A^t_{p^\infty}(L))\,.$$

Lemma 4.2.3. *All the groups $\mathrm{H}^1\big(\Gamma^{(n)}, A^t_{p^\infty}(L)\big)$ and $\mathrm{H}^2\big(\Gamma^{(n)}, A^t_{p^\infty}(L)\big)$ are finite.*

Proof. It follows from [Gr03, Proposition 3.3]. Here we partially prove the $d = 1$ case, because some ingredient of this proof will be applied later. Write

$$D := A^t_{p^\infty}(L) = A^t(L)[p^\infty] \tag{36}$$

and let D_{div} be its p-divisible part. We have an exact sequence

$$(D/D_{div})^{\Gamma^{(n)}} \longrightarrow \mathrm{H}^1(\Gamma^{(n)}, D_{div}) \longrightarrow \mathrm{H}^1(\Gamma^{(n)}, D) \longrightarrow \mathrm{H}^1(\Gamma^{(n)}, D/D_{div})\,. \tag{37}$$

If $d = 1$ and $\Gamma = \gamma^{\mathbb{Z}_p}$, then we observe that

$$(\gamma^{p^n} - 1)D_{div} = D_{div},$$

since $\mathrm{Ker}(D \xrightarrow{\gamma^{p^n}-1} D) = D^{\Gamma^{(n)}}$ is finite. Therefore, $\mathrm{H}^1(\Gamma^{(n)}, D_{div}) = 0$ and hence, since D/D_{div} is finite, from the exact sequence (37) we deduce (see e.g. [BL09, Lemma 4.1])

$$|\,\mathrm{H}^1(\Gamma^{(n)}, D)| \le |D/D_{div}|. \tag{38}$$

□

Lemma 4.2.4. *The projective limit*

$$\mathfrak{a}^{00} := \varprojlim \mathfrak{a}_n^{00}$$

is pseudo-null.

Proof. If $d = 1$, $\mathfrak{a}^{00}$ is pseudo-null since it is a finite set: inequality (38) together with the surjection $\mathfrak{s}_n^{00} \twoheadrightarrow \mathfrak{a}_n^{00}$ gives a bound on its cardinality.

Let D be as in (36) and let r be the $\mathbb{Z}_p$-rank of its Pontryagin dual $D^\vee$. Then the action of Γ gives rise to a representation

$$\rho\colon \Gamma \longrightarrow \mathrm{Aut}(D_{div}) \simeq \mathrm{GL}(r, \mathbb{Z}_p)\,. \tag{39}$$

For each γ, let $f_\gamma(x)$ be the characteristic polynomial of $\rho(\gamma)$. Then $f_\gamma(\gamma)$ is an element in Λ which annihilates D_{div}. Let m_0 be large enough such that $A^t(K_{m_0})[p^\infty]$ generates D/D_{div}. Then for every γ, $(\gamma^{p^{m_0}} - 1)f_\gamma(\gamma)$ annihilates both $\mathfrak{s}_n^{00}$ and $\mathfrak{a}_n^{00}$ for $n \ge m_0$, since we have

$$(\gamma^{p^{m_0}} - 1)f_\gamma(\gamma) \cdot D = 0.$$

If $d \geq 2$ and $\Gamma = \bigoplus_{i=1}^{d} \gamma_i^{\mathbb{Z}_p}$, then each $\delta_i := (\gamma_i^{p^{m_0}} - 1) f_{\gamma_i}(\gamma_i)$ lives in a different $\mathbb{Z}_p[T_i]$ under the identification $\Lambda = \mathbb{Z}_p[[T_1, ..., T_d]]$, $\gamma_i - 1 = T_i$. Therefore $\delta_1, ..., \delta_d$ are relatively prime and $\mathfrak{a}^{00}$ is pseudo-null by Lemma 2.1.1. □

Put $\bar{\mathfrak{a}}_n^0 := \mathfrak{a}_n^0 / \mathfrak{a}_n^{00}$. By construction we have an exact sequence

$$0 \longrightarrow \mathfrak{a}^{00} \longrightarrow \mathfrak{a}^0 \longrightarrow \bar{\mathfrak{a}}^0 := \varprojlim_n \bar{\mathfrak{a}}_n^0 \longrightarrow 0, \tag{40}$$

and hence $\mathfrak{a}^0 \sim \bar{\mathfrak{a}}^0$. Applying the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(A^t/K_n)_{div} & \longrightarrow & \mathrm{Sel}_{p^\infty}(A^t/K_n) & \longrightarrow & \mathfrak{a}_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Sel}_{div}(A^t/L) & \longrightarrow & \mathrm{Sel}_{p^\infty}(A^t/L) & \longrightarrow & \varinjlim \mathfrak{a}_n & \longrightarrow & 0 \end{array}$$

we find an injection

$$\bar{\mathfrak{a}}_n^0 \hookrightarrow \mathrm{Sel}_{div}(A^t/L) / \mathrm{Sel}_{p^\infty}(A^t/K_n)_{div}\,. \tag{41}$$

4.3. **The proof of Theorem 2.** First we consider the case where $X_p(A/L)$ is a torsion Λ-module.

Lemma 4.3.1. *The Λ-module $X_p(A^t/L)$ is torsion if and only if so is $X_p(A/L)$.*

Proof. Any isogeny $\varphi\colon A \to A^t$ defined over K gives rise, via $\varphi_*\colon \mathrm{Sel}_{p^\infty}(A/L) \to \mathrm{Sel}_{p^\infty}(A^t/L)$, to a homomorphism of Λ-modules $\varphi_*^\vee\colon X_p(A^t/L) \to X_p(A/L)$ with kernel and cokernel annihilated by $\deg(\varphi)$. □

Corollary 4.3.2. *If $X_p(A^t/L)$ is torsion over Λ, then $[X_p(A/L)]_{si} = [X_p(A^t/L)]_{si}$ and $[Y_p(A/L)] = [Y_p(A^t/L)]$.*

Proof. Let φ be as in the proof of Lemma 4.3.1. Define $\alpha\colon [X_p(A^t/L)]_{si} \to [X_p(A/L)]_{si}$ as the composition

$$[X_p(A^t/L)]_{si} \hookrightarrow X_p(A^t/L) \xrightarrow{\alpha_1} X_p(A/L) \xrightarrow{\alpha_2} [X_p(A/L)] \xrightarrow{\alpha_3} [X_p(A/L)]_{si},$$

where $\alpha_1 = \varphi_*^\vee$, α_2 is a pseudo-isomorphism and α_3 is the projection. We claim

(C) α is a pseudo-injection.

By symmetry, there is also a pseudo-injection from $[X_p(A/L)]_{si}$ to $[X_p(A^t/L)]_{si}$. Then the first equality follows from Lemma 2.1.3.

To prove claim (C), suppose $[X_p(A^t/L)]_{si}$ is annihilated by $f \in \Lambda$, which is a product of simple elements. The kernel of each α_i is annihilated by some $g_i \in \Lambda$ relatively prime to f. Thus the kernel of α is annihilated by both f and $g_1 g_2 g_3$. Then apply Lemma 2.1.1.

The second equality can be proved similarly, since $\varphi_*^\vee$ sends $Y_p(A^t/L)$ to $Y_p(A/L)$ and $[Y_p(A/L)]_{si} = [Y_p(A/L)]$, $[Y_p(A^t/L)]_{si} = [Y_p(A^t/L)]$ by Corollary 4.1.4. □

Lemma 4.3.3. *If $X_p(A/L)$ is torsion over Λ, then*

$$[\mathfrak{a}]_{ns}^\sharp = [\mathfrak{b}]_{ns}.$$

Proof. By (35), $\mathfrak{a}$ is torsion, and similarly so is $\mathfrak{b}$: hence $\mathfrak{A}$ is a Γ-system. Let $f_1, ..., f_m$ be those simple elements in Theorem 4.1.2 (applied to A^t). By (41), we have $f_1 \cdots f_m \cdot \bar{\mathfrak{a}}^0 = 0$, and hence $[\bar{\mathfrak{a}}^0] = [\bar{\mathfrak{a}}^0]_{si}$. Then Lemma 4.2.4 and (40) together imply that $[\mathfrak{a}^0] = [\mathfrak{a}^0]_{si}$. Hence, by (16), we have $[\mathfrak{a}]_{ns} = [\mathfrak{a}']_{ns}$. Similarly, $[\mathfrak{b}]_{ns} = [\mathfrak{b}']_{ns}$. Then apply Corollary 3.3.4. □

Proposition 4.3.4. *If $X_p(A/L)$ is torsion over Λ, then*

$$[X_p(A/L)]^\sharp = [X_p(A^t/L)] = [X_p(A/L)] = [X_p(A^t/L)]^\sharp.$$

Proof. Lemma 4.2.2 and Lemma 4.3.3 imply $[X_p(A/L)]^\sharp_{ns} = [X_p(A^t/L)]_{ns}$, while (9) and Corollary 4.3.2 yield $[X_p(A/L)]^\sharp_{si} = [X_p(A^t/L)]_{si}$. Thus, the first equality is proved, and the third one is obtained by a similar argument. To proceed, for a finitely generated torsion Λ-module M, we define a decomposition in *p part* and *non-p part*

$$[M] = [M]_p \oplus [M]_{np},$$

in the following way: if $[M]$ is a direct sum of components $\Lambda/\xi_i^{r_i}\Lambda$, we define $[M]_p$ as the sum over those with $\xi_i = (p)$ and $[M]_{np}$ as its complement. We have $[M]^\sharp_p = [M]_p$. This and the first equality imply

$$[X_p(A/L)]_p = [X_p(A/L)]^\sharp_p = [X_p(A^t/L)]_p.$$

Let φ be the isogeny in the proof of Lemma 4.3.1 and write $\deg(\varphi) = p^n \cdot u$ with u relatively prime to p. Then the kernel and the cokernel of φ_* are annihilated by p^n. This then leads to

$$[X_p(A/L)]_{np} = [X_p(A^t/L)]_{np}.$$

□

Proof of Theorem 2. The proof is divided into two cases. If $X_p(A/L)$ is torsion, then $\mathfrak{a} \times \mathfrak{b}$ is torsion and Theorem 2 is a consequence of Proposition 4.3.4. If $X_p(A/L)$ is non-torsion, then Theorem 2 holds trivially, since all terms in the equation equal 0. □

Remark. For the proof of Theorem 2, we don't use the fact that the Cassels-Tate system is a Γ-system (as we are going to show).

4.4. **$\mathfrak{A}$ is a Γ-system.** Now we prove Theorem 3. Denote $I_n := \mathrm{Ker}(\Lambda \twoheadrightarrow \mathbb{Z}_p[\Gamma_n])$.

Lemma 4.4.1. *If $\eta \in \Lambda$ is a non-zero element, then*

$$\mathrm{rank}_{\mathbb{Z}_p} \Lambda/(I_n + (\eta)) = O(p^{n(d-1)}).$$

Proof. The proof of [Tan14, Lemma1.13] yields $\mathrm{rank}_{\mathbb{Z}_p} \Lambda/(I_n + (\eta)) = O(p^{n(d-k)})$, where k is the smallest codimension of the $\mathbb{Z}_p$-flats in Δ_η. Monsky's Theorem 3.2.5 shows that $k \geq 1$ if $\eta \neq 0$. □

Lemma 4.4.2. *Let $\mathcal{K}$ be a local field of finite residue field. Let $B/\mathcal{K}$ be an abelian variety and $\mathcal{K}'/\mathcal{K}$ be a finite Galois extension with $G := \mathrm{Gal}(\mathcal{K}'/\mathcal{K})$. Then $\mathrm{H}^1(G, B(\mathcal{K}'))$ is finite.*

Proof. Let B^t be the dual abelian variety. We need to show that $B^t(\mathcal{K})/\mathrm{N}_G(B^t(\mathcal{K}'))$ is finite, because by the local duality of Tate it is the dual group of $\mathrm{H}^1(G, B(\mathcal{K}'))$ (see [Tan10, Corollary 2.3.3]).

Let $\mathfrak{F}$ denote the formal group law associated to $B/\mathcal{K}$. Let $\mathfrak{m}$ and $\mathfrak{p}$ denote the maximal ideals of $\mathcal{K}'$ and $\mathcal{K}$. For every $x \in \mathfrak{F}(\mathfrak{m})$, the norm $\mathrm{N}_G(x)$ is expressed by an analytic function whose linear term is the trace $\mathrm{tr}_G(x)$. Since $\mathcal{K}'/\mathcal{K}$ is separable, for any n we can find k such that $\mathfrak{p}^k \subset \mathrm{tr}_G(\mathfrak{m}^n)$ and then Hensel's lemma guarantees that, taking n sufficiently large, $\mathrm{N}_G(x) = y$ has a solution in $\mathfrak{F}(\mathfrak{m}^n)$ for any $y \in \mathfrak{F}(\mathfrak{p}^k)$.

Let $\mathbf{B}$ and $\mathbf{B}'$ be the Néron model of B over $\mathcal{O}$ and $\mathcal{O}'$, the ring of integers of $\mathcal{K}$ and $\mathcal{K}'$ respectively. Then the identity map on B extends to a unique homomorphism $\mathbf{B}_{\mathcal{O}'} \longrightarrow \mathbf{B}'$ that respects the actions of G (here $\mathbf{B}_{\mathcal{O}'}$ is the base change of $\mathbf{B}$ to $\mathcal{O}'$). The above result implies

$$\mathfrak{F}(\mathfrak{p}^k) \subset \mathrm{N}_G(\mathbf{B}(\mathcal{O}')) \subset \mathrm{N}_G(\mathbf{B}'(\mathcal{O}')) = \mathrm{N}_G(B(\mathcal{K}')).$$

Then the lemma follows, since $B(\mathcal{K})/\mathfrak{F}(\mathfrak{p}^k)$ is finite. □

For each n, denote $\mathcal{H}_n := \bigoplus_{\text{all } w} \mathrm{H}^1(\Gamma_w^{(n)}, A(L_w))$, the direct sum over all places of K_n.

Lemma 4.4.3. *The module $\mathcal{H}_n$ is cofinitely generated over $\mathbb{Z}_p$, and*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_n = O(p^{n(d-1)}), \quad \textit{as } n \to \infty.$$

Proof. Write $w \mid S$, if w is a place of K_n sitting above some place $v \in S$; otherwise, write $w \nmid S$. Then $\bigoplus_{w \nmid S} \mathrm{H}^1(\Gamma_w^{(n)}, A(L_w))$ is finite, by [Tan14, Lemma 3.4].

Suppose $w \mid S$. If A has good ordinary reduction at w, then $\mathrm{H}^1(\Gamma_w^{(n)}, A(L_w))$ is finite [Tan10, Theorem 3]. The same holds, if A acquires good ordinary reduction under a finite Galois extension $\mathcal{K}'/K_{n\,w}$, because then $\mathrm{H}^1(\mathcal{K}'L_w/\mathcal{K}', A(\mathcal{K}'L_w))$ is finite [*op. cit.*] and the kernel of the composition

$$\mathrm{H}^1(\Gamma_w^{(n)}, A(L_w)) \hookrightarrow \mathrm{H}^1(\mathcal{K}'L_w/K_{n\,w}, A(\mathcal{K}'L_w)) \longrightarrow \mathrm{H}^1(\mathcal{K}'L_w/\mathcal{K}', A(\mathcal{K}'L_w))$$

is contained in $\mathrm{H}^1(\mathcal{K}'/K_{n\,w}, A(\mathcal{K}'))$ that is finite, by Lemma 4.4.2.

Suppose that A has split multiplicative reduction at some w. By [Tan14, Lemma 3.8] as well as its proof, if $g = \dim A$, we have

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{H}^1(\Gamma_w^{(n)}, A(L_w)) \leq \mathrm{rank}_{\mathbb{Z}_p}(K_{n\,w}^\times / \mathrm{N}_{L_w/K_{n\,w}}(L_w^\times))^g = g \cdot \mathrm{rank}_{\mathbb{Z}_p} \Gamma_w^{(n)} \leq g \cdot d.$$

By applying Lemma 4.4.2 and the above argument, the same inequality also holds if A has potential multiplicative reduction at w. Then we note that for $v \in S$, because the decomposition subgroup Γ_v is of positive rank, the number of places of K_n sitting over v is of order $O(p^{n(d-1)})$, as $n \to \infty$. □

We state our next theorem in the notation of §4.2.2.

Theorem 4.4.4. *Let K be a global field, L/K a $\mathbb{Z}_p^d$-extension with a finite ramification locus, and let A be an abelian variety over K which has potentially ordinary reduction over the ramification locus of L/K. Let $\mathfrak{A}$ be the Cassels-Tate system of A. Then $\mathfrak{a}$ and $\mathfrak{b}$ are finitely generated torsion Λ-modules and $\mathfrak{A}$ is a Γ-system.*

Proof. Recall that $Q(\Lambda)$ denotes the fraction field of Λ. Suppose $\mathfrak{a}$ were non-torsion. Let r and s denote respectively the dimensions over $Q(\Lambda)$ of the vector spaces $Q(\Lambda)\mathfrak{a}$ and $Q(\Lambda)X_p(A/L)$: by (35), the former is contained in the latter. Let $e_1, ..., e_r, ..., e_s \in X_p(A/L)$ form a basis of $Q(\Lambda)X_p(A/L)$ such that $e_1, ..., e_r$ are in $\mathfrak{a}$. Write $\mathfrak{a}' = \Lambda \cdot e_1 + \cdots + \Lambda \cdot e_r \subset \mathfrak{a}$ and $X' = \Lambda \cdot e_1 + \cdots + \Lambda \cdot e_s \subset X_p(A/L)$. Then $X_p(A/L)/X'$ is torsion over Λ, and hence is annihilated by some non-zero $\eta \in \Lambda$.

Let $\omega \in \Gamma^\vee$ be a character not contained in Δ_η (see (19)). Extend it as in §3.2.3 to a ring homomorphism $\omega\colon \Lambda \twoheadrightarrow \mathcal{O}_\omega$ whose kernel we denote by $\ker_\omega$. Then we have the exact sequences

$$\begin{aligned} \mathrm{Tor}_\Lambda(\Lambda \,/\, \ker_\omega, X_p(A/L)/\mathfrak{a}') &\longrightarrow (\Lambda/\ker_\omega) \otimes_\Lambda \mathfrak{a} \\ &\xrightarrow{id_\omega \otimes i} (\Lambda \,/\, \ker_\omega) \otimes_\Lambda X_p(A/L)\,, \end{aligned} \tag{42}$$

where $i : \mathfrak{a}' \longrightarrow X_p(A/L)$ is the inclusion, and

$$0 \longrightarrow X'/\mathfrak{a}' \longrightarrow X_p(A/L)/\mathfrak{a}' \longrightarrow X_p(A/L)/X' \longrightarrow 0\,.$$

The fact that $X'/\mathfrak{a}'$ is free over Λ implies that the natural map

$$\mathrm{Tor}_\Lambda(\Lambda\,/\ker_\omega, X_p(A/L)/\mathfrak{a}') \longrightarrow \mathrm{Tor}_\Lambda(\Lambda\,/\ker_\omega, X_p(A/L)/X')$$

is an injection. Then the group $\mathrm{Tor}_\Lambda(\Lambda\,/\ker_\omega, X_p(A/L)/\mathfrak{a}')$ must be finite, because the quotient $\Lambda\,/\ker_\omega \simeq \mathcal{O}_\omega$ has finite residue modulo $\omega(\eta)$ and $\mathrm{Tor}_\Lambda(\Lambda\,/\ker_\omega, X_p(A/L)/X')$, being annihilated by the non-zero residue class of η in $\Lambda\,/\ker_\omega$, is finite. Thus, the homomorphism $id_\omega \otimes i$ in (42) must be injective, because $(\Lambda/\ker_\omega) \otimes_\Lambda \mathfrak{a}'$ is a free $\mathcal{O}_\omega$-module. Hence its image is free of positive rank over $\mathcal{O}_\omega$.

Now assume that $\omega \in \Gamma_n^\vee \subset \Gamma^\vee$. Denote $E_n := \mathbb{Q}_p(\boldsymbol{\mu}_{p^n})$ and $V_n := E_n \otimes_{\mathbb{Z}_p} \Lambda\,/I_n$. Then $\mathcal{O}_\omega \subset E_n$ and ω extends to a ring homomorphism $\omega : V_n \to E_n$. We have

$$V_n = \bigoplus_{\omega \in \Gamma_n^\vee} V_n^{(\omega)}$$

with $V_n^{(\omega)} = E_n$ and the projection $V_n \to V_n^{(\omega)} = E_n$ given by ω. The above discussion shows if $\omega \notin \Delta_\eta$, then the image of $id_\omega \otimes i \colon V_n^{(\omega)} \otimes_\Lambda \mathfrak{a}' \longrightarrow V_n^{(\omega)} \otimes_\Lambda X_p(A/L)$ is a positive dimensional vector space on E_n. Since $\omega \in \Delta_\eta$ if and only if ω factors through $\Lambda\,/(I_n + (\eta))$, in view of Lemma 4.4.1, we conclude that as $n \to \infty$, the $\mathbb{Z}_p$-rank of the image of

$$\mathfrak{a}' \longrightarrow \Lambda\,/I_n \otimes_\Lambda \mathfrak{a}' \longrightarrow \Lambda\,/I_n \otimes_\Lambda X_p(A/L)$$

is at least of order $p^{dn} + O(p^{n(d-1)})$. Then the same holds for the image of

$$\mathfrak{a} \longrightarrow \Lambda\,/I_n \otimes_\Lambda X_p(A/L),$$

since $\mathfrak{a}' \to X_p(A/L)$ factors through $\mathfrak{a}' \to \mathfrak{a}$. By duality, the image of

$$\mathrm{Sel}_{p^\infty}(A/L)^{\Gamma^{(n)}} \longrightarrow \mathrm{Sel}_{p^\infty}(A/L)/\,\mathrm{Sel}_{div}(A/L)$$

has $\mathbb{Z}_p$-corank at least of order $p^{dn} + O(p^{n(d-1)})$. Let $\mathcal{S}(L/K_n)$ denote the preimage of $\mathrm{Sel}_{p^\infty}(A/L)^{\Gamma^{(n)}}$ under the restriction $\mathrm{H}^1(K_n, A_{p^\infty}) \longrightarrow \mathrm{H}^1(L, A_{p^\infty})$. Since the composition

$$\mathcal{S}(L/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}(A/L)^{\Gamma^{(n)}} \longrightarrow \mathrm{Sel}_{p^\infty}(A/L)/\,\mathrm{Sel}_{div}(A/L)$$

factors through $\mathcal{S}(L/K_n) \longrightarrow \mathcal{S}(L/K_n)/\,\mathrm{Sel}_{p^\infty}(A/K_n)_{div}$, while by the Hochschild-Serre spectral sequence and Lemma 4.2.3, the left morphism has finite cokernel, the $\mathbb{Z}_p$-corank of $\mathcal{S}(L/K_n)/\,\mathrm{Sel}_{p^\infty}(A/K_n)_{div}$ is at least of order $p^{dn} + O(p^{n(d-1)})$. Then the same holds for the $\mathbb{Z}_p$-corank of $\mathcal{S}(L/K_n)/\,\mathrm{Sel}_{p^\infty}(A/K_n)$, and hence for that of $\mathcal{H}_n$, because of the exact sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(A/K_n) \longrightarrow \mathcal{S}(L/K_n) \longrightarrow \mathcal{H}_n$$

due to the localization map. But Lemma 4.4.3 says this is absurd. The proof for $\mathfrak{b}$ just replaces A with A^t. □

Proof of Theorem 3. The first assertion results from Theorem 4.4.4 and the second from Corollary 4.3.2 and Lemma 4.3.3. □

Remark 4.4.5. Theorem 4.4.4 says $\mathfrak{a} \times \mathfrak{b}$ is torsion even when $X_p(A/L)$ is not. It is worthwhile to mention that Theorem 4.4.4 also implies that $\mathfrak{A}$ enjoys property (**T**) (just replace L/K with an arbitrary $\mathbb{Z}_p^{d-1}$-subextension L'/F).

4.5. **Is $\mathfrak{A}$ pseudo-controlled?** It is natural to ask if the Cassels-Tate system $\mathfrak{A}$ is pseudo-controlled: we tend to believe that this actually holds as long as $X_p(A/L)$ is torsion. Propositions 4.5.3 and 4.5.4 below give evidence to support our belief.

Lemma 4.5.1. *For $n \geq m$ the restriction map*

$$\mathrm{Sel}_{p^\infty}(A/K_m)_{div} \longrightarrow (\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div}$$

is surjective.

Proof. The commutative diagram of exact sequences

$$\begin{array}{ccccc}
\mathrm{Sel}_{p^\infty}(A/K_m)_{div} = \mathrm{Sel}_{p^\infty}(A/K_m)_{div} & \hookrightarrow & \mathrm{Sel}_{p^\infty}(A/K_m) & \twoheadrightarrow & \mathfrak{b}_m \\
\downarrow{\scriptstyle j'} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathfrak{r}_m^n} \\
(\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div} \subset (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^{\Gamma^{(m)}} & \hookrightarrow & \mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}} & \longrightarrow & \mathfrak{b}_n^{\Gamma^{(m)}}
\end{array}$$

induces the exact sequence

$$\mathrm{Ker}(\mathfrak{r}_m^n) \longrightarrow \mathrm{Coker}(j) \longrightarrow \mathrm{Coker}(i).$$

Since $\mathrm{Ker}(\mathfrak{r}_m^n)$ is finite while $\mathrm{Coker}(j')$ is p-divisible, it is sufficient to show that $\mathrm{Coker}(i)$ is annihilated by some positive integer. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccc}
\mathrm{Sel}_{p^\infty}(A/K_m) & \hookrightarrow & \mathrm{H}^1_{\mathrm{fl}}(K_m, A_{p^\infty}) & \xrightarrow{loc_m} & \prod_{\mathrm{all}\ v} \mathrm{H}^1(K_{mv}, A) \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle res_m^n} & & \downarrow{\scriptstyle r_m^n} \\
\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}} & \hookrightarrow & \mathrm{H}^1_{\mathrm{fl}}(K_n, A_{p^\infty})^{\Gamma^{(m)}} & \xrightarrow{loc_n} & \prod_{\mathrm{all}\ w} \mathrm{H}^1(K_{nw}, A)^{\Gamma_w^{(m)}}
\end{array}$$

that induces the exact sequence

$$\mathrm{Ker}\left(\ \mathrm{Im}(loc_m) \xrightarrow{r_m^n} \mathrm{Im}(loc_n)\ \right) \longrightarrow\ \mathrm{Coker}(i) \longrightarrow\ \mathrm{Coker}(res_m^n)\,.$$

By the Hochschild-Serre spectral sequence, the right-hand term $\mathrm{Coker}(res_m^n)$ is a subgroup of $\mathrm{H}^2(K_n/K_m, A_{p^\infty}(K_n))$, and hence is annihilated by $p^{d(n-m)} = [K_n : K_m]$. Similarly, the left-hand term, being a subgroup of $\prod_v \mathrm{H}^1(K_{nv}/K_{mv}, A(K_{nv}))$, is also annihilated by $[K_n : K_m]$. □

Lemma 4.5.2. *If L/K is a $\mathbb{Z}_p$-extension and $X_p(A/L)$ is a torsion Λ-module, then there exists some N such that*

$$\mathrm{Sel}_{p^\infty}(A/K_n)_{div} = (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^{\Gamma^{(m)}} = (\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div}$$

holds for all $n \geq m \geq N$.

Proof. The second equality is an easy consequence of the first one. The assumption $\Gamma = \gamma^{\mathbb{Z}_p}$ implies that if $f \in \Lambda$ is simple, then f divides $\gamma^{p^m} - 1$ for some m. Therefore, by Theorem 4.1.2, there exists an integer N such that $(\gamma^{p^N} - 1)\,\mathrm{Sel}_{div}(A/L)^{\Gamma^{(n)}} = 0$ for every n. The kernel of the map $\mathrm{Sel}_{p^\infty}(A/K_n)_{div} \to \mathrm{Sel}_{div}(A/L)^{\Gamma^{(n)}}$ is finite by Lemma 4.2.3. This implies that $(\gamma^{p^N}-1)\,\mathrm{Sel}_{p^\infty}(A/K_n)_{div}$ must be trivial, since it is both finite and p-divisible. □

Proposition 4.5.3. *If L/K is a $\mathbb{Z}_p$-extension and $X_p(A/L)$ is a torsion Λ-module, then $\mathfrak{A}$ is pseudo-controlled.*

Proof. We apply Lemma 4.5.1 and Lemma 4.5.2. If we are given an element $x \in \mathrm{Sel}_{p^\infty}(A^t/K_n)$ with $res_n^l(x) \in \mathrm{Sel}_{p^\infty}(A^t/K_l)_{div}$ for some $l \geq n \geq N$, then we can find $y \in \mathrm{Sel}_{p^\infty}(A^t/K_N)_{div}$ such that $res_N^l(y) = res_n^l(x)$. Then $x - res_N^n(y) \in \mathrm{Ker}(res_n^l) \subset \mathfrak{s}_n^{00}$. This actually shows that $\mathfrak{a}_n^0 = \mathfrak{a}_n^{00}$. Then apply Lemma 4.2.4. □

Proposition 4.5.4. *If L/K is a $\mathbb{Z}_p^d$-extension ramified only at good ordinary places and $X_p(A/L)$ is a torsion Λ-module, then $\mathfrak{A}$ is pseudo-controlled.*

Proof. Let $f_1, ..., f_m$ be those simple elements described in Theorem 4.1.2. and write $g_i := f_i^{-1} f_1 \dots f_m$. Since f_i divides $\gamma_i^{p^{r_i}} - 1$, for some γ_i and r_i, by Theorem 4.1.2 we get

$$g_i \cdot \mathrm{Sel}_{div}(A^t/L) \subset \mathrm{Sel}_{p^\infty}(A^t/L)^{\Psi_i^{(r_i)}}, \tag{43}$$

where $\Psi_i \subset \Gamma$ is the closed subgroup topologically generated by γ_i and we use the notation $H^{(i)} := H^{p^{r_i}}$ for any subgroup $H < \Gamma$. In view of Proposition 4.5.3, we may assume that $d \geq 2$. Then we can find $\delta_1, ..., \delta_d$ as in the proof of Lemma 4.2.4 and such that the elements $\delta_j g_i$, $i = 1, ..., m$, $j = 1, ..., d$, are coprime. By construction each δ_i annihilates $\mathfrak{s}_n^0$ for all n. We are going to show that if $a = (a_n)_n$, $a_n \in \mathfrak{a}_n^0$, is an element in $\mathfrak{a}^0$, then for $n \geq r_i$,

$$\delta_j g_i \cdot a_n = 0, \ j = 1, ..., d. \tag{44}$$

Then it follows that $\delta_j g_i \cdot \mathfrak{a}^0 = 0$ for every i and j, and hence $\mathfrak{a}^0$ is pseudo-null.

Fix $n \geq r_i$. Choose closed subgroups $\Phi_i \subset \Gamma$, $i = 1, ..., m$, isomorphic to $\mathbb{Z}_p^{d-1}$ such that $\Gamma = \Psi_i \oplus \Phi_i$, and then set $L^{(i)} := L^{\Phi_i^{(n)}}$ and let $L_l^{(i)}$ denote the lth layer of the $\mathbb{Z}_p$-extension $L^{(i)}/K_n$, so that $\mathrm{Gal}(L^{(i)}/L_l^{(i)})$ is canonically isomorphic to $\Psi_i^{(l+n)}$.

For each $l \geq n$, let ξ_l be a preimage of a_l under

$$\mathrm{Sel}_{p^\infty}(A^t/K_l) \xrightarrow{\pi_l} \mathfrak{a}_l$$

and denote by ξ_l' the image of ξ_l under the corestriction map $\mathrm{Sel}_{p^\infty}(A^t/K_l) \to \mathrm{Sel}_{p^\infty}(A^t/L_{l-n}^{(i)})$. Note that K_l is an extension of $L_{l-n}^{(i)}$ because $\Gamma_l \subset \Psi_i^{(l)} \Phi_i^{(n)} = \mathrm{Gal}(L/L_{l-n}^{(i)})$. Thus, the restriction map sends ξ_l' to an element $\theta_l \in \mathrm{Sel}_{div}(A^t/L)^{\Psi_i^{(l)}\Phi_i^{(n)}}$. Then by (43)

$$g_i \cdot \theta_l \in \mathrm{Sel}_{div}(A^t/L)^{\Gamma^{(n)}}. \tag{45}$$

By the control theorem [Tan10, Theorem 4] the cokernel of the restriction map

$$\mathrm{Sel}_{p^\infty}(A^t/K_n)_{div} \xrightarrow{res_n} \mathrm{Sel}_{div}(A^t/L)^{\Gamma^{(n)}}$$

is finite: we denote by p^e its order. Choose $l \geq n + e$ and choose ξ_n to be the image of ξ_l under the corestriction map $\mathrm{Sel}_{p^\infty}(A^t/K_l) \to \mathrm{Sel}_{p^\infty}(A^t/K_n)$. Then (45) implies that $g_i \cdot \theta_n = p^e g_i \cdot \theta_l$, which shows that $g_i \cdot \theta_n = res_n(\theta_n')$, for some $\theta_n' \in \mathrm{Sel}_{div}(A^t/K_n)$. Then $\pi_n(g_i \cdot \xi_n - \theta_n') = g_i \cdot a_n$. Since $g_i \cdot \xi_n - \theta_n'$ belongs to $\mathfrak{s}_n^0$, which is annihilated by δ_j, we have $\delta_j g_i \cdot a_n = 0$ as desired. □

5. Central idempotents of the endomorphism ring of A

Let $\mathcal{E}$ denote the ring of endomorphisms of A/K and write $\mathbb{Z}_p\mathcal{E} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{E}$. We assume that there exists a non-trivial idempotent e_1 contained in the center of $\mathbb{Z}_p\mathcal{E}$. Set $e_2 := 1 - e_1$. Then we have the decomposition:

$$\mathbb{Z}_p\mathcal{E} = e_1\mathbb{Z}_p\mathcal{E} \times e_2\mathbb{Z}_p\mathcal{E}. \tag{46}$$

5.1. **The endomorphism rings.** Let $\mathcal{E}^t$ denote the endomorphism ring of A^t/K. Since the assignment $\psi \mapsto \psi^t$ sending an endomorphism $\psi \in \mathcal{E}$ to its dual endomorphism can be uniquely extended to a $\mathbb{Z}_p$-algebra anti-isomorphism $\cdot^t \colon \mathbb{Z}_p\mathcal{E} \to \mathbb{Z}_p\mathcal{E}^t$, we find idempotents e_1^t, e_2^t and the analogue of (46). If $\mathcal{E}$ and $\mathcal{E}^t$ act respectively on p-primary abelian groups M and N, then these actions can be extended to those of $\mathbb{Z}_p\mathcal{E}$ and $\mathbb{Z}_p\mathcal{E}^t$. We have the following $\mathbb{Z}_p$-version of Proposition 4.2.1.

Lemma 5.1.1. *For every $a \in \mathfrak{a}_n$, $b \in \mathfrak{b}_n$ and $\psi \in \mathbb{Z}_p\mathcal{E}$ we have*

$$\langle a, \psi_*(b)\rangle_n = \langle \psi^t_*(a), b\rangle_n\,. \tag{47}$$

Proof. First note that any $\psi \in \mathcal{E}$ can be obtained as a sum of two isogenies (e.g., because $k + \psi$ is an isogeny for some $k \in \mathbb{Z}$). Thus Proposition 4.2.1 and linearity of the Cassels-Tate pairing imply that (47) holds for such ψ.

In the general case, since $\mathbb{Z}_p\mathcal{E}$ is the p-completion of $\mathcal{E}$, for each positive integer m there exists $\varphi_m \in \mathcal{E}$ such that $\psi - \varphi_m \in p^m\mathbb{Z}_p\mathcal{E}$. Choose m such that $p^m a = p^m b = 0$. Then

$$\langle a, \psi_*(b)\rangle_n = \langle a, \varphi_{m*}(b)\rangle_n = \langle \varphi^t_{m*}(a), b\rangle_n = \langle \psi^t_*(a), b\rangle_n.$$

□

If M and N are respectively $\mathbb{Z}_p\mathcal{E}$ and $\mathbb{Z}_p\mathcal{E}^t$ modules, write $M^{(i)}$ for $e_i \cdot M$ and $N^{(i)}$ for $e_i^t \cdot N$. Then (46) implies $M = M^{(1)} \oplus M^{(2)}$ and $N = N^{(1)} \oplus N^{(2)}$. In particular,

$$\mathfrak{a} = \mathfrak{a}^{(1)} \oplus \mathfrak{a}^{(2)} \text{ and } \mathfrak{b} = \mathfrak{b}^{(1)} \oplus \mathfrak{b}^{(2)}\,,$$

with $\mathfrak{a}^{(i)} = \varprojlim_n \mathfrak{a}_n^{(i)}$ and $\mathfrak{b}^{(i)} = \varprojlim_n \mathfrak{b}_n^{(i)}$.

Corollary 5.1.2. *For every n, we have a perfect duality between $\mathfrak{a}_n^{(1)}$, $\mathfrak{b}_n^{(1)}$ and one between $\mathfrak{a}_n^{(2)}$, $\mathfrak{b}_n^{(2)}$.*

Proof. We just need to check $\langle \mathfrak{a}_n^{(1)}, \mathfrak{b}_n^{(2)}\rangle_n = \langle \mathfrak{a}_n^{(2)}, \mathfrak{b}_n^{(1)}\rangle_n = 0$. If $a \in \mathfrak{a}_n^{(1)}$ and $b \in \mathfrak{b}_n^{(2)}$, then $\langle a, b\rangle_n = \langle e_1^t \cdot a, e_2 \cdot b\rangle_n = \langle a, e_1e_2 \cdot b\rangle_n = \langle a, 0\rangle_n = 0$. □

Then $\mathfrak{A}^{(i)} := \{\mathfrak{a}_n^{(i)}, \mathfrak{b}_n^{(i)}, \langle\,,\,\rangle, \mathfrak{r}_m^n, \mathfrak{k}_m^n\}$, $i = 1, 2$, satisfy conditions (Γ-1) to (Γ-4) and hence by Theorem 4.4.4 and Remark 4.4.5, are Γ-systems and part of **T**-systems. They are pseudo-controlled if and only if so is $\mathfrak{A}$. By Theorem 1(3) and Proposition 4.5.4 we have the following.

Theorem 5.1.3. *If $\mathfrak{A}$ is pseudo-controlled, then*

$$[\mathfrak{a}^{(1)}] = [\mathfrak{b}^{(1)}]^\sharp \quad \textit{and} \quad [\mathfrak{a}^{(2)}] = [\mathfrak{b}^{(2)}]^\sharp. \tag{48}$$

Corollary 5.1.4. *If L/K is a $\mathbb{Z}_p^d$-extension ramified only at good ordinary places and $X_p(A/L)$ is a torsion Λ-module, then* (48) *holds.*

5.2. **The height pairing.** Applying e_i to the exact sequence (35) we get

$$0 \longrightarrow \mathfrak{a}^{(i)} \longrightarrow X_p(A/L)^{(i)} \longrightarrow Y_p(A/L)^{(i)} \longrightarrow 0\,. \tag{49}$$

Unfortunately in general we are unable to compare either $X_p(A/L)^{(i)}$ with $X_p(A^t/L)^{(i)}$ or $Y_p(A/L)^{(i)}$ with $Y_p(A^t/L)^{(i)}$. However, we can get some partial results as follows.

5.2.1. *The Néron-Tate height pairing.* First we briefly recall the definition of the Néron-Tate height pairing

$$\tilde{h}_{A/K}\colon A(K) \times A^t(K) \longrightarrow \mathbb{R}\,. \tag{50}$$

For details, see [Lan83, V, §4]. Let

$$P_A \longrightarrow A \times A^t$$

denote the Poincaré line bundle: then $\tilde{h}_{A/K}$ is the canonical height on $A \times A^t$ associated with the divisor class corresponding to P_A.

Proposition 5.2.1. *Let A, B be abelian varieties defined over the global field K. Let $\phi\colon A \to B$ and $\phi^t\colon B^t \to A^t$ be an isogeny and its dual. Then the following diagram is commutative:*

$$\begin{array}{ccc} \tilde{h}_{A/K}\colon A(K) \times A^t(K) & \longrightarrow & \mathbb{R} \\ \big\downarrow{\scriptstyle \phi} \quad \big\uparrow{\scriptstyle \phi^t} & & \| \\ \tilde{h}_{B/K}\colon B(K) \times B^t(K) & \longrightarrow & \mathbb{R}. \end{array}$$

Proof. By definition of the Néron-Tate pairing and functorial properties of the height ([Lan83, Proposition V.3.3]), $\tilde{h}_{A/K}(\cdot, \phi^t(\cdot))$ and $\tilde{h}_{B/K}(\phi(\cdot), \cdot)$ are the canonical heights on $A \times B^t$ associated with the divisor classes corresponding respectively to $(1 \times \phi^t)^*(P_A)$ and $(\phi \times 1)^*(P_B)$. But the theorem in [Mum74, §13] implies

$$(1 \times \phi^t)^*(P_A) \simeq (\phi \times 1)^*(P_B) \tag{51}$$

(see [Mum74, p. 130]). □

5.2.2. *The p-adic height pairing.* We extend (50) to a pairing of $\mathbb{Z}_p$-modules.

Lemma 5.2.2. *Let A be an abelian variety defined over the global field K. For every finite extension F/K there exists a p-adic height pairing*

$$h_{A/F}\colon \big(\mathbb{Z}_p \otimes A(F)\big) \times \big(\mathbb{Z}_p \otimes A^t(F)\big) \longrightarrow E_F, \tag{52}$$

where E_F is a finite extension of $\mathbb{Q}_p$, with the left and right kernels equal to the torsion parts of $\mathbb{Z}_p \otimes A(F)$ and $\mathbb{Z}_p \otimes A^t(F)$. If $char(K) = p$ one can choose $E_F = \mathbb{Q}_p$.

Proof. If $char(K) = p$, then after scaling by a factor $\log(p)$, the pairing $\tilde{h}_{A/F}$ takes values in $\mathbb{Q}$ (see for example [Sch82, §3]): in this case we define $h_{A/F}$ by $\tilde{h}_{A/F} = -\log(p) h_{A/F}$ and extend it to get (52). In general, the image of the Néron-Tate height $\tilde{h}_{A/F}$ generates a subfield $E'_F \subset \mathbb{R}$. By the Mordell-Weil theorem, E'_F is

finitely generated over $\mathbb{Q}$, and hence can be embedded into a finite extension E_F of $\mathbb{Q}_p$. Then we have the pairing

$$\tilde{h}_{A/F}\colon A(F)\times A^t(F)\longrightarrow E'_F\subset E_F\,,$$

which is obviously continuous in the p-adic topology, and thus can be extended to a pairing $h_{A/F}$ as required. Since the left and right kernels of $\tilde{h}_{A/F}$ are the torsion parts of $A(F)$ and $A^t(F)$, if $x_1,...,x_r$ and $y_1,...,y_r$ are respectively $\mathbb{Z}$-basis of the free parts of $A(F)$ and $A^t(F)$, then

$$\det_{i,j}(h_{A/F}(x_i,y_j))=\det_{i,j}(\tilde{h}_{A/F}(x_i,y_j))\neq 0,$$

which actually means that $h_{A/F}$ is non-degenerate on the free part of its domain. □

5.2.3. For each finite extension F/K let $h_{A/F}$ be the p-adic height pairing established in Lemma 5.2.2. The action of $\mathcal{E}$ on $A(F)$ extends to that of $\mathbb{Z}_p\,\mathcal{E}$ on $\mathbb{Z}_p\otimes A(F)$ and the following results are proven by the same reasoning as in the proofs of Lemma 5.1.1 and Corollary 5.1.2.

Lemma 5.2.3. *For every $x\in\mathbb{Z}_p\otimes A(F)$, $y\in\mathbb{Z}_p\otimes A^t(F)$ and $\psi\in\mathbb{Z}_p\,\mathcal{E}$ we have*

$$h_{A/F}(\psi(x),y)=h_{A/F}(x,\psi^t(y))\,. \tag{53}$$

Corollary 5.2.4. *For $i=1,2$, the modules $\mathbb{Z}_p\otimes A(F)^{(i)}$ and $\mathbb{Z}_p\otimes A^t(F)^{(i)}$ have equal rank over $\mathbb{Z}_p$.*

5.2.4. Write $\mathcal{M}(A/F):=\mathbb{Q}_p/\mathbb{Z}_p\otimes A(F)$. Now we assume that all Tate-Shafarevich groups are finite. Hence $\mathcal{M}(A/F)=\mathrm{Sel}_{p^\infty}(A/F)_{div}$ and $\mathcal{M}(A/L):=\varinjlim_F\mathcal{M}(A/F)$ $=\mathrm{Sel}_{div}(A/L)$. The action of $\mathbb{Z}_p\,\mathcal{E}$ on $\mathcal{M}(A/L)$ extends to its dual as $(e\cdot\varphi)(x):=\varphi(ex)$. We have $Y_p(A/L)^{(i)}=(\mathcal{M}(A/L)^{(i)})^\vee$ and

$$Y_p(A/L)=Y_p(A/L)^{(1)}\oplus Y_p(A/L)^{(2)}. \tag{54}$$

Theorem 5.2.5. *If $X_p(A/L)$ is a torsion Λ-module, L/K is ramified only at good ordinary places and $Ш_{p^\infty}(A/F)$ is finite for every finite intermediate extension of L/K, then*

$$[Y_p(A/L)^{(1)}]=[Y_p(A^t/L)^{(1)}]^\sharp\ \text{ and }\ [Y_p(A/L)^{(2)}]=[Y_p(A^t/L)^{(2)}]^\sharp.$$

Proof. Fix $i\in\{1,2\}$. By Theorem 4.1.2, we write

$$[Y_p(A/L)^{(i)}]=\bigoplus_{\nu=1}^m(\Lambda/(f_\nu))^{r_\nu},\quad [Y_p(A^t/L)^{(i)}]=\bigoplus_{\nu=1}^m(\Lambda/(f_\nu))^{s_\nu},$$

where $f_1,...,f_m$ are coprime simple elements and r_ν, s_ν are non-negative integers. We need to show that $r_\nu=s_\nu$ for every ν, since $\Lambda/(f_\nu)=(\Lambda/(f_\nu))^\sharp$.

Let P_1 denote the quotient $Y_p(A/L)^{(i)}/[Y_p(A/L)^{(i)}]$ and P_2 the analogue for A^t. Since P_1, P_2 are pseudo-null Λ-modules, there are $\eta_1,\eta_2\in\Lambda$ coprime to $f:=f_1\cdots f_m$ such that $\eta_jP_j=0$. Then f_ν is coprime to $\eta_1\eta_2ff_\nu^{-1}$ for each ν. We choose $\omega\in\Gamma^\vee$ such that $\omega(f_\nu)=0$ and $\omega(\eta_1\eta_2ff_\nu^{-1})\neq 0$. Let E be a finite extension of $\mathbb{Q}_p$ containing the values of ω. Set $EM:=E\otimes_{\mathbb{Z}_p}M$ for any $\mathbb{Z}_p$-module M. We see E as a module over $E\,\Lambda$ via the ring epimorphism $E\,\Lambda\to E$ induced by ω. The exact sequence

$$0=\mathrm{Tor}^1_{E\,\Lambda}(E,EP_1)\longrightarrow E\otimes_{E\,\Lambda}E[Y_p(A/L)^{(i)}]$$
$$\longrightarrow E\otimes_{E\,\Lambda}EY_p(A/L)^{(i)}\longrightarrow E\otimes_{E\,\Lambda}EP_1=0$$

yields

$$r_\nu = \dim_E(E \otimes_{E\Lambda} EY_p(A/L)^{(i)})\,.$$

Let $\Gamma^\omega \subset \Gamma$ denote the kernel of ω and write $W_\omega(A)$ for the coinvariants $EY_p(A/L)^{(i)}_{\Gamma^\omega}$. The isomorphisms

$$E \otimes_{E\Lambda} EY_p(A/L)^{(i)} \simeq E \otimes_{E\Lambda} EY_p(A/L)^{(i)}_{\Gamma^\omega} \simeq (EY_p(A/L)^{(i)}_{\Gamma^\omega})^{(\omega)}$$

show that $r_\nu = \dim_E W_\omega(A)^{(\omega)}$. A similar argument proves $s_\nu = \dim_E W_\omega(A^t)^{(\omega)}$.

Write $K_\omega := L^{\Gamma^\omega}$ and $\Gamma_\omega := \mathrm{Gal}(K_\omega/K)$. Since $Ш_{p^\infty}(A/K_\omega)$ is finite, the control theorem [Tan10, Theorem 4] implies that the restriction map $\mathcal{M}(A/K_\omega) \to \mathcal{M}(A/L)^{\Gamma^\omega}$ has finite kernel and cokernel. Thus we find

$$\mathrm{rank}_{\mathbb{Z}_p}\left(\mathcal{M}(A/K_\omega)^{(i)}\right)^\vee = \mathrm{rank}_{\mathbb{Z}_p}\left((\mathcal{M}(A/L)^{\Gamma^\omega})^{(i)}\right)^\vee = \mathrm{rank}_{\mathbb{Z}_p} Y_p(A/L)^{(i)}_{\Gamma^\omega}.$$

This and Corollary 5.2.4 yield

$$\mathrm{rank}_{\mathbb{Z}_p} Y_p(A/L)^{(i)}_{\Gamma^\omega} = \mathrm{rank}_{\mathbb{Z}_p} Y_p(A^t/L)^{(i)}_{\Gamma^\omega}.$$

Similarly, for the character $\varpi = \omega^p$, we have

$$\mathrm{rank}_{\mathbb{Z}_p} Y_p(A/L)^{(i)}_{\Gamma^\varpi} = \mathrm{rank}_{\mathbb{Z}_p} Y_p(A^t/L)^{(i)}_{\Gamma^\varpi}.$$

As in §3.2.4, let $[\omega]$ denote the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of ω. By $\Gamma^\vee_\omega = [\omega] \sqcup \Gamma^\vee_{\omega^p}$ we get the exact sequence of $E[\Gamma_\omega]$-modules:

$$0 \longrightarrow \prod_{\chi\in[\omega]}(W_\omega(A))^{(\chi)} \longrightarrow W_\omega(A) \longrightarrow W_{\omega^p}(A) \longrightarrow 0\,.$$

Since for all $\chi \in [\omega]$ the eigenspaces $(W_\omega(A))^{(\chi)}$ have the same dimension over E, the two equalities and the exact sequence above imply

$$\dim_E(W_\omega(A))^{(\omega)} = \dim_E(W_\omega(A^t))^{(\omega)}\,,$$

which completes the proof. □

Theorem 5.2.6. *If $X_p(A/L)$ is a torsion Λ-module, L/K is ramified only at good ordinary places and $Ш_{p^\infty}(A/F)$ is finite for every finite intermediate extension of L/K, then*

$$\begin{aligned}\chi(X_p(A/L)) &= \chi(X_p(A^t/L)^{(1)})^\sharp \cdot \chi(X_p(A/L)^{(2)}) \\ &= \chi(X_p(A/L)^{(1)}) \cdot \chi(X_p(A^t/L)^{(2)})^\sharp\,.\end{aligned}$$

Proof. Just use the exact sequence (49) (together with its A^t-analogue with $\mathfrak{b}^{(i)}$), Corollary 5.1.4 and Theorem 5.2.5 to get

$$\chi(X_p(A^t/L)^{(i)})^\sharp = \chi(X_p(A/L)^{(i)})\,. \tag{55}$$

□

In the next paper [LLTT] of this series we shall apply Theorem 5.2.6 to prove the Iwasawa Main Conjecture for constant ordinary abelian varieties over function fields.

Acknowledgments

The second, third, and fourth authors thank Centre de Recerca Matemàtica for their hospitality while working on part of this paper. The fourth author would like to express his gratitude to Takeshi Saito for his hospitality at the University of Tokyo where part of this work was written. Finally, it is our pleasure to thank NCTS/TPE for supporting a number of meetings of the authors at National Taiwan University.

References

[BL09] A. Bandini and I. Longhi, *Control theorems for elliptic curves over function fields*, Int. J. Number Theory **5** (2009), no. 2, 229–256, DOI 10.1142/S1793042109002067. MR2502807

[Bou65] N. Bourbaki, *Éléments de mathématique. Fasc. XXXI. Algèbre commutative. Chapitre 7: Diviseurs*, Actualités Scientifiques et Industrielles, No. 1314, Hermann, Paris, 1965. MR0260715

[Gr89] Ralph Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137. MR1097613

[Gr03] Ralph Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. **136** (2003), no. 3, 255–297, DOI 10.1023/A:1023251032273. MR1977007

[Lan83] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983. MR715605

[LLTT] King Fai Lai, Ignazio Longhi, Ki-Seng Tan, and Fabien Trihan, *The Iwasawa Main Conjecture for constant ordinary abelian varieties over function fields*, Proc. Lond. Math. Soc. (3) **112** (2016), no. 6, 1040–1058, DOI 10.1112/plms/pdw019. MR3537332

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266, DOI 10.1007/BF01389815. MR0444670

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330, DOI 10.1007/BF01388599. MR742853

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986. MR881804

[Mon81] Paul Monsky, *On p-adic power series*, Math. Ann. **255** (1981), no. 2, 217–227, DOI 10.1007/BF01450672. MR614398

[Nek06] Jan Nekovář, *Selmer complexes*, Astérisque **310** (2006), viii+559. MR2333680

[Mum74] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. MR0282985

[OT09] Tadashi Ochiai and Fabien Trihan, *On the Selmer groups of abelian varieties over function fields of characteristic* $p > 0$, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 1, 23–43, DOI 10.1017/S0305004108001801. MR2461865

[P03] Bernadette Perrin-Riou, *Groupes de Selmer et accouplements: cas particulier des courbes elliptiques*, Doc. Math. **Extra Vol.** (2003), 725–760. Kazuya Kato's fiftieth birthday. MR2046613

[Sch82] Peter Schneider, *Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern*, Math. Ann. **260** (1982), no. 4, 495–510, DOI 10.1007/BF01457028. MR670197

[Tan10] Ki-Seng Tan, *A generalized Mazur's theorem and its applications*, Trans. Amer. Math. Soc. **362** (2010), no. 8, 4433–4450, DOI 10.1090/S0002-9947-10-05042-7. MR2608412

[Tan14] Ki-Seng Tan, *Selmer groups over* $\mathbb{Z}_p^d$*-extensions*, Math. Ann. **359** (2014), no. 3-4, 1025–1075, DOI 10.1007/s00208-014-1023-9. MR3231024

[Vau09] David Vauclair, *Sur la dualité et la descente d'Iwasawa*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 2, 691–767. MR2521434

[Zab10] Gergely Zábrádi, *Pairings and functional equations over the* GL_2*-extension*, Proc. Lond. Math. Soc. (3) **101** (2010), no. 3, 893–930, DOI 10.1112/plms/pdq015. MR2734964

School of Mathematical Sciences, Capital Normal University, Beijing 100048, People's Republic of China

E-mail address: kinglaihonkon@gmail.com

Department of Mathematical Sciences, Xi'an Jiaotong-Liverpool University, No.111 Ren'ai Road, Suzhou Dushu Lake Higher Education Town, Suzhou Industrial Park, Jiangsu, People's Republic of China

E-mail address: Ignazio.Longhi@xjtlu.edu.cn

Department of Mathematics, National Taiwan University, Taipei 10764, Taiwan

E-mail address: tan@math.ntu.edu.tw

Department of Information and Communication Sciences, Faculty of Science and Technology, Sophia University, 4 Yonbancho, Chiyoda-ku, Tokyo 102-0081, Japan

E-mail address: f-trihan-52m@sophia.ac.jp