COMPOSITIO MATHEMATICA

LI GUO

On a generalization of Tate dualities with application to Iwasawa theory

Compositio Mathematica, tome 85, n° 2 (1993), p. 125-161

<http://www.numdam.org/item?id=CM_1993__85_2_125_0>

Compositio Mathematica **85**: 125–161, 1993.

On a generalization of Tate dualities with application to Iwasawa theory

LI GUO*

Department of Mathematics, University of Washington, Seattle, WA98195

Received 8 April 1991; accepted 15 November 1991

Let E be an abelian variety defined over a number field K. Let p be a prime number. Let $Ш(K, E)_{p^\infty}$ be the p-Tate-Shafarevich group of E and $S^{\text{class}}_{E_{p^\infty}}(K)$ the p^∞-Selmer group of E. Thirty years ago, Tate proved a local duality theorem for E and used it to establish a global duality for E, later called Cassels-Tate pairing [3, 14]. It states that there is a pairing between $Ш(K, E)_{p^\infty}$ and the p-Tate-Shafarevich group $Ш(K, E^*)_{p^\infty}$ for the dual abelian variety E^* of E and that this pairing is nondegenerate modulo the maximal divisible subgroups. In terms of the Selmer groups, it states that there is a pairing between $S^{\text{class}}_{E_{p^\infty}}(K)$ and $S^{\text{class}}_{E^*_{p^\infty}}(K)$ which is nondegenerate modulo the maximal divisible subgroups.

Let $\{V_l\}$ be a compatible system of l-adic representations of $\text{Gal}(\bar{K}/K)$ which are ordinary at p. Let T_p be a $\text{Gal}(\bar{K}/K)$-invariant lattice of V_p and define $A = V_p/T_p$. R. Greenberg has recently defined the concept of a p^∞-Selmer group for such an A. This concept is a generalization of the classical Selmer group for an abelian variety with good, ordinary reduction or multiplicative reduction at p (Theorem 5). We will prove a local duality theorem (Theorem 1) for such an A and use it to construct a Cassels-Tate type pairing for Greenberg's general Selmer groups (Theorem 2).

Let K_∞ be any $\mathbb{Z}_p$-extension of K. Greenberg [5, 6] also defines a (strict) Selmer group $S^{\text{str}}_A(K_\infty)$ for a compatible system as above. Greenberg uses $S^{\text{str}}_A(K_\infty)$ and its nonstrict version to formulate his motivic Iwasawa theory. We will give an application of the general Cassels-Tate pairing to the study of $S^{\text{str}}_A(K_\infty)$ (Theorem 3).

After fixing some notations and conventions in Section 1, we will state the main theorems in Section 2. Theorem 1 will be proved in Section 3. The proof of Theorem 2 will be sketched in Section 4. We will also discuss some examples there. In Section 5 we prove the result on Greenberg's strict Selmer groups.

I wish to thank my advisor, R. Greenberg. He suggested this problem to me, and his encouragement and helpful conversations were essential to the completion of this work. I would like to thank M. Flach for sending his work [4] on the similar subject to us (see Section 2 for details) and would like to thank J. S. Milne for referring us to McCallum's related work [9] and for his well-written book [10] on this subject.

1. Notations and Conventions

We will use the following notation throughout this paper.

Let l, p be two primes of $\mathbb{Q}$. Let $K/\mathbb{Q}$ be a finite Galois extension, $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. For a prime v over l, let K_v be the completion of K at v and let $G_{K_v} = \mathrm{Gal}(\bar{K}_v/K_v)$. For any p-primary abelian group M, denote M_n for $\ker\{p^n: M \to M\}$ unless defined otherwise. M_{div} is used to denote its maximal divisible subgroup, and $M_{\mathrm{cot}} \cong M/M_{\mathrm{div}}$ is used to denote the cotorsion part. $M^\wedge$ is the Pontryagin dual of M. If M is moreover a discrete G_F-module, where $F = K$ or K_v, then for any integers r, s, the maps $M_r \hookrightarrow M_{r+s}$ and $p^n: M_{r+s} \to M_s$ induce maps $\phi_{r,r+s}: H^1(F, M_r) \to H^1(F, M_{r+s})$ and $\pi_{r+s,s}: H^1(F, M_{r+s}) \to H^1(F, M_s)$. Thus we have $\phi_{s,r+s} \circ \pi_{r+s,s} = p^r$ on $H^1(F, M_{r+s})$. Let I_v be the inertia subgroup of G_{K_v}, let $g_v = G_{K_v}/I_v$ be the Galois group for the maximal unramified extension of K_v. Let Frob_v be the Frobenius element which generates g_v as a profinite group. Thus $H^1(g_v, M^{I_v}) = M^{I_v}/(\mathrm{Frob}_v - \mathrm{id})M^{I_v}$. It can be regarded as a subgroup of $H^1(K_v, M)$ by the inflation map. We say that M is unramified at v if $M^{I_v} = M$.

The subject to study in the following will be a discrete G_K-module A such that $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^d$ as an abelian group. So $A_n \cong (\mathbb{Z}/p^n\mathbb{Z})^d$. Define $\phi_r = \varinjlim \phi_{r,r+s}$ when $s \to \infty$. For each $v|p$, we fix a G_{K_v}-submodule $F_v^+ A \subseteq A$ that is divisible. We use ε_∞ to denote the natural map $H^1(K_v, F_v^+ A) \to H^1(K_v, A)$ induced by $F_v^+ A \hookrightarrow A$. Let T_A be the Tate module of A and define $A^* = \mathrm{Hom}(T_A, \mathbb{Q}_p/\mathbb{Z}_p(1))$. We also choose $F_v^+ A^* = \mathrm{Hom}(T_{A/F_v^+ A}, \mathbb{Q}_p/\mathbb{Z}_p(1))$ for each $v|p$. It is a divisible G_{K_v}-submodule of A^*. It follows that under the pairing between $\mathrm{Hom}(T_A, \mathbb{Q}_p/\mathbb{Z}_p(1))$ and A^*, $T_{F_v^+ A}$ and $F_v^+ A^*$ are the exact annihilators of each other. Thus for any n, $A_n/F_v^+ A_n$ is dual to $F_v^+ A_n^*$ under the pairing $A_n \times A_n^* \to \mathbb{Q}/\mathbb{Z}(1)$. It can be easily checked that the operations $F_v^+(-), (-)_n, (-)^*$ on A are interchangeable, so we will ignore the order in which they are performed.

2. Statement of the main theorems

Let A be a divisible G_K-module as above. Consider a compatible system $V = \{V_l\}$ of l-adic representations of G_k (e.g., the l-adic homology of a motive) such that V_p is ordinary in the sense of [5]. Thus, for each $v|p$, there is a canonical subspace $F_v^+ V_p$ of V_p that is invariant under the action of G_{K_v}. Let T_p be a G_K-invariant lattice in V_p. Let $A = V_p/T_p$. Let $F_v^+ A$ be the image of $F_v^+ V$ in A. Then A is an example of such a G_K-module. The results below can be easily reformulated in terms of the compatible systems. But the setting here is purely Galois cohomological and might be applied to other situations.

DEFINITION 1. For each natural number n and prime v of K, define

$$E_{v,n} = \ker\{H^1(K_v, A_n) \to H^1(K_v, A)/H^1(g_v, A^{I_v})_{\mathrm{div}}\}, \text{ if } v \nmid p;$$

$$E_{v,n} = \ker\{H^1(K_v, A_n) \to H^1(K_v, A)/\varepsilon_\infty(H^1(K_v, F_v^+ A)_{\mathrm{div}})\}, \text{ if } v \mid p.$$

Here in each case the map is the composition of maps through $H^1(K_v, A)$.

The subgroup $E'_{v,n}$ of $H^1(K_v, A_n^*)$ is defined in the same way. For $v \mid p$, choose $F_v^+ A^* = \mathrm{Hom}(T_{A/F_v^+ A}, \mathbb{Q}_p/\mathbb{Z}_p(1))$ to be the divisible subgroup of A^* that is G_{K_v}-invariant.

THEOREM 1. $\{E_{v,n}\}$ *form a right exact duality system in the following sense*:

(1) (*right exactness*) *From the exact sequence*

$$0 \longrightarrow A_r \longrightarrow A_{r+s} \xrightarrow{p^r} A_s \longrightarrow 0,$$

we have the induced exact sequence

$$E_{v,r} \xrightarrow{\phi_{r,r+s}} E_{v,r+s} \xrightarrow{\pi_{r+s,s}} E_{v,s} \longrightarrow 0$$

for r, s large.

(2) (*local duality*) $E_{v,n}$ *and* $E'_{v,n}$ *are exactly the annihilators of each other under the Tate pairing*

$$H^1(K_v, A_n) \times H^1(K_v, A_n^*) \to \mathbb{Q}/\mathbb{Z}$$

for n large.

If A is unramified at a finite prime v, and $v \nmid p$, *then* (1) *and* (2) *are true for all r, s and n.*

Let $A = E_{p^\infty}$, where E/K is an abelian variety with good, ordinary reduction or multiplicative reduction at p. By Theorem 5, $E_{v,n} = E(K_v)/p^n E(K_v)$ if we regard the latter as a subgroup of $H^1(K_v, E_n)$ via the Kummer sequence

$$0 \to E(K_v)/p^n E(K_v) \to H^1(K_v, E_n) \to H^1(K_v, E)_n \to 0.$$

Thus (2) in the theorem is just the local Tate duality for E. In this case, (1) in the theorem is the trivial fact that the sequence

$$E(K_v)/p^r E(K_v) \xrightarrow{p^s} E(K_v)/p^{r+s} E(K_v) \to E(K_v)/p^s E(K_v) \to 0$$

is exact. This exactness is an essential property of E used to construct the Cassels-Tate pairing.

Let

$$S_A^{\mathrm{str}}(K) = \ker(H^1(K, A) \to \Pi_{v\nmid p} H^1(K_v, A)/H^1(g_v, A^{I_v})_{\mathrm{div}} \times \Pi_{v|p} H^1(K_v, A)/\varepsilon_\infty(H^1(K_v, F_v^+ A)_{\mathrm{div}}))$$

be the strict Selmer group over K defined by Greenberg.

THEOREM 2. *Assume that A is unramified at almost all primes of K. Then there is a canonical pairing*

$$\langle\ ,\ \rangle: S_A^{\mathrm{str}}(K) \times S_{A^*}^{\mathrm{str}}(K) \to \mathbb{Q}_p/\mathbb{Z}_p$$

whose kernel on either side is precisely the maximal divisible subgroup. If moreover there is a G_K-module isomorphism

$$\eta: A \to A^* = \mathrm{Hom}(T_A, \mathbb{Q}_p/\mathbb{Z}_p(1))$$

such that $(\eta a)(a) = 0$ for $a \in A$, then this pairing induces a skew-symmetric pairing on $S_A^{\mathrm{str}}(K)$.

A classical example of A in Theorem 2 is $A = E_{p^\infty}$ where E is an elliptic curve over K with good, ordinary reduction or multiplicative reduction at p. For any abelian variety E with such reduction at p, fix a divisor D on A rational over K, and let $\phi_D: E \to E^*$ be the induced isogeny. Restricted to E_{p^∞}, the map ϕ_D gives a map $\eta_p: E_{p^\infty} \to E_{p^\infty}^*$ such that $(\eta_p(a))(a) = 0$ for $a \in A$. The map η_p is actually an isomorphism for almost all p since ϕ_D has finite kernel. Thus the conclusion of Theorem 2 is true for $A = E_{p^\infty}$ for almost all p. See Section 4 for more details and other examples.

Let K_∞ be any $\mathbb{Z}_p$-extension of K. Let

$$S_A^{\mathrm{str}}(K_\infty) = \ker(H^1(K_\infty, A) \to \Pi_{\lambda\nmid p} H^1(I_\lambda, A) \times \Pi_{\lambda|p} H^1((K_\infty)_\lambda, A/F_v^+ A)).$$

be the strict Selmer group over K_∞ defined by Greenberg in [5]. We have the following application of Theorem 2.

THEOREM 3. *Let $p \neq 2$. With the same setting as in Theorem 2 and with the additional assumption that $S_A^{\mathrm{str}}(K_\infty)$ is Λ-cotorsion and that $A(K_\infty)$ is finite, we have*

$$\mathrm{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_\infty) \equiv \mathrm{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K) (\mathrm{mod}\ 2).$$

If $A = E_{p^\infty}$, where E is an elliptic curve over $\mathbb{Q}$ with complex multiplication

and with good, ordinary reduction at p, and if K_∞ is the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$, then the conditions in Theorem 3 are satisfied by Proposition 2 of [6], Theorem 4.4 of [11] and Proposition 6.12 of [8]. Further, by Theorem 5, $S^{\text{class}}_{E_p^\infty}(K) = S^{\text{str}}_{E_p^\infty}(K)$ in this case. Thus a consequence of Theorem 3 is

$$\text{corank}_{\mathbb{Z}_p} S^{\text{class}}_{E_p^\infty}(\mathbb{Q}_\infty) \equiv \text{corank}_{\mathbb{Z}_p} S^{\text{class}}_{E_p^\infty}(\mathbb{Q}) (\text{mod } 2).$$

There are other applications of Theorem 2 and Theorem 3. We plan to discuss them in a subsequent paper.

M. Flach [4] has proved a result similar to Theorem 2. The generalization given here, excluding the skew-symmetric property, was obtained before we knew his work. The skew-symmetric property was proved by combining the methods used in his paper and McCallum's paper [9]. There are differences between the two generalizations. Flach's result generalizes the Cassels-Tate pairing for an abelian variety with any kind of reduction at p while the approach here only generalizes for an abelian variety with good, ordinary reduction or multiplicative reduction at p though these are the most interesting cases in connection with Iwasawa theory. On the other hand, as indicated before, the setting and method here is purely Galois cohomological and might be applied to other cases. Flach's work is based on the theory of Fontaine and Bloch-Kato [1] which was not known to us before. In particular, the local theory had been formulated in his case. The approach here is self-contained, starting from the local theory. Once the local theory is established, the global result can be proved by a method analogous to that used to prove the classical case. In both cases, the idea of the classical proof given in [10] is adapted to the generalized situations.

3. The local theory

We prove Theorem 1 in this section. The proof is divided into three parts. The right exactness is proved in Section 3.1. To prove the local duality, we first shown in Section 3.2, that $E_{v,n}$ and $H^1(K_v, A_n^*)/E'_{v,n}$ have the same order. Then it is proved in Section 3.3 that $E_{v,n}$ and $E'_{v,n}$ annihilate each other under the Tate pairing

$$H^1(K_v, A_n) \times H^1(K_v, A_n^*) \to \mathbb{Q}/\mathbb{Z}.$$

Now the local duality follows since the Tate pairing is nondegenerate.

Recall that for each n we define

$$E_{v,n} = \ker\{H^1(K_v, A_n) \xrightarrow{\phi_n} H^1(K_v, A) \to H^1(K_v, A)/H^1(g_v, A^{I_v})_{\mathrm{div}}\}, \text{ if } v \nmid p;$$

$$E_{v,n} = \ker\{H^1(K_v, A_n) \xrightarrow{\phi_n} H^1(K_v, A) \to H^1(K_v, A)/\varepsilon_\infty(H^1(K_v, F_v^+ A)_{\mathrm{div}})\}, \text{ if } v \mid p.$$

If v is an archimedean prime of K, then $|G_{K_v}| = 1$ or 2, hence $H^1(K_v, A)$ is finite and $H^1(g_v, A^{I_v})_{\mathrm{div}} = 0$. Thus $E_{v,n} = \ker(H^1(K_v, A_n) \to H^1(K_v, A))$.

If A is nonarchimedean and is unramified at v, then $A^{I_v} = A$. Hence $H^2(g_v, -)$ being zero implies that $H^1(g_v, A)$ is divisible. Since $H^0(g_v, A^{I_v}) = H^0(K_v, A)$, we have

$$0 \to H^0(K_v, A)/p^n H^0(K_v, A) \to H^1(g_v, A_n) \to H^1(g_v, A^{I_v})_n \to 0.$$

Thus $H^1(g_v, A_n) = E_{v,n}$ for all n if v is nonarchimedean and does not divide p.

3.1. Proof of the right exactness

We will prove the following more general result.

PROPOSITION 1. *Let D be a divisible subgroup of $H^1(K_v, A)$ and define*

$$J_n = \ker\{H^1(K_v, A_n) \to H^1(K_v, A) \to H^1(K_v, A)/D\}.$$

Then from the exact sequence $0 \to A_r \to A_{r+s} \xrightarrow{p^r} A_s \to 0$, we have the induced exact sequence,

$$J_r \xrightarrow{\phi_{r,r+s}} J_{r+s} \xrightarrow{\pi_{r+s,s}} J_s \to 0$$

for r, s large.

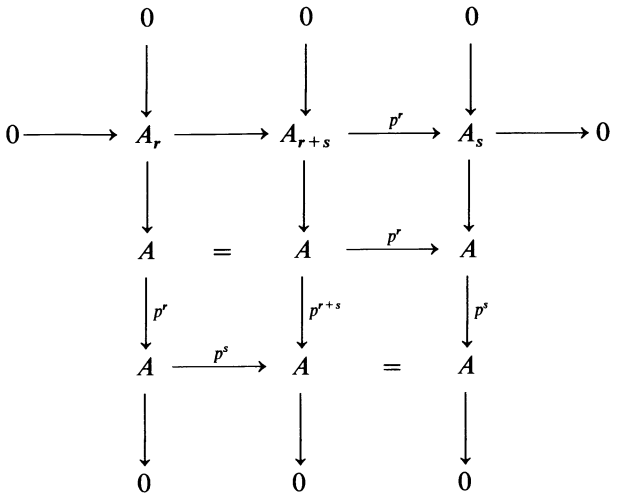
We start with a simple lemma.

LEMMA 1. *If M is a cofinitely generated torsion $\mathbb{Z}_p$-module, then for any m and any $n \geqslant |M/M_{\mathrm{div}}|$ we have $p^n M = M_{\mathrm{div}}$ and $p^n M_{m+n} = (M_{\mathrm{div}})_m$.*

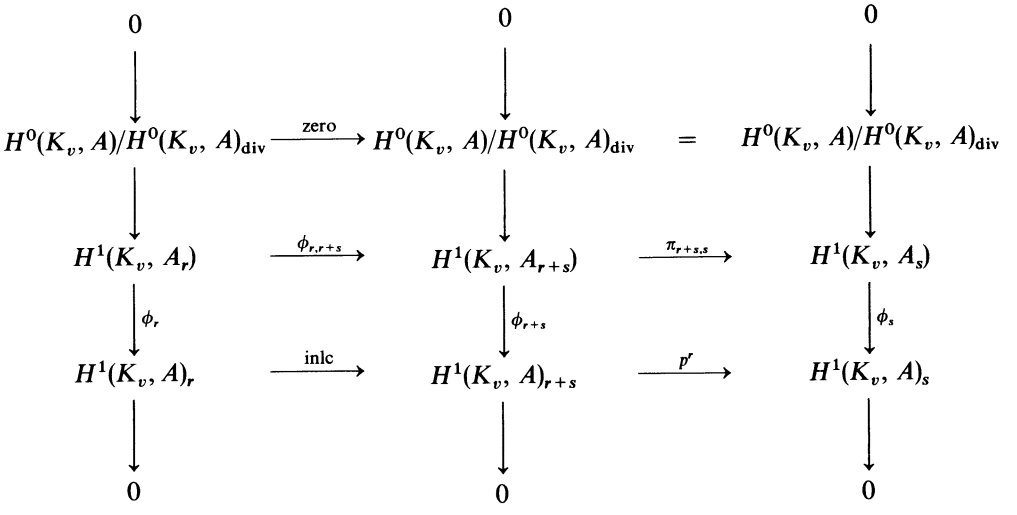
Proof. This is clear since $M \cong M_{\mathrm{div}} \oplus M/M_{\mathrm{div}}$ and $M_{n+m} \cong (M_{\mathrm{div}})_{n+m} \oplus M/M_{\mathrm{div}}$ for $n \geqslant |M/M_{\mathrm{div}}|$. □

Proof of Proposition. Choose r, $s \geqslant N$ with $p^N \geqslant |H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}}|$.

Then $p^r H^0(K_v, A) = p^s H^0(K_v, A) = H^0(K_v, A)_{\text{div}}$. In the commutative diagram,

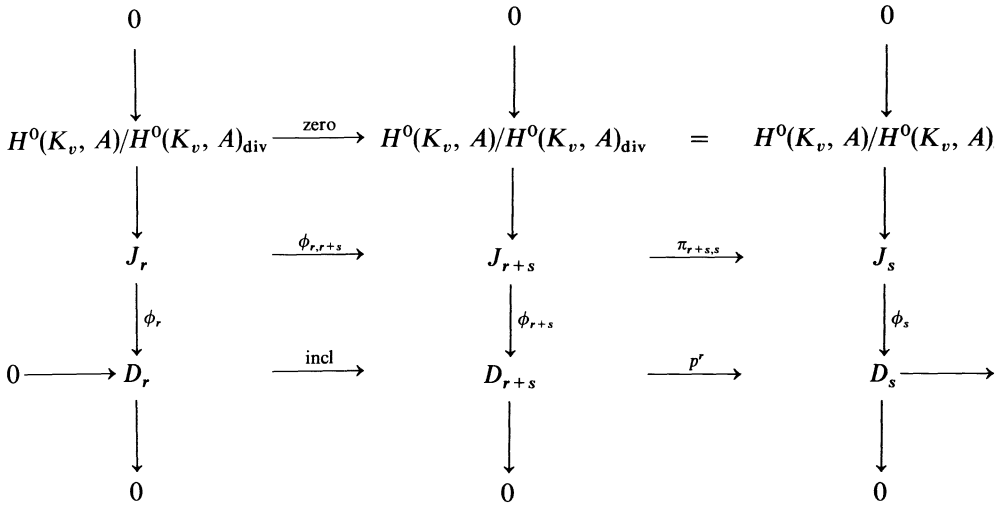


we have exact columns and exact upper row. Thus we have the induced commutative diagram for cohomology groups,



with exact columns and exact central row. From this diagram we can extract the

commutative diagram with exact columns,



Now the lower row is exact because of the divisibility of D. Since

$$H^1(K_v, A_r) \xrightarrow{\phi_{r,r+s}} H^1(K_v, A_{r+s}) \xrightarrow{\pi_{r+s,s}} H^1(K_v, A_s)$$

is exact, the middle row $J_r \xrightarrow{\phi_{r,r+s}} J_{r+s} \xrightarrow{\pi_{r+s,s}} J_s$ is zero. So $\phi_{r,r+s}(J_r) \subseteq \ker(\pi_{r+s}: J_{r+s} \to J_s)$. Applying the snake lemma to the left half and right half of the diagram, we have

$$|J_{r+s}/\phi_{r,r+s}(J_r)| = |H^0(K_v, A)/H^0(K_v, A)_{\text{div}}||D_s| = |J_s|$$

and that $\pi_{r+s}: J_{r+s} \to J_s$ is onto. Hence $|\phi_{r,r+s}(J_r)| = |\ker(\pi_{r+s}: J_{r+s} \to J_s)|$. Thus the middle row must be exact at J_{r+s}, hence $J_r \xrightarrow{\phi_{r,r+s}} J_{r+s} \xrightarrow{\pi_{r+s,s}} J_s \to 0$ is exact. □

The first part of Theorem 1 follows if we let $D = H^1(g_v, A^{I_v})_{\text{div}}$ when $v \nmid p$ and let $D = \varepsilon_\infty(H^1(K_v, F_v^+ A)_{\text{div}})$ when $v \mid p$.

If A is unramified at a finite prime v and $v \nmid p$, then $E_{v,n} = H^1(g_v, A_n)$ for any n by the remark after Definition 1. Since the sequence

$$H^1(g_v, A_r) \to H^1(g_v, A_{r+s}) \to H^1(g_v, A_s) \to 0.$$

is exact for all r and s, the sequence

$$E_{v,r} \to E_{v,r+s} \to E_{v,s} \to 0$$

is exact for all r and s. This completes the proof of the right exact property.

Next we prove the duality property in the theorem. When v is archimedean, it has been proved in [5, p. 129]. So in the following we will assume that v is a finite prime of K.

3.2. A characteristic formula

Let n be any positive integer.

LEMMA 2. $|H^0(K_v, A)_n| = |H^0(K_v, A)/p^nH^0(K_v, A)||(H^0(K_v, A)_{\mathrm{div}})_n|$.

Proof. Since $H^0(K_v, A)$ is cofinitely generated over $\mathbb{Z}_p$, we have $H^0(K_v, A) = H^0(K_v, A)_{\mathrm{div}} \oplus X$ for some finite X. So $H^0(K_v, A)_n = (H^0(K_v, A)_{\mathrm{div}})_n \oplus X_n$. Since X is finite, $|X_n| = |X/p^nX|$. Since $H^0(K_v, A)_{\mathrm{div}}$ is divisible, $H^0(K_v, A)/p^nH^0(K_v, A) = X/p^nX$, hence the lemma. □

We will prove the following result which will be used in the proof of the local duality.

PROPOSITION 2. (*characteristic formula*)

$$|E_{v,n}||E'_{v,n}| = |H^1(K_v, A_n)| = |H^1(K_v, A_n^*)|.$$

Proof. First consider $v \nmid p$. Let $D = H^1(g_v, A^{I_v})_{\mathrm{div}}$, by definition we have the exact sequence,

$$0 \to H^0(K_v, A)/p^nH^0(K_v, A) \to E_{v,n} \to D_n \to 0.$$

Thus $|E_{v,n}| = |H^0(K_v, A)/p^nH^0(K_v, A)||D_n|$. Being cyclic, g_v has cohomological dimension 1. So

$$\begin{aligned}\mathrm{corank}_{\mathbb{Z}_p} D &= \mathrm{corank}_{\mathbb{Z}_p}(H^1(g_v, A^{I_v})) = \mathrm{corank}_{\mathbb{Z}_p}(H^0(g_v, A^{I_v})) \\ &= \mathrm{corank}_{\mathbb{Z}_p}(H^0(K_v, A)).\end{aligned}$$

Hence $|D_n| = |(H^0(K_v, A)_{\mathrm{div}})_n|$. Thus from Lemma 2 we have

$$|E_{v,n}| = |H^0(K_v, A)_n| = |H^0(K_v, A_n)|.$$

Similarly,

$$|E'_{v,n}| = |H^0(K_v, A_n^*)| = |H^2(K_v, A_n)|.$$

Hence $|H^1(K_v, A_n)| = |E_{v,n}||E'_{v,n}| = |H^1(K_v, A_n^*)|$ by Tate's characteristic formula.

Now consider $v \mid p$. Let $D = \varepsilon_\infty(H^1(K_v, F_v^+ A)_{\text{div}})$. From the exact sequence of $\mathbb{Z}_p$-cofinitely generated abelian groups

$$0 \to H^0(K_v, F_v^+ A) \to H^0(K_v, A) \to H^0(K_v, (A/F_v^+ A))$$
$$\to H^1(K_v, F_v^+ A) \to \text{im}(\varepsilon_\infty) \to 0$$

and $\text{corank}_{\mathbb{Z}_p} H^1(K_v, F_v^+ A)_{\text{div}} = \text{corank}_{\mathbb{Z}_p} H^1(K_v, F_v^+ A)$, we have

$$\begin{aligned}\text{corank}_{\mathbb{Z}_p}(D) &= \text{corank}_{\mathbb{Z}_p}(\text{im}(\varepsilon_\infty)) \\ &= \text{corank}_{\mathbb{Z}_p}(H^1(K_v, F_v^+ A)) - \text{corank}_{\mathbb{Z}_p}(H^0(K_v, (A/F_v^+ A))) \\ &\quad + \text{corank}_{\mathbb{Z}_p}(H^0(K_v, A)) - \text{corank}_{\mathbb{Z}_p}(H^0(K_v, F_v^+ A)).\end{aligned}$$

By Tate characteristic formula,

$$\begin{aligned}\text{corank}_{\mathbb{Z}_p}(H^1(K_v, F_v^+ A)) &= [K_v : \mathbb{Q}_p]\text{corank}_{\mathbb{Z}_p} F_v^+ A \\ &\quad + \text{corank}_{\mathbb{Z}_p}(H^0(K_v, F_v^+ A)) \\ &\quad + \text{corank}_{\mathbb{Z}_p}(H^2(K_v, F_v^+ A)).\end{aligned}$$

Hence

$$\begin{aligned}\text{corank}_{\mathbb{Z}_p}(D) &= [K_v : \mathbb{Q}_p]\text{corank}_{\mathbb{Z}_p}(F_v^+ A) + \text{corank}_{\mathbb{Z}_p}(H^0(K_v, A)) \\ &\quad + \text{corank}_{\mathbb{Z}_p}(H^2(K_v, F_v^+ A)) - \text{corank}_{\mathbb{Z}_p}(H^0(K_v, (A/F_v^+ A))).\end{aligned}$$

By the definition of $E_{v,n}$

$$\begin{aligned}|E_{v,n}| &= |H^0(K_v, A)/p^n H^0(K_v, A)||D_n| \\ &= |H^0(K_v, A)p^n H^0(K_v, A)|p^{n\,\text{corank}_{\mathbb{Z}_p}(D)} \\ &= |H^0(K_v, A_n)\| F_v^+ A_n|^{[K_v : \mathbb{Q}_p]} p^{n(\text{corank}_{\mathbb{Z}_p} H^2(K_v, F_v^+ A) - \text{corank}_{\mathbb{Z}_p} H^0(K_v, (A/F_v^+ A)))}\end{aligned}$$

Since $|H^0(K_v, A_n)| = |H^0(K_v, A)_n| = |H^0(K_v, A)/p^n H^0(K_v, A)|p^{n\,\text{corank}_{\mathbb{Z}_p} H^0(K_v, A)}$ by Lemma 2. On the dual side, for A^*, we have

$$|E'_{v,n}| = |H^0(K_v, A_n^*)||F_v^+ A_n^*|^{[K_v : \mathbb{Q}_p]} p^{n(\text{corank}_{\mathbb{Z}_p} H^2(K_v, F_v^+ A^*) - \text{corank}_{\mathbb{Z}_p} H^0(K_v, A^*/F_v^+ A^*))}.$$

Since $A_n/F_v^+ A_n$ is dual to $F_v^+ A_n^*$ under the pairing $A_n \times A_n^* \to \mathbb{Q}_p/\mathbb{Z}_p(1)$, Tate's duality theorem says that $H^0(K_v, A_n/F_v^+ A_n)$ is dual to $H^2(K_v, F_v^+ A_n^*)$. This implies that $\text{corank}_{\mathbb{Z}_p} H^0(K_v, A/F_v^+ A) = \text{corank}_{\mathbb{Z}_p} H^2(K_v, F_v^+ A^*)$. Similarly,

$\operatorname{corank}_{\mathbb{Z}_p} H^0(K_v, A^*/F_v^+ A^*) = \operatorname{corank}_{\mathbb{Z}_p} H^2(K_v, F_v^+ A)$. Thus

$$\begin{aligned}|E_{v,n}||E'_{v,n}| &= |H^0(K_v, A_n)||H^0(K_v, A_n^*)|(|F_v^+ A_n||F_v^+ A_n^*|)^{[K_v:\mathbb{Q}_p]} \\ &= |H^0(K_v, A_n)||H^2(K_v, A_n)||A_n|^{[K_v:\mathbb{Q}_p]} \\ &= |H^1(K_v, A_n)| = |H^1(K_v, A_n^*)|.\end{aligned}$$

This completes the proof of Proposition 2.

3.3. Proof of the local duality

We consider two cases.

3.3.1. *The case when* $v \nmid p$

Consider the following commutative diagram,

$$\begin{array}{ccccc} H^1(g_v, (A^{I_v})_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(g_v, (A^{I_v})_n) & \longrightarrow & H^1(K_v, A_n) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(g_v, A^{I_v})_{2n} & \xrightarrow{p^n} & H^1(g_v, A^{I_v})_n & \longrightarrow & H^1(K_v, A)_n \end{array} \tag{1}$$

Since A is cofinitely generated over $\mathbb{Z}_p$, so is A^{I_v}. Thus $H^1(g_v, A^{I_v}) \cong A^{I_v}/(Frob_v - \mathrm{id})A^{I_v}$ is cofinitely generated over $\mathbb{Z}_p$. So by Lemma 1, for large n with $n \geqslant \max\{|H^1(g_v, A^{I_v})/H^1(g_v, A^{I_v})_{\mathrm{div}}|, |A^{I_v}/(A^{I_v})_{\mathrm{div}}|\}$, we have $p^n H^1(g_v, A^{I_v}) = H^1(g_v, A^{I_v})_{\mathrm{div}}$ and $p^n H^1(g_v, A^{I_v})_{2n} = (H^1(g_v, A^{I_v})_{\mathrm{div}})_n$. Also the exact sequence $0 \to (A^{I_v})_{2n} \to A^{I_v} \xrightarrow{p^{2n}} (A^{I_v})_{\mathrm{div}} \to 0$ and $A^{I_v} = (A^{I_v})_{\mathrm{div}} \oplus (A^{I_v})_{\mathrm{cot}}$ give surjective map $H^1(g_v, A^{I_v}) \to H^1(g_v, (A^{I_v})_{\mathrm{div}})$ and injective map $H^1(g_v, (A^{I_v})_{\mathrm{div}}) \to H^1(g_v, A^{I_v})$. Thus $H^1(g_v, (A^{I_v})_{2n}) \to H^1(g_v, A^{I_v})_{2n}$ is onto. Therefore in the diagram (1), the diagonal map $\Delta: H^1(g_v, (A^{I_v})_{2n}) \to H^1(K_v, A)_n$ has image $(H^1(g_v, A^{I_v})_{\mathrm{div}})_n$. Thus by the definition of $E_{v,n}$,

$$\begin{aligned} E_{v,n} &= \operatorname{im}(H^1(g_v, (A^{I_v})_{2n}) \xrightarrow{\pi_{2n,n}} H^1(g_v, (A^{I_v})_n) \to H^1(K_v, A_n)) \\ &\quad + \ker(H^1(K_v, A_n) \to H^1(K_v, A)_n) \\ &= \operatorname{im}(H^1(g_v, (A^{I_v})_{2n}) \xrightarrow{\pi_{2n,n}} H^1(g_v, (A^{I_v})_n) \to H^1(K_v, A_n)) \\ &\quad + \operatorname{im}(H^0(K_v, A) \xrightarrow{\partial} H^1(K_v, A_n)), \end{aligned}$$

where ∂ is the boundary map. Similarly,

$$E'_{v,n} = \mathrm{im}(H^1(g_v, (A^*)^{I_v}_{2n}) \xrightarrow{\pi_{2n,n}} H^1(g_v, (A^*)^{I_v}_n \to H^1(K_v, A^*_n))$$

$$+ \mathrm{im}(H^0(K_v, A^*) \xrightarrow{\partial} H^1(K_v, A^*_n)).$$

From Proposition 2 $|E_{v,n}| = |H^1(K_v, A^*_n)|/|E'_{v,n}|$. Therefore, to prove that $E_{v,n}$ and $E'_{v,n}$ are the exact annihilator of each other under the pairing $H^1(K_v, A_n) \times H^1(K_v, A^*_n) \to \mathbb{Q}_p/\mathbb{Z}_p$, We only need to show that they annihilate each other, that is, that the composition map $E_{v,n} \to H^1(K_v, A_n) \cong H^1(K_v, A^*_n)^\wedge \to (E'_{v,n})^\wedge$ is zero, where for a finite group X, $X^\wedge$ is the Pontryagin dual of X. By our descriptions of $E_{v,n}$ and $E'_{v,n}$ above, this means that the composition map

$$H^1(g_v, A^{I_v}_{2n}) \oplus H^0(K_v, A) \xrightarrow{\pi_{2n,n} \oplus \partial} H^1(K_v, A_n)$$

$$\cong H^1(K_v, A^*_n)^\wedge \xrightarrow{\widehat{(\pi_{2n,n} \oplus \partial)}} (H^1(g_v, (A^*)^{I_v}_{2n}) \oplus H^0(K_v, A^*))^\wedge$$

is zero. As $(H^1(g_v, (A^*)^{I_v}_{2n}) \oplus H^0(K_v, A^*))^\wedge \cong H^1(g_v, (A^*)^{I_v}_{2n})^\wedge \oplus H^0(K_v, A^*)^\wedge$, the proof can be accomplished in the following four steps,

(1) The map $H^0(K_v, A) \xrightarrow{\partial} H^1(K_v, A_n) \cong H^1(K_v, A^*_n)^\wedge \xrightarrow{\hat{\partial}} H^0(K_v, A^*)^\wedge$ is zero.

For n large we have $p^n H^0(K_v, A) = H^0(K_v, A)_{\mathrm{div}}$. Hence we have the commutative diagram of exact sequences,

$$\begin{array}{ccccccc}
H^0(K_v, A_{2n}) & \xrightarrow{p^n} & H^0(K_v, A_n) & \longrightarrow & X & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \| & & \\
H^0(K_v, A) & \xrightarrow{p^n} & H^0(K_v, A) & \longrightarrow & X & \longrightarrow & 0
\end{array}$$

Thus $\mathrm{im}(\partial: H^0(K_v, A) \to H^1(K_v, A_n)) = \mathrm{im}(\partial: H^0(K_v, A_n) \to H^1(K_v, A_n)) \cong X$. The same applies to A^*. So we only need to show that the map $H^0(K_v, A_n) \xrightarrow{\partial} H^1(K_v, A_n) \cong H^1(K_v, A^*_n)^\wedge \xrightarrow{\hat{\partial}} H^0(K_v, A^*_n)^\wedge$ is zero. But the map fits into the commutative diagram,

$$\begin{array}{ccccc}
H^0(K_v, A_n) & \xrightarrow{\partial} & H^1(K_v, A_n) & \xrightarrow{\partial} & H^2(K_v, A_n) \\
 & & \downarrow \cong & & \downarrow \cong \\
 & & H^1(K_v, A^*_n)^\wedge & \xrightarrow{\hat{\partial}} & H^0(K_v, A^*_n)^\wedge
\end{array}$$

where the vertical maps are from Tate's local duality. To prove that the top row is zero, consider the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{2n} & \longrightarrow & A_{3n} & \xrightarrow{p^{2n}} & A_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \| & & \\ 0 & \longrightarrow & A_n & \longrightarrow & A_{2n} & \xrightarrow{p^n} & A_n & \longrightarrow & 0 \end{array}$$

In the induced cohomological diagram we have the commutative square

$$\begin{array}{ccc} H^0(K_v, A_n) & \xrightarrow{\partial} & H^1(K_v, A_{2n}) \\ \| & & \downarrow{\scriptstyle \pi_{2n,n}} \\ H^0(K_v, A_n) & \xrightarrow{\partial} & H^1(K_v, A_n) \end{array}$$

from which we get

$$\begin{aligned} &\operatorname{im}(\partial: H^0(K_v, A_n) \to H^1(K_v, A_n)) \\ &\quad \subseteq \operatorname{im}(\pi_{2n,n}: H^1(K_v, A_n) \to H^2(K_v, A_n)) \\ &\quad = \ker(\partial: H^1(K_v, A_n) \to H^2(K_v, A_n)). \end{aligned}$$

Hence the top row is zero and (1) is proved.

(2) The map

$$\begin{aligned} &H^1(g_v, A_{2n}^{I_v}) \xrightarrow{\pi_{2n,n}} H^1(g_v, A_n^{I_v}) \to H^1(K_v, A_n) \\ &\quad \cong H^1(K_v, A_n^*)^\wedge \to H^0(K_v, A^*)^\wedge \end{aligned}$$

is zero.

For the same reason as in (1), we only need to prove that the map

$$H^1(g_v, A_{2n}^{I_v}) \xrightarrow{\pi_{2n,n}} H^1(g_v, A_n^{I_v}) \to H^1(K_v, A_n) \to H^2(K_v, A_n)$$

is zero. But the map fits into the commutative diagram,

$$\begin{array}{ccccc} H^1(g_v, A_{2n}^{I_v}) & \xrightarrow{\pi_{2n,n}} & H^1(g_v, A_n^{I_v}) & & \\ \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \\ H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(K_v, A_n) & \longrightarrow & H^2(K_v, A_n), \end{array}$$

where the bottom row is exact. This proves (2).

(3) The map

$$H^1(g_v, A_{2n}^{I_v}) \xrightarrow{\pi_{2n,n}} H^1(g_v, A_n^{I_v}) \to H^1(K_v, A_n)$$

$$\cong H^1(K_v, A_n^*)^\wedge \to H^1(g_v, (A^*)_n^{I_v})^\wedge \xrightarrow{\hat{\pi}_{2n,n}} H^1(g_v, (A^*)_{2n}^{I_v})^\wedge$$

is zero.

This is clear since

$$H^1(g_v, A_n^{I_v}) \to H^1(K_v, A_n) \cong H^1(K_v, A_n^*)^\wedge \to H^1(g_v, (A^*)_n^{I_v})^\wedge$$

is already zero, as shown by Greenberg in [5, p. 113].

(4) The map

$$H^0(K_v, A) \xrightarrow{\partial} H^1(K_v, A_n)$$

$$\cong H^1(K_v, A_n^*)^\wedge \to H^1(g_v, (A^*)_n^{I_v})^\wedge \xrightarrow{\hat{\pi}_{2n,n}} H^1(g_v, (A^*)_{2n}^{I_v})^\wedge$$

is zero.

As in (1), we can replace $H^0(K_v, A)$ by $H^0(K_v, A_n)$ and the rest of the proof is the same as for 2).

If A is unramified at v, then $E_{v,n} = H^1(g_v, A_n)$ for all n by the remark after Definition 1. Also, $E'_{v,n} = H^1(g_v, A_n^*)$ for all n. Thus the result follows from the fact that $H^1(g_v, A_n)$ and $H^1(g_v, A_n^*)$ are the duals of each other under the local Tate pairing.

Now the proof of local duality for $v \nmid p$ is completed.

3.3.2. *The case when* $v \mid p$

Now we assume that $v \mid p$. We define the maps ϕ_n, ϕ_n^+, ε_n, ε_∞ to be the natural maps in the following diagram,

$$\begin{array}{ccc} H^1(K_v, F_v^+ A_n) & \xrightarrow{\varepsilon_n} & H^1(K_v, A_n) \\ \downarrow{\scriptstyle \phi_n^+} & & \downarrow{\scriptstyle \phi_n} \\ H^1(K_v, F_v^+ A) & \xrightarrow{\varepsilon_\infty} & H^1(K_v, A). \end{array}$$

Let D^+ be the maximal divisible subgroup of $H^1(K_v, F_v^+A)$, and set $D = \varepsilon_\infty(D^+)$. By definition, $E_{v,n} = (\phi_n)^{-1}(D)$.

As in the case when $v \nmid p$, we first express $E_{v,n}$ as the image of a proper map. Since $H^1(K_v, F_v^+A_n)$ is finite, $H^1(K_v, F_v^+A)_n$ is finite. Hence $H^1(K_v, F_v^+A)$ is cofinitely generated as $\mathbb{Z}_p$-module. By Lemma 1 $p^nH^1(K_v, F_v^+A)_{3n} = D_{2n}^+$ for $p^n \geqslant |H^1(K_v, F_v^+A)/D^+|$. Thus in the following diagram

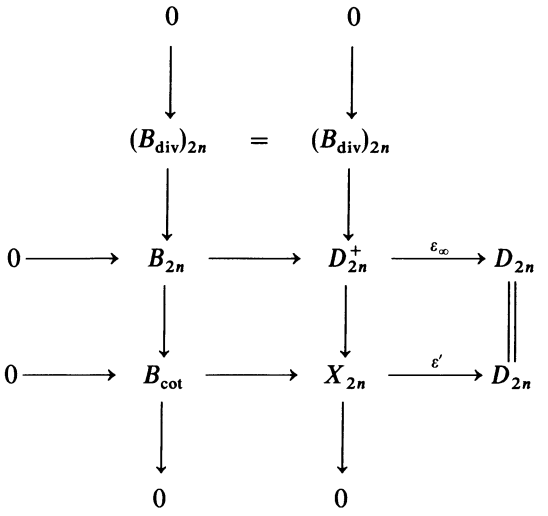
$$\begin{array}{ccccc} H^1(K_v, F_v^+A_{3n}) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, F_v^+A_{2n}) & \xrightarrow{\varepsilon_{2n}} & H^1(K_v, A_{2n}) \\ \downarrow{\scriptstyle \phi_{3n}^+} & & \downarrow{\scriptstyle \phi_{2n}^+} & & \downarrow{\scriptstyle \phi_{2n}} \\ H^1(K_v, F_v^+A)_{3n} & \xrightarrow{p^n} & H^1(K_v, F_v^+A)_{2n} & \xrightarrow{\varepsilon_\infty} & H^1(K_v, A)_{2n} \end{array} \tag{2}$$

where the left column is surjective, the image of the diagonal map Δ is the same as the image of the map $D_{2n}^+ \xrightarrow{\varepsilon_\infty} D_{2n}$. Let $B = \ker(D^+ \xrightarrow{\varepsilon_\infty} D)$, then B is cofinitely generated over $\mathbb{Z}_p$, hence $B_{\text{cot}} \overset{\text{def}}{=} B/B_{\text{div}}$ is finite. Putting $X = D^+/B_{\text{div}}$, we have the following commutative diagram of exact sequences,

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & B_{\text{div}} & = & B_{\text{div}} & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & B & \longrightarrow & D^+ & \xrightarrow{\varepsilon_\infty} & D & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & B_{\text{cot}} & \longrightarrow & X & \xrightarrow{\varepsilon'} & D & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

where ε' is induced from ε_∞. Since $B \cong B_{\text{div}} \oplus B_{\text{cot}}$, $D^+ \cong B_{\text{div}} \oplus X$ by the

property of divisible groups, for $p^n \geqslant |B_{\mathrm{cot}}|$ we have

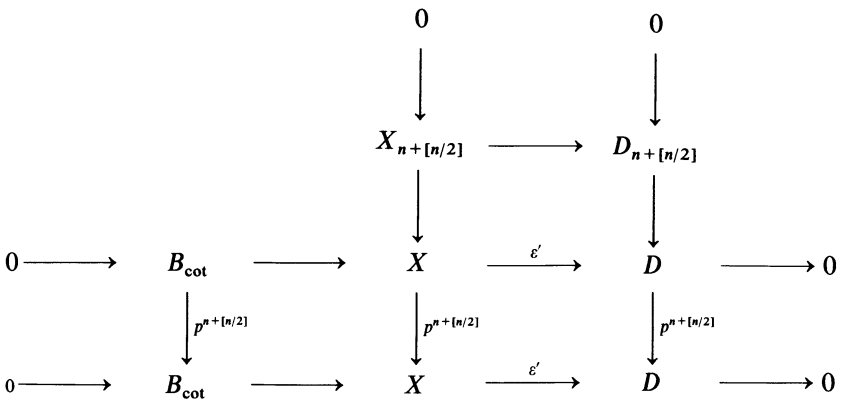


(3)

Now choose n such that

$$p^{[n/2]} \geqslant \max\{|H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}}|, |H^1(K_v, F_v^+ A)/D^+|, |B_{\mathrm{cot}}|\},$$

and consider the following commutative diagram of exact sequences



The left column is zero, and $B_{\mathrm{cot}} \subseteq X_{n-[n/2]}$ since $n - [n/2] \geqslant [n/2]$. Let $d \in D_{n+[n/2]}$ and choose $x \in X$ such that $\varepsilon'(x) = d$, then $p^{n+[n/2]}x \in \ker(\varepsilon') = B_{\mathrm{cot}} \subseteq X_{n-[n/2]}$. Hence $x \in X_{2n}$. This shows that $\varepsilon'(X_{2n}) \supseteq D_{n+[n/2]}$

and by diagram (3),

$$D_{2n} \supseteq \varepsilon_\infty(D_{2n}^+) \supseteq D_{n+[n/2]}.$$

That is

$$D_{2n} \supseteq \mathrm{im}(\Delta) \supseteq D_{n+[n/2]},$$

where Δ is defined to be the diagonal map in the diagram (2). From our choice of n and Lemma 1 we have $p^n H^0(K_v, A) = H^0(K_v, A)_{\mathrm{div}}$. Thus we have the exact sequence

$$0 \longrightarrow H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}} \longrightarrow E_{v,2n} \xrightarrow{\phi_{2n}} D_{2n} \longrightarrow 0$$

of $\mathbb{Z}/p^{2n}\mathbb{Z}$-modules. But D_{2n} is a free $\mathbb{Z}/p^{2n}\mathbb{Z}$-module, hence the above sequence splits. Therefore we have exact sequence

$$0 \to H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}} \to (E_{v,2n})_{n+[n/2]} \xrightarrow{\phi_{2n}} D_{n+[n/2]} \to 0.$$

Therefore from the inclusions $D_{2n} \supseteq \mathrm{im}(\Delta) \supseteq D_{n+[n/2]}$ obtained above we have

$$\begin{aligned}(E_{v,2n})_{n+[n/2]} &= \phi_{2n}^{-1}(D_{n+[n/2]}) \subseteq \phi_{2n}^{-1}(\mathrm{im}\,\Delta) \\ &= \mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}) + H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}} \\ &\subseteq \phi_{2n}^{-1}(D_{2n}) = E_{v,2n}.\end{aligned}$$

Thus

$$\begin{aligned}p^{[n/2]}(E_{v,2n})_{n+[n/2]} &\subseteq p^{[n/2]}(\mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}) + H^0(K_v, A)/H^0(K_v, A)_{\mathrm{div}}) \\ &= p^{[n/2]}(\mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}).\end{aligned}$$

Therefore

$$\begin{aligned}p^n E_{v,2n} &= p^{[n/2]}(p^{n-[n/2]} E_{v,2n}) \\ &\subseteq p^{[n/2]}((E_{v,2n})_{n+[n/2]}) \\ &\subseteq p^{[n/2]}(\mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n})) \\ &\subseteq \mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}) \subseteq E_{v,2n}.\end{aligned}$$

From property (1) of Theorem 1, $\pi_{2n,n}: E_{v,2n}: E_{v,2n} \to E_{v,n}$ is surjective. So the image of $\phi_{n,2n}: E_{v,n} \to E_{v,2n}$ is $p^n E_{v,2n}$. Hence

$$\phi_{n,2n}(E_{v,n}) = p^n E_{v,2n} \subseteq \mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}) \subseteq E_{v,2n}.$$

Since $E_{v,n} = \phi_n^{-1}(D) = \phi_{n,2n}^{-1}(\phi_{2n}^{-1}(D)) = \phi_{n,2n}^{-1}(E_{v,2n})$ and $E_{v,n} = \phi_{n,2n}^{-1}(\phi_{n,2n}(E_{v,n}))$, from the above inclusions we have $E_{v,n} = \phi_{n,2n}^{-1}(\mathrm{im}(\varepsilon_{2n} \circ \pi_{3n,2n}))$. Thus $E_{v,n}$ can be described as the image of σ in the following diagram

$$\begin{array}{ccccc}
P & & \xrightarrow{\quad\sigma\quad} & & H^1(K_v, A_n) \\
\downarrow{\scriptstyle \tau} & & & & \downarrow{\scriptstyle \phi_{n,2n}} \\
H^1(K_v, F_v^+ A_{3n}) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, F_v^+ A_{2n}) & \xrightarrow{\varepsilon_{2n}} & H^1(K_v, A_{2n})
\end{array}$$

where P is the pullback of $\phi_{n,2n}$ and $\varepsilon_{2n} \circ \pi_{3n,2n}$. On the dual side $E'_{v,n}$ is the image of σ' in the pullback diagram

$$\begin{array}{ccccc}
P' & & \xrightarrow{\quad\sigma'\quad} & & H^1(K_v, A_n^*) \\
\downarrow{\scriptstyle \tau'} & & & & \downarrow{\scriptstyle \phi_{n,2n}} \\
H^1(K_v, F_v^+ A_{3n}^*) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, F_v^+ A_{2n}^*) & \xrightarrow{\varepsilon_{2n}} & H^1(K_v, F_v^+ A_{2n}^*)
\end{array}$$

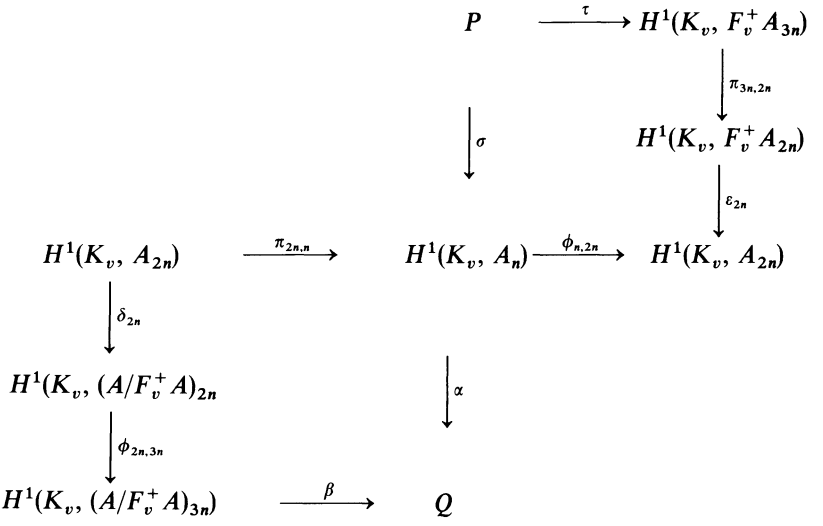
By Pontryagin duality, $(P')^\wedge$ is determined by the pushout diagram

$$\begin{array}{ccccc}
H^1(K_v, A_n^*)^\wedge & & \xrightarrow{\quad\alpha\quad} & & (P')^\wedge \\
\uparrow{\scriptstyle (\phi_{n,2n})^\wedge} & & & & \uparrow{\scriptstyle \beta} \\
H^1(K_v, A_{2n}^*)^\wedge & \xrightarrow{(\varepsilon_{2n})^\wedge} & H^1(K_v, F_v^+ A_{2n}^*)^\wedge & \xrightarrow{(\pi_{3n,2n})^\wedge} & H^1(K_v, F_v^+ A_{3n}^*)^\wedge
\end{array}$$

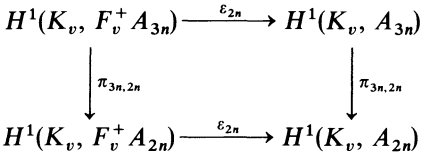
By local Tate duality for finite modules, this diagram is naturally equivalent to the pushout diagram

$$\begin{array}{ccccc}
H^1(K_v, A_n) & & \xrightarrow{\quad\alpha\quad} & & Q \\
\uparrow{\scriptstyle \pi_{2n,n}} & & & & \uparrow{\scriptstyle \beta} \\
H^1(K_v, A_{2n}) & \xrightarrow{\delta_{2n}} & H^1(K_v, (A/F_v^+ A)_{2n}) & \xrightarrow{\phi_{2n,3n}} & H^1(K_v, (A/F_v^+ A)_{3n})
\end{array}$$

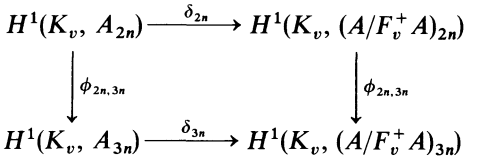
Our goal is to prove that $E_{v,n}$ and $E'_{v,n}$ are the exact annihilator of each other under the pairing $H^1(K_v, A_n) \times H^1(K_v, A_n^*) \to \mathbb{Q}_p/\mathbb{Z}_p$, that is, $\sigma(P)$ is the kernel of the map $\alpha: H^1(K_v, A_n) \to Q$. As $|E_{v,n}||E'_{v,n}| = |H^1(K_v, A_n)| = |H^1(K_v, A_n^*)|$ by Proposition 2, we only need to prove that $\alpha \circ \sigma = 0$ in the following diagram



From the commutative diagrams

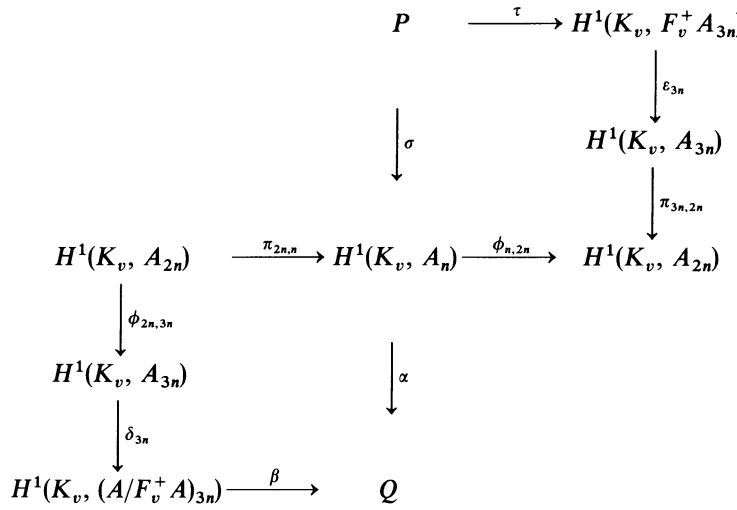


and

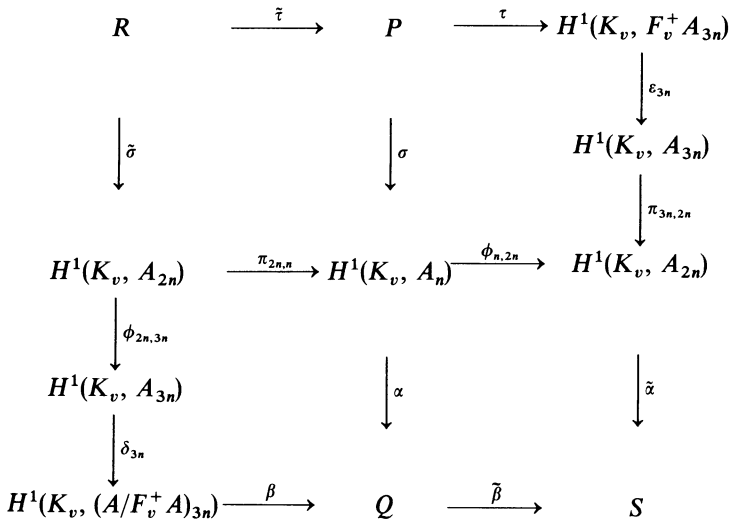


we have $\varepsilon_{2n} \circ \pi_{3n,2n} = \pi_{3n,2n} \circ \varepsilon_{3n}$ and $\phi_{2n,3n} \circ \delta_{2n} = \delta_{3n} \circ \phi_{2n,3n}$. Thus we only

need to show that $\alpha \circ \sigma = 0$ in the commutative diagram



Next, we complete the diagram by taking the obvious pullback R and pushout S and get the commutative diagram



We can attach the upper-right square to a commutative diagram with exact

rows and get

$$\begin{array}{ccccc}
H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(K_v, A_n) & \longrightarrow & H^2(K_v, A_n) \\
\downarrow{\scriptstyle \phi_{2n,3n}} & & \downarrow{\scriptstyle \phi_{n,2n}} & & \| \\
H^1(K_v, A_{3n}) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, A_{2n}) & \longrightarrow & H^2(K_v, A_n) \\
\uparrow{\scriptstyle \varepsilon_{3n}\circ\tau} & & \uparrow{\scriptstyle \phi_{n,2n}} & & \\
P & \xrightarrow{\sigma} & H^1(K_v, A_n) & &
\end{array}$$

A diagram chase shows that $\mathrm{im}(\sigma) \subseteq \mathrm{im}(\pi_{2n,n}: H^1(K_v, A_{2n}) \to H^1(K_v, A_n))$. Thus the projective system

$$\begin{array}{ccc}
 & & P \\
 & & \downarrow{\scriptstyle \sigma} \\
H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(K_v, A_n)
\end{array}$$

is equivalent to the projective system

$$\begin{array}{ccc}
 & & P \\
 & & \downarrow{\scriptstyle \sigma} \\
H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & \mathrm{im}(\pi_{2n,n})
\end{array}$$

with surjective row. Hence $\tilde{\tau}$ is surjective by the property of pullbacks. Similarly, from lower-left square of the commutative diagram (4) we get commutative diagram with exact rows

$$\begin{array}{ccccc}
 & & H^1(K_v, A_n) & \xrightarrow{\alpha} & Q \\
 & & \downarrow{\scriptstyle \pi_{2n,n}} & & \uparrow{\scriptstyle \beta\circ\delta_{3n}} \\
H^0(K_v, A_n) & \xrightarrow{\partial} & H^1(K_v, A_{2n}) & \xrightarrow{\phi_{2n,3n}} & H^1(K_v, A_{3n}) \\
\| & & \downarrow{\scriptstyle \pi_{2n,n}} & & \downarrow{\scriptstyle \pi_{3n,2n}} \\
H^0(K_v, A_n) & \xrightarrow{\partial} & H^1(K_v, A_n) & \xrightarrow{\phi_{n,2n}} & H^1(K_v, A_{2n})
\end{array}$$

Another diagram chase shows that $\ker(\alpha) \supseteq \ker(\phi_{n,2n}: H^1(K_v, A_n) \to H^1(K_v, A_{2n}))$. Thus the injective system

$$\begin{array}{ccc} H^1(K_v, A_n) & \xrightarrow{\phi_{n,2n}} & H^1(K_v, A_{2n}) \\ \downarrow{\scriptstyle \alpha} & & \\ Q & & \end{array}$$

is equivalent to the injective system

$$\begin{array}{ccc} H^1(K_v, A_n)/\partial(H^0(K_v, A_n)) & \xrightarrow{\phi_{n,2n}} & H^1(K_v, A_{2n}) \\ \downarrow{\scriptstyle \alpha} & & \\ Q & & \end{array}$$

with injective row. Hence $\tilde{\beta}$ is injective. Therefore, to prove that $\alpha \circ \sigma = 0$ we only need to prove that R is sent to zero in S following any path in the diagram (4). We will show that $\tilde{\beta} \circ \beta \circ \delta_{3n} \circ \phi_{2n,3n} \circ \tilde{\sigma} = 0$.

From the upper half of the diagram (4) we get the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\tilde{\sigma}} & H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(K_v, A_n) \\ \downarrow{\scriptstyle \tau\circ\tilde{\tau}} & & \downarrow{\scriptstyle \phi_{2n,3n}} & & \downarrow{\scriptstyle \phi_{n,2n}} \\ H^1(K_v, F_v^+ A_{3n}) & \xrightarrow{\varepsilon_{3n}} & H^1(K_v, A_{3n}) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, A_{2n}) \end{array}$$

in which the outer rectangle and the right square are commutative. It follows that

$$\begin{aligned} \operatorname{im}((\phi_{2n,3n} \circ \tilde{\sigma}) - (\varepsilon_{3n} \circ (\tau \circ \tilde{\tau})) &\subseteq \ker(\pi_{3n,2n}: H^1(K_v, A_{3n}) \to H^1(K_v, A_{2n})) \\ &= \operatorname{im}(\phi_{n,3n}: H^1(K_v, A_n) \to H^1(K_v, A_{3n})). \end{aligned}$$

Thus

$$\begin{aligned} \operatorname{im}(\phi_{2n,3n} \circ \tilde{\sigma}) \subseteq &\operatorname{im}(\varepsilon_{3n}: H^1(K_v, F_v^+ A_{3n}) \to H^1(K_v, A_{3n})) \\ &+ \operatorname{im}(\phi_{n,3n}: H^1(K_v, A_n) \to H^1(K_v, A_{3n})). \end{aligned}$$

Thus $\operatorname{im}(\phi_{2n,3n} \circ \tilde{\sigma}) \subseteq \operatorname{im}(\varepsilon_{3n}) + \operatorname{im}(\phi_{n,3n})$ in the group $H^1(K_v, A_{3n})$ in the lower half of the diagram (4). So we only need to show that the subgroup

$\mathrm{im}(\varepsilon_{3n}) + \mathrm{im}(\phi_{n,3n})$ of $H^1(K_v, A_{3n})$ in the lower half of diagram (4) will go to zero in S via $(\beta \circ \tilde{\beta}) \circ \delta_{3n}$. But if $k \in \mathrm{im}(\varepsilon_{3n})$, then $\delta_{3n}(k) = 0$, hence $((\tilde{\beta} \circ \beta) \circ \delta_{3n})(k) = 0$. On the other hand, let $k \in \mathrm{im}(\phi_{n,3n})$. From the commutative diagram of exact sequences

$$\begin{array}{ccccc} H^1(K_v, A_n) & \xrightarrow{\phi_{n,2n}} & H^1(K_v, A_{2n}) & \xrightarrow{\pi_{2n,n}} & H^1(K_v, A_n) \\ \| & & \downarrow{\scriptstyle \phi_{2n,3n}} & & \downarrow{\scriptstyle \phi_{n,2n}} \\ H^1(K_v, A_n) & \xrightarrow{\phi_{n,3n}} & H^1(K_v, A_{3n}) & \xrightarrow{\pi_{3n,2n}} & H^1(K_v, A_{2n}) \end{array}$$

$k = \phi_{n,3n}(u) = \phi_{2n,3n}(\phi_{n,2n}(u))$ for some $u \in H^1(K_v, A_n)$. By the commutativity of the lower half of the diagram (4),

$$\begin{aligned} ((\tilde{\beta} \circ \beta) \circ \delta_{3n})(k) &= (((\tilde{\beta} \circ \beta) \circ \delta_{3n}) \circ \phi_{n,3n})(u) \\ &= ((\tilde{\beta} \circ \beta \circ \delta_{3n}) \circ \phi_{2n,3n})(\phi_{n,2n}(u)) \\ &= (\tilde{\alpha} \circ (\phi_{n,2n} \circ \pi_{2n,n}))(\phi_{n,2n}(u)) \\ &= (\tilde{\alpha} \circ \phi_{n,2n})(\pi_{2n,n} \circ \phi_{n,2n}(u)) \\ &= 0 \end{aligned}$$

Now we have finished the proof of the local duality, hence finishing the proof of Theorem 1.

3.4. Cocyle property of $E_{v,n}$

Let $E_{v,n}$ be defined as before. Let $Z_{v,n}$ be the subgroup of elements in $Z^1(K_v, A_n)$ representing elements in $E_{v,n}$. The following is a version of Theorem 1.1 and will be used to prove Theorem 2.

PROPOSITION 3. *The exact sequence*

$$0 \longrightarrow A_s \longrightarrow A_{r+s} \xrightarrow{p^s} A_r \longrightarrow 0$$

induces the exact sequence

$$0 \longrightarrow Z_{v,s} \longrightarrow Z_{v,r+s} \xrightarrow{p^s} Z_{v,r} \longrightarrow 0$$

Proof. We have the following diagram

$$\begin{array}{ccccccccc}
 & & C^0(K_v, A_s) & \xrightarrow{d} & B^1(K_v, A_s) & \longrightarrow & Z_{v,s} & \xrightarrow{\gamma_s} & E_{v,s} \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \phi_{s,r+s}} & & \downarrow{\scriptstyle \phi_{s,r+s}} \\
 & & C^0(K_v, A_{r+s}) & \xrightarrow{d} & B^1(K_v, A_{r+s}) & \longrightarrow & Z_{v,r+s} & \xrightarrow{\gamma_{r+s}} & E_{v,r+s} \\
 & & \downarrow{\scriptstyle p^s} & & \downarrow{\scriptstyle p^s} & & \downarrow{\scriptstyle p^s} & & \downarrow{\scriptstyle \pi_{r+s,r}} \\
Z^0(K_v, A_r) & \longrightarrow & C^0(K_v, A_r) & \xrightarrow{d} & B^1(K_v, A_r) & \longrightarrow & Z_{v,r} & \xrightarrow{\gamma_r} & E_{v,r}.
\end{array}$$

where the d's are the differential maps and the γ's are the quotient maps from cocycle groups to cohomology groups. By the commutativity of the square in the lower-right corner and that $\pi_{r+s,r}: E_{v,r+s} \to E_{v,r}$ is surjective (Theorem 1.1), $Z_{v,r} = B^1(K_v, A_r) + p^s Z_{v,r+s}$. Since $p^s: B^1(K_v, A_{r+s}) \to B^1(K_v, A_r)$ is surjective, we have $Z_{v,r} = p^s(B^1(K_v, A_{r+s}) + Z_{v,r+s}) = p^s Z_{v,r+s}$. This proves the required surjectivity. The injectivity of $Z_{v,s} \to Z_{v,r+s}$ is clear. Also $\mathrm{im}(Z_{v,s} \to Z_{v,r+s}) \subseteq \ker(Z_{v,r+s} \to Z_{v,r})$. So we only need to prove the inverse inclusion. From the above diagram,

$$\begin{aligned}
&\ker(p^n: Z_{v,r+s} \longrightarrow Z_{v,r}) \\
&\subseteq \ker(Z_{v,r+s} \xrightarrow{p^s} Z_{v,r} \xrightarrow{\gamma_r} E_{v,r}) \\
&= \ker(Z_{v,r+s} \xrightarrow{\gamma_{r+s}} E_{v,r+s} \xrightarrow{\pi_{r+s,r}} E_{v,r}) \\
&= \gamma_{r+s}^{-1}(\ker(\pi_{r+s,r}: E_{v,r+s} \longrightarrow E_{v,r})) \\
&= \gamma_{r+s}^{-1}(\mathrm{im}(\phi_{s,r+s}: E_{v,s} \longrightarrow E_{v,r+s})) \\
&= \gamma_{r+s}^{-1}(\mathrm{im}(\phi_{s,r+s} \circ \gamma_s)) \\
&= \gamma_{r+s}^{-1}(\mathrm{im}(\gamma_{r+s} \circ \phi_{s,r+s})) \\
&= B^1(K_v, A_{r+s}) + Z_{v,s}.
\end{aligned}$$

As $\ker(p^s: C^1(K_v, A_{r+s}) \to C^1(K_v, A_r)) = C^1(K_v, A_s)$,

$$\begin{aligned}
&\ker(p^s: Z_{v,r+s} \to Z_{v,r}) \\
&= C^1(K_v, A_s) \cap \ker(p^s: Z_{v,r+s} \to Z_{v,r}) \\
&\subseteq C^1(K_v, A_s) \cap (B^1(K_v, A_{r+s}) + Z_{v,s}) \\
&= C^1(K_v, A_s) \cap B^1(K_v, A_{r+s}) + Z_{v,s}.
\end{aligned}$$

But

$$
\begin{aligned}
&C^1(K_v, A_s) \cap B^1(K_v, A_{r+s}) \\
&= d(\ker(p^s \circ \mathrm{d}) : C^0(K_v, A_{r+s}) \to B^1(K_v, A_{r+s}) \to B^1(K_v, A_r) \\
&= d(\ker(d \circ p^s) : C^0(K_v, A_{r+s}) \to C^0(K_v, A_r) \to B^1(K_v, A_r) \\
&= d((p^s)^{-1}(Z^0(K_v, A_r)) \\
&= \partial(Z^0(K_v, A_r))
\end{aligned}
$$

where ∂ is the boundary map from $Z^0(K_v, A_r)$ to $Z^1(K_v, A_s)$. By the definition of $E_{v,s}$, $\partial H^0(K_v, A_r) \subseteq E_{v,s}$, hence $\partial Z^0(K_v, A_r) \subseteq Z_{v,s}$. This proves the proposition.

4. The global theory

Because of the space limitations, we will only give the construction of the pairing on $S_A(K)$ and give an indication of the proof of Theorem 2. The full details will be included in [7].

Assume that v is unramified at A for almost all v. For such a v with $v \nmid p$, we show in Section 1 that $E_{v,n} = H^1(g_v, A_n^{I_v})$. Thus the restricted direct product $\Pi'_v H^1(K_v, A_n)$ of $H^1(K_v, A_n)$ relative to the subgroups $E_{v,n}$ is equal to the restricted direct product $P^1(K, A_n)$ of $H^1(K_v, A_n)$ relative to the subgroups $H^1(g_v, A^{I_v})$ defined by Tate [14]. This implies that the image of the localization map

$$H^1(K, A_n) \to \prod_v H^1(K_v, A_n)$$

is contained in $\Pi'_v H^1(K_v, A_n)$. Similarly, $H^1(K, A_n^*) \to \Pi_v H^1(K_v, A_n^*)$ has its image contained in $\Pi'_v H^1(K_v, A_n^*)$ relative to $E'_{v,n}$.

DEFINITION 2. Define the p^n(strict) Selmer group $S_{A_n}^{\mathrm{str}}(K)$ to be the kernel of the map

$$H^1(K, A_n) \to \bigoplus_v H^1(K_v, A_n)/E_{v,n}.$$

Here one can take a direct sum instead of a direct product because of the above remark. In $H^1(K, A)$, define

$$S_A^{\mathrm{str}}(K) = \varinjlim S_{A_n}^{\mathrm{str}}(K).$$

This is the strict Selmer group over K defined by Greenberg.

Let N be an integer such that (1) and (2) in Theorem 1 hold for all primes v of K and all $r, s, n \geqslant N$. Such N exists since A is unramified for almost all primes of K. Theorem 2 is a consequence of the following result,

THEOREM 4. *Assume that A is unramified at almost all primes of K. For each pair $r, s \geqslant N$, there is a canonical pairing*

$$\langle , \rangle_{r,s}: S^{\mathrm{str}}_{A_r}(K) \times S^{\mathrm{str}}_{A^*_s}(K) \to \mathbb{Q}_p/\mathbb{Z}_p$$

whose kernels in the two sides are precisely the images of the induced maps $\pi_{r+s,r}: S^{\mathrm{str}}_{A_{r+s}}(K) \to S^{\mathrm{str}}_{A_r}(K)$ and $\pi_{r+s,s}: S^{\mathrm{str}}_{A^*_{r+s}}(K) \to S^{\mathrm{str}}_{A^*_s}(K)$. If moreover there is a G_K-module isomorphism

$$\eta: A \to A^* = \mathrm{Hom}(T_A, \mathbb{Q}_p/\mathbb{Z}_p(1))$$

such that $(\eta a)(a) = 0$ for $a \in A$, then this pairing induces a skew-symmetric pairing

$$\langle , \rangle_{r,s}: S^{\mathrm{str}}_{A_r}(K) \times S^{\mathrm{str}}_{A_s}(K) \to \mathbb{Q}_p/\mathbb{Z}_p$$

in the sense that

$$\langle b, b' \rangle_{r,s} + \langle b', b \rangle_{s,r} = 0 \quad \text{for } b \in S^{\mathrm{str}}_{A_r}(K),\ b' \in S^{\mathrm{str}}_{A_s}(K).$$

It can be verified that the pairing $\langle , \rangle_{r,s}$ is compatible with the direct systems $\{S^{\mathrm{str}}_{A_r}(K)\}$ and $\{S^{\mathrm{str}}_{A^*_s}(K)\}$, hence induces the required pairing $\langle , \rangle$ on the direct limits.

The pairing $\langle , \rangle_{r,s}$ is constructed as follows. For any positive integer n, the pairing $e_n: A_n \times A^*_n \to \mathbb{Q}_p/\mathbb{Z}_p(1)$ induces the local Tate pairing

$$\bigcup_n: C^i(K_v, A_n) \times C^j(K_v, A^*_n) \to C^{i+j}(K_v, \mathbb{Q}_p/\mathbb{Z}_p(1)).$$

Fix a pair r and s with $r \geqslant N$, $s \geqslant N$. Let $b \in S^{\mathrm{str}}_{A_r}(K)$, $b' \in S^{\mathrm{str}}_{A^*_s}(K)$. Choose a $\beta \in Z^1(K, A_r)$ representing b and $\beta' \in Z^1(K, A^*_s)$ representing b'. Lift β to a cochain $\beta_s \in C^1(K, A_{r+s})$ with $p^s\beta_s = \beta$. The coboundary $d\beta_s$ of β_s takes values in A_s, hence is an element of $Z^2(K, A_s)$. Thus $d\beta_s \cup_s \beta'$ represents an element of $Z^3(K, \mathbb{Q}_p/\mathbb{Z}_p)$ and therefore an element in $H^3(K, \bar{K}^\times)$. But this last group is zero by [10, I.4.18], so $d\beta_s \cup_s \beta' = d\varepsilon$ for some 2-cochain $\varepsilon \in C^2(K, \bar{K}^\times)$.

Now for each v, let $\beta_v \in Z^1(K_v, A_r)$, $\beta_{s,v} \in C^1(K_v, A_{r+s})$ be the images of β and β_s under the localization (restriction) maps. Thus $p^s\beta_{s,v} = \beta_v$. By Proposition 3, $\beta_v \in Z_{v,r}$ and we can find $\beta_{v,s} \in Z_{v,r+s}$ such that $p^s\beta_{v,s} = \beta_v$. Thus

$\beta_{v,s}-\beta_{s,v}\in C^1(K_v, A_s)$ and $(\beta_{v,s}-\beta_{s,v})\cup_s \beta'_v \in C^2(K_v, \mathbb{Q}_p/\mathbb{Z}_p)$. We have

$$d((\beta_{v,s}-\beta_{s,v})\cup_s \beta'_v) = -d(\beta_{s,v})\cup_s \beta'_v = -(d\beta_s)_v \cup_s \beta'_v = -d\varepsilon_v.$$

Hence $(\beta_{v,s}-\beta_{s,v})\cup_s \beta'_v + \varepsilon_v \in Z^2(K_v, \bar{K}^\times)$ and represents an element of $H^2(K_v, \bar{K}^\times)$. We define

$$\langle b, b'\rangle_{r,s} = \sum_v \mathrm{inv}_v((\beta_{v,s}-\beta_{s,v})\cup_s \beta'_v + \varepsilon_v). \tag{5}$$

In the special case when b is divisible by p^s in the sense that there is an element $b_s \in H^1(K, A_{r+s})$ such that $\pi_{r+s,r}(b_s) = b$, where $\pi_{r+s,r}: H^1(K, A_{r+s}) \to H^1(K, A_r)$ is the map induced by $p^s: A_{r+s} \to A_r$, we could choose β_s to be a cocyle and choose $\varepsilon = 0$. Then we actually have

$$\langle b, b'\rangle_{r,s} = \sum_v \mathrm{inv}_v((\beta_{v,s}-\beta_{s,v})\cup_s \beta'_v) = \sum_v \mathrm{inv}_v((b_{v,s}-b_{s,v})\cup_s b'_v),$$

where $\beta_{v,s}$ represents $b_{v,s}$, $\beta_{s,v}$ represents $b_{s,v}$.

It can be verified that the pairing $\langle , \rangle_{r,s}$ is well-defined. The proof of the non-degeneracy in Theorem 4 is analogous to the proof used for the classical case. Here, we use the idea in [10] with some modifications. The key for the generalization is the observation that the proof of the classical case in [10] uses only the following properties of an abelian variety E, together with some general facts from Galois cohomology:

(1) The local Tate duality for E.

(2) The sequence

$$E(K_v)/p^r E(K_v) \xrightarrow{p^s} E(K_v)/p^{r+s}E(K_v) \longrightarrow E(K_v)/p^s E(K_v) \longrightarrow 0$$

is exact.

(3) E_{p^∞} is unramified at almost all primes v of K.

The proof of the skew-symmetry of the pairing is similar to those used in [4] and [9].

Let E be an abelian variety over K. We say that E has ordinary reduction at p if for each v of K over p, there is a divisible G_{K_v}-submodule $F_v^+ E_{p^\infty}$ of E_{p^∞} such that $\mathrm{corank}_{\mathbb{Z}_p} F_v^+ E_{p^\infty} = (1/2)\mathrm{corank}_{\mathbb{Z}_p} E_{p^\infty}$, I_v acts trivially on $E_{p^\infty}/F_v^+ E_{p^\infty}$ and such that $(E_{p^\infty}/F_v^+ E_{p^\infty})(K_v)$ is $E_{p^\infty}/F_v^+ E_{p^\infty}$ or is finite. It is the case if E has good, ordinary reduction or multiplicative reduction at p. The following result shows that $S_A^{\mathrm{str}}(K)$ is a generalization of the classical Selmer group for an abelian variety.

THEOREM 5. *Let $A = E_{p^\infty}$, where E is an abelian variety over K with ordinary reduction at p. We have $S_A^{\text{class}}(K) = S_A^{\text{str}}(K)$.*

Proof. Recall that $S_A^{\text{class}}(K)$ is defined to be the kernel of the map

$$H^1(K, A) \to \bigoplus_v H^1(K_v, A)/(E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$$

and $S_A^{\text{str}}(K)$ is defined to be the kernel of the map

$$H^1(K, A) \to \bigoplus_{v \nmid p} H^1(K_v, A)/(H^1(g_v, A^{I_v}))_{\text{div}} \oplus \bigoplus_{v|p} H^1(K_v, A)/(\text{im}(\varepsilon_\infty))_{\text{div}}$$

where $\varepsilon_\infty : H^1(K_v, F_v^+ A) \to H^1(K_v, A)$ is the natural map. So we only need to show that $E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = H^1(g_v, A^{I_v})_{\text{div}}$ for $v \nmid p$ and that $E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = (\text{im}(\varepsilon_\infty))_{\text{div}}$ for $v \mid p$.

Let $v \nmid p$. By Lutz's theorem, $E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = 0$. On the other hand, $H^1(g_v, A^{I_v}) = A^{I_v}/(\text{Frob}_v - \text{id})A^{I_v}$. In the exact sequence

$$0 \to \ker(\text{Frob}_v - \text{id}) \to A^{I_v} \xrightarrow{(\text{Frob}_v - \text{id})} A^{I_v} \to A^{I_v}/(\text{Frob}_v - \text{id})A^{I_v} \to 0,$$

$\ker(\text{Frob}_v - \text{id}) = A(K_v)$ and is finite. Hence $\text{corank}_{\mathbb{Z}_p} \ker(\text{Frob}_v - \text{id}) = 0$. Therefore $\text{corank}_{\mathbb{Z}_p} H^1(g_v, A^{I_v}) = \text{corank}_{\mathbb{Z}_p} A^{I_v}/(\text{Frob}_v - \text{id})A^{I_v} = 0$ and $H^1(g_v, A^{I_v})_{\text{div}} = 0$.

Now consider $v \mid p$. We have the following diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\delta} & H^1(K_v, A) & \longrightarrow & H^1(K_v, E(\overline{K_v})) \\ & & & & \| & & \\ & & H^1(K_v, F_v^+ A) & \xrightarrow{\varepsilon_\infty} & H^1(K_v, A) & \longrightarrow & H^1(K_v, A/F_v^+ A) \end{array}$$

We will first prove that $\text{im}\,\delta \subseteq \text{im}\,\varepsilon_\infty$, hence $\text{im}\,\delta \subseteq (\text{im}\,\varepsilon_\infty)_{\text{div}}$ since $\text{im}\,\delta = E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is divisible. Then we will show that $\text{im}\,\delta$ and $\text{im}\,\varepsilon_\infty$ have the same $\mathbb{Z}_p$-corank. Thus $\text{im}\,\delta = (\text{im}\,\varepsilon_\infty)_{\text{div}}$. For any $P \otimes (1/p^t) \in E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$, choose $Q \in E(\overline{K_v})$ with $p^t Q = P$. Then $\delta(P \otimes (1/p^t))$ is the cocyle σ in $Z^1(K_v, A)$ such that $\sigma(g) = g(Q) - Q$ for any $g \in G_{K_v}$. Since the natural map $A \to A/F_v^+ A$, $x \mapsto \bar{x}$, is a G_{K_v}-homomorphism, we have $\overline{\sigma(g)} = g(\bar{Q}) - \bar{Q}$. Since I_v acts trivially on $A/F_v^+ A$, this shows that $\overline{\sigma(g)} = 0$ for $\sigma \in I_v$. Thus from the inflation-restriction sequence

$$0 \to H^1(g_v, A/F_v^+ A) \to H^1(K_v, A/F_v^+ A) \to H^1(I_v, A/F_v^+ A)$$

this σ represents an element in $H^1(g_v, A/F_v^+A)$. If G_{K_v} acts trivially on A/F_v^+A, then $\overline{\sigma(g)}=0$ for all $\sigma\in G_{K_v}$. Thus σ represents an element in $\operatorname{im}\varepsilon_\infty$. Let $(A/F_v^+A)(g_v)$ be finite. It follows that $H^1(g_v, A/F_v^+A)$ is finite. Then this group must be zero because $H^1(g_v, A/F_v^+A)=(A/F_v^+A)/(\mathrm{Frob}_v-\mathrm{id})(A/F_v^+A)$ is divisible. Therefore σ represents zero in $H^1(K_v, A/F_v^+A)$, and σ represents an element in $\operatorname{im}\varepsilon_\infty$.

Next we compare the $\mathbb{Z}_p$-coranks of $E(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ and $\operatorname{im}\varepsilon_\infty$. By [13, VII.6.3] and its generalization to an abelian variety, $\operatorname{corank}_{\mathbb{Z}_p}E(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p=[K_v:\mathbb{Q}_p]\dim E$ where $\dim E$ is the geometric dimension of E. From the exact sequence

$$0\to H^0(K_v, F_v^+A)\to H^0(K_v, A)\to H^0(K_v, (A/F_v^+A))$$
$$\to H^1(K_v, F_v^+A)\to \operatorname{im}(\varepsilon_\infty)\to 0$$

and Tate characteristic formula, we have

$$\operatorname{corank}_{\mathbb{Z}_p}\operatorname{im}(\varepsilon_\infty)=[K_v:\mathbb{Q}_p]\operatorname{corank}_{\mathbb{Z}_p}(F_v^+A)+\operatorname{corank}_{\mathbb{Z}_p}(H^0(K_v, A))$$
$$+\operatorname{corank}_{\mathbb{Z}_p}(H^2(K_v, F_v^+A))-\operatorname{corank}_{\mathbb{Z}_p}(H^0(K_v, (A/F_v^+A))).$$

By the basic properties of such an abelian variety,

$$\operatorname{corank}_{\mathbb{Z}_p}F_v^+A=\dim E \quad\text{and}\quad \operatorname{corank}_{\mathbb{Z}_p}H^0(K_v, A)=0.$$

By local Tate duality between $F_v^+A_n$ and $A_n^*/F_v^+A_n^*$ (see the proof of Proposition 2 for details), $\operatorname{corank}_{\mathbb{Z}_p}H^2(K_v, F_v^+A)=\operatorname{corank}_{\mathbb{Z}_p}H^0(K_v, A^*/F_v^+A^*)$. Since E is isogenous to its dual abelian variety E^*, the restriction of this isogeny to A sends A onto A^* with finite kernel. Hence the reduced map sends A/F_v^+A onto $A^*/F_v^+A^*$ with finite kernel. This implies that $\operatorname{corank}_{\mathbb{Z}_p}H^0(K_v, A/F_v^+A)=\operatorname{corank}_{\mathbb{Z}_p}H^0(K_v, A^*/F_v^+A^*)$. Thus $\operatorname{corank}_{\mathbb{Z}_p}\varepsilon_\infty=[K_v:\mathbb{Q}_p]\dim E$, as is required. □

To obtain nontrivial examples of G_K-modules where Theorem 2 can be applied to, consider a compatible system $V=\{V_l\}$ of l-adic representations of $G=\mathrm{Gal}(\bar{K}/K)$ which are ordinary at p and suppose that there is a G_K-invariant, nondegenerate and skew-symmetric pairing on V_p with values in $\mathbb{Q}_p$. Let T_p be a G_K-invariant lattice of V_p that is its own annihilator $T_p^\perp$ under the induced pairing on V_p with values in $\mathbb{Q}_p/\mathbb{Z}_p$. This requirement is equivalent to the existence of the isomorphism η on $A=V_p/T_p$ in Theorem 2. If $V_p=T_p(E)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, where $T_p(E)$ is the Tate module of an elliptic curve E/K, then $T_p(E)$ is such a lattice. For an odd number r, let $\mathrm{Sym}_r(V_l)$ be the rth symmetric power of V_l. It is easy to see that the system $\mathrm{Sym}_r(V)=\{\mathrm{Sym}_r(V_l)\}$ with the induced representation is also a compatible system of l-adic representations which are ordinary at

p. Let

$$\langle , \rangle : V_p \times V_p \to \mathbb{Q}_p$$

be the skew-symmetric pairing defined on V_p. For decomposable tensors $\{x_1, \ldots, x_r\}$ and $\{y_1, \ldots, y_r\}$ in $\mathrm{Sym}_r(V_p)$ define

$$\langle \{x_1, \ldots, x_r\}, \{y_1, \ldots, y_r\} \rangle = \sum_{\sigma \in S_r} \langle x_{\sigma(1)}, y_1 \rangle \cdots \langle x_{\sigma(r)}, y_r \rangle.$$

Extending by bilinearity we get a G_K-invariant pairing $\langle , \rangle^r$ defined on $\mathrm{Sym}_r(V_p)$. By [12, p. 404], this pairing is also nondegenerate. Since r is odd,

$$\begin{aligned}
\langle \{x_1, \ldots, x_r\}, \{y_1, \ldots, y_r\} \rangle &= \sum_{\sigma \in S_r} \langle x_{\sigma(1)}, y_1 \rangle \cdots \langle x_{\sigma(r)}, y_r \rangle \\
&= -\sum_{\sigma \in S_r} \langle y_1, x_{\sigma(1)} \rangle \cdots \langle y_r, x_{\sigma(r)} \rangle \\
&= -\sum_{\sigma \in S_r} \langle y_{\sigma^{-1}(1)}, x_1 \rangle \cdots \langle y_{\sigma^{-1}(r)}, x_r \rangle \\
&= -\sum_{\sigma \in S_r} \langle y_{\sigma(1)}, x_1 \rangle \cdots \langle y_{\sigma(r)}, x_r \rangle \\
&= -\langle \{y_1, \ldots, y_r\}, \{x_1, \ldots, x_r\} \rangle.
\end{aligned}$$

Hence this pairing is also skew-symmetric.

Let $\{v_1, \ldots, v_d\}$ be a basis of V_p such that $T_p = \oplus_{i=1}^d \mathbb{Z}_p v_i$. Let $a = \min\{|\langle v_1, v_i \rangle|_p : v_i \in \{v_i\}\}$. Then $|\langle p^{-a} v_1, v_i \rangle|_p = |\langle v_1, p^{-a} v_i \rangle|_p \geqslant 0$. Since $T_p = T_p^{\perp}$, $a = 0$. Thus there is a v_i, say v_2, such that $\langle v_1, v_2 \rangle \in \mathbb{Z}_p^{\times}$. Multiplying v_2 with a unit in $\mathbb{Z}_p$ if necessary, we have $\langle v_1, v_2 \rangle = 1$. Letting $H_1 = \mathbb{Z}_p v_1 \oplus \mathbb{Z}_p v_2$, we have $T_p = H_1 \oplus H_1^{\perp}$ and the same can be applied to $H_1^{\perp}$. Finally we get a $\mathbb{Z}_p$ basis $\{v_i\}$ of T_p such that $\langle v_{2i-1}, v_{2i} \rangle = -\langle v_{2i}, v_{2i-1} \rangle = 1$ and $\langle v_i, v_j \rangle = 0$ for any other choices of i and j.

$\mathrm{Sym}_r(T_p)$ is a lattice in $\mathrm{Sym}_r(V_p)$ and is G_K-invariant. It has a basis of the form

$$\{\{x_1^{i_1} \cdots x_d^{i_d}\} | i_j \geqslant 0,\ i_1 + \cdots + i_d = r\},$$

where

$$\{x_1^{i_1} \cdots x_d^{i_d}\} = \{\underbrace{x_1, \ldots, x_1}_{i_1 \text{ terms}}, \underbrace{x_2, \ldots, x_2}_{i_2 \text{ terms}}, \ldots, \underbrace{x_d, \ldots, x_d}_{i_d \text{ terms}}\}.$$

It can be easily verified that

$$\langle\{x_1^{i_1}\cdots x_d^{i_d}\},\{x_1^{j_1}\cdots x_d^{j_d}\}\rangle = \begin{cases}(-1)^{\Sigma i_{2k}}(i_1!)(i_2!)\cdots(i_d!) & \text{if } i_{2k-1}=j_{2k},\ k=1,\ldots,d/2\\ 0 & \text{otherwise.}\end{cases}$$

It follows that if $p \geqslant r+1$, then $\mathrm{Sym}_r(T_p)$ is its own annihilator under the pairing

$$\mathrm{Sym}_r(V_p)\times\mathrm{Sym}_r(V_p)\xrightarrow{\langle,\rangle}\mathbb{Q}_p\longrightarrow\mathbb{Q}_p/\mathbb{Z}_p.$$

Thus we have

THEOREM 6. *If V_p satisfies the conditions in Theorem* 2, *and r is odd with $p \geqslant r+1$, then the same conditions are satisfied by* $\mathrm{Sym}_r(V_p)$. *Consequently, let*

$$\mathrm{Sym}_r(A) = \mathrm{Sym}_r(V_p)/\mathrm{Sym}_r(T_p),$$

then $|S^{\mathrm{str}}_{\mathrm{Sym}_r(A)}(K)/S^{\mathrm{str}}_{\mathrm{Sym}_r(A)}(K)_{\mathrm{div}}|$ *is a square.*

5. Infinite extensions

The aim of this section is to give a proof of Theorem 3.

Let K_∞ be any $\mathbb{Z}_p$-extension of K with $p \neq 2$. We have made the following restrictions on A in Theorem 3:

(1) A is unramified at almost all primes of K.
(2) There is a G_K-module isomorphism $\eta: A \to A^*$ such that $(\eta a)(a)=0$ for $a \in A$.
(3) The strict Selmer group $S_A^{\mathrm{str}}(K_\infty)$ of Greenberg is Λ-cotorsion.
(4) $A(K_\infty)$ is finite.

Let K_n be the unique extension of K contained in K_∞ of degree p^n. For each prime λ of K_∞, let I_λ denote the inertia group for some prime of $\bar{K}$ lying over λ. Let $g_\lambda = G_{(K_\infty)_\lambda}/I_\lambda$. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n = \mathrm{Gal}(K_n/K)$. Then $\{H^1(K_n, A)\}$ is a direct system of abelian groups with an action of the inverse system $\{\Gamma_n\}$. Thus $H^1(K_\infty, A) = \varinjlim H^1(K_n, A)$ is a Γ-module. It is clear that the system $\{S_A^{\mathrm{str}}(K_n)\}$ is a submodule of the $\{\Gamma_n\}$-module $\{H^1(K_n, A)\}$. Therefore $\varinjlim S_A^{\mathrm{str}}(K_n)$ is a Γ-submodule of $H^1(K_\infty, A)$.

PROPOSITION 4. *If $A^*(K_\infty)$ is finite, then*

$$\varinjlim S_A^{\mathrm{str}}(K_n) = S_A^{\mathrm{str}}(K_\infty),$$

where

$$S_A^{\mathrm{str}}(K_\infty) = \ker(H^1(K_\infty, A) \to \prod_{\lambda \nmid p} H^1(I_\lambda, A) \times \prod_{\lambda \mid p} H^1((K_\infty)_\lambda, A/F_v^+ A)).$$

is the strict Selmer group defined by Greenberg in [5].

Proposition 4 applies to our situation since assumptions (2) and (4) combine to show that $A^*(K_\infty)$ is finite.

Proof. Let λ be a prime of K_∞ over a prime v of K, and let v_n be the prime of K_n lying below λ. We only need to show that

$$\varinjlim H^1(g_{v_n}, A^{I_{v_n}})_{\mathrm{div}} = H^1(g_\lambda, A^{I_\lambda})$$

for $v \nmid p$ and

$$\varinjlim H^1((K_n)_{v_n}, F_v^+ A)_{\mathrm{div}} = H^1((K_\infty)_\lambda, F_v^+ A)$$

for $v \mid p$ when $n \to \infty$. For $v \nmid p$, $(K_\infty)_\lambda / K_v$ is unramified, so g_λ has profinite order prime to p. Thus $H^1(g_\lambda, A^{I_\lambda}) = 0$. Hence the proof in this case is clear. Suppose $v \mid p$. As $H^1((K_n)_{v_n}, F_v^+ A)$ is cofinitely generated over $\mathbb{Z}_p$, $p^m H^1((K_n)_{v_n}, F_v^+ A) = H^1((K_n)_{v_n}, F_v^+ A)_{\mathrm{div}}$ for m large. From the proof of Corollary 1 in [5, p. 111],

$$H^1((K_n)_{v_n}, F_v^+ A)/H^1((K_n)_{v_n}, F_v^+ A)_{\mathrm{div}} \cong H^0((K_n)_{v_n}, F_v^+ A_m^*) \subseteq F_v^+ A^*(K_\infty).$$

Hence the order of the first group is bounded when $n \to \infty$. Therefore

$$H^1((K_\infty)_\lambda, F_v^+ A)/(\varinjlim H^1((K_n)_{v_n}, F_v^+ A)_{\mathrm{div}})$$

is finite. Since $H^1((K_\infty)_\lambda, F_v^+ A)$ is divisible [5, p. 111], this quotient must be zero. □

By our assumption and Theorem 2, there is a skew-symmetric pairing on $S_A^{\mathrm{str}}(K_n)$ which is nondegenerate modulo its maximal divisible subgroup. We will use it to prove Theorem 3.

Since, by the assumption, $S_A^{\mathrm{str}}(K_\infty)$ is a cofinitely generated $\mathbb{Z}_p$-module, the image of $D_n = S_A^{\mathrm{str}}(K_n)_{\mathrm{div}}$ in $S_A^{\mathrm{str}}(K_\infty)$ becomes stabilized for large n, denoted it by D_∞. Thus we have the exact sequence of $\{\Gamma_n\}$-modules

$$0 \to \{D_n\} \to \{S_A^{\mathrm{str}}(K_n)\} \to \{S_A^{\mathrm{str}}(K_n)/D_n\} \to 0$$

which gives the exact sequence of Λ-modules

$$0 \to D_\infty \to S_A^{\mathrm{str}}(K_\infty) \to S_A^{\mathrm{str}}(K_\infty)/D_\infty \to 0.$$

We first consider the direct system $\{T_n\} = \{S_A^{\mathrm{str}}(K_n)/D_n\}$ with direct limit $T_\infty = S_A^{\mathrm{str}}(K_\infty)/D_\infty$.

THEOREM 7. *With the same assumption as in Theorem* 3, *the* $\mathbb{Z}_p$-corank *of* T_∞ *is even.*

First we need a lemma.

LEMMA 3. *Let* N *be a finite abelian p-group with* $p \neq 2$. *Let* $\langle , \rangle$ *be a nondegenerate skew-symmetric pairing on* N. *Then* N *has a maximal isotropic subgroup* B *that is a direct summand of* N. *Thus* $N \cong B \times N/B$ *and* $N/B \cong B$.

Proof. Let $N = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r$, with $\mathbb{Z}x_i \cong \mathbb{Z}/p^{a_i}\mathbb{Z}$ for $i = 1, \ldots, r$ and $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_r$. The pairing gives an isomorphism $N \cong \mathrm{Hom}(N, \mathbb{Q}/\mathbb{Z})$. Thus the image of x_1 in $\mathrm{Hom}(N, \mathbb{Q}/\mathbb{Z})$ is of order p^{a_1}. This implies that there is an $x_{i_1} \in \{x_1, \ldots, x_r\}$ such that $\langle x_1, x_{i_1} \rangle$ is of order p^{a_1}. Thus changing a generator of $\mathbb{Z}x_{i_1}$ if necessary, we might assume that $\langle x_1, x_{i_1} \rangle = 1/p^{a_1} (\mathrm{mod}\ 1)$. Thus the pairing is nondegenerate on $H_1 = \mathbb{Z}x_1 \oplus \mathbb{Z}x_{i_1}$. Hence $H_1 \cap H_1^\perp = 0$ and this in turn shows that the restriction of the pairing is nondegenerate on $H_1^\perp$. We have $N = H_1 \oplus H_1^\perp$. Repeat the above procedure to $H_1^\perp$. At the end we get a orthogonal decomposition $N = H_1 \oplus \cdots \oplus H_s$, $H_i = \mathbb{Z}b_{2i-1} \oplus \mathbb{Z}b_{2i}$ and the matrix of the pairing with respect to b_{2i-1}, b_{2i} is of the form $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Let $B = \oplus_{i=1}^{s} \mathbb{Z}b_{2i-1}$, then the size of B is half of N and $B \subseteq B^\perp$, so $B = B^\perp$. Thus B is a maximal isotropic subgroup. From the construction, B is a direct summand of N. □

By the fundamental theorem of finitely generated abelian groups, N can be uniquely expressed as a direct sum $\mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^z\mathbb{Z}$ with $a \geqslant b \geqslant \cdots \geqslant z$. We call $(a, b, \ldots, z)$ the index of N. Let $\{A_n\}$ be a direct system of finite abelian p-groups with bounded number of generators. For each n, let $(a_n, \ldots, z_n)$ be the index of A_n. Then $\{\alpha_n\}$ for $\alpha = a, \ldots, z$ are sequences of non-negative integers. We say that $\{A_n\}$ is homogeneous if each of these sequences either goes to infinity or remains bounded as n goes to infinity. For a homogeneous system $\{A_n\}$, the number of sequences $\{\alpha_n\}$ that is convergent to infinity is called the corank of $\{A_n\}$ and is denoted by $\mathrm{corank}(\{A_n\})$.

PROPOSITION 5. *Let* $\{A_n\}$ *be a homogeneous direct system of finite abelian p-groups with* corank d. *Let* $A_\infty = \varinjlim A_n$. *Then*

(1) $d \geqslant \mathrm{corank}_{\mathbb{Z}_p}(A_\infty)$,

(2) *if the bounded sequences have bound less than* M, *then for* n *large we have* $(A_n)_M \cong (\mathbb{Z}/p^M\mathbb{Z})^d \times B_n$, *where* $(A_n)_M = \ker(p^M : A_n \to A_n)$ *and* B_n *has exponent less than* M.

Proof. Let $i_n : A_n \to A_\infty$ be the natural map. Since $i_n(A_n)$ is a quotient of A_n the index of $i_n(A_n)$ is less than the index of A_n. Thus $d = \mathrm{corank}(\{A_n\}) \geqslant$

corank$(\{i_n(A_n)\})$. But the last term is precisely the $\mathbb{Z}_p$-corank of A. This proves (1). (2) is clear.

PROPOSITION 6. *Let $\{A_n\}$ be a direct system of finite abelian p-groups with a bounded number of generators. Let $A_\infty = \varinjlim A_n$ and let $i_n: A_n \to A_\infty$ be the canonical map. The following statements are equivalent*:

(1) *the exponents of* $\ker(i_n)$ *are bounded.*

(2) $\{A_n\}$ *is homogeneous and* $\operatorname{corank}_{\mathbb{Z}_p}(A_\infty) = \operatorname{corank}(\{A_n\})$.

Proof. (1)⇒(2). Let $(a'_n, \ldots, z'_n)$ be the index of $i_n(A_n)$. Since $i_n(A_n) \subseteq i_{n+1}(A_{n+1})$, each sequence $\{\alpha'_n\}$, $\alpha = a, \ldots, z$ is a monotonely increasing sequence of non-negative integers. Hence it either has infinity as limit or is bounded. Thus it is homogeneous and $\operatorname{corank}(\{i_n(A_n)\}) = \operatorname{corank}_{\mathbb{Z}_p}(A_\infty)$. Since $\ker(i_n)$ have bounded exponents, there is integer N such that $\ker(i_n) \subseteq (A_n)_N$ for any n. Thus we have surjective maps $A_n \to A_n/\ker(i_n) \cong i_n(A_n)$, and $i_n(A_n) \cong A_n/\ker(i_n) \to A_n/(A_n)_N$. Let $(a''_n, \ldots, z''_n)$ be the index of $A_n/(A_n)_N$. It is clear that $\alpha''_n = \max\{\alpha_n - N, 0\}$, $\alpha_n = a, \ldots, z$ since the index of $(A_n)_N$ is $(\min\{a_n, N\}, \ldots, \min\{z_n, N\})$. Note that if A and A' are finite abelian p-groups with indices $(a, \ldots, z)$ and $(a', \ldots, z')$ and if we have a surjective map $A \to A'$, then $\alpha \geqslant \alpha'$ for $\alpha = a, \ldots, z$. Thus we have $\alpha_n \geqslant \alpha'_n \geqslant \alpha''_n \geqslant \alpha_n - N$. This shows that $\alpha_n - \alpha'_n$ is bounded. Hence the sequences $\{\alpha_n\}$ and $\{\alpha'_n\}$ both go to infinity or both remain bounded. This implies that $\{A_n\}$ is homogeneous and $\operatorname{corank}(\{A_n\}) = \operatorname{corank}(\{i_n(A_n)\}) = \operatorname{corank}_{\mathbb{Z}_p}(A_\infty)$.

(2)⇒(1). Suppose $\ker(i_n)$ have unbounded exponents. Let d be the $\mathbb{Z}_p$-corank of A_∞. Choose M such that p^M is larger than the exponent of the cotorsion part of A_∞ and such that M is a uniform bound for the bounded sequences from $\{\alpha_n\}$, $\alpha = a, \ldots, z$. Then $(A_\infty)_M \cong (\mathbb{Z}/p^M\mathbb{Z})^d \times$ (finite group of exponent $< M$) and $(A_n)_M \cong (\mathbb{Z}/p^M\mathbb{Z})^d \times$ (finite group of exponent $< M$) for n large. Let $H \subseteq (A_\infty)_M$ be a subgroup isomorphic to $(\mathbb{Z}/p^M\mathbb{Z})^d$ and choose N such that $i_N(A_N) \supseteq H$ and such that $(A_n)_M \cong (\mathbb{Z}/p^M\mathbb{Z})^d \times$ (finite group of exponent $< M$) for $n > N$. Since $\ker(i_N)$ is finite and $\ker(i_N) = \varinjlim \ker(i_{N,N+n})$, where $i_{N,N+n}: A_N \to A_{N+n}$ is the natural map, $\ker(i_N) = \ker(i_{N+n})$ for n large. Since $\ker(i_n)$ have unbounded exponents, we can find $N_1 > N$ such that $\ker(i_N) = \ker(i_{N,N_1})$ and such that $\ker(i_{N_1})$ has exponent greater than M. Thus $\ker(i_{N_1})$ contains a copy of $\mathbb{Z}/p^M\mathbb{Z}$. Now $\ker(i_N) = \ker(i_{N,N_1})$ implies that $i_{N,N_1}(A_N) \cap \ker(i_{N_1}) = 0$. So $i_{N,N_1}(A_N) \oplus \ker(i_{N_1}) \subseteq A_{N_1}$. Since

$$i_{N,N_1}(i_N^{-1}(H)) \cong i_N^{-1}(H)/(i_N^{-1}(H) \cap \ker i_{N,N_1}) = i_N^{-1}(H)/(i_N^{-1}(H) \cap \ker i_N)$$
$$\cong i_N(i_N^{-1}(H)) = H \cong (\mathbb{Z}/p^M\mathbb{Z})^d$$

is contained in $i_{N,N_1}(A_N)$, A_{N_1} contains at least $d+1$ copies of $\mathbb{Z}/p^M\mathbb{Z}$. So $(A_{N_1})_M \cong (\mathbb{Z}/p^M\mathbb{Z})^c \times$ (finite group of exponent $< M$) with $c > d$. But by the choice of N, $(A_{N_1})_M \cong (\mathbb{Z}/p^M\mathbb{Z})^d \times$ (finite group of exponent $< M$). This is a contradiction. □

LEMMA 4. *Assume that $A(K_\infty)$ is finite. The natural maps $i_n: T_n \to T_\infty$ have bounded kernels.*

Proof. The kernel of $H^1(K_n, A) \to H^1(K_\infty, A)$ is $H^1(\Gamma^{p^n}, A(K_\infty)) \cong A(K_\infty)/(\gamma^{p^n}-1)A(K_\infty)$ which has bounded order for all n. Hence the kernel of the induced map $f_n: S_A^{\mathrm{str}}(K_n) \to S_A^{\mathrm{str}}(K_\infty)$ has bounded order. By the remark made before Theorem 7, $f_n(D_n) = D_\infty$ for n large. Thus the kernel of i_n is $(\ker(f_n) + D_n)/D_n$ for n large. Hence it also has bounded order. □

Proof of Theorem 7. From Theorem 2, there is a nondegenerate skew-symmetric pairing defined on T_n. By Lemma 3, we can find a maximal isotropical subgroup M_n of T_n such that we have a (noncanonical) decomposition $T_n \cong M_n \times T_n/M_n$ as abelian groups.

By assumption, $S_A^{\mathrm{str}}(K_\infty)$, hence T_∞ are finitely cogenerated over $\mathbb{Z}_p$. This implies that the finite subgroup of T_∞ has a uniform bound for the number of generators. In particular, the images of $T_n \to T_\infty$ have a uniform bound for the number of generators. Since by Lemma 4, the kernels of $T_n \to T_\infty$ also have a uniform bound for the number of generators, the T_n's have a uniform bound for the number of generators. Thus by Proposition 6, $\{T_n\}$ is homogeneous and $\operatorname{corank}\{T_n\} = \operatorname{corank}_{\mathbb{Z}_p} T_\infty$. Since M_n is a maximal isotropic subgroup of T_n under the pairing $\langle , \rangle_n$, we have $T_n/M_n \cong \operatorname{Hom}(M_n, \mathbb{Q}_p/\mathbb{Z}_p) \cong M_n$ as abelian groups. By Lemma 3, $T_n \cong M_n \times T_n/M_n$ as abelian groups. Thus the index of T_n is two copies of the index of M_n after proper permutations. In particular, $\operatorname{corank}\{T_n\} = 2\operatorname{corank}\{M_n\}$. Thus by Proposition 6, $\operatorname{corank}_{\mathbb{Z}_p} T_\infty = 2\operatorname{corank}_{\mathbb{Z}_p} M_\infty$, and hence is even. □

LEMMA 5. *Let p be odd. Let Y be a Γ_n-module which is a finite dimensional $\mathbb{Q}_p$-space. Then* $\dim_{\mathbb{Q}_p} Y \equiv \dim_{\mathbb{Q}_p} Y/(\gamma-1)Y \pmod 2$, *where γ is a generator of Γ_n.*

Proof. From the exact sequence

$$0 \longrightarrow Y^{\Gamma_n} \longrightarrow Y \xrightarrow{\gamma-1} Y \longrightarrow Y/(\gamma-1)Y \longrightarrow 0,$$

we have $\dim_{\mathbb{Q}_p}(Y/(\gamma-1)Y) = \dim_{\mathbb{Q}_p}(Y^{\Gamma_n})$. Since $\mathbb{Q}_p[\Gamma_n] \cong \mathbb{Q}_p[T]/(T^{p^n}-1) \cong \oplus_{i=0}^n \mathbb{Q}_p(\mu_{p^i})$, the $\mathbb{Q}_p[\Gamma_n]$-module Y is completely reducible and $Y \cong \oplus_{i=0}^n \mathbb{Q}_p(\mu_{p^i})^{c_i}$, for some $c_i \geqslant 0$. Since each $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p(\mu_{p^i}))$ is even for $i \geqslant 1$, we have

$$\dim_{\mathbb{Q}_p} Y \equiv c_0 \equiv \dim_{\mathbb{Q}_p}(Y^{\Gamma_n}) \pmod 2,$$

hence the result.

LEMMA 6. *Let X be a Γ_n-module which is a finitely generated $\mathbb{Z}_p$-module. Then* $\operatorname{rank}_{\mathbb{Z}_p} X \equiv \operatorname{rank}_{\mathbb{Z}_p}(X/(\gamma-1)X) \pmod 2$.

Proof. From Lemma 5 we have

$$\operatorname{rank}_{\mathbb{Z}_p} X = \dim_{\mathbb{Q}_p}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \equiv \dim_{\mathbb{Q}_p}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/(\gamma-1)(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \pmod 2.$$

Also $\operatorname{rank}_{\mathbb{Z}_p} X/(\gamma-1)X = \dim_{\mathbb{Q}_p}(X/(\gamma-1)X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. So we only need to show that

$$\dim_{\mathbb{Q}_p}(X/(\gamma-1)X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \dim_{\mathbb{Q}_p}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/(\gamma-1)(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

From the exact sequence

$$0 \to (\gamma-1)X \to X \to X/(\gamma-1)X \to 0, \quad \operatorname{rank} X/(\gamma-1)X = \operatorname{rank} X - \operatorname{rank}(\gamma-1)X.$$

So

$$\dim(X/(\gamma-1)X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \dim(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) - \dim((\gamma \div 1)X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$$

$$= \dim((X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/((\gamma-1)X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)).$$ This completes the proof.

Now we can give a proof of Theorem 3. From Theorem 7, $\operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_\infty) \equiv \operatorname{corank}_{\mathbb{Z}_p} D_\infty \pmod 2$. By the remark before Theorem 7, $D_\infty = D_n$ for n large, where $D_n = S_A^{\mathrm{str}}(K_n)_{\mathrm{div}}$. Thus $\operatorname{corank}_{\mathbb{Z}_p} D_\infty = \operatorname{corank}_{\mathbb{Z}_p} D_n = \operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_n)$. As $S_A^{\mathrm{str}}(K_n)$ is a $\mathbb{Z}_p[\Gamma_n]$-module of finite $\mathbb{Z}_p$-corank, Lemma 6 implies that

$$\operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_n) \equiv \operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_n)^{\Gamma_n} \pmod 2.$$

Consider the inflation-restriction sequence

$$0 \to H^1(\Gamma_n, A^{\Gamma^{p^n}}) \to H^1(K, A) \to H^1(K_n, A)^{\Gamma_n} \to H^2(\Gamma_n, A^{\Gamma^{p^n}}).$$

Since $H^1(\Gamma_n, A^{\Gamma^{p^n}})$ and $H^2(\Gamma_n, A^{\Gamma^{p^n}})$ are both finite, $\operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K) = \operatorname{corank}_{\mathbb{Z}_p} S_A^{\mathrm{str}}(K_n)^{\Gamma_n}$, hence the theorem.

References

[1] S. Bloch and K. Kato: *L*-functions and Tamagawa numbers of motives, The Grothendieck Festschrift, vol. 1, Birkhäuser (1990), 333–400.

[2] K. S. Brown: Cohomology of groups, Springer-Verlag (1982).

[3] J. Cassels: Arithmetic on curves of genus 1 (IV). Proof of the Hauptvermutung, *J. Reine Angew. Math.* 211 (1962), 95–112.

[4] M. Flach: A generalization of the Cassels-Tate pairing, *J. Reine Angew. Math.* 412 (1990), 113–127.
[5] R. Greenberg: Iwasawa theory for p-adic representations, *Adv. Stud. in Pure Math.* 17, Academic Press (1989), 97–137.
[6] R. Greenberg: Iwasawa theory for motives, in *L-functions and Arithmetic, Proceedings of the Durham Symposium, London Math. Soc. Lecture Notes Series*, vol. 153 (1991), pp. 211–233.
[7] L. Guo: On a generalization of Tate dualities with application to Iwasawa theory, Thesis, University of Washington, in preparation.
[8] B. Mazur: Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* 18 (1972), 183–266.
[9] W. G. McCallum: On the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve, *Invent. Math.* 93 (1988), 637–666.
[10] J. S. Milne: Arithmetic duality theorem, Academic Press (1986).
[11] K. Rubin: On the main conjecture of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* 93 (1988), 701–713.
[12] R. Shaw: Linear algebra and group representations, Academic Press (1983).
[13] J. H. Silverman: The arithmetic of elliptic curves, Springer-Verlag (1986).
[14] J. Tate: Duality theorems in Galois cohomology over number fields, *Proc. Intern. Congress Math.*, Stockholm (1962), 234–241.
[15] E. Weiss: Cohomology of groups, Academic Press (1969).