to show that $A_{-7}(\mathbf{Q})$ has positive rank. This is easily accomplished by searching for a rational point, and having the computer check that it has infinite order.

As a final note on this example, we thought that it would be interesting to know if A and A_{-7} have $\mathbf{Q}$-ranks of exactly 1 (although this is not needed to satisfy the proposition above). It turns out that they do, assuming standard conjectures (according Connell's Maple package Apecs). Then, we can specify the ranks of S_1 and S_2. If $\Sigma_K = \{\bar{P}\}$, then S_1 and S_2 each have $\mathbf{Z}_p$-ranks of one (we are assuming here that $<,>_p$ is non-degenerate to claim that S_2 has only rank 1). If $\Sigma_K = \{P, \bar{P}\}$, then S_1 has $\mathbf{Z}_p$-rank of 0 and S_2 has rank 2. In the latter case, inequalities of Proposition 7.1 predict that $0 \leq \mathrm{rank}_{\mathbf{Z}_p}(S_1) \leq 1$, and so the lower bound is achieved.

We conclude by considering an example which is similar to the previous one, except that rank $A(\mathbf{Q}) =$ rank $A(K) = 2$. Then, Proposition 7.1 again predicts $0 \leq \mathrm{rank}_{\mathbf{Z}_p}(S_1) \leq 1$ in the case that Σ_K is both primes above p. However, now the map in equation 11 must have an image of rank 1 (since $A(\mathbf{Q}) \otimes \mathbf{Z}_p$ is a subgroup of finite index in $A(K) \otimes \mathbf{Z}_p$, and it factors through $A(\mathbf{Q}_p)\hat{\otimes}\mathbf{Z}_p$ which is a rank one $\mathbf{Z}_p$-module). Thus in this case, the upper bound of Proposition 7.1 is achieved.

As an example of such a curve, we take

$$A: \quad y^2 = x^3 - 179x^2 + x$$

We found this curve by searching the tables of elliptic curves in [1]. It has rank 2 over $\mathbf{Q}$. It also has rank 2 over $K = \mathbf{Q}(\imath)$ since its twist by -1 has rank 0 over $\mathbf{Q}$. To complete the example, we only need to find a prime for which A has ordinary reduction which splits in K; $p = 5$ does the trick.

References

[1] Bremner, A., Jones, J.: On the equation $x^4 + mx^2y^2 + y^4 = z^2$. (to appear in J. Number Th.)

[2] Greenberg, R.: Iwasawa theory for p-adic representations, in Advanced Studies in Pure Mathematics **17**, 97-137 (1989)

[3] Jones, J.: A comparison of Selmer groups. Manuscripta Math. **68**, 391-398 (1990)

[4] Jones, J.: p-adic heights for semi-stable Abelian varieties. Comp. Math. **73**, 31-56 (1990)

[5] Mazur, B.: Rational points on abelian varieties with values in towers of number fields. Invent. math. **18**, 183-266 (1972)

[6] Mazur, B., Tate, J.: "Canonical heights via biextensions", in Arithmetic and Geometry, vol I, Birkhäuser, 195-238 (1983)

[7] Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. math. **84**, 1-48 (1986)

[8] McCallum, W.: Duality theorems for Neŕon models. Duke Math. J. **53**, 1093-1124 (1986)

[9] Milne, J.: Arithmetic Duality Theorems. Academic Press (1986)

[10] Nasybullin, A.: Elliptic Tate curves over local Γ-extensions. Math. Notes of U.S.S.R. **13** 322-327 (1973)

[11] Plater, A.: An Orthogonality Relation on the points of an elliptic curve. J. London Math. Soc. (2) **44**, 227-249 (1991)

[12] Schneider, P.: p-adic height pairings I. Invent. math. **69**, 401-409 (1982)

[13] Schneider, P.: Iwasawa L-functions of varieties over algebraic number fields. A first approach. Invent. math. **71**, 251-293 (1983)

[14] Schneider, P.: p-adic height pairings II. Invent. math. **79**, 329-374 (1985)

Department of Mathematics, Arizona State University, Tempe, AZ 85287

7.3. **Variation of Σ_K.** As mentioned in the introduction, one of the surprising benefits of the generalization of Plater's work given in this paper is the choice of the set Σ_K. Moreover, we suspect that the subgroups S_1 and S_2 depend on this choice in an essential way.

To produce an example, we will start with a quadratic imaginary field K and a rational prime p which splits in K, $(p) = P\bar{P}$. Then, K will have a Γ-extension L in which P is unramified, and we have two choices for Σ_K, namely $\{\bar{P}\}$ and $\{P, \bar{P}\}$. We will use $S_1(\Sigma_K)$ to indicate the choice of Σ_K.

Proposition 7.2. *If A is an elliptic curve over $\mathbf{Q}$ so that*

$$0 < \text{rank } A(\mathbf{Q}) < \text{rank } A(K)$$

then $S_1(\{P, \bar{P}\}) \neq S_1(\{\bar{P}\})$.

Proof: From the inequalities of Proposition 7.1, we get immediately that $\text{rank}_{\mathbf{Z}_p}(S_1(\{\bar{P}\})) = r - 1$ (since in this case $d = e = 1$). So, it suffices to show that $\text{rank}_{\mathbf{Z}_p}(S_1(\{P, \bar{P}\})) \leq r - 2$.

Since p splits in K, the completions K_P and $K_{\bar{P}}$ are each equal to $\mathbf{Q}_p$, and consequently $A(K_P)\hat{\otimes}\mathbf{Z}_p$ is a rank one $\mathbf{Z}_p$-module (and similarly for $\bar{P}$). So, the result follows provided we can show that the following map has an image with rank 2 over $\mathbf{Z}_p$:

$$A(\mathcal{O}_K) \otimes \mathbf{Z}_p \to \left(A(\mathcal{O}_{K_P})\hat{\otimes}\mathbf{Z}_p \times A(\mathcal{O}_{K_{\bar{P}}})\hat{\otimes}\mathbf{Z}_p\right)$$

Since $0 < \text{rank } A(\mathbf{Q})$, we have at least a rank one submodule in the image which is invariant under $\text{Gal}(K/\mathbf{Q})$. Hence, it maps diagonally into the product. On the other hand, since rank $A(\mathbf{Q}) <$ rank $A(K)$, we have a rank one submodule in the image which is not $\text{Gal}(K/\mathbf{Q})$ invariant, and hence is not mapped in diagonally. Thus, we have two rank one submodules which are clearly independent (i.e., span a rank 2 $\mathbf{Z}_p$-submodule as desired). $\square$

7.4. **Examples.** We start with an example of an elliptic curve which satisfies Proposition 7.2. Consider the field $K = \mathbf{Q}(\sqrt{-7})$ and let $p = 11$. Note that 11 splits in K: $(11) = (\pi)(\bar{\pi})$ where $\pi = 2 + \sqrt{-7}$. For our elliptic curve we take:

$$A: \quad y^2 = x^3 - 5x^2 + 15x - 10 \tag{12}$$

The choice here was not entirely random. To increase our chances of finding a curve satisfying Proposition 7.2, we looked at curves whose cubic was of the form

$$(x-1)(x-\pi)(x-\bar{\pi}) + d^2$$

since they would have a $\mathbf{Q}$ rational point $(1, d)$ and a K rational point (π, d). By picking different values for d, we hoped to find a curve where the two aforementioned points would be independent. The curve in equation 12 was the first one we tried, namely with $d = 1$. It turns out to be ordinary at 11 (although we could use any prime which splits in K and at which A has ordinary reduction).

It is not hard to have a computer estimate the height-regulator for the two points mentioned above to verify that they are independent points of infinite order. However, this can be accomplished even more easily using computing packages for elliptic curves over $\mathbf{Q}$ as follows. First check that $(1, 1)$ has infinite order on the curve 12 above. Then, note that $A(K)$ has a subgroup of finite index which is the direct sum of $A(\mathbf{Q})$ and $A_{-7}(\mathbf{Q})$ where A_{-7} is the twist of A by -7 (decomposing $A(K)$ into $\pm$ eigenspaces for the nontrivial element of $\text{Gal}(K/\mathbf{Q})$). So, it suffices

as the kernel of $g'_\Sigma \circ \eta$, which in turn is quasi-isomorphic to the image of S_2 at $\mathfrak{S}_L(\Sigma_L)^\Gamma$. $\square$

7. Discussion

Here we discuss special situations and examples. For simplicity, we will assume throughout this discussion that Sh_K is finite. Fixing an isogeny between A and $\tilde{A}$, $<,>_p$ becomes a pairing on $A(K)\otimes\mathbf{Z}_p$. We will focus our attention on the behavior of the first subgroup S_1 since it, along with $<,>_p$ determines S_2.

7.1. Ranks.

We will investigate the possibilities for the ranks of S_1 and S_2 as $\mathbf{Z}_p$-modules (following the corresponding analysis in [11]).

Assume that d is the dimension of A as an abelian variety, and that $A(K)$ has rank $r > 0$ as an abelian group (or else S_1 and S_2 must have rank 0). Recall that by equation 1,

$$S_1 = \ker : A(K) \otimes \mathbf{Z}_p \to \prod_{v\in\Sigma_K} A(K_v)\hat{\otimes}\mathbf{Z}_p. \tag{11}$$

Now, $\operatorname{rank}_{\mathbf{Z}_p}(A(K)\otimes\mathbf{Z}_p) = r$. On the other hand, $A(K_v)$ has a subgroup of finite index which is isomorphic to ${\mathbf{Z}_p}^{e_v d}$ where $e_v = [K_v : \mathbf{Q}_p]$. Let $e = \sum_{v\in\Sigma_K} e_v$. Since Σ_K is contained in the places of K above over p we have $e \leq [K\colon \mathbf{Q}]$. In any case, $\operatorname{rank}_{\mathbf{Z}_p}(\prod_{v\in\Sigma_K} A(K_v)\hat{\otimes}\mathbf{Z}_p) = de$. Finally, the image of the map in equation 11 is at least 1 since $A(K)$ injects into the sets of local points. So we have

Proposition 7.1.

$$\max\{0, r - de\} \leq \operatorname{rank}_{\mathbf{Z}_p}(S_1) \leq r - 1.$$

Then, by the main theorem, $\operatorname{rank}_{\mathbf{Z}_p}(S_2) \geq r - \operatorname{rank}_{\mathbf{Z}_p}(S_1)$ with equality if $<,>_p$ is non-degenerate. Note in the case of an elliptic curve over $\mathbf{Q}$, $d = e = 1$, so this reduces to $\operatorname{rank}_{\mathbf{Z}_p}(S_1) = r - 1$ and $\operatorname{rank}_{\mathbf{Z}_p}(S_2) = 1$.

We are unable to pin down the rank of S_1 any more than Proposition 7.1. One expects that in general, the image of the map in 11 will be large, and hence, S_1 will be relatively small. However, as we will see below, this is not always the case.

7.2. Variation of the Γ-extension.

It is natural to ask how the subgroups in the main theorem behave as we vary the choice of Γ-extension, and more specifically, does the cyclotomic Γ-extension play a special role. So, fix A and the ground field K (which is not totally real so that there will be a choice of Γ-extension), and vary L. For different choices of L, ramification of the primes over p may vary. So, to be consistent we also fix Σ_K to be all places over p.

Interestingly, the first subgroup S_1 is clearly independent of the choice of L. However, variation of L will affect $<,>_p$, and consequently, S_2. Exactly how S_2 changes then reduces to how $<,>_p$ is affected by variation of L, or equivalently, to the choice of a p-adic logarithm. See section 4 of [6] for a discussion of this point.

There is very little we can add by assuming that L is the cyclotomic Γ-extension, except in regard to degeneracy of the p-adic height pairing (which in turn, affects S_2). One expects that for almost all choices of L, $<,>_p$ will be non-degenerate. However, it has been conjectured by Schneider that $<,>_p$ is *always* non-degenerate for the cyclotomic Γ-extension of K.

The image of μ_Σ then, is the subset of $H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ which maps to 0 in $H^2(\mathcal{O}_L, A^0_{p^\infty})^\Gamma$.

Let

$$X = \ker : H^2_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty}) \to H^2(\mathcal{O}_L, A^0_{p^\infty}).$$

The image of $H^2_\Sigma(\mathcal{O}_L, A^0_{p^\infty})^\Gamma \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ intersected with the image of μ_Σ is then the image of X^Γ in $H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$. We now pull this subgroup back via μ_Σ.

We have the commutative diagram

$$\begin{array}{ccc} H^2_\Sigma(\mathcal{O}_L, A^0_{p^\infty})^\Gamma & \longleftarrow & X^\Gamma \\ \| & & \downarrow \delta \\ H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & & \mathfrak{S}_L(\Sigma_L)_\Gamma \\ \downarrow & & \| \\ H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & \xleftarrow{\mu_\Sigma} & H^1(\mathcal{O}_L, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \end{array} \quad (9)$$

We have encountered the left column and μ_Σ before. Since X is a subgroup of $H^2_\Sigma(\mathcal{O}_L, A^0_{p^\infty})$, the map in the top row is the induced map on invariants. The identification of $\mathfrak{S}_L(\Sigma_L)_\Gamma$ with $H^1(\mathcal{O}_L, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ occurs in the height pairing 5, and the proof of which is essentially in [4], pp. 36-37.

To define δ, we start with the exact sequence

$$0 \to \mathfrak{S}_L(\Sigma_L) \to H^1(\mathcal{O}_L - \Sigma, A^0_{p^\infty}) \to X \to 0$$

which is truncated from the relative cohomology sequence. Taking cohomology of Γ for this short exact sequence, we get the following exact sequence (which includes δ).

$$\begin{aligned} 0 \to \mathfrak{S}_L(\Sigma_L)^\Gamma \to H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})^\Gamma \to X^\Gamma \xrightarrow{\delta} \mathfrak{S}_L(\Sigma_L)_\Gamma \\ \longrightarrow H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})_\Gamma \to X_\Gamma \to 0 \quad (10) \end{aligned}$$

Note that the bottom row of 9 along with the identification $\mathfrak{S}_L(\Sigma_L)_\Gamma = H^1(\mathcal{O}_L, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ comes from the height pairing, and the image of the composition in the left column is quasi-isomorphic to S_1^{ann} at $H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$. To pull back S_1^{ann} through μ_Σ, we consider the image of the left column intersected with the image of μ_Σ. As mentioned above, this is precisely the image of X^Γ. So, S_1^{ann} at $(\mathfrak{S}_L(\Sigma_L))_\Gamma$ is quasi-isomorphic to the image of δ. From the exact sequence 10, this is the same as the kernel of $\mathfrak{S}_L(\Sigma_L)_\Gamma \to H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})_\Gamma$. $\square$

To finish the proof of theorem 6.1, we consider the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{S}_L(\Sigma_L)^\Gamma & \xrightarrow{g_\Sigma} & \mathfrak{S}_L(\Sigma_L)_\Gamma \\ \downarrow \eta & & \downarrow \pi \\ H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})^\Gamma & \xrightarrow{g'_\Sigma} & H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})_\Gamma \end{array}$$

We know that S_1^{ann} at $\mathfrak{S}_L(\Sigma_L)_\Gamma$ is quasi-isomorphic to the kernel of π, and so S_1^{ann} at $\mathfrak{S}_L(\Sigma_L)^\Gamma$ is quasi-isomorphic to the kernel of $\pi \circ g_\Sigma$. This is the same

To see that $H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) \to H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ is surjective, we analyze the group $H^2_{\Sigma_K}(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})$ using the spectral sequence (see the appendix to [13])

$$H^p(\Gamma, H^q_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})) \Rightarrow H^{p+q}_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty}).$$

The long exact sequence of low order terms (combined with the fact that Γ has p-cohomological dimension 1) gives

$$0 \to H^1(\Gamma, H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})) \to H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty}) \to H^2_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})^\Gamma \to 0.$$

Thus, $H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} = H^2_\Sigma(\mathcal{O}_L, A^0_{p^\infty})^\Gamma$.

Now, it suffices to show that $H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) \to H^2_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})^\Gamma$ is surjective. We apply Lemma 6.5 below. For primes which ramify in $\mathcal{O}_L/\mathcal{O}_K$, the hypothesis that $A(K_v)/\mathbf{N}A(K_v)$ is finite is satisfied by assumption. For the unramified primes in Σ_K we appeal to [5], section 4.

By the commutativity of diagram 7, S_1^{ann} is quasi-isomorphic to the image of the composition of the maps

$$\bigoplus_{v\in\Sigma_K} H^1(K_v, A_{p^\infty}) = \bigoplus_{v\in\Sigma_K} H^1(K_v, A^0_{p^\infty}) \xrightarrow{\tau}\!\!\!\!\!\rightarrow H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) \twoheadrightarrow$$
$$H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$$

Because the first three maps in this composition are surjective, this can be abbreviated to

$$\mathrm{Im} : H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}.$$

□

Lemma 6.5. *If $A(K_v)/\mathbf{N}A(K_v)$ is finite for all $v \in V_K$ (V_K a set of places of $\mathcal{O}_K$), and V_L are the places of $\mathcal{O}_L$ lying over V_K, then*

$$H^2_{V_K}(\mathcal{O}_K, A^0_{p^\infty}) \to H^2_{V_L}(\mathcal{O}_L, A^0_{p^\infty})^\Gamma$$

is surjective.

Proof: This is Corollary 5.4 of [5] in a more general context. However, the proof carries over without difficulty. □

Lemma 6.6. *The image of S_1^{ann} at $\mathfrak{S}_L(\Sigma_L)_\Gamma$ is quasi-isomorphic to*

$$\ker : \mathfrak{S}_L(\Sigma_L)_\Gamma \to H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})_\Gamma.$$

Proof: We consider the map μ_Σ. It is defined as follows. From the spectral sequence (appendix to [13])

$$H^p(\Gamma, H^q(\mathcal{O}_L, A^0_{p^\infty})) \Rightarrow H^{p+q}(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty}) \tag{8}$$

we get the following exact sequence from the low order terms:

$$0 \to H^1(\Gamma, H^1(\mathcal{O}_L, A^0_{p^\infty})) \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty}) \to H^2(\mathcal{O}_L, A^0_{p^\infty})^\Gamma \to 0.$$

The group $H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})$ maps to $H^1(\mathcal{O}_L, A^0_{p^\infty})$ by the relative cohomology sequence. Hence we get the short exact sequence defining μ_Σ,

$$0 \to H^1(\Gamma, H^1(\mathcal{O}_L, A^0_{p^\infty}))/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \xrightarrow{\mu_\Sigma}$$
$$H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \to H^2(\mathcal{O}_L, A^0_{p^\infty})^\Gamma \to 0.$$

We break the proof into a series of lemmas.

Lemma 6.4. *S_1^{ann} at $H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ is quasi-isomorphic to* $\mathrm{Im} : H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$.

Proof: The identification $H^1(\mathcal{O}_K, T_p(\tilde{A}))^* = H^2(\mathcal{O}_K, A_{p^\infty})$ in the height pairing comes from taking the limit over ν in McCallum's duality $H^1(\mathcal{O}_K, \tilde{A}_{p^\nu})^* = H^2(\mathcal{O}_K, A_{p^\nu})$ (see [8]). Using the local analogue as well (i.e., $H^1(K_v, \tilde{A}_{p^\nu})^* = H^1(K_v, A_{p^\nu})$), we find that S_1^{ann} maps to

$$\mathrm{Im}\colon \bigoplus_{v \in \Sigma_K} H^1(K_v, A_{p^\infty}) \xrightarrow{f} H^2(\mathcal{O}_K, A_{p^\infty}). \tag{6}$$

Now, consider the following commutative diagram:

$$\begin{array}{ccccc}
\bigoplus_{v\in\Sigma_K} H^1(K_v, A_{p^\infty}) & \to & H^2_{\Sigma_K}(\mathcal{O}_K, A_{p^\infty}) & \to & H^2(\mathcal{O}_K, A_{p^\infty}) \\
\| & & \uparrow & & \uparrow{\scriptstyle\varphi_2} \\
\bigoplus_{v\in\Sigma_K} H^1(K_v, A^0_{p^\infty}) & \overset{\tau}{\twoheadrightarrow} & H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) & \to & H^2(\mathcal{O}_K, A^0_{p^\infty}) \\
 & & \twoheaddownarrow & & \downarrow{\scriptstyle\theta_\Sigma} \\
 & & H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & \to & H^2(\mathcal{O}_L/\mathcal{O}_K)/\overline{H^1_{\Sigma_L}}
\end{array} \tag{7}$$

where $H^2(\mathcal{O}_L/\mathcal{O}_K)/\overline{H^1_{\Sigma_L}}$ is a shorthand for $H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$.

Note that the composition of the maps in the top row is the map f in 6 above and the right column comes from the height pairing 5. In the top row, the first map comes from the relative cohomology sequence locally, giving

$$\bigoplus_{v\in\Sigma_K} H^1(K_v, A_{p^\infty}) \to \bigoplus_{v\in\Sigma_K} H^2_?(\mathcal{O}_K, A_{p^\infty}) = H^2_{\Sigma_K}(\mathcal{O}_K, A_{p^\infty}).$$

The second map comes from the global relative cohomology sequence. The same is true for the second row, except with the sheaf $A^0_{p^\infty}$, and for the third row, but in equivariant cohomology.

The map τ is surjective for the following reason. Making the identification, $H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) = \bigoplus_{v\in\Sigma_K} H^2_?(\mathcal{O}_{K_v}, A^0_{p^\infty})$, we reduce to showing that

$$H^1(K_v, A^0_{p^\infty}) \to H^2_?(\mathcal{O}_{K_v}, A^0_{p^\infty})$$

is onto. But, the cokernel is bounded by the next term in the relative cohomology sequence, namely $H^2(\mathcal{O}_{K_v}, A^0_{p^\infty})$. From the Kummer sequence

$$0 \to H^1(\mathcal{O}_{K_v}, A^0) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to H^2(\mathcal{O}_{K_v}, A^0_{p^\infty}) \to H^2(\mathcal{O}_{K_v}, A^0)_{p^\infty} \to 0$$

we learn that $H^2(\mathcal{O}_{K_v}, A^0_{p^\infty}) = 0$ because $H^i(\mathcal{O}_{K_v}, A^0) = 0$ for $i = 1, 2$ ([8] Proposition 3.1).

The maps from the second row to the first come from the map on sheaves $A^0_{p^\infty} \to A_{p^\infty}$. The equality in the leftmost column then follows since $A^0_{p^\infty}$ and A_{p^∞} have the same generic fibers, hence they give the same sheaf over $spec(K_v)$.

As previously mentioned, the map θ_Σ comes from the natural map $H^2(\mathcal{O}_K, A^0_{p^\infty}) \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})$, composed with the projection to the indicated quotient. The map $H^2_{\Sigma_K}(\mathcal{O}_K, A^0_{p^\infty}) \to H^2_\Sigma(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}$ is defined in a similar fashion.

bounded in the extensions L_v/K_v. Moreover, the contribution from a prime of good reduction is trivial, and primes of bad reduction split finitely in L. Hence, $\bigoplus_{v\in\Sigma_L - T_L} H^1(\mathcal{O}_{L_v}, A^0_{p^\infty})$ is also finite.

Since, each of the horizontal maps is a quasi-isomorphism, diagram 5 defines the same pairing as diagram 4. □

6. The Main Result

We repeat our assumptions here for the convenience of the reader.

Theorem 6.1. *Let A be an abelian variety over a number field K. Let $<,>_p$ be a p-adic height pairing affiliated to a Γ-extension L/K, such that every prime of bad reduction for A splits finitely in L. Assume that A has semi-stable reduction at every prime of K dividing p, and that at every prime v of K which ramifies in L, A has ordinary reduction such that $A(K_v)/\mathbf{N}A(K_v)$ is finite. Then, the annihilator of S_1 is S_2.*

Remark 6.2. *In general, one expects the local assumption at places v of K ramifying in L (that $A(K_v)/\mathbf{N}A(K_v)$ is finite) to hold automatically provided A has ordinary reduction at v. On one hand, it is conjectured to always hold for the cyclotomic Γ-extension. Furthermore, it is known to hold in the following cases:*

1. *A has good ordinary reduction at v (see [5])*
2. *A is an elliptic curve with non-split multiplicative reduction at v (see [10])*
3. *A is an elliptic curve with split multiplicative reduction with Tate parameter q such that $\log_v(q) \neq 0$, where $\log_v$ is the p-adic logarithm of K_v associated with the extension L/K (see [10]).*

Corollary 6.3. *With the assumptions above, if $<,>_p$ is non-degenerate, then S_1 and S_2 are orthogonal complements for $<,>_p$.*

Proof of corollary: All we need to check is that $H^1(\mathcal{O}_K, T_p(A))$ and $H^1(\mathcal{O}_K, T_p(\tilde{A}))$ have the same $\mathbf{Z}_p$-ranks. But this follows since A and $\tilde{A}$ are isogenous. □

Proof of theorem 6.1: We will trace the subgroups S_1 and S_2 through the height pairing 5 to a common point, namely $\mathfrak{S}_L(\Sigma_L)^\Gamma$. Note, we only need to know the images of the subgroups up to quasi-isomorphism. This is especially helpful since each of the maps in the pairing is a quasi-isomorphism, with the possible exception of μ_Σ and g_Σ, and μ_Σ is injective (the proofs are the same as for the corresponding statements in [4]). For example, S_2 at $\mathfrak{S}_L(\Sigma_L)^\Gamma$ is quasi-isomorphic to

$$\ker : \mathfrak{S}_L(\Sigma_L)^\Gamma \to H^1(\mathcal{O}_L, -\Sigma_L, A^0_{p^\infty})_\Gamma$$

by its definition (sequence 2) and the fact that each of the each of the maps in the right column of the height pairing 5 is a quasi-isomorphism.

In the case of S_1, we consider the dual of its annihilator at various points in the height pairing, which we denote by S_1^{ann}. For example, since

$$S_1^* = \mathrm{cok} : \bigoplus_{v\in\Sigma_K} H^1(K_v, T_p(\tilde{A}))^* \to H^1(\mathcal{O}_K, T_p(\tilde{A}))^*,$$

S_1^{ann} at $H^1(\mathcal{O}_K, T_p(\tilde{A}))^*$ is given by the

$$\mathrm{Im} : \bigoplus_{v\in\Sigma_K} H^1(K_v, T_p(\tilde{A}))^* \to H^1(\mathcal{O}_K, T_p(\tilde{A}))^*.$$

Proposition 5.1. *The height pairing defined by 3 can be induced by*

$$
\begin{tikzcd}
H^1(\mathcal{O}_K, T_p(\tilde{A}))^* \arrow[d, equal] & \mathrm{Hom}_{\mathbf{Z}_p}(H^1(\mathcal{O}_K, T_p(A)), \mathbf{Z}_p)^* \arrow[d, equal] \\
H^2(\mathcal{O}_K, A_{p^\infty}) & \mathrm{Div}\, H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d] \\
H^2(\mathcal{O}_K, A^0_{p^\infty}) \arrow[u, "\varphi_2"] \arrow[d, "\theta_\Sigma"] & H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d, "i_\Sigma"] \\
H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & \mathfrak{S}_K(\Sigma_K) \arrow[dd, "\alpha_\Sigma"] \\
H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \arrow[u, "\mu_\Sigma"] \arrow[d, equal] & \\
H^1(\Gamma, \mathfrak{S}_L(\Sigma_L)) & H^0(\Gamma, \mathfrak{S}_L(\Sigma_L)) \arrow[l, "g"']
\end{tikzcd}
\tag{5}
$$

Proof: The transition from diagram 4 to diagram 5 is given by the commutative diagram:

$$
\begin{tikzcd}
H^2(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d, "\theta"] & = & H^2(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d, "\theta_\Sigma"] \\
H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & \rightarrow & H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \\
H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \arrow[u, "\mu"] \arrow[d, equal] & \rightarrow & H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{\Sigma_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \arrow[u, "\mu_\Sigma"] \arrow[d, equal] \\
H^1(\Gamma, \mathfrak{S}_L(T_L)) & \rightarrow & H^1(\Gamma, \mathfrak{S}_L(\Sigma_L)) \\
H^0(\Gamma, \mathfrak{S}_L(T_L)) \arrow[u, "g"] & \rightarrow & H^0(\Gamma, \mathfrak{S}_L(\Sigma_L)) \arrow[u, "g_\Sigma"] \\
\mathfrak{S}_K(T_K) \arrow[u, "\alpha"] & \rightarrow & \mathfrak{S}_K(\Sigma_K) \arrow[u, "\alpha_\Sigma"] \\
H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[u, "i"] & = & H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[u, "i_\Sigma"]
\end{tikzcd}
$$

Each of the maps in the right column are the analogues of the corresponding maps in the left column. All we need is that each of the horizontal maps is a quasi-isomorphism. Each kernel and cokernel is either trivial or is bounded by the orders of the groups $\bigoplus_{v\in\Sigma_L-T_L} H^1_{\cdot}(\mathcal{O}_{L_v}, A^0_{p^\infty})$ or $\bigoplus_{v\in\Sigma_K-T_K} H^1_{\cdot}(\mathcal{O}_{K_v}, A^0_{p^\infty})$. We illustrate this in the case of rows 4 and 5 of the diagram. From the definition of $\mathfrak{S}_L(V)$, we get the exact sequence

$$\bigoplus_{v\in\Sigma_L-T_L} H^1_{\cdot}(\mathcal{O}_{L_v}, A^0_{p^\infty}) \to \mathfrak{S}_L(T_L) \to \mathfrak{S}_L(\Sigma_L) \to 0.$$

Taking cohomology for Γ and noting that Γ has p-cohomological dimension 1, we find that row 4 has trivial cokernel and the kernel of row 4, as well as the kernel and cokernel of row 5 are bounded by $\bigoplus_{v\in\Sigma_L-T_L} H^1_{\cdot}(\mathcal{O}_{L_v}, A^0_{p^\infty})$.

Now, by Lemma 3.1 of [4] $H^1_{\cdot}(\mathcal{O}_{K_v}, A^0_{p^\infty}) = \Phi(\mathcal{O}_{K_v})_{p^\infty}$, the group of connected components in the Néron model of A over $\mathcal{O}_{K_v}$. Certainly, these groups are finite over K. For the analogues over L, note that each of the primes in $\Sigma_K - T_K$ is unramified in L. So, the order of the groups of connected components are

$$
\begin{tikzcd}
H^1(\mathcal{O}_K, T_p(\tilde{A}))^* \arrow[d, equal] & \mathrm{Hom}_{\mathbf{Z}_p}(H^1(\mathcal{O}_K, T_p(A)), \mathbf{Z}_p)^* \arrow[d, equal] \\
H^2(\mathcal{O}_K, A_{p^\infty}) & \mathrm{Div}\, H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d] \\
H^2(\mathcal{O}_K, A^0_{p^\infty}) \arrow[u, "\varphi_2"'] \arrow[d, "\theta"] & H^1(\mathcal{O}_K, A^0_{p^\infty}) \arrow[d, "i"] \\
H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} & \mathfrak{S}_K(T_K) \arrow[dd, "\alpha"] \\
H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} \arrow[u, "\mu"'] \arrow[d, equal] & \\
H^1(\Gamma, \mathfrak{S}_L(T_L)) & H^0(\Gamma, \mathfrak{S}_L(T_L)) \arrow[l, "g"']
\end{tikzcd}
\tag{4}
$$

We now describe the maps.

- Starting in the upper left, the equality comes from McCallum's duality theorem (Theorem 5.3 in [8]) and taking limits.
- The map φ_2 is induced by the mapping of sheaves $A^0_{p^\infty} \to A_{p^\infty}$.
- The map θ is induced by a natural map $H^2(\mathcal{O}_K, A^0_{p^\infty}) \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})$ and projecting to the indicated quotient.
- The map μ is described in detail further in Lemma 6.6 below. It is induced by the map $H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma \to H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})$ which comes from the spectral sequence 8.
- The equality $H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma} = H^1(\Gamma, \mathfrak{S}_L(T_L))$ is induced by the exact sequence

$$H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty}) \to H^1(\mathcal{O}_L, A^0_{p^\infty}) \to \mathfrak{S}_L(T_L) \to 0$$

  and taking cohomology for Γ.
- The map g is a standard Iwasawa theoretic map. For any Γ-module M, we define the map g in general as the composition

$$H^0(\Gamma, M) = M^\Gamma \hookrightarrow M \to M_\Gamma = H^1(\Gamma, M).$$

  Since the final equality depends on a choice of generator $\gamma \in \Gamma$, so does g.
- The map α is induced by $\mathfrak{S}_K(T_K) \to \mathfrak{S}_L(T_L)$, which follows from the definitions.
- The map i comes from the definition of $\mathfrak{S}_K(T_K)$.
- The map $\mathrm{Div}\, H^1(\mathcal{O}_K, A^0_{p^\infty}) \to H^1(\mathcal{O}_K, A^0_{p^\infty})$ is the inclusion of the divisible subgroup of $H^1(\mathcal{O}_K, A^0_{p^\infty})$.
- The equality in the upper right comes from [14] p. 334.

For our purposes, however, the following variation will be most useful.

allows one to prove that the resulting S_2 is a subgroup of rank 1. In our generality, we do not predict the rank of S_2, and so we equivalently pull back B_1 through S_L^Γ. The choice of maps in 2 below is guided by the p-adic height pairing in section 5.

We now take the inverse image of B_1 through the following sequence of maps, which we denote B_2.

$$\begin{aligned}\mathrm{Hom}_{\mathbf{Z}_p}(H^1(\mathcal{O}_K, T_p(A)), \mathbf{Z}_p)^* = \mathrm{Div}\ H^1(\mathcal{O}_K, A^0_{p^\infty}) \to H^1(\mathcal{O}_K, A^0_{p^\infty}) \xrightarrow{i_\Sigma} \\ \mathfrak{S}_K(\Sigma_K) \xrightarrow{\alpha_\Sigma} \mathfrak{S}_L(\Sigma_L)^\Gamma \xrightarrow{\eta} H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})^\Gamma \quad (2)\end{aligned}$$

The subgroup S_2 is then defined as Div B_2. All of the maps, with the exception of η, come from the p-adic height pairing and are described below. From the definition of $\mathfrak{S}_L(\Sigma_L)$ we get the map $\mathfrak{S}_L(\Sigma_L) \to H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})$ which induces η.

5. The Height Pairing

In [4], we define the following height pairing. It differs from Schneider's analytic height [12] and Mazur-Tate canonical height [6] by a non-zero constant multiple. The pairing, as defined on pro-finite Selmer groups,

$$\langle\ ,\ \rangle_\gamma : H^1(\mathcal{O}_K, T_p(\tilde{A})) \times H^1(\mathcal{O}_K, T_p(A)) \to \mathbf{Q}_p$$

is given by:

$$\begin{tikzcd}
H^1(\mathcal{O}_K, T_p(\tilde{A})) \arrow[d, equal] & \mathrm{Hom}_{\mathbf{Z}_p}(H^1(\mathcal{O}_K, T_p(A)), \mathbf{Z}_p) \arrow[d, equal] \\
H^2(\mathcal{O}_K, A_{p^\infty})^* \arrow[d, "\varphi_2^*"] & (H^1(\mathcal{O}_K, A^0_{p^\infty})^*)_{\mathrm{Tor}} \\
H^2(\mathcal{O}_K, A^0_{p^\infty})^* & H^1(\mathcal{O}_K, A^0_{p^\infty})^* \arrow[u] \\
{[H^2(\mathcal{O}_L/\mathcal{O}_K, A^0_{p^\infty})/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}]^*} \arrow[u, "\theta^*"] \arrow[d, "\mu^*"] & \mathfrak{S}_K(T_K)^* \arrow[u, "i^*"] \\
{[H^1(\mathcal{O}_L, A^0_{p^\infty})_\Gamma/\overline{H^1_{T_L}(\mathcal{O}_L, A^0_{p^\infty})_\Gamma}]^*} \arrow[d, equal] & \\
H^1(\Gamma, \mathfrak{S}_L(T_L))^* \arrow[r, "g^*"] & H^0(\Gamma, \mathfrak{S}_L(T_L))^* \arrow[uu, "\alpha^*"]
\end{tikzcd} \quad (3)$$

The definitions of the maps for this pairing are given in [4]. We sketch their origins below.

It is more natural to consider the dual of the above diagram:

But, $H^1(\mathcal{O}_{K_v}, \tilde{A})$ is finite (Proposition 3.1 of [8]), so its Tate module is trivial. Thus, $H^1(\mathcal{O}_{K_v}, T_p(\tilde{A})) = \tilde{A}^0(K_v)\hat{\otimes}\mathbf{Z}_p$ and

$$S_1 = \ker : \tilde{A}^0(\mathcal{O}_K) \otimes \mathbf{Z}_p \to \prod_{v \in \Sigma_K} \tilde{A}^0(\mathcal{O}_{K_v})\hat{\otimes}\mathbf{Z}_p.$$

This, in turn, is quasi-isomorphic to $\ker : \tilde{A}(\mathcal{O}_K) \otimes \mathbf{Z}_p \to \prod_{v\in\Sigma_K} \tilde{A}(\mathcal{O}_{K_v})\hat{\otimes}\mathbf{Z}_p$. From the universal property of the Néron model, this reduces to

$$\ker : \tilde{A}(K) \otimes \mathbf{Z}_p \to \prod_{v \in \Sigma_K} \tilde{A}(K_v)\hat{\otimes}\mathbf{Z}_p \qquad (1)$$

as described in the introduction.

4. The second subgroup

The second subgroup S_2 is our analogue of Greenberg's subgroup [2]. We sketch its definition here.

Assume that A is an elliptic curve over $\mathbf{Q}$ such that $E(\mathbf{Q})$ has positive rank. There is only one Γ-extension of $K = \mathbf{Q}$, namely the cyclotomic Γ-extension. Moreover, the only choice for $\Sigma_{\mathbf{Q}}$ is $\{p\}$.

If the p-adic height pairing is non-degenerate, S'_L is a $\mathbf{Z}_p[[\Gamma]]$-module of corank 1. As such, $(S'_L)^\Gamma$ has a canonical subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$. Consider the commutative diagram

$$\begin{array}{ccc} S_K & \to & S'_K \\ \downarrow & & \downarrow \\ S_L^\Gamma & \to & (S'_L)^\Gamma \end{array}$$

The pullback of this subgroup, isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$, gives a subgroup first of S'_K (via the restriction map $S'_K \to S'_L$), and then of S_K (under the natural inclusion $S_K \to S'_K$). This subgroup of S_K has $\mathbf{Z}_p$-corank 1, and so its maximal divisible subgroup is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$. Now,

$$S_K = \varinjlim_n \ \ker : H^1(K, A_{p^n}) \to \prod_v H^1(K_v, A)$$

and the pro-finite Selmer group is defined as

$$\varprojlim_n \ \ker : H^1(K, A_{p^n}) \to \prod_v H^1(K_v, A).$$

So, pulling back our $\mathbf{Q}_p/\mathbf{Z}_p \subseteq S_K$ to the groups in its definition as a direct limit, we get a sequence of groups which can also be pieced together in the inverse limit for the pro-finite Selmer group. The result is the desired S_2.

We now recast this definition to fit our generalization. The modified Selmer group over L is quasi-isomorphic to $H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})$. Note that if A is an elliptic curve and the p-adic height pairing is non-degenerate, the desired subgroup of $(S')^\Gamma$ can be described as

$$B_1 = \ker : H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})^\Gamma \to H^1(\mathcal{O}_L - \Sigma_L, A^0_{p^\infty})_\Gamma.$$

Note, if the height pairing is degenerate, then this subgroup is larger accordingly. So, we start with this subgroup B_1 in general (i.e., without assuming that A is an elliptic curve, that $K = \mathbf{Q}$, that the rank of $A(K)$ is positive, or that the height pairing is non-degenerate). Note that in the case of an elliptic curve over $\mathbf{Q}$, it is advantageous to pull back the subgroup B_1 through S'_K and then to S_K which

Over L, the situation becomes more complicated. We still have $S_L = \text{Im} : H^1(\mathcal{O}_L, A^0_{p^\infty}) \to H^1(\mathcal{O}_L, A_{p^\infty})$ and $\mathfrak{S}_L(V)$ is quasi-isomorphic to S_L if $T_L \subset V$. But, neither $H^1(\mathcal{O}_L, A^0_{p^\infty})$ nor $H^1(\mathcal{O}_L, A_{p^\infty})$ is necessarily quasi-isomorphic to S_L. (The discrepancy can be traced to primes of K ramifying in L where the reduction of A contains a split torus.)

The modified Selmer group, S'_K, is quasi-isomorphic to both $H^1(\mathcal{O}_K - \Sigma_K, A^0_{p^\infty})$ and $H^1(\mathcal{O}_K - \Sigma_K, A_{p^\infty})$. Moreover, these quasi-isomorphisms remain true over L.

We will also consider the pro-finite Selmer group of A over K. Classically, the pro-finite Selmer group is

$$\varprojlim_n \ker : H^1(K, A_{p^n}) \to \prod_v H^1(K_v, A).$$

In terms of flat cohomology, it is quasi-isomorphic to $H^1(\mathcal{O}_K, T_p(A))$ and $H^1(\mathcal{O}_K, T_p(A^0))$.

3. The first subgroup

The first subgroup of the pro-finite Selmer group is defined as follows:

$$S_1 := \ker : H^1(\mathcal{O}_K, T_p(\tilde{A})) \to \prod_{v \in \Sigma_K} H^1(\mathcal{O}_{K_v}, T_p(\tilde{A})).$$

Note that since $H^1_\cdot(\mathcal{O}_{K_v}, \tilde{A}_{p^\nu}) = 0$ (see the proof of Lemma 3.1 of [4]), the map $H^1(\mathcal{O}_{K_v}, T_p(\tilde{A})) \to H^1(K_v, T_p(\tilde{A}))$ is injective (from the relative cohomology sequence, and that taking inverse limits is left exact). So, we can equivalently describe S_1 by

$$S_1 = \ker : H^1(\mathcal{O}_K, T_p(\tilde{A})) \to \prod_{v \in \Sigma_K} H^1(K_v, T_p(\tilde{A})).$$

This is the form used in our main theorem below.

Alternatively, we can consider the following which is quasi-isomorphic to S_1:

$$\ker : H^1\left(\mathcal{O}_K, T_p\left(\tilde{A}^0\right)\right) \to \prod_{v \in \Sigma_K} H^1\left(\mathcal{O}_{K_v}, T_p\left(\tilde{A}^0\right)\right).$$

Then, from the Kummer sequence we derive the exact sequence

$$0 \to \tilde{A}^0(\mathcal{O}_{K_v})/p^n \tilde{A}^0(\mathcal{O}_{K_v}) \to H^1\left(\mathcal{O}_{K_v}, \tilde{A}^0_{p^n}\right) \to H^1\left(\mathcal{O}_{K_v}, \tilde{A}^0\right)_{p^n} \to 0.$$

Since $H^1\left(\mathcal{O}_{K_v}, \tilde{A}^0\right)_{p^\infty}$ is finite (Proposition 3.1 of [8]), $T_p\left(H^1\left(\mathcal{O}_{K_v}, \tilde{A}^0\right)\right)$ is trivial and $H^1\left(\mathcal{O}_{K_v}, T_p\left(\tilde{A}^0\right)\right) = \varprojlim \tilde{A}^0(\mathcal{O}_{K_v})/p^n \tilde{A}^0(\mathcal{O}_{K_v})$. Hence S_1 is quasi-isomorphic to

$$\ker : H^1\left(\mathcal{O}_K, T_p\left(\tilde{A}^0\right)\right) \to \varprojlim \tilde{A}^0(\mathcal{O}_{K_v})/p^n \tilde{A}^0(\mathcal{O}_{K_v}).$$

This is quasi-isomorphic to the definition given in [11].

For the remainder of this section, we assume that Sh_K is finite. Then, $H^1(\mathcal{O}_K, T_p(\tilde{A})) = \tilde{A}^0(\mathcal{O}_K) \otimes \mathbf{Z}_p$ by Lemma 4 of [14]. Hence,

$$S_1 = \ker : \tilde{A}^0(K) \otimes \mathbf{Z}_p \to \prod_{v \in \Sigma_K} H^1(\mathcal{O}_{K_v}, T_p(\tilde{A})).$$

However, from the Kummer sequence over K_v we get,

$$0 \to \tilde{A}^0(\mathcal{O}_{K_v}) \hat{\otimes} \mathbf{Z}_p \to H^1(\mathcal{O}_{K_v}, T_p(\tilde{A})) \to T_p(H^1(\mathcal{O}_{K_v}, \tilde{A})) \to 0$$

- The Pontryagin dual of G is denoted by G^*.
- If there is a natural homomorphism $G_1 \xrightarrow{f} G_2$, we shall denote $G_2/\operatorname{Im} f$ by $G_2/\overline{G_1}$.

If M is a $\mathbf{Z}_p$-module whose dual M^* is a $\mathbf{Z}_p$-module of rank m, we say that M has $\mathbf{Z}_p$-corank m.

Our conventions for cohomology groups are as follows. Groups $H^i(\Gamma, \mathcal{F})$ denote Galois cohomology of the group Γ acting on the Γ-module $\mathcal{F}$. All other cohomology groups will be for the *fpqf* site. Cohomology of the spectrum of a ring R (with coefficients in a sheaf $\mathcal{F}$) will be denoted by $H^i(R, \mathcal{F})$. When appropriate, the corresponding relative cohomology groups will be denoted by $H^i_\cdot(R, \mathcal{F})$. In the case of $H^i(K, A)$, we can equivalently view this as a flat cohomology group, or Galois cohomology for $\mathrm{Gal}(\bar{K}/K)$.

We will make use of Schneider's equivariant cohomology, and relative equivariant cohomology (see the appendix to [13]). We will limit ourselves to the following situation. If S is ring containing R so that the corresponding fields of fractions form a Galois extension, we denote equivariant cohomology by $H^i(S/R, \mathcal{F})$, and $H^i_V(S/R, \mathcal{F})$ for relative equivariant cohomology with V_R a closed set in $spec(R)$ and V_S is its inverse image in $spec(S)$.

Cohomology with coefficients in a Tate module will be interpreted as: $H^i(R, T_p(A)) := \varprojlim H^i(R, A_{p^\nu})$.

A p-adic height pairing is $<,>_p$ affiliated with a Γ-extension L/K if it differs by a non-zero constant multiple with the pairing defined in [4]. For a given Γ-extension, Schneider's analytic height [12] and Mazur Tate canonical height [6] are affiliated with L/K.

2. Selmer groups

The classical definition of the Selmer group, as well as the definitions given in [11] of the two subgroups involved in our main theorem, are given in terms of Galois cohomology. At the core of our proof is a definition of the p-adic height pairing in terms of flat cohomology. We recall a few facts on the relationship between these two types of cohomology. For more details on the comparison, see [3] or [9]. Note, it suffices, for our purposes, that the flat analogue of the Selmer group be only quasi-isomorphic to classical Selmer group. Naturally, all comments here are subject to our assumptions described in section 1.

The classical p-power Selmer group, S_K, is the kernel of $H^1(K, A_{p^\infty}) \to \prod_v H^1(K_v, A)$. Here the product is taken over all places v of K. The modified Selmer group relative to Σ_K, S'_K, is defined similarly as the kernel of the map $H^1(K, A_{p^\infty}) \to \prod_{v \notin \Sigma_K} H^1(K_v, A_{p^\infty})$.

There are several flat analogues for S_K. In particular, by Proposition 2.1 of [4]

$$S_K = \operatorname{Im} : H^1(\mathcal{O}_K, A^0_{p^\infty}) \to H^1(\mathcal{O}_K, A_{p^\infty}).$$

Moreover, the groups $H^1(\mathcal{O}_K, A^0_{p^\infty})$ and $H^1(\mathcal{O}_K, A_{p^\infty})$ are each quasi-isomorphic to the classical Selmer group. Finally,

$$\mathfrak{S}_K(V) = \operatorname{Im} : H^1(\mathcal{O}_K, A^0_{p^\infty}) \to H^1(\mathcal{O}_K - V, A^0_{p^\infty})$$

is quasi-isomorphic to the classical Selmer group as well and is technically convenient to work with. We will use $\mathfrak{S}_K(V)$ for $V = T_K$ and $V = \Sigma_K$.

Letting the base field K be an arbitrary number field naturally opens certain areas for generalization. For example, there is now a choice of Γ-extension. We were surprised to also find that we gained a choice in the set Σ_K. In section 7, we show that the subgroups S_1 and S_2 may in fact be sensitive to this choice.

The more general definition of the second subgroup S_2 given in section 4 allows us to extend the results to the case where $<,>_p$ degenerates. This is a real possibility with an arbitrary Γ-extension (as opposed to the situation over $\mathbf{Q}$ where $<,>_p$ is expected to always be non-degenerate).

In [11], the $\mathbf{Z}_p$-ranks of S_1 and S_2 are determined precisely for elliptic curves over $\mathbf{Q}$. See section 7 for a discussion of the $\mathbf{Z}_p$-ranks of S_1 and S_2 in our more general setting.

1. Notation

As above, let p be an odd prime, A an abelian variety defined over a number field K. We will not distinguish in our notation between A and its Néron model over $\mathcal{O}_K$, the integers of K. Let $\tilde{A}$ be the dual abelian variety to A.

Let L be a Γ-extension of K. That is, L is a Galois extension of K so that $\mathrm{Gal}(L/K) = \Gamma \cong \mathbf{Z}_p$. We fix a continuous isomorphism $\Gamma \cong \mathbf{Z}_p$ by choosing a topological generator $\gamma \in \Gamma$. We assume that all primes of $\mathcal{O}_K$ for which A has bad reduction split finitely in L. The set of primes of K ramifying in L is denoted by T_K, and T_L are the places of L lying over T_K. Then, Σ_K is a set of places of K dividing p and containing T_K, and Σ_L are the places of L lying above Σ_K. We assume that A has semi-stable reduction at all places of K dividing p, and ordinary reduction at the primes in T_K (i.e., the reduction of A at a place $v \in T_K$ is an extension of an ordinary abelian variety by a torus).

For any place v of K, we denote the completion of K at v by K_v. The compositum LK_v is denoted by L_v.

If E/F is a finite Galois extension of fields, then we denote the norms of the points of A by

$$\mathbf{N}_{E/F}A := \left\{ \sum_{g \in \mathrm{Gal}(E/F)} g\, x \;\middle|\; x \in A(E) \right\}$$

where the sum is taken under the group law of A.

The *universal norms* of A for a Γ-extension L_v/K_v is the intersection of the groups of norms from each finite subextension E

$$\mathbf{N}A(K_v) := \bigcap_{K_v \subset E \subset L_v} \mathbf{N}_{E/K_v}A.$$

For the following notation, let G be an abelian group (or a group scheme, or sheaf of abelian groups where applicable).

- The kernel of multiplication by n will be denoted by G_n.
- We let G_{p^∞} denote $\varinjlim G_{p^n}$.
- We write $G\hat{\otimes}\mathbf{Z}_p$ for $\varprojlim G/p^nG$.
- The divisible and torsion subgroups of G are denoted by $\mathrm{Div}\, G$ and $\mathrm{Tor}\, G$ respectively. Moreover, we let $G_{\mathrm{Div}} = G/(\mathrm{Div}\, G)$ and $G_{\mathrm{Tor}} = G/(\mathrm{Tor}\, G)$.
- A homomorphism is a *quasi-isomorphism* if it has finite kernel and cokernel.
- We denote by $\ker f$ (resp. $\mathrm{Im}\, f$) the kernel (resp. image) of a homomorphism f.

PLATER'S P-ADIC ORTHOGONALITY RELATION FOR ABELIAN VARIETIES

JOHN W. JONES

In this paper we prove an orthogonality relation on Selmer groups of an abelian variety under p-adic height pairing. One subgroup is a generalization of one defined by Greenberg using Iwasawa theory. The other comes naturally as essentially the kernel of localization.

Let A be an abelian variety defined over a number field K, and let p be a prime number different from 2. Pick a Γ-extension L/K, and let $<,>_p$ be a p-adic height pairing affiliated with L/K (see section 1 for details on notation and terminology). Moreover, we assume that A has ordinary reduction at every place of K ramifying in L. Let $\tilde{A}$ be the dual abelian variety to A. Choose a set of primes Σ_K of K dividing p and containing the primes which ramify in L. We consider natural subgroups (depending on Σ_K) of the pro-finite Selmer groups of A and $\tilde{A}$ respectively and show that one is the annihilator of the other under $<,>_p$. If $<,>_p$ is non-degenerate, then each subgroup is the annihilator of the other.

Although $<,>_p$ is naturally a pairing on the Selmer groups of A and $\tilde{A}$, one can use a non-zero isogeny $A \to \tilde{A}$ to induce a self pairing on the Selmer group of A. The main theorem then implies the corresponding results for the Selmer group of A, and these results do not depend on the choice of isogeny.

If, Sh_K, the Tate-Shafarevich group of A is finite, then the subgroups in question lie in $A(K) \otimes \mathbf{Z}_p$ and $\tilde{A}(K) \otimes \mathbf{Z}_p$ respectively. In that case, the first subgroup, S_1, is quasi-isomorphic to the kernel of the map $A(K) \otimes \mathbf{Z}_p \to \prod_{v \in \Sigma_K} A(K_v) \hat{\otimes} \mathbf{Z}_p$ (see section 3 for alternative descriptions of this subgroup).

The second subgroup, S_2, was defined by Greenberg in [2] using Iwasawa theory. Details of the definition and a generalization more suitable to our purposes are given in section 4.

Our results generalize those of Plater in [11]. Here we highlight some of the differences. In [11], A is assumed to be an elliptic curve with complex multiplication, p is a prime of good ordinary reduction, the height pairing is non-degenerate, and the base field is either $\mathbf{Q}$ or the quadratic imaginary field of complex multiplication.

Most of the differences from [11] come from the use of the more general version of the p-adic height pairing defined in [4]. On one hand, the proof has been completely reworked to accommodate this change. In some ways, this simplifies the proof. The most difficult part occurs in Lemma 6.6, but even that would flow more smoothly if we assumed the p-adic height pairing to be non-degenerate.

This work was partially supported by NSF grant DMS-9100238.