TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 362, Number 8, August 2010, Pages 4433–4450
S 0002-9947(10)05042-7
Article electronically published on March 17, 2010

A GENERALIZED MAZUR'S THEOREM AND ITS APPLICATIONS

KI-SENG TAN

Abstract. We generalize a theorem of Mazur concerning the universal norms of an abelian variety over a $\mathbb{Z}_p^d$-extension of a complete local field. Then we apply it to the proof of a control theorem for abelian varieties over global function fields.

1. Introduction

Consider an abelian variety A/K of dimension g and let B be its dual abelian variety. At first we assume that K is a complete local field with a finite residue field $\mathbb{F}_K$ which is of characteristic p and that A (hence B) has good ordinary reduction. Write $\bar{A}$, $\widehat{A}$ (resp. $\bar{B}$, $\widehat{B}$) for the reduction and the formal group of A (resp. B) so that we have the exact sequence induced from the reduction map:

$$\begin{aligned} 0 \longrightarrow \quad & \widehat{A}(\mathcal{O}_{\bar{K}^a}) \longrightarrow A(\bar{K}^a) \longrightarrow \bar{A}(\bar{\mathbb{F}}_K) \longrightarrow 0 \\ (\text{resp. } 0 \longrightarrow \quad & \widehat{B}(\mathcal{O}_{\bar{K}^a}) \longrightarrow B(\bar{K}^a) \longrightarrow \bar{B}(\bar{\mathbb{F}}_K) \longrightarrow 0). \end{aligned} \tag{1}$$

Here $\bar{K}^a$ is a fixed algebraic closure of K. For an algebraic extension L/K, $\mathcal{O}_L$ and $\mathbb{F}_L$ denote the ring of integers and the residue field.

Let L/K be a $\mathbb{Z}_p^d$-extension with $\mathrm{Gal}(L/K) = \Gamma$ and for a Γ-module M let $\mathrm{N}_{L/K}(M) = \bigcap \mathrm{N}_{F/K}(M)$, where F runs through all finite intermediate fields, denote the universal norm. Then (1) and the surjectivity of the reduction map $B(K) \longrightarrow \bar{B}(\mathbb{F}_K)$ (see Lemma 2.1.1) induce the exact sequence:

$$\widehat{B}(\mathcal{O}_K)/\,\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)) \longrightarrow B(K)/\,\mathrm{N}_{L/K}(B(L)) \twoheadrightarrow \bar{B}(\mathbb{F}_K)/\,\mathrm{N}_{L/K}(\bar{B}(\mathbb{F}_L)). \tag{2}$$

Let $u \in \mathrm{GL}(g, \mathbb{Z}_p)$ be the twist matrix given by the action of the Frobenius substitution $\mathrm{Frob} \in \mathrm{Gal}(\bar{\mathbb{F}}_K/\mathbb{F}_K)$ on the group of torsion points $\bar{A}[p^\infty] := \bigcup_n \bar{A}[p^n] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^g$ (see [Maz72], p.216). The following is a strengthened theorem of Mazur (see [Maz72], Proposition 4.3.9 and [Sch83], Proposition 7.2).

Theorem 1. *Suppose K is a finite extension field of $\mathbb{Q}_p$ and L/K is a totally ramified $\mathbb{Z}_p$-extension so that $\Gamma = \mathrm{Gal}(L/K) \simeq \mathbb{Z}_p$. If A/K is an abelian variety with good ordinary reduction, then $\widehat{B}(\mathcal{O}_K)/\,\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)) \simeq \Gamma^g/(I-u)\Gamma^g$ and*

$$\widehat{B}(\mathcal{O}_K)/\,\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)) \longrightarrow B(K)/\,\mathrm{N}_{L/K}(B(L))$$

is injective.

Received by the editors December 4, 2008 and, in revised form, March 6, 2009.
2010 *Mathematics Subject Classification.* Primary 11R23, 11S25.
This research was supported in part by the National Science Council of Taiwan, NSC95-2115-M-002-017-MY2.

Our goal is to generalize this theorem to all $\mathbb{Z}_p^d$-extensions over local fields in any characteristic. A simplified proof of Theorem 1 can be found in [Jon91, LuR78]. Although not mentioned in the articles, the methods they use are likely to work in the case of positive characteristic. However, the "totally ramified" condition seems indispensable to the methods. It might be possible to lift this restriction by considering the situation in which k is a subfield of K, L/k is a $\mathbb{Z}_p$-extension, Γ is the inertia subgroup of $\mathrm{Gal}(L/k)$, and trying to deduce, from the statements of (B, L, K) in Theorem 1, the corresponding statements of (B, L, k). To do so, there is still work to be done. Especially, whether or not the isomorphism in Theorem 1 is compatible with $\mathrm{Gal}(K/k)$-actions is yet to be checked.

We take a different approach. Again, (1) and the surjectivity of the reduction map $A(K) \longrightarrow \bar{A}(\mathbb{F}_K)$ induce the inclusion $\mathrm{H}^1(K, \widehat{A}) \hookrightarrow \mathrm{H}^1(K, A)$. Here $\mathrm{H}^1(K, \widehat{A})$ means $\mathrm{H}^1(\mathrm{Gal}(\bar{K}/K), \widehat{A}(\mathcal{O}_{\bar{K}}))$. Also,

$$0 \longrightarrow \mathrm{H}^1(\Gamma, \widehat{A}(\mathcal{O}_L)) \longrightarrow \mathrm{H}^1(\Gamma, A(L)) \xrightarrow{\Phi_*} \mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L)), \tag{3}$$

where Φ_* is induced from the reduction map $\Phi : A \longrightarrow \bar{A}$, is exact. By Tate's local duality theorem, the Pontryagin dual to the compact group $B(K)/\mathrm{N}_{L/K}(B(L))$, via the local pairing, is the local cohomology group $\mathrm{H}^1(L/K, A(L))$ (with discrete topology; see Corollary 2.3.3). Comparing (2) and (3), one might ask if these two exact sequences are actually the dual to each other. The answer turns out to be "yes", and here comes our generalized dual version of Mazur's Theorem.

Theorem 2. *Let K be a complete local field with a finite residue field $\mathbb{F}_K$ of characteristic p and let L/K be a $\mathbb{Z}_p^d$-extension with $\mathrm{Gal}(L/K) = \Gamma$. If A/K is an abelian variety with good ordinary reduction, then the following holds:*

(a) *Via the local pairing, the group $\mathrm{H}^1(K, \widehat{A})$ is the annihilator of $\widehat{B}(\mathcal{O}_K)$ and is isomorphic to the Pontryagin dual of $\bar{B}(\mathbb{F}_K)_p$.*
(b) *If L/K is ramified, then $\mathrm{H}^1(\Gamma, \widehat{A}(\mathcal{O}_L)) = \mathrm{H}^1(K, \widehat{A})$.*
(c) *The map Φ_* is surjective. If $\Gamma' \subset \Gamma$ is the inertia subgroup, then the group $\mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L))$ is canonically isomorphic to $\mathrm{Hom}(\Gamma', \bar{A}(\mathbb{F}_K))$.*

The theorem will be proved in Section 2.7. Note that if L/K is ramified, then we know that $\widehat{B}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)) \longrightarrow B(K)/\mathrm{N}_{L/K}(B(L))$ is injective (see Lemma 2.7.1) and $\bar{B}(\mathbb{F}_K)/\mathrm{N}_{L/K}(\bar{B}(\mathbb{F}_L))$ is naturally isomorphic to $\bar{B}(\mathbb{F}_K)_p$. Theorem 2 implies that (3) is indeed dual to (2). If L/K is unramified, all six terms in two exact sequences are trivial (by Lemma 3.3.1 and Lang's theorem). It is also interesting to see that $\bar{A}(\mathbb{F}_K)_p = (A[p^\infty])^{\mathrm{Frob}}$ is isomorphic to the dual group of $\mathbb{Z}_p^g/(I-u)\mathbb{Z}_p^g$ and hence by (c), $\mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L))$ is dual to $(\Gamma')^g/(I-u)(\Gamma')^g$.

In general, the order $|\mathrm{Hom}(\Gamma', \bar{A}(\mathbb{F}_K))| = |\bar{A}(\mathbb{F}_K)_p|^{rk(\Gamma')}$ and, since $\bar{A}$ and $\bar{B}$ are isogenous, $|\bar{B}(\mathbb{F}_K)_p| = |\bar{A}(\mathbb{F}_K)_p|$. Thus, Theorem 2 implies the following local control theorem. Let $sign(e) = 1$ if $e > 0$; $sign(e) = 0$ if $e = 0$.

Theorem 3 (The local control theorem)**.** *Suppose K is a complete local field with a finite residue field $\mathbb{F}_K$ of characteristic p, L/K is a $\mathbb{Z}_p^d$-extension with Galois group Γ, and the inertia subgroup $\Gamma' \subset \Gamma$ is isomorphic to $\mathbb{Z}_p^e$. If A/K is an abelian variety with good ordinary reduction, then we have the following estimate on the size of the Galois cohomology group:*

$$|\mathrm{H}^1(\Gamma, A(L))| = |\bar{A}(\mathbb{F}_K)_p|^{sign(e)+e} \leq |\bar{A}(\mathbb{F}_K)_p|^{d+1}.$$

Theorem 3 will be applied to prove a global control theorem. Regard A as a sheaf for the flat topology on K and denote $\mathcal{A}[p^m] = \ker(A \xrightarrow{[p^m]} A)$, where $[p^m]$ denotes the multiplication by p^m on A. If K is a global field, the p^m-Selmer group $\mathrm{Sel}_{p^m}(F)$ for a finite extension field F of K is defined to be the kernel of the composition

$$\mathrm{H}^1(F, \mathcal{A}[p^m]) \longrightarrow \mathrm{H}^1(F, A) \xrightarrow{loc} \bigoplus_v \mathrm{H}^1(F_v, A),$$

where *loc* is the localization map to the direct sum of local cohomology groups over all places of F. The direct limit of $\mathrm{Sel}_{p^m}(F)$ as $m \to \infty$ is denoted by $\mathrm{Sel}_{p^\infty}(F)$. For any Galois extension L/K, the p-primary part of the Selmer group of A over L is taken to be the direct limit of $\mathrm{Sel}_{p^\infty}(F)$ over all finite intermediate fields F of L/K. We write Γ_F for the Galois group of L/F and let

$$res_{L/F} : \mathrm{Sel}_{p^\infty}(F) \longrightarrow \mathrm{Sel}_{p^\infty}(L)^{\Gamma_F}$$

be the restriction map.

Theorem 4 (The control theorem)**.** *Let L be a $\mathbb{Z}_p^d$-extension of a global field K of characteristic p with Galois group $\mathrm{Gal}(L/K) = \Gamma$. Assume that L/K is unramified outside a finite set S of places of K. Let A be an abelian variety over K with good ordinary reduction at every place in S. Then for every finite intermediate extension F of L/K, the kernel and the cokernel of the restriction map $res_{L/F}$ on the p-primary Selmer groups $\mathrm{Sel}_{p^\infty}(F)$ are finite. Furthermore, if $d = 1$, then the orders of the kernel and the cokernel of $res_{L/F}$ are bounded as F varies.*

The theorem will be proved in Section 3.3. The number field counterpart of this theorem appears in Mazur ([Maz72]) and Greenberg ([Gre03]).

We shall also apply our result to compact Iwasawa modules. Denote by Λ_Γ the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$ and denote the Pontryagin dual $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(L), \mathbb{Q}_p/\mathbb{Z}_p)$ by X_L.

We say that A has split multiplicative reduction at v, if there is a rank g lattice $\Omega \simeq \mathbb{Z} \times \cdots \times \mathbb{Z}$ inside the torus $T = (K_v)^g$ so that T/Ω is isomorphic to the rigid analytic space associated to A (see [Ger72]). For example, the Jacobian varieties of Drinfeld modular curves over K (for $\infty = v$) all have split multiplicative reduction at v (see [GkR96]).

Theorem 5. *Let L be a $\mathbb{Z}_p^d$-extension of a global field K of characteristic p with Galois group $\mathrm{Gal}(L/K) = \Gamma$. Assume that L/K is unramified outside a finite set S of places of K. Let A be an abelian variety over K with either good ordinary reduction or split multiplicative reduction at each place in S. Then X_L is a finitely generated module over Λ_Γ.*

The proof of the theorem (in Section 3.3) uses a standard tool that consists of two parts: one is a version of Nakayama's Lemma (see [Was82], p.279); the other is the assertion, which holds automatically if K is a number field, that at each $v \in S$, the local cohomology group $\mathrm{H}^1(\Gamma_v, A(L_v))$ is co-finitely generated. Several articles have used this tool to prove results of this kind. However, lacking our local control theorem, to make sure the above-mentioned assertion holds (over function fields) they need to depend on additional assumptions. For example, in Ochiai and Trihan ([OTr06, OTr08]), they assume that L/K is the constant $\mathbb{Z}_p$-extension unramified at every place of K, while Bandini and Longhi ([BL06]) treat the case of an elliptic curve with split multiplicative reduction at every place of S.

Finally, we set some notation. We use $\bar{K}$ to denote the separable closure of K and write $G_K = \mathrm{Gal}(\bar{K}/K)$. Denote $A(K)_{tor,p} = A[p^\infty] \cap A(K)$, the p-primary part of $A(K)_{tor}$. If K is a complete local field of residual characteristic p, we use $A(K)_p$ to denote the maximal pro-p subgroup of $A(K)$. Thus $A(K)_p$ contains $\widehat{A}(\mathcal{O}_K)$ and $A(K)_p/\widehat{A}(\mathcal{O}_K) \simeq \bar{A}(\mathbb{F}_K)_p$.

For a global or local field K of characteristic $p > 0$ and for each n, we use $K^{(1/p^n)}/K$ to denote the unique purely inseparable extension of degree p^n. Observe that $\bar{K}^{(1/p^n)} = \overline{K^{(1/p^n)}}$. Therefore, $\bar{K}^a = \bar{K}^{(1/p^\infty)} := \bigcup_{n=1}^{\infty} \bar{K}^{(1/p^n)}$. The Frobenius substitution

$$\mathrm{Frob}_{p^n} : K^{(1/p^n)} \longrightarrow K, \;\; x \mapsto x^{p^n},$$

is an isomorphism. Thus, we use it to identify $G_{K^{(1/p^n)}}$, for $n = 1, ..., \infty$, with G_K.

The author would like to thank A. Bandini, W.-C. Chi, C. D. González-Avilés, K.F. Lai, I. Longhi, D. Rockmore and F. Trihan for many valuable suggestions.

2. Abelian varieties with good ordinary reduction

As above, A denotes an an abelian variety defined over a field K. Except in the beginning of Section 2.1, K will be a complete local field with finite residue field $\mathbb{F}_K$ of characteristic p. From Section 2.2 to Section 2.7, A will have good ordinary reduction.

2.1. **Ordinary abelian varieties.** In this paragraph, we review some facts on ordinary abelian varieties as well as abelian varieties with good reduction. For the convenience of the readers, we give detailed proofs of all statements.

Suppose K is a field of characteristic $p > 0$. Then A is ordinary if and only if (over $\bar{K}^a$) the group scheme $\mathcal{A}[p^m]$ can be decomposed as (see [Mum74], p.147 and [Maz72], Lemma 4.27):

$$\mathcal{A}[p^m] = (\mathbb{Z}/p^m\mathbb{Z})^g \times (\mu_{p^m})^g. \tag{4}$$

This condition is equivalent to

$$A[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^g. \tag{5}$$

In this case, the multiplication by p^m on A is decomposed as

$$[p^m] = \mathrm{V}^{(m)} \circ \mathrm{F}^{(m)}, \tag{6}$$

where $\mathrm{F}^{(m)} : A \longrightarrow A^{(p^m)}$ is the Frobenius isogeny and $\mathrm{V}^{(m)} : A^{(p^m)} \longrightarrow A$ is separable.

From now on, we assume that K is a complete local field (of any characteristic) with a finite residue field $\mathbb{F}_K$ of characteristic p.

Suppose A has good reduction. Then $\mathbf{A}$, the Néron model of A over $\mathcal{O}_K$, is an abelian scheme. By definition, we have $\mathbf{A}(\mathcal{O}_{\bar{K}^a}) = A(\bar{K}^a)$. The reduction map $A(\bar{K}^a) \longrightarrow \bar{A}(\bar{\mathbb{F}}_K)$ is formed by the composition of $\mathrm{spec}\, \bar{\mathbb{F}}_K \longrightarrow \mathrm{spec}\, \mathcal{O}_{\bar{K}^a}$ with elements in $\mathbf{A}(\mathcal{O}_{\bar{K}^a}) = \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{spec}\, \mathcal{O}_{\bar{K}^a}, \mathbf{A})$.

Lemma 2.1.1. *The reduction $A(K) \longrightarrow \bar{A}(\mathbb{F}_K)$ is surjective.*

Proof. This holds because $\mathbf{A}$ is smooth and $\mathcal{O}_K$ is Henselian (see [Mil80], I.4.13.) □

Let $[\mathbf{p^m}] : \mathbf{A} \longrightarrow \mathbf{A}$ denote the multiplication by p^m. Then the restriction of $[\mathbf{p^m}]$ to the generic (resp. special) fibre of $\mathbf{A}$ is just the multiplication by p^m on A (resp. $\bar{A}$). Suppose $f : A \longrightarrow A'$ (resp. $g : A' \longrightarrow A$) is an isogeny over K with $\ker(f) \subset \mathcal{A}[p^m]$ so that $[p^m]$ on A is decomposed as $g \circ f$. Then f (resp. g) extends to an isogeny $\mathbf{f} : \mathbf{A} \longrightarrow \mathbf{A}'$ (resp. $\mathbf{g} : \mathbf{A}' \longrightarrow \mathbf{A}$) (see [BLR90], 7.3, Lemma 6). From the definition of the Néron model, the extension of each isogeny is unique, and this implies $[\mathbf{p^m}] = \mathbf{g} \circ \mathbf{f}$. Let $\bar{f} : \bar{A} \longrightarrow \bar{A}'$ (resp. $\bar{g} : \bar{A}' \longrightarrow \bar{A}$) denote the restriction of $\mathbf{f}$ (resp. $\mathbf{g}$) to the special fibres. Then on $\bar{A}$, we have

$$[p^m] = \bar{g} \circ \bar{f}. \tag{7}$$

Also, f, $\bar{f}$ and the reductions commute, as shown by the diagram:

$$\begin{array}{ccccc} A(\bar{K}^a) & = & \mathbf{A}(\mathcal{O}_{\bar{K}^a}) & \longrightarrow & \bar{A}(\bar{\mathbb{F}}_K) \\ \downarrow f & \circlearrowright & \downarrow \mathbf{f} & \circlearrowright & \downarrow \bar{f} \\ A'(\bar{K}^a) & = & \mathbf{A}'(\mathcal{O}_{\bar{K}^a}) & \longrightarrow & \bar{A}'(\bar{\mathbb{F}}_K), \end{array} \tag{8}$$

where both right-arrows are reduction maps. Note that in the diagram all the arrows are homomorphisms of G_K-modules. Here G_K acts on $\bar{A}(\bar{\mathbb{F}}_K)$ and $\bar{A}'(\bar{\mathbb{F}}_K)$ via the quotient map $G_K \longrightarrow \mathrm{Gal}(\bar{\mathbb{F}}_K/\mathbb{F}_K)$.

Let $\mathbf{A}[\mathbf{p^m}] = \ker([\mathbf{p^m}])$. The closed subgroup scheme $\ker(\mathbf{f}) \subset \mathbf{A}[\mathbf{p^m}]$ is finite flat over $\mathcal{O}_K$ (op. cit. 7.3, Lemma 1). Since $\mathcal{O}_K$ is a complete discrete valuation ring, we have $\ker(\mathbf{f}) = \operatorname{spec} R$, with $R = \prod R_i$, where each R_i is a local ring finite free over $\mathcal{O}_K$ ([Mil80], I.4.2(b)). By (8), we have the reduction map:

$$\ker(f)(\bar{K}^a) \longrightarrow \ker(\bar{f})(\bar{\mathbb{F}}_K). \tag{9}$$

Lemma 2.1.2. *The G_K-module homomorphism* (9) *is surjective.*

Proof. By replacing K with a suitable finite unramified extension field of it, we may assume that each point in $\ker(\bar{f})(\bar{\mathbb{F}}_K)$ is rational over $\mathbb{F}_K$. Let $\ker(\mathbf{f}) = \operatorname{spec} R$ and $R = \prod_i R_i$ be as above. Then the residue field of each R_i equals $\mathbb{F}_K$. The flatness of R_i over O_K implies that $\mathrm{Hom}_{\mathcal{O}_K}(R_i, \mathcal{O}_{\bar{K}^a})$ (in the category of $\mathcal{O}_K$-algebras) is non-empty and hence the natural map from $\mathrm{Hom}_{\mathcal{O}_K}(R_i, \mathcal{O}_{\bar{K}^a})$ to $\mathrm{Hom}_{\mathcal{O}_K}(R_i, \bar{\mathbb{F}}_K)$ (which consists of a single element) is surjective. Therefore, the reduction map from $\mathrm{Hom}_{\mathcal{O}_K}(R, \mathcal{O}_{\bar{K}^a})$ to $\mathrm{Hom}_{\mathcal{O}_K}(R, \bar{\mathbb{F}}_K)$ is also surjective. □

Corollary 2.1.3. *Suppose A has good reduction, $\bar{A}$. Then for each positive integer m, the reduction induces a surjective homomorphism of G_K-modules:*

$$A[p^m] \longrightarrow \bar{A}[p^m]. \tag{10}$$

Furthermore, if char.$(K) = p$ and A has good ordinary reduction, then A is ordinary and (10) *is an isomorphism.*

Proof. Take $f = [p^m]$. To prove the second statement, we apply (5) and assert that the order $|\bar{A}[p^m]| = p^{gm}$, while $|A[p^m]| \leq p^{gm}$ and the equality holds if and only if A is ordinary. Also, the surjectivity of (10) implies the injectivity. □

2.2. **The isogeny $\mathrm{F}^{(m)}$.** Until the end of Section 2.7, we assume that A has good ordinary reduction. For each positive integer m, denote $\widehat{A}[p^m] = \widehat{A}(\mathcal{O}_{\bar{K}}) \cap A[p^m]$, which is the kernel of (10).

If *char.*$(K) = 0$, then $\mathcal{A}[p^m]$ is étale and hence $\widehat{A}[p^m]$ can be viewed as a closed subgroup scheme of it. Let $A^{(p^m)}$ denote the quotient $A/\widehat{A}[p^m]$. Then $A^{(p^m)}$ is

an abelian variety defined over K and there is a K-isogeny (unique up to K-automorphisms of $A^{(p^m)}$) $A \longrightarrow A^{(p^m)}$ that realizes the quotient map (see [Cho52]). We fix one such isogeny and denote it by $\mathrm{F}^{(m)}$. By (8), we have (over $\bar{\mathbb{F}}_K$)

$$\ker(\bar{\mathrm{F}}^{(m)}) = (\mu_{p^m})^g. \tag{11}$$

This means that $\bar{\mathrm{F}}^{(m)} = \beth \circ \mathrm{F}^{(m)}_{\bar{A}}$, where $\mathrm{F}^{(m)}_{\bar{A}}$ is the Frobenius isogeny and $\beth$ is an automorphism of $\bar{A}^{(p^m)}$. If $char.(K) = p$, let $\mathrm{F}^{(m)} : A \longrightarrow A^{(p^m)}$ be the Frobenius isogeny. Then $\bar{\mathrm{F}}^{(m)}$ is actually the Frobenius isogeny $\mathrm{F}^{(m)}_{\bar{A}}$. In either case, the isogeny $\bar{\mathrm{F}}^{(m)}$ gives rise to an isomorphism of G_K-modules:

$$\bar{\mathrm{F}}^{(m)} : \bar{A}(\bar{\mathbb{F}}_K) \xrightarrow{\sim} \bar{A}^{(p^m)}(\bar{\mathbb{F}}_K). \tag{12}$$

Let $\mathrm{V}^{(m)} : A^{(p^m)} \longrightarrow A$ be the isogeny so that $[p^m] = \mathrm{V}^{(m)} \circ \mathrm{F}^{(m)}$ on A. Then, over $\bar{K}^a$, we have $\ker(\mathrm{V}^{(m)}) = \mathcal{A}[p^m]/\ker(\mathrm{F}^{(m)}) = (\mathbb{Z}/p^m\mathbb{Z})^g$. In particular, $\ker(\mathrm{V}^{(m)})$ is étale, and consequently, $\ker(\mathrm{V}^{(m)})(\bar{K}^a) = \ker(\mathrm{V}^{(m)})(\bar{K})$. Also, over $\bar{\mathbb{F}}_K$, we have $\ker(\bar{\mathrm{V}}^{(m)}) = \bar{\mathcal{A}}[p^m]/\ker(\bar{\mathrm{F}}^{(m)}) = (\mathbb{Z}/p^m\mathbb{Z})^g$ (by (4), (7) and (11)), and hence $\ker(\bar{\mathrm{V}}^{(m)})(\bar{\mathbb{F}}_K) = \bar{A}^{(p^m)}[p^m]$. Therefore, by Lemma 2.1.2, the reduction map induces the G_K-isomorphism:

$$\ker(\mathrm{V}^{(m)})(\bar{K}) \xrightarrow{\sim} \bar{A}^{(p^m)}[p^m].$$

In particular, if m is greater than the exponent of $\bar{A}(\mathbb{F}_K)_p$, which is isomorphic to $\bar{A}^{(p^m)}(\mathbb{F}_K)_p$ by (12), then $\bar{A}^{(p^m)}(\mathbb{F}_K)_p$ is contained in $\bar{A}^{(p^m)}[p^m]$ and, being fixed by the G_K-action, is isomorphic to a subgroup of $\ker(\mathrm{V}^{(m)})(K) \subset A^{(p^m)}(K)_p$. Therefore, the exact sequence

$$0 \longrightarrow \widehat{A}^{(p^m)}(\mathcal{O}_K) \longrightarrow A^{(p^m)}(K)_p \longrightarrow \bar{A}^{(p^m)}(\mathbb{F}_K)_p \longrightarrow 0$$

actually splits. If L/K is a pro-finite field extension, then by taking the direct limit over finite intermediate extensions, we obtain the following:

Lemma 2.2.1. *If m is greater than the exponent of $\bar{A}(\mathbb{F}_L)_p$, where L/K is a pro-finite field extension, then we have the splitting exact sequence*

$$0 \longrightarrow \widehat{A}^{(p^m)}(\mathcal{O}_L) \longrightarrow A^{(p^m)}(L)_p \longrightarrow \bar{A}^{(p^m)}(\mathbb{F}_L)_p \longrightarrow 0.$$

2.3. **The local duality.** For the convenience of the reader, we put in the content of this paragraph some well-known facts on local duality. Via the Poincaré biextension $W \longrightarrow A \times B$ (which is the complement of the zero section in the Poincaré line bundle over $A \times B$, [Mum68]), a point on B is regarded as an element in $\mathrm{Ext}(A, \mathbb{G}_m)$, and hence a point $Q \in B(K)$ gives rise to an exact sequence of G_K-modules:

$$0 \longrightarrow \bar{K}^* \longrightarrow W_Q \longrightarrow A(\bar{K}) \longrightarrow 0.$$

Using the induced long exact sequence:

$$\cdots \longrightarrow \mathrm{H}^1(K, W_Q) \longrightarrow \mathrm{H}^1(K, A) \xrightarrow{\delta_Q} \mathrm{H}^2(K, \bar{K}^*) \longrightarrow \cdots,$$

we define (cf. [Mil86], Appendix C) the local pairing of Q and a class $\xi \in \mathrm{H}^1(K, A)$ as

$$\langle \xi, Q \rangle_{A,B,K} := inv(\delta_Q(\xi)).$$

Here $inv : \mathrm{H}^2(K, \bar{K}^*) \longrightarrow \mathbb{Q}/\mathbb{Z}$ gives the invariants of the local Brauer group.

Theorem 6 (Tate's local duality theorem [Tat62, Mil70/72])**.** *The discrete group* $\mathrm{H}^1(K,A)$ *and the compact group* $A(K)$ *are Pontryagin dual to each other, via the local pairing.*

If W_A, $W_{A'}$ are Poincaré biextensions associated to A, A' and $f : A \longrightarrow A'$ and $\hat{f} : B' \longrightarrow B$ are dual isogenies, then $(1 \times \hat{f})^* W_A \simeq (f \times 1)^* W_{A'}$ ([Mum74], p.130). From this, we see that the local pairings are compatible with isogenies. In particular, the following holds.

Lemma 2.3.1. *We have the commutative diagram:*

$$\begin{array}{lccc} \langle , \rangle_{A,B,K} : & \mathrm{H}^1(K,A) \times B(K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & \mathrm{F}_*^{(m)} \downarrow \quad \uparrow \hat{\mathrm{F}}_*^{(m)} & & \| \\ \langle , \rangle_{A^{(p^m)},B^{(p^m)},K} : & \mathrm{H}^1(K,A^{(p^m)}) \times B^{(p^m)}(K) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{13}$$

Lemma 2.3.2. *If* L/K *is a finite Galois extension, then we have the following commutative diagrams:*

$$\begin{array}{lccc} \langle , \rangle_{A,B,L} : & \mathrm{H}^1(L,A) \times B(L) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & cor \downarrow \quad \uparrow & & \| \\ \langle , \rangle_{A,B,K} : & \mathrm{H}^1(K,A) \times B(K) & \longrightarrow & \mathbb{Q}/\mathbb{Z}, \end{array} \tag{14}$$

and

$$\begin{array}{lccc} \langle , \rangle_{A,B,L} : & \mathrm{H}^1(L,A) \times B(L) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & res \uparrow \quad \downarrow \mathrm{N}_{L/K} & & \| \\ \langle , \rangle_{A,B,K} : & \mathrm{H}^1(K,A) \times B(K) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{15}$$

Proof. The diagram (14) is from the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^2(L,\bar{L}^*) & \xrightarrow{inv} & \mathbb{Q}/\mathbb{Z} \\ \downarrow cor & & \| \\ \mathrm{H}^2(K,\bar{K}^*) & \xrightarrow{inv} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Since $B(K) \longrightarrow B(L)$ is an injection onto a closed subgroup, Theorem 6 and (14) imply that $cor : \mathrm{H}^1(L,A) \longrightarrow \mathrm{H}^1(K,A)$ is surjective. Let $\xi \in \mathrm{H}^1(K,A)$, $Q \in B(L)$ and let $\psi \in \mathrm{H}^1(L,A)$ be such that $cor(\psi) = \xi$. Then

$$\langle \xi, \mathrm{N}_{L/K}(Q) \rangle_{A,B,K} = \sum_{\sigma \in \mathrm{Gal}(L/K)} \langle \psi, {}^{\sigma}Q \rangle_{A,B,L} = \langle \mathrm{N}_{L/K}(\psi), Q \rangle_{A,B,L}.$$

Here we use (14) as well as the $\mathrm{Gal}(L/K)$-equivariant property of the local pairing. But $\mathrm{N}_{L/K}(\psi) = res(cor(\psi)) = res(\xi)$. □

Corollary 2.3.3. *If* L/K *is a Galois extension, then via the local pairing the discrete group* $\mathrm{H}^1(\mathrm{Gal}(L/K), A(L))$ *and the compact group* $B(K)/\mathrm{N}_{L/K}(B(L))$ *can be identified as the Pontryagin dual to each other.*

Proof. Since $\mathrm{H}^1(\mathrm{Gal}(L/K), A(L))$ is the direct limit of $\mathrm{H}^1(\mathrm{Gal}(F/K), A(F))$ and $B(K)/\mathrm{N}_{L/K}(B(L))$ is the project limit of $B(K)/\mathrm{N}_{F/K}(B(F))$, where F runs through all finite intermediate Galois extensions, it is enough to consider the case where L/K is finite. Then we note that $\mathrm{H}^1(\mathrm{Gal}(L/K), A(L))$ is the kernel of the restriction map $res : \mathrm{H}^1(K,A) \longrightarrow \mathrm{H}^1(L,A)$, and hence it is the annihilator of $\mathrm{N}_{L/K}(B(L))$. □

2.4. **The characteristic 0 case.** In this paragraph, we assume that K is of zero characteristic. For each m, let e_m denote the Weil pairing:

$$e_m : A[p^m] \times B[p^m] \longrightarrow \bar{K}^*.$$

Also, denote $\widehat{A}[p^m] = \widehat{A}(\mathcal{O}_{\bar{K}}) \cap A[p^m]$ and $\widehat{B}[p^m] = \widehat{B}(\mathcal{O}_{\bar{K}}) \cap A[p^m]$, as before.

Lemma 2.4.1. *Assume that K is of characteristic 0 and that A has good ordinary reduction. Then the restriction of e_m on $\widehat{A}[p^m] \times \widehat{B}[p^m]$ is trivial.*

Proof. For simplicity, we replace K by a suitable finite extension field so that $A[p^m]$, $B[p^m]$, $\bar{A}[p^m]$ and $\bar{B}[p^m]$ are all rational over K and the decomposition (4) for $\bar{A}$ (resp. $\bar{B}$) holds over $\mathbb{F}_K$.

As in Section 2.2, we view $\widehat{A}[p^m]$ as the kernel of the isogeny $\mathrm{F}^{(m)}$ and let $\widehat{\mathbf{A}}[p^m]$ denote the kernel of the isogeny $\mathbf{A} \longrightarrow \mathbf{A}^{(p^m)}$ that extends $\mathrm{F}^{(m)}$. Then $\widehat{\mathbf{A}}[p^m]$ is a finite flat closed subgroup scheme of $\mathbf{A}[p^m]$ (see Section 2.1). In view of (11), we see that

$$\widehat{\mathbf{A}}[p^m] \otimes_{\mathcal{O}_K} \mathbb{F}_K = (\mu_{p^m})^g, \quad \text{over } \mathbb{F}_K. \tag{16}$$

For the dual abelian variety B, let $\mathbf{B}[p^m]$ and $\widehat{\mathbf{B}}[p^m]$ denote the corresponding group schemes. Let $\tilde{\mathbf{C}}$ and $\mathbf{C}$ be respectively the Cartier duals of $\mathbf{B}[p^m]$ and $\widehat{\mathbf{B}}[p^m]$. Then

$$\mathbf{C} \otimes_{\mathcal{O}_K} \mathbb{F}_K = (\mathbb{Z}/p^m\mathbb{Z})^g, \quad \text{over } \mathbb{F}_K \tag{17}$$

and

$$\mathbf{C} \otimes_{\mathcal{O}_K} K = (\mathbb{Z}/p^m\mathbb{Z})^g, \quad \text{over } K. \tag{18}$$

The Poincaré biextension of $A \times B$ extends uniquely to a biextension of $\mathbf{A} \times \mathbf{B}$ by $\mathbb{G}_m$ (see [Gth72], VIII.7.1b, or [Mil86], C.12) that defines in a canonical way a pairing $\mathbf{A}[p^m] \times \mathbf{B}[p^m] \longrightarrow \mathbb{G}_m$ (see [Gth72], VIII.2.2.2). This pairing extends the Weil pairing and it gives rise to the isomorphism $\mathbf{A}[p^m] \xrightarrow{\sim} \tilde{\mathbf{C}}$ (see [Mil86], p.398). Let Ψ be the composition $\Psi : \widehat{\mathbf{A}}[p^m] \longrightarrow \mathbf{A}[p^m] \xrightarrow{\sim} \tilde{\mathbf{C}} \longrightarrow \mathbf{C}$, where the first map is the inclusion and the last is the dual to the inclusion. It is enough to show that $\Psi \otimes K$ is the trivial homomorphism of group schemes.

Now that $\mathbf{C}$ is finite flat over $\mathcal{O}_K$, we write $\mathbf{C} = \operatorname{spec} T$, with $T = \prod_{i \in I} T_i$, a direct product of local rings over $\mathcal{O}_K$ ([Mil80], I.2.4(b)). The equalities (17) and (18) together say that $T_i \otimes_{\mathcal{O}_K} \mathbb{F}_K = \mathbb{F}_K$ and $T_i \otimes_{\mathcal{O}_K} K = K$, for each i. This implies that each $T_i = \mathcal{O}_K$. Also, write $\widehat{\mathbf{A}}[p^m] = \operatorname{spec} R$ and let $\Psi^* : T \longrightarrow R$ denote the morphism of Hopf algebras over $\mathcal{O}_K$ corresponding to Ψ. Since the homomorphism $\Psi \otimes \mathbb{F}_v$, sending $(\mu_{p^n})^g$ to $(\mathbb{Z}/p^n\mathbb{Z})^g$ (see (16) and (17)), is trivial, there is a factor T_0 of T so that $\Psi^* \otimes_{\mathcal{O}_K} \mathbb{F}_K : T \otimes_{\mathcal{O}_K} \mathbb{F}_K \longrightarrow R \otimes_{\mathcal{O}_K} \mathbb{F}_K$ factors through the projection $T \otimes_{\mathcal{O}_K} \mathbb{F}_K \longrightarrow T_0 \otimes_{\mathcal{O}_K} \mathbb{F}_K$. It follows that Ψ^* itself factors through the projection $T \longrightarrow T_0$. This means that Ψ factors as $\widehat{\mathbf{A}}[p^m] \longrightarrow \operatorname{spec} \mathcal{O}_K \longrightarrow \mathbf{C}$, where the first arrow is the natural map. Since Ψ is a homomorphism of group schemes over $\mathcal{O}_K$, the second arrow must be the identity section, and hence Ψ must be trivial. □

Corollary 2.4.2. *Assume that K is of characteristic 0 and A has good ordinary reduction. Then the restriction of the local pairing $\langle\ ,\ \rangle_{A,B,K}$ on $\mathrm{H}^1(K, \widehat{A}) \times \widehat{B}(\mathcal{O}_K)$ is trivial.*

Proof. Consider the commutative diagram induced from (1):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{A}(\mathcal{O}_{\bar{K}}) & \longrightarrow & A(\bar{K}) & \longrightarrow & \bar{A}(\bar{\mathbb{F}}_K) & \longrightarrow & 0 \\ & & \downarrow [p^m] & & \downarrow [p^m] & & \downarrow [p^m] & & \\ 0 & \longrightarrow & \widehat{A}(\mathcal{O}_{\bar{K}}) & \longrightarrow & A(\bar{K}) & \longrightarrow & \bar{A}(\bar{\mathbb{F}}_K) & \longrightarrow & 0. \end{array}$$

By Corollary 2.1.3 and the snake lemma, we have the Kummer exact sequence:

$$0 \longrightarrow \widehat{A}[p^m] \longrightarrow \widehat{A}(\bar{\mathcal{O}}_K) \xrightarrow{p^m} \widehat{A}(\bar{\mathcal{O}}_K) \longrightarrow 0,$$

which induces the exact sequence

$$0 \longrightarrow \widehat{A}(\mathcal{O}_K)/p^m\widehat{A}(\mathcal{O}_K) \longrightarrow \mathrm{H}^1(K, \widehat{A}[p^m]) \longrightarrow \mathrm{H}^1(K, \widehat{A})[p^m] \longrightarrow 0.$$

Similarly, we have

$$0 \longrightarrow \widehat{B}(\mathcal{O}_K)/p^m\widehat{B}(\mathcal{O}_K) \longrightarrow \mathrm{H}^1(K, \widehat{B}[p^m]) \longrightarrow \mathrm{H}^1(K, \widehat{B})[p^m] \longrightarrow 0.$$

If $\xi \in \mathrm{H}^1(K, \widehat{A})[p^m]$, then it annihilates $p^m\widehat{B}(\mathcal{O}_K)$ via the local pairing. Let α be an element in $\mathrm{H}^1(K, \widehat{A}[p^m])$ giving rise to ξ. For a point $Q \in \widehat{B}(\mathcal{O}_K)$, we identify its residue class modulo $p^m\widehat{B}(\mathcal{O}_K)$ with an $\eta \in \mathrm{H}^1(K, \widehat{B}[p^m])$. Then the value of $\langle \xi, Q\rangle_{A,B,K}$ equals the image of $\alpha \cup \eta$ under the composition (see [Mil86], p.54)

$$\mathrm{H}^2(K, \widehat{A}[p^m] \otimes \widehat{B}[p^m]) \longrightarrow \mathrm{H}^2(K, \mathbb{G}_m) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

where the first map is induced from the Weil pairing and the second gives the invariants of the local Brauer group. □

2.5. **The characteristic p case.** In this paragraph, we assume that $char.(K) = p$.

Lemma 2.5.1. *Suppose A has good ordinary reduction and K is of characteristic p. If L/K is a field extension, then the following hold:*

- **(a):** *If P is a point in $A(L)$, then all the p^m-division points of P are contained in $A(\bar{L}^{(1/p^m)})$. In particular, the p^m-torsion points $A[p^m] \subset A(\bar{K}^{(1/p^m)})$.*
- **(b):** *If L/K is separable, then the group $A(L)_{tor,p}$ is unramified over K. In other words, we have $A(L)_{tor,p} = A(L^{un})_{tor,p}$, where L^{un} is the maximal unramified intermediate extension of L/K.*
- **(c):** *The group $\widehat{A}(\mathcal{O}_L)$ is a torsion free $\mathbb{Z}_p$-module.*
- **(d):** *For each $P \in \widehat{A}(\mathcal{O}_L)$ there is a unique $P' \in \widehat{A}(\mathcal{O}_{L^{(1/p^m)}})$ such that $p^mP' = P$, and vice versa. In other words, we have*

$$\widehat{A}(\mathcal{O}_L) = p^m\widehat{A}(\mathcal{O}_{L^{(1/p^m)}}). \tag{19}$$

Proof. By Corollary 2.1.3, A itself is ordinary. The statement (a) follows directly from the decomposition (6), while (b) and (c) come from the G_K-isomorphism (10).

To see (d), let $Q \in A(\bar{L}^{(1/p^m)})$ be a p^m-division point of $P \in \widehat{A}(\mathcal{O}_L)$. Since the reduction $\bar{Q}$ is contained in $\bar{A}[p^m]$, there is a point $R \in A[p^m] \subset A(\bar{L}^{(1/p^m)})$ such that $P' := Q - R \in \widehat{A}(\mathcal{O}_{\bar{L}^{(1/p^m)}})$. Obviously, P' is also a p^m-division point of P, and for $\sigma \in G_L$, we have (from (c))

$${}^{\sigma}P' - P' \in A[p^m] \cap \widehat{A}(\mathcal{O}_{\bar{L}^{(1/p^m)}}) = \{0\}.$$

□

Let $i_{m*}\colon \mathrm{H}^1(K, A)_p \longrightarrow \mathrm{H}^1(K^{(1/p^m)}, A)_p$ be the map induced from the natural embedding $i_m : A(\bar{K}) \longrightarrow A(\bar{K}^{(1/p^m)})$.

Corollary 2.5.2. *If an element $\xi \in \mathrm{H}^1(K, \widehat{A}) \subset \mathrm{H}^1(K, A)_p$ satisfies $p^m\xi = 0$, then $\xi \in \ker(i_{m*})$.*

Proof. Let ρ be a 1-cocycle representing ξ and let P be a point in $\widehat{A}(\mathcal{O}_{\bar{K}})$ so that ${}^{\sigma}P - P = p^m\rho_\sigma$, for every $\sigma \in G_K$. Since every element in $\widehat{A}(\mathcal{O}_{\bar{K}})$ is uniquely divisible by p^m in $\widehat{A}(\mathcal{O}_{\bar{K}^{(1/p^m)}})$, there is a unique point $Q \in \widehat{A}(\mathcal{O}_{\bar{K}^{(1/p^m)}})$ so that $p^mQ = P$ and ${}^{\sigma}Q - Q = \rho_\sigma$, for every $\sigma \in G_K$.

□

Let $\hat{\mathrm{F}}^{(m)} : B^{(p^m)} \longrightarrow B$ be the dual to the Frobenius isogeny $\mathrm{F}^{(m)}$.

Corollary 2.5.3. *The isogeny $\hat{\mathrm{F}}^{(m)}$ that is dual to $\mathrm{F}^{(m)}$ gives rise to a surjection:*

$$\widehat{B}^{(p^m)}(\mathcal{O}_K) \overset{\hat{\mathrm{F}}^{(m)}}{\twoheadrightarrow} \widehat{B}(\mathcal{O}_K).$$

Proof. The Frobenius substitution Frob_{p^m} induces a G_K-isomorphism:

$$\begin{array}{rccc} \mathrm{Frob}_{p^m} : A(\bar{K}^{(1/p^m)}) & \xrightarrow{\sim} & A^{(p^m)}(\bar{K}) \\ P & \mapsto & \mathrm{F}^{(m)}(P). \end{array} \tag{20}$$

Using Lemma 2.5.1(c) to rewrite the equality (19) as $\widehat{A}(\mathcal{O}_{K^{(1/p^m)}}) = (1/p^m)\widehat{A}(\mathcal{O}_K)$ and then applying (20), we get

$$\mathrm{V}^{(m)}(\widehat{A}^{(p^m)}(\mathcal{O}_K)) = \mathrm{V}^{(m)}(\mathrm{F}^{(m)}(\widehat{A}(\mathcal{O}_{K^{(1/p^m)}}))) = \mathrm{V}^{(m)}(\mathrm{F}^{(m)}((1/p^m)\widehat{A}(\mathcal{O}_K))).$$

Consequently (by (6)), $\mathrm{V}^{(m)}(\widehat{A}^{(p^m)}(\mathcal{O}_K)) = \widehat{A}(\mathcal{O}_K)$. The dual abelian variety B, being isogenous to A, also has ordinary reduction. By letting B play the role of A in the above discussion, we get

$$\mathrm{V}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K)) = \widehat{B}(\mathcal{O}_K). \tag{21}$$

The kernel of $\hat{\mathrm{F}}^{(m)}$, which is the dual of $\ker(\mathrm{F}^{(m)}) = (\mu_{p^m})^g$, is exactly the maximal étale subgroup of the group scheme $\mathcal{B}^{(p^m)}[p^m]$ (the kernel of the multiplication by p^m on $B^{(p^m)}$). On the other hand, if we write $[p^m]_B$, the multiplication by p^m on B, as the composition $\mathrm{V}_B^{(m)} \circ \mathrm{F}_B^{(m)}$, then $\mathrm{V}_B^{(m)}$ is separable and hence its kernel also equals the maximal étale subgroup of $\mathcal{B}^{(p^m)}[p^m]$. In view of these, we see that $\hat{\mathrm{F}}^{(m)} = \beth \circ \mathrm{V}_B^{(m)}$, for some isomorphism $\beth : B/K \longrightarrow B/K$. In particular, we have

$$\hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_L)) = \mathrm{V}_B^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_L)).$$

By this and (21), we prove the surjectivity of the map $\widehat{B}^{(p^m)}(\mathcal{O}_L) \xrightarrow{\hat{\mathrm{F}}^{(m)}} \widehat{B}(\mathcal{O}_L)$. □

2.6. **The map $\mathrm{F}_*^{(m)}$.** For each m, let $\mathrm{F}_*^{(m)} : \mathrm{H}^1(K, A)_p \longrightarrow \mathrm{H}^1(K, A^{(p^m)})_p$ be the map induced from $\mathrm{F}^{(m)}$.

Proposition 2.6.1. *Suppose A has good ordinary reduction and $\xi \in \mathrm{H}^1(K, A)_p$. The following statements are equivalent:*

- **(a):** *The element $\xi \in \mathrm{H}^1(K, \widehat{A})$.*
- **(b):** *We have $\langle \xi, P\rangle_{A,B,K} = 0$, for every $P \in \widehat{B}(\mathcal{O}_K)$.*
- **(c):** *The image $\mathrm{F}_*^{(m)}(\xi) = 0$, for some m.*

For each m, let $\mho_m$ denote the kernel of the homomorphism $B^{(p^m)}(\bar{K}) \overset{\hat{\mathrm{F}}^{(m)}}{\longrightarrow} B(\bar{K})$. Then $\mho_m \simeq (\mathbb{Z}/p^m\mathbb{Z})^g$, since it is the group of geometric points of the étale group scheme $\ker(\hat{\mathrm{F}}^{(m)})$ which is isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^g$ over the algebraic closure of K. Since $\ker(\bar{\hat{\mathrm{F}}}^{(m)})$ is also isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^g$, Lemma 2.1.2 tells us that the reduction map $\ker(\hat{\mathrm{F}}^{(m)}) \longrightarrow \ker(\bar{\hat{\mathrm{F}}}^{(m)}) \hookrightarrow \bar{\mathcal{B}}^{(p^m)}[p^m]$ induces a G_K-isomorphism $\mho_m \longrightarrow \bar{B}^{(p^m)}[p^m]$. Consequently, the intersection $\mho_m \cap \widehat{B}^{(p^m)}(\mathcal{O}_K) = \{0\}$, as $\widehat{B}^{(p^m)}(\mathcal{O}_K)$ has trivial reduction. Therefore, the isogeny $\hat{\mathrm{F}}^{(m)}$ induces an injection

$$\widehat{B}^{(p^m)}(\mathcal{O}_K) \overset{\hat{\mathrm{F}}^{(m)}}{\hookrightarrow} \widehat{B}(\mathcal{O}_K). \tag{22}$$

If m is greater than the exponent of $\bar{B}(\mathbb{F}_K)_p$, then $\bar{B}(\mathbb{F}_K)_p \subset \bar{B}^{(p^m)}[p^m]$ and Lemma 2.2.1 says that $B^{(p^m)}(K)$ is the direct product of $\widehat{B}^{(p^m)}(\mathcal{O}_K)$ and a subgroup contained in the kernel of $\hat{\mathrm{F}}^{(m)}$. In particular, we have

$$\hat{\mathrm{F}}^{(m)}(B^{(p^m)}(K)) = \hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K)). \tag{23}$$

Proof. First, we show (c) $\Longrightarrow$ (a). Suppose $\xi \in \ker(\mathrm{F}_*^{(m)})$. To assert $\xi \in \mathrm{H}^1(K, \widehat{A}(\mathcal{O}_{\bar{K}}))$, we recall that $\bar{\mathrm{F}}^{(m)}$ induces a G_K-isomorphism $\bar{A}(\bar{\mathbb{F}}_K) \overset{\sim}{\longrightarrow} \bar{A}^{(p^m)}(\bar{\mathbb{F}}_K)$ (see (12)) and then use the commutative diagram:

$$\begin{array}{ccccc} \mathrm{H}^1(K, \widehat{A}) & \longrightarrow & \mathrm{H}^1(K, A)_p & \longrightarrow & \mathrm{H}^1(K, \bar{A})_p \\ \downarrow & & \downarrow \mathrm{F}_*^{(m)} & & \downarrow \simeq \\ \mathrm{H}^1(K, \widehat{A}^{(p^m)}) & \longrightarrow & \mathrm{H}^1(K, A^{(p^m)})_p & \longrightarrow & \mathrm{H}^1(K, \bar{A}^{(p^m)})_p. \end{array}$$

Suppose m is greater than the exponent of $\bar{B}(\mathbb{F}_K)_p$. If ξ satisfies the condition of (b), then (23) tells us that it annihilates every element in $\hat{\mathrm{F}}^{(m)}(B^{(p^m)}(K))$. By Lemma 2.3.1, we know that $\mathrm{F}_*^{(m)}(\xi)$ annihilates every element in $B^{(p^m)}(K)$. Then Theorem 6 says that $\mathrm{F}_*^{(m)}(\xi) = 0$. This shows (b) $\Longrightarrow$ (c).

Suppose $char.(K) = p$. Then Corollary 2.5.3 says that

$$\hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K)) = \widehat{B}(\mathcal{O}_K), \text{ for every } m,$$

and we can apply Lemma 2.3.1 and Theorem 6 again to show (c) $\Longrightarrow$ (b). Also, if an element $\xi \in \mathrm{H}^1(K, \widehat{A})$ satisfies $p^m\xi = 0$, then $\xi \in \ker(i_{m*})$ (see Corollary 2.5.2). We can deduce $\ker(i_m) = \ker(\mathrm{F}_*^{(m)})$ from the commutative diagram of G_K-modules:

$$\begin{array}{ccc} A(\bar{K}) & \longrightarrow & A(\bar{K}^{(1/p^m)}) \\ \| & & \downarrow \mathrm{Frob}_{p^m} \\ A(\bar{K}) & \overset{\mathrm{F}^{(m)}}{\longrightarrow} & A^{(p^m)}(\bar{K}), \end{array}$$

where the right down-arrow is an isomorphism of G_K-modules induced from the Frobenius substitution. This proves (a) $\Longrightarrow$ (c).

If $char.(K) = 0$, then (a) $\Longrightarrow$ (b) is proved by applying Corollary 2.4.2. □

In view of the equivalence "(b) $\Leftrightarrow$ (c)", by Lemma 2.3.1 and (23) we see that if m is greater than the exponent of $\bar{B}(\mathbb{F}_K)_p$, then the annihilator of $\widehat{B}(\mathcal{O}_K)$ is the same as that of $\hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K))$. Then Theorem 6 implies that

$$\hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K)) = \widehat{B}(\mathcal{O}_K).$$

The equality actually holds for every m, because we have the obvious inclusion $\hat{\mathrm{F}}^{(m+k)}(\widehat{B}^{(p^{m+k})}(\mathcal{O}_K)) \subset \hat{\mathrm{F}}^{(m)}(\widehat{B}^{(p^m)}(\mathcal{O}_K))$.

Corollary 2.6.2. *For every pro-finite extension L/K, we have the isomorphism:*

$$\widehat{B}^{(p^m)}(\mathcal{O}_L) \xrightarrow{\hat{\mathrm{F}}^{(m)}} \widehat{B}(\mathcal{O}_L), \ \textit{for every } m.$$

Proof. It is proved by taking the direct limit over all finite intermediate extensions. The injectivity is due to (22). □

2.7. **The proof of Theorem 2.** The statement (a) is a consequence of Proposition 2.6.1. Since $\mathrm{H}^1(\Gamma, \widehat{A}(\mathcal{O}_L)) \subset \mathrm{H}^1(K, \widehat{A})$ obviously holds, to prove (b), we only need to show that $\mathrm{H}^1(K, \widehat{A}) \subset \mathrm{H}^1(\Gamma, \widehat{A}(\mathcal{O}_L))$, which is the kernel of the homomorphism Φ_*. Therefore, it is enough to show that

$$\mathrm{H}^1(K, \widehat{A}) \subset \mathrm{H}^1(\Gamma, A(L))_p,$$

because $\widehat{A}$ is the kernel of the reduction map. Via the duality, the statement (a) and Corollary 2.3.3 together assert that the above inclusion is equivalent to

$$\mathrm{N}_{L/K}(B(L)_p) \subset \widehat{A}(\mathcal{O}_K).$$

Thus, the statement (b) can be proved by applying the following:

Lemma 2.7.1. *If L/K is ramified, then* $\mathrm{N}_{L/K}(B(L)_p) = \mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)) \subset \widehat{A}(\mathcal{O}_K)$.

Proof. For a given finite intermediate extension F/K of L/K, choose a ramified intermediate $\mathbb{Z}_p$-extension L'/F of L/F and let L'_0/F denote its maximal unramified intermediate extension. Let m be the exponent of $\bar{B}(\mathbb{F}_{L'})_p$ (which is a finite p-group) and let F'/L'_0 be the mth layer of the $\mathbb{Z}_p$-extension L'/L'_0. Suppose $x \in \mathrm{N}_{L/K}(B(L)_p)$ and $y \in B(F')_p$ are such that $\mathrm{N}_{F'/K}(y) = x$. Since $\mathrm{Gal}(F'/L'_0)$ fixes the reduction of y, we have $\mathrm{N}_{F'/L'_0}(y) \in \widehat{B}(\mathcal{O}_{L'_0})$ and hence $z := \mathrm{N}_{F'/F}(y) = \mathrm{N}_{L'_0/F}(\mathrm{N}_{F'/L'_0}(y))$ is contained in $\widehat{B}(\mathcal{O}_F)$. Therefore, $x = \mathrm{N}_{F/K}(z) \in \mathrm{N}_{F/K}(\widehat{B}(\mathcal{O}_F))$. □

Suppose L_0/K is a finite intermediate extension of L/K and let L'_0/K be its maximal unramified intermediate extension. Then by Lang's Theorem,

$$\mathrm{H}^1(\mathrm{Gal}(L'_0/K), \bar{A}(\mathbb{F}_{L'_0})) = \mathrm{H}^2(\mathrm{Gal}(L'_0/K), \bar{A}(\mathbb{F}_{L'_0})) = 0.$$

Therefore, the Hochschild-Serre spectral sequence implies that

$$\mathrm{H}^1(L_0/K, \bar{A}(\mathbb{F}_{L_0})) = \mathrm{H}^1(L_0/L'_0, \bar{A}(\mathbb{F}_{L_0}))^{\mathrm{Gal}(L'_0/K)} = \mathrm{Hom}(\mathrm{Gal}(L_0/L'_0), \bar{A}(\mathbb{F}_K)).$$

The second part of (c) is proved by taking the direct limit over L_0.

If L/K is unramified, then by Lemma 3.3.1 and Lang's Theorem, both $\mathrm{H}^1(\Gamma, A(L))$ and $\mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L))$ are trivial and there is nothing remaining to prove. Suppose L/K is ramified. By (a) and Lemma 2.7.1, we can identify $\mathrm{Im}(\Phi_*)$ with the dual group of the quotient $\widehat{B}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L))$. Thus, the surjectivity of Φ_* is equivalent to the equality

$$|\widehat{B}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L))| = |\mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L))|. \tag{24}$$

Assume that the inertia subgroup of Γ is of finite index. Then $\bar{A}(\mathbb{F}_L)$ is finite. If m is greater than the exponent of $\bar{A}(\mathbb{F}_L)_p$, then by Lemma 2.2.1 the exact sequence

$$0 \longrightarrow \widehat{A}^{(p^m)}(\mathcal{O}_L) \longrightarrow A^{(p^m)}(L)_p \longrightarrow \bar{A}^{(p^m)}(\mathbb{F}_L)_p \longrightarrow 0$$

splits. In particular, the map $\mathrm{H}^1(\Gamma, A^{(p^m)}(L)) \xrightarrow{\Phi_*^{(m)}} \mathrm{H}^1(\Gamma, \bar{A}^{(p^m)}(\mathbb{F}_L))$ induced from the reduction map is surjective. By the criterion (24), the order of the group $\widehat{B}^{(p^m)}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}^{(p^m)}(\mathcal{O}_L))$ is equal to that of $\mathrm{H}^1(\Gamma, \bar{A}(\mathbb{F}_L))$. But Corollary 2.6.2 says that $\hat{\mathrm{F}}^{(m)}$ induces an isomorphism

$$\widehat{B}^{(p^m)}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}^{(p^m)}(\mathcal{O}_L)) \xrightarrow{\sim} \widehat{B}(\mathcal{O}_K)/\mathrm{N}_{L/K}(\widehat{B}(\mathcal{O}_L)).$$

By the criterion (24) again, the map Φ_* is surjective.

In general, we choose an intermediate $\mathbb{Z}_p^e$-extension L_1/K of L/K so that the inertia subgroup of $\mathrm{Gal}(L_1/K)$ is of finite index and L/L_1 is unramified. Then we apply the commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^1(L_1/K, A(L_1)) & \hookrightarrow & \mathrm{H}^1(L/K, A(L)) \\ \downarrow & & \downarrow \Phi_* \\ \mathrm{H}^1(L_1/K, \bar{A}(\mathbb{F}_{L_1})) & = & \mathrm{H}^1(L/K, \bar{A}(\mathbb{F}_L)), \end{array}$$

where the first down-arrow is surjective and the identity is from the second part of (c).

3. The Selmer groups

In this section, we prove Theorem 4 and Theorem 5 by using Theorem 3. Let K be a global field of characteristic p and let L/K be a $\mathbb{Z}_p^d$-extension unramified outside a finite set S of places of K.

3.1. **The torsion points.** Let Γ_0 denote the stabilizer of $A(L)_{tor,p}$ for the action of $\Gamma := \mathrm{Gal}(L/K)$ and let L_0 denote the fixed field of Γ_0. We call a pro-p Galois extension pro-p cyclic if its Galois group is either finite cyclic or isomorphic to $\mathbb{Z}_p$.

Lemma 3.1.1. *Let the notation be as above. Assume that A has either good ordinary reduction or split multiplicative reduction at each place of S. Then there is a finite intermediate extension $K_0/K \subset L_0/K$ such that L_0/K_0 is a pro-p cyclic extension.*

Proof. Note that if A has good, ordinary reduction at a place v, then A/K_v is ordinary and hence K_vL_0 is unramified over K_v (Lemma 2.5.1(b)). Also, if A has split multiplicative reduction at some $v \in S$ so that $\Omega = \langle Q_1, ..., Q_g \rangle \subset (K_v)^g$ is the period lattice with $Q_i = (Q_{i,1}, ..., Q_{i,g})$, $Q_{i,j} \in K_v^*$, then

$$K_vL_0 \subset \overline{K_v} \cap \bigcup_{n=1}^{\infty} K_v(Q_{1,1}^{1/p^n}, ..., Q_{g,g}^{1/p^n}) = K_v.$$

This shows that L_0/K is everywhere unramified.

We then apply the global class field theory (cf. [Tat67]) which tells us that the Galois group $W_{K,p}$ of the maximal everywhere unramified pro-p abelian extension of K fits into an exact sequence

$$0 \longrightarrow C_{K,p} \longrightarrow W_{K,p} \xrightarrow{\deg} \mathbb{Z}_p \longrightarrow 0,$$

where $C_{K,p}$ is the p-Sylow subgroup of the class group of K and deg is induced from the degree map on the group of ideles. We choose a subgroup $W_0 \simeq \mathbb{Z}_p$ of $W_{K,p}$ and choose K_0 to be the fixed field of W_0 under the action of $W_{K,p}$ on L_0. □

3.2. **Cohomology groups of the torsion points.** In the next step, our goal is to bound, for $i = 1, 2$, the order of the cohomology group $\mathrm{H}^i(L'/K, A(L')_{tor,p})$, where L'/K is a finite intermediate field extension of some given $\mathbb{Z}_p^d$-extension. To achieve this goal, we first establish the following lemma in which G is a finite p-abelian group with d generators acting on a finite p-abelian group M. We assume that there is a subgroup $H_0 \subset G$ such that G/H_0 is cyclic and $M^{H_0} = M$. The following is similar to the estimate in [BL06].

Lemma 3.2.1. *Let the notation and conditions be as above. Then we have*

$$|\,\mathrm{H}^1(G, M)| \leq |M^G|^d \tag{25}$$

and

$$|\,\mathrm{H}^2(G, M)| \leq |M^G|^{d^2}. \tag{26}$$

Proof. Consider the inflation-restriction exact sequence:

$$0 \longrightarrow \mathrm{H}^1(G/H_0, M^{H_0}) \longrightarrow \mathrm{H}^1(G, M) \xrightarrow{res} \mathrm{H}^1(H_0, M)^{G/H_0}.$$

We shall bound the orders of $\ker(res)$ and $\mathrm{Im}(res)$. Since G/H_0 is cyclic, by computing the Herbrand quotient, we see that the order of $\mathrm{H}^1(G/H_0, M^{H_0})$ equals $|M^G/\mathcal{N}|$, where $\mathcal{N}$ is the image of the norm map $\mathrm{N}_{G/H_0} : M = M^{H_0} \longrightarrow M^G$. Also, since M is fixed by the action of H_0, we have

$$\mathrm{H}^1(H_0, M)^{G/H_0} = \mathrm{Hom}(H_0, M^G).$$

To proceed further, choose a basis $e_1, ..., e_c$ of G, for some $c \leq d$, so that $e_1' := p^m e_1, e_2, ..., e_c$, for some non-negative integer m, form a basis of H_0. The cocycle condition implies that if ρ is a 1-cocycle representing a class in $\mathrm{H}^1(G, M)$, then the value $\rho(e_1')$ equals $\mathrm{N}_{G/H_0}(\rho(e_1))$. This implies that the image of res must be contained in the subgroup

$$\{\phi \in \mathrm{Hom}(H_0, M^G) \mid \phi(e_1') \in \mathcal{N}\},$$

whose order is bounded by $|M^G|^{c-1} \cdot |\mathcal{N}|$. Therefore, the inequality (25) holds, since

$$|\ker(res)| \cdot |\,\mathrm{Im}(res)| \leq |M^G/\mathcal{N}| \cdot |M^G|^{c-1} \cdot |\mathcal{N}|.$$

We prove the inequality (26) by induction on d. The case where $d = 1$ is easy, since $\mathrm{H}^2(G, M) = M^G/N_G(M)$. If $d > 1$, we choose a cyclic subgroup $H_1 \subset H_0$ such that G/H_1 is generated by $d-1$ elements. According to the associated Hochschild-Serre spectral sequence (cf. [Sha72]), we have the exact sequences

$$0 \longrightarrow E_1^2 \longrightarrow \mathrm{H}^2(G, M) \longrightarrow \mathrm{H}^2(H_1, M)^{G/H_1}$$

and

$$\mathrm{H}^2(G/H_1, M^{H_1}) \longrightarrow E_1^2 \longrightarrow \mathrm{H}^1(G/H_1, \mathrm{H}^1(H_1, M)).$$

Therefore, the desired bound for the order of $\mathrm{H}^2(G, M)$ can be derived from the following lemma. □

Lemma 3.2.2. *Under the above assumptions, we have*

$$|\,\mathrm{H}^2(G/H_1, M^{H_1})| \leq |M^G|^{(d-1)^2}, \tag{27}$$

$$|\,\mathrm{H}^1(G/H_1, \mathrm{H}^1(H_1, M))| \leq |M^G|^{d-1}, \tag{28}$$

$$|\,\mathrm{H}^2(H_1, M)^{G/H_1}| \leq |M^G|^d. \tag{29}$$

Proof. The inequality (27) is in fact the induction hypothesis. To show (28), we first note that since H_1 is cyclic and acting trivially on M, the group $N := \mathrm{H}^1(H_1, M)$ satisfies $N^G = \mathrm{Hom}(H_1, M^G)$ and $|N^G| \leq |M^G|$. In view of this, we see that the inequality (25) for the pair $(G/H_1, N)$ implies (28).

Again, since H_1 is cyclic, acting trivially on M, we have

$$\mathrm{H}^2(H_1, M)^{G/H_1} = (M/p^l M)^{G/H_1},$$

where p^l is the order of H_1. To bound the order of this group, we consider the exact sequence

$$M^G \longrightarrow (M/p^l M)^{G/H_1} \longrightarrow \mathrm{H}^1(G/H_1, p^l M^G),$$

which is induced from

$$0 \longrightarrow p^l M \longrightarrow M \longrightarrow M/p^l M \longrightarrow 0.$$

We have

$$|\,\mathrm{H}^1(G/H_1, p^l M^G)| = |\,\mathrm{Hom}(G/H_1, p^l M^G)| \leq |M^G|^{d-1}.$$

□

Corollary 3.2.3. *Suppose that K is a local field of characteristic p, L/K is a $\mathbb{Z}_p^d$-extension and A/K is an abelian variety with good, ordinary reduction. Then for every finite intermediate extension $L'/K \subset L/K$ we have*

$$|\,\mathrm{H}^1(L'/K, A(L')_{tor,p})| \leq |A(K)_{tor,p}|^d$$

and

$$|\,\mathrm{H}^2(L'/K, A(L')_{tor,p})| \leq |A(K)_{tor,p}|^{d^2}.$$

Proof. Corollary 2.1.3(b) says that $A(L)_{tor,p}$ is unramified. Let L_0/K be the maximal unramified intermediate extension of L/K and put $G = \mathrm{Gal}(L'/K)$, $H_0 = \mathrm{Gal}(L'/L_0 \cap L')$. Then apply Lemma 3.2.1. □

Corollary 3.2.4. *Suppose that A, K, L satisfy the condition of* Lemma 3.1.1. *Let F/K be a finite intermediate extension of L/K. Then for every intermediate extension $L'/F \subset L/F$, the orders of $\mathrm{H}^1(L'/F, A(L')_{tor,p})$ and $\mathrm{H}^2(L'/F, A(L')_{tor,p})$ are bounded. Furthermore, if $d = 1$, then the bounds can be chosen to be independent of F.*

Proof. Let $K_0 \subset L_0 \subset L$ be as in Lemma 3.1.1. Without loss of generality, we may assume that $F = K$ for the proof of the first statement. Put $K_0' = L' \cap K_0$, $G = \mathrm{Gal}(L'/K_0')$ and $H_0 = \mathrm{Gal}(L'/L_0 \cap L')$. Obviously, $A(K_0')_{tor,p}$ is contained in $A(K_0)_{tor,p}$. Therefore, from Lemma 3.2.1 we see that for $j = 0, 1, 2$, the order of the $\mathrm{Gal}(K_0'/K)$-module $\mathrm{H}^j(L'/K_0', A(L')_{tor,p})$ is bounded by $|A(K_0)_{tor,p}|^{d^j}$, which is independent of L'. This implies that the orders $|\,\mathrm{H}^i(K_0'/K, \mathrm{H}^j(L'/K_0', A(L')_{tor,p}))|$, for $i + j = 1, 2$, are also bounded. Then we use the Hochschild-Serre spectral sequence

$$\mathrm{H}^i(K_0'/K, \mathrm{H}^j(L'/K_0', A(L')_{tor,p})) \Longrightarrow \mathrm{H}^{i+j}(L'/K, A(L')_{tor,p})$$

to verify the first statement.

Now consider the case where $d = 1$. Let K_n be the nth layer of L/K. Using the Herbrand quotient, we see that for $F = K_n$,

$$|\,\mathrm{H}^1(L'/F, A(L')_{tor,p})| = |\,\mathrm{H}^2(L'/F, A(L')_{tor,p})| \leq |A(K_n)_{tor,p}|.$$

This bound increases with n. To find a bound independent of n, we first note that $A(L)_{tor,p}$ is cofinitely generated over $\mathbb{Z}_p$ and consider the p-divisible part $A(L)_{tor,\infty}$ of $A(L)_{tor,p}$. Let T denote the finite quotient $A(L)_{tor,p}/A(L)_{tor,\infty}$, and let n_0 be a positive integer such that if $n \geq n_0$, then $A(K_n)_{tor,p}$ contains $A[p^2] \cap A(L)_{tor,p}$ and is sent surjectively onto T by the projection $A(L)_{tor,p} \longrightarrow T$.

Suppose $n \geq n_0$ and $Q \in A(K_n) \cap A(L)_{tor,\infty}$. Let $Q' \in A(L)_{tor,\infty}$ be such that $pQ' = Q$. Then for each $\sigma \in \mathrm{Gal}(L/K_n)$, the point $P_\sigma := {}^\sigma Q' - Q'$ is contained in $A[p] \cap A(L)_{tor,\infty} \subset A(K_n)$. Thus, the assignment $\sigma \mapsto P_\sigma$ gives rise to a $\xi_Q \in \mathrm{Hom}(\mathrm{Gal}(L/K_n), A[p])$. Then we have $p\xi_Q = 0$, and hence $P_\sigma = 0$ for $\sigma \in \mathrm{Gal}(L/K_{n+1})$. This shows that $Q' \in A(K_{n+1}) \cap A(L)_{tor,\infty}$.

Note that $A[p] \cap A(L)_{tor,\infty}$ is a subgroup of $p(A(K_n) \cap A(L)_{tor,\infty})$ and is contained in $\mathrm{N}_{K_{n+1}/K_n}(A(K_{n+1}) \cap A(L)_{tor,\infty})$. Also, Q can be expressed as the difference $\mathrm{N}_{K_{n+1}/K_n}(Q') - \sum_{\sigma \in \mathrm{Gal}(K_{n+1}/K_n)} P_\sigma$. Therefore, Q is contained in the intersection $\mathrm{N}_{K_{n+1}/K_n}(A(K_{n+1}) \cap A(L)_{tor,\infty})$. This shows that

$$A(K_n) \cap A(L)_{tor,\infty} \subset \mathrm{N}_{K_m/K_n}(A(K_m) \cap A(L)_{tor,\infty}), \text{ if } m \geq n.$$

Therefore, we have, for $F = K_n$, $L' = K_m$, $m \geq n \geq n_0$,

$$|\,\mathrm{H}^2(L'/F, A(L')_{tor,p})| = |A(K_n)_{tor,p}/\mathrm{N}_{K_m/K_n}(A(K_m)_{tor,p})| \leq |T|.$$

We can choose $|A(K_{n_0})_{tor,p}|$ as the desired bound, since it is an upper bound of $|T|$ and $|A(K_n)_{tor,p}|$ for $n \leq n_0$. □

3.3. **The proofs of Theorem 4 and Theorem 5.** We first prove Theorem 4. Let $S(F)$ denote the set of places of F sitting over S. Let L'/F be a finite intermediate extension of L/F and put $G = \mathrm{Gal}(L'/F)$. For $m = 1, 2, ..., \infty$, consider the restriction map

$$res_m : \mathrm{H}^1(F, \mathcal{A}[p^m]) \longrightarrow \mathrm{H}^1(L', \mathcal{A}[p^m])^G,$$

and define

$$\mathrm{Sel}_{p^\infty}(L'/F) := \{\eta \in \mathrm{H}^1(F, \mathcal{A}[p^\infty]) \mid res_\infty(\eta) \in \mathrm{Sel}_{p^\infty}(L')\}.$$

Then $\mathrm{Sel}_{p^\infty}(F) \subset \mathrm{Sel}_{p^\infty}(L'/F)$ and for the restriction map

$$res_{L'/F} : \mathrm{Sel}_{p^\infty}(F) \longrightarrow \mathrm{Sel}_{p^\infty}(L')^G,$$

we have the inequalities:

$$|\ker(res_{L'/F})| \leq |\ker(res_\infty)| \tag{30}$$

and

$$|\,\mathrm{coker}(res_{L'/F})| \leq |\,\mathrm{coker}(res_\infty)| \cdot |\,\mathrm{Sel}_{p^\infty}(L'/F) : \mathrm{Sel}_{p^\infty}(F)|. \tag{31}$$

For every m apply the Hochschild-Serre spectral sequence ([Mil80], p. 105)

$$\mathrm{H}^i(G, \mathrm{H}^j(L', \mathcal{A}[p^m])) \Longrightarrow \mathrm{H}^{i+j}(F, \mathcal{A}[p^m]).$$

The spectral sequence says that $\ker(res_m)$ equals $\mathrm{H}^1(G, \mathcal{A}[p^m](L'))$ and $\mathrm{coker}(res_m)$ is isomorphic to a subgroup of $\mathrm{H}^2(G, \mathcal{A}[p^m](L'))$. We have $\mathcal{A}[p^m](L') = A(L')[p^m]$, which equals $A(L')_{tor,p}$ for m large enough. By letting m go to ∞ and by applying Corollary 3.2.4, we conclude that the orders $|\ker(res_\infty)|$, $|\,\mathrm{coker}(res_\infty)|$ have finite upper bounds independent of L'. Also, if $d = 1$, these bounds can be chosen to be independent of F.

Consider the exact sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(F) \longrightarrow \mathrm{Sel}_{p^\infty}(L'/F) \longrightarrow \bigoplus_v \mathrm{H}^1(L_v/F_v, A(L_v)), \tag{32}$$

where in the right term v runs through all places of F. We have

$$I_{L'/F} := \mathrm{Sel}_{p^\infty}(L'/F)/\mathrm{Sel}_{p^\infty}(F) \subset \prod_v \mathrm{H}^1(L_v/F_v, A(L_v)). \tag{33}$$

It remains to show that the index $|I_{L'/K}|$ has an upper bound that is independent of L'.

Suppose that $v \notin S$ and let $\mathbb{F}_v$ denote the residue field. Then $L_v \subset \bar{K}_v^{un}$, the maximal unramified extension of K_v, and consequently, $\mathrm{H}^1(L_v/K_v, A(L_v))$ is a subgroup (through the inflation map) of $\mathrm{H}^1(\bar{K}_v^{un}/K_v, A(\bar{K}_v^{un}))$. Let $\pi_0(A)$ be the group of connected components of the special fiber of the Néron model of A at v and let m_v be the order of $\pi_0(A)^{\mathrm{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v)}$.

Lemma 3.3.1. *If L_v/K_v is unramified, then $|\mathrm{H}^1(L_v/K_v, A(L_v))| \leq m_v$. In particular, if A has good reduction at v, then the group $\mathrm{H}^1(L_v/K_v, A(L_v)) = 0$.*

Proof. By Proposition I.3.8, [Mil86], we have

$$\mathrm{H}^1(\bar{K}_v^{un}/K_v, A(\bar{K}_v^{un})) = \mathrm{H}^1(\bar{K}_v^{un}/K_v, \pi_0(A)).$$

Observe that for each finite unramified (and hence cyclic) extension K_v'/K_v the group order $|\mathrm{H}^1(K_v'/K_v, \pi_0(A))| = |\hat{\mathrm{H}}^0(K_v'/K_v, \pi_0(A))|$ is bounded by m_v. Then we see that m_v also bounds the order of $\mathrm{H}^1(\bar{K}_v^{un}/K_v, \pi_0(A))$, which is in fact the union of all $\mathrm{H}^1(K_v'/K_v, \pi_0(A))$. □

If v splits completely in L, then the cohomology group $\mathrm{H}^1(L_v/F_v, A(L_v))$ is trivial. We apply Theorem 3 (for $v \in S$) and conclude that

$$|I_{L'/F}| \leq \mathbf{B}_F := \prod_{v \in S(F)} |\bar{A}(\mathbb{F}_v)_p|^{d+1} \cdot \prod_{v \notin S(F)} m_v.$$

Here, in the second product, v runs through all the places not splitting completely in L. Therefore, the index $|I_{L'/K}|$ has a finite upper bound that is independent of L'. Since $\mathrm{coker}(res_{L/F})$ is the direct limit of $\mathrm{coker}(res_{L'/F})$, the first statement of Theorem 4 is proved. Moreover, if $d = 1$ and v_0 is a place of K not splitting completely in L, then the decomposition group of v_0 is a non-trivial closed subgroup of $\Gamma \simeq \mathbb{Z}_p$ with finite index, and hence the number of places of L sitting over v_0 is finite. This implies that the number of places of F sitting over v_0 is bounded as F varies. Therefore, the product $\mathbf{B}_F$ has an upper bound that is independent of F. This completes the proof of Theorem 4.

To prove Theorem 5, we use the Nakayama lemma. We need to show that for each finite intermediate extension $L'/K \subset L/K$, the order of the p-torsion subgroup of $\mathrm{coker}(res_{L'/K})$ is bounded. We apply Corollary 3.2.4 again and use an argument similar to the above. By (33), we reduce the proof to showing that the group $\prod_v \mathrm{H}^1(L_v/K_v, A(L_v))$ is co-finitely generated. By Theorem 3 and Lemma 3.3.1, we need to show that if A has split multiplicative reduction at $v \in S$, then the local cohomology group $\mathrm{H}^1(L_v/K_v, A(L_v))$ is co-finitely generated. For this, we use the exact sequence

$$0 \longrightarrow \Omega \longrightarrow ((L_v)^*)^g \longrightarrow A(L_v) \longrightarrow 0,$$

where $\Omega = \langle Q_1, ..., Q_g \rangle$ is the local period lattice. Hilbert's theorem 90 implies that $\mathrm{H}^1(L_v/K_v, A(L'_v))$ is isomorphic to a subgroup of

$$\mathrm{H}^2(\mathrm{Gal}(L_v/K_v), \Omega) \simeq \mathrm{H}^2(\mathrm{Gal}(L_v/K_v), \mathbb{Z}^g) \simeq \mathrm{H}^1(\mathrm{Gal}(L_v/K_v), (\mathbb{Q}/\mathbb{Z})^g).$$

Obviously, this group contains at most p^{dg} elements of order p.

References

[BL06] A. Bandini and I. Longhi, *Control theorems for elliptic curves over function fields,* International Journal of Number Theory **5**(2009), 229–256. MR2502807

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models,* Springer-Verlag, Berlin, Heidelberg, 1990. MR1045822 (91i:14034)

[Cho52] W.-L. Chow, *On the quotient variety of an abelian variety,* Proc. Natl. Acad. Sci., Vol. **38**(1952), 1039-1044. MR0052156 (14:580c)

[Ger72] L. Gerritzen, *On non-Archinedean representations of abelian varieties,* Math. Ann. **196**(1972), 323-346. MR0308132 (46:7247)

[GkR96] U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves,* J. reine angew. Math. **476**(1996), 27-93. MR1401696 (97f:11043)

[Gre03] R. Greenberg, *Galois theory for the Selmer group for an abelian variety,* Compositio Math. **136**(2003), 255-297. MR1977007 (2004c:11097)

[Gth72] A. Grothendieck, *Groupes de monodromie en Géométrie Algébrique.* I. Séminaire de Géométrie Algébrique du Bois-Marie 1967-1969 (SGA 7 I). Lecture Notes in Math. 288. Springer, Heidelberg, 1972. MR0354656 (50:7134)

[Jon91] J. Jones, *On the local norm map for abelian varieties with good ordinary reduction,* J. Algebra **138** no.2(2003), 420-423. MR1102817 (92d:11062)

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields,* Invent. Math. **18**(1972), 183-266. MR0444670 (56:3020)

[Mil70/72] J.S. Milne, *Weil-Chatelet groups over local fields,* Ann. Sci. Ecole Norm. Sup. **3** (1970), 273-284; ibid., **5** (1972), 261-264. MR0276249 (43:1996)

[Mil80] J.S. Milne, *Étale Cohomology,* Princeton University Press, Princeton, 1980. MR559531 (81j:14002)

[Mil86] J.S. Milne, *Arithmetic duality theorems,* Academic Press, New York, 1986. MR881804 (88e:14028)

[Mum68] D. Mumford, *Biextension of formal groups,* in the proceedings of the Bombay Colloquium on Algebraic Geometry, Tata Institute of Fundamental Research Studies in Mathematics 4, London, Oxford University Press, 1968.

[Mum74] D. Mumford, *Abelian Varieties,* Oxford Univ. Press, 1974. MR0282985 (44:219)

[LuR78] J. Lubin and M. Rosen, *The norm map for ordinary abelian varieties,* J. Algebra **52**(1978), 236-240. MR0491735 (58:10936)

[OTr06] T. Ochiai and F. Trihan, *On the Selmer groups of abelian varieties over function fields of characteristic $p > 0$,* Mathematical Proceedings Cambridge Philosophical Society **146**(2009), 23–43. MR2461865

[OTr08] T. Ochiai and F. Trihan, *On the Iwasawa main conjecture of abelian varieties over function fields of characteristic $p > 0$,* manuscript 2008.

[Sha72] S. Shatz, *Profinite Groups, Arithmetic, and Geometry.* Annals of Math. Studies **67**, Princeton University Press, Princeton, 1972. MR0347778 (50:279)

[Sch83] P. Schneider, *Iwasawa L-functions of abelian varieties over algebraic number fields. A first approach,* Invent. Math. **71** (1983), 251-293. MR689645 (85d:11063)

[Tat62] J. Tate, *Duality theorems in Galois cohomology over number fields,* Proc. Intern. Congress Math. Stockholm, 234-241.

[Tat67] J. Tate, *Global Class Field Theory.* In Algebraic Number Theory, J.W.S. Cassels and A. Frölich, eds., Academic Press, 1967, 162-203. MR0220697 (36:3749)

[Was82] L. Washington, *Introduction to Cyclotomic Fields,* Springer-Verlag, 1982. MR718674 (85g:11001)

Department of Mathematics, National Taiwan University, Taipei 10764, Taiwan
E-mail address: tan@math.ntu.edu.tw