ISOGENY INVARIANCE OF THE BSD CONJECTURE OVER NUMBER FIELDS

JEREMY BOOHER

1. Introduction

Let A be an abelian variety over a number field K. The Birch and Swinnerton-Dyer conjecture states that $L(A/K, s)$ has a pole of order $\mathrm{rank}(A)$ at $s = 1$, and that

$$\lim_{s\to 1} \frac{L(A/K,s)}{(s-1)^{\mathrm{rank}(A)}} = \frac{\#Ш_A R_A \Omega_A}{\#A(K)_{\mathrm{tors}} \# \widehat{A}(K)_{\mathrm{tors}}} \tag{1.1}$$

Implicit in this are the assertions that $L(A/K, s)$ has an analytic continuation and that the Tate-Shafarevich group $Ш_A$ is finite.

Suppose $f : A \to B$ is an isogeny of abelian varieties over K. As a sanity check for the BSD conjecture, the right side of (1.1) should be the same for A and for B. We have seen examples where the individual pieces of this expression change under an isogeny (see [L5]). It requires a delicate analysis to show that the entire expression is invariant under isogeny. In Section 2 we analyze the effect of an isogeny on the terms in the conjecture. In Section 3 we review important results in Galois cohomology and illustrate them, and in Section 4 we use them to deduce an isogeny has no overall effect on the constant:

Theorem 1.1 (Tate)**.** *If the Birch and Swinnerton-Dyer conjecture is true for A, it is true for all K-isogenous abelian varieties.*

Proof. Combine Lemma 2.1, the calculations (2.2), (2.3), and (2.4), and Proposition 4.1. □

Remark 1.2. The arguments we give come from [Mil06, §I.7] (itself modeled on Tate's Bourbaki talk on BSD), with minor adaptations to fit in with the rest of the learning seminar.

Remark 1.3. Everything we do can be easily adapted to case of a global function field K when $\mathrm{char}(K)$ does not divide the degree of the isogeny. One has to use flat cohomology and infinitesimal group schemes to push through a generalization of the technique to prove Theorem 1.1 without restriction on the degree of the isogeny.

Notational Conventions. Let S denote a finite set of places of K that contains the archimedean places, and define K_S to be the maximal extension of K unramified outside of S. Let $G_S = \mathrm{Gal}(K_S/K)$ and $\mathcal{O}_{K,S}$ be the ring of S-integers of K. When we talk about cohomology groups, we always use continuous cohomology.

If $g : X \to Y$ is a homomorphism of abelian groups with finite kernel and cokernel, we define

$$h(g) = \frac{\#\ker(g)}{\#\mathrm{coker}(g)};$$

this is a measure of how g effects the size of the groups: if X and Y are finite, $h(g) = \#X/\#Y$.

If $f : A \to B$ is a K-homomorphism of abelian varieties over K, denote the induced maps on K points and K_v points by $f(K)$ and $f(K_v)$ respectively.

We also need to consider several types of duality.

Date: October 28 and November 4, 2015.

- For a locally compact Hausdorff topological abelian group X, we define the dual $X^* = \mathrm{Hom}_{\mathrm{cont}}(M, S^1)$. (If M is torsion and discrete then this is the same as $\mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$.
- For a finite flat (locally free) commutative group scheme G over a base T, the *Cartier dual* G^D represents the functor on T-schemes given by $T' \rightsquigarrow \mathrm{Hom}_{T'}(G_{T'}, \mathbf{G}_{m,T'})$.
- If M is a finite discrete G_k-module for some field k, we define $M^D = \mathrm{Hom}_{\mathrm{Ab}}(M, k_s^\times)$ (with its evident structure of finite discrete G_k-module).

2. The Effect of Isogenies

Let $f : A \to B$ be a degree-n isogeny of abelian varieties over K. Let S be a finite set of places of K containing: the archimedean places, the places where A (and B) have bad reduction, and the places dividing n. (Later we will add a few more places into S.)

The significance of such a choice of S is that f extends to a map of abelian schemes $\widetilde{f} : \mathcal{A} \to \mathcal{B}$ over $\mathcal{O}_{K,S}$ (namely, the Néron models over $\mathcal{O}_{K,S}$ are abelian schemes). The kernel of this map is finite étale by using properness, fibral flatness, and degree considerations, so passing to $\mathcal{O}_{K_S}$-points gives an exact sequence (exercise!) and hence by properness this is an exact sequence

$$0 \to \ker(f)(K_S) \to A(K_S) \to B(K_S) \to 0; \tag{2.1}$$

for details on this see [Mil06, Lemma I.6.1].

Before analyzing the effect of an isogeny on the terms in the BSD conjecture, we first check some basic compatibilities:

Lemma 2.1. *We have:*

1. *The L-functions $L(A/K, s)$ and $L(B/K, s)$ are equal.*
2. *The ranks of A and B are the same.*
3. *$Ш_A$ is finite if and only if $Ш_B$ is finite.*

Proof. The key is that since $\ker f$ is killed by $[n]_A$, there exists a K-isogeny

$$g : B = A/\ker(f) \to A/A[n] = A$$

such that $f \circ g = [n]_B$ and $g \circ f = [n]_A$. In particular, $V_\ell(g)$ is an inverse to $V_\ell(f)$ up to invertible n-multiplication on the rationalized ℓ-adic Tate module. Since the L-function was defined solely in terms of the rationalized Tate module $V_\ell(A)$ (see [L1, §1.3]), we get the equality of L-functions. Likewise, the induced map $A(K)_{\mathbf{Q}} \to B(K)_{\mathbf{Q}}$ via f is an isomorphism, or more concretely $A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}}$ is injective since $\ker f$ is finite, giving that $\mathrm{rank}(A) \leq \mathrm{rank}(B)$, and g provides the reverse inequality.

The third assertion follows from (2.1): taking the long exact sequence of G_S-cohomology gives an exact sequence

$$\ldots \to H^1(G_S, \ker(f)) \to H^1(G_S, A) \to H^1(G_S, B) \to \ldots$$

Finiteness results for Galois cohomology (see Fact 3.11 below) gives that $H^1(G_S, \ker(f))$ is finite. Thus,

$$\ker(Ш_A \to Ш_B) \subset \ker(H^1(G_S, A) \to H^1(G_S, B)) = \mathrm{Im}(H^1(G_S, \ker(f)) \to H^1(G_S, A))$$

is finite. Hence, if $Ш_B$ is finite, we deduce that $Ш_A$ is finite. For the converse, apply the same argument with g in place of f. □

The main work is analyze the effect of an isogeny on each of the pieces of (1.1), and then to assemble them all together to show that the product of the discrepancies is equal to 1; this product calculation will use essentially all of Tate's global duality theorems.

2.1. **The Tate-Shafarevich Group.** Recall we defined the Tate-Shafarevich group as

$$Ш_A = \ker(H^1(K, A) \to \prod_v H^1(K, B))$$

in [L3, §5]. As A is K-isogenous to B, $\widehat{A}$, and $\widehat{B}$, Lemma 2.1 shows that if $Ш_A$ is finite then so are $Ш_B$, $Ш_{\widehat{A}}$, and $Ш_{\widehat{B}}$.

The Cassels-Tate pairing will be defined and analyzed in an upcoming lecture. We need the following result, which is also proven in [Mil06, Theorem I.6.13a].

Fact 2.2. *Assuming $Ш_A$ is finite, the Cassels-Tate pairing $Ш_A \times Ш_{\widehat{A}} \to \mathbf{Q}/\mathbf{Z}$ is non-degenerate. Furthermore, it is functorial in the sense that*

$$\begin{array}{ccccc} Ш_A & \times & Ш_{\widehat{A}} & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \downarrow{\scriptstyle Ш(f)} & & \uparrow{\scriptstyle Ш(\widehat{f})} & & \| \\ Ш_B & \times & Ш_{\widehat{B}} & \longrightarrow & \mathbf{Q}/\mathbf{Z} \end{array}$$

is commutative.

We now assume finiteness of $Ш_A$, hence the Tate–Shafarevich groups of $\widehat{A}$, B, and $\widehat{B}$ are all finite. The perfectness of the Cassels–Tate pairing and its functoriality give that $\#\mathrm{coker}(Ш(f)) = \#\ker(Ш(\widehat{f}))$.

Now let us consider the effect of an isogeny on $\#Ш_A$. Looking at the tautological exact sequence

$$0 \to \ker Ш(f) \to Ш_A \stackrel{Ш(f)}{\to} Ш_B \to \mathrm{coker}(Ш(f)) \to 0,$$

we see that

$$\frac{\#Ш_A}{\#Ш_B} = \frac{\#\ker(Ш(f))}{\#\mathrm{coker}(Ш(f))} = \frac{\#\ker(Ш(f))}{\#\ker(Ш(\widehat{f}))}. \tag{2.2}$$

Put this in the fridge; we'll take it out later.

2.2. **Regulators.** We start by reviewing the setup in [L2, §3]. The *canonical height pairing* is a bi-additive function

$$A(\overline{K}) \times \widehat{A}(\overline{K}) \to \mathbf{R}$$

defined for $a \in A(K')$ and $\mathcal{L} \in \widehat{A}(K')$ via

$$\langle a, \mathcal{L}\rangle = \frac{1}{[K' : K]} \widehat{h}_{K',\mathcal{L}}(a);$$

note that $\mathcal{L}$ is not ample (and moreover it is anti-symmetric), this is not a height on projective space and it required a more complicated definition.

For a K-isogeny $f : A \to B$, the pairing is functorial in the sense that the following diagram commutes:

$$\begin{array}{ccccc} A(\overline{K}) & \times & \widehat{A}(\overline{K}) & \longrightarrow & \mathbf{R} \\ \downarrow{\scriptstyle f} & & \uparrow{\scriptstyle \widehat{f}} & & \| \\ B(\overline{K}) & \times & \widehat{B}(\overline{K}) & \longrightarrow & \mathbf{R} \end{array}$$

Let $\{a_i\}$ and $\{\mathcal{L}_j\}$ be bases for the Mordell-Weil lattices $A(K)/A(K)_{\mathrm{tors}}$ and $\widehat{A}(K)/\widehat{A}(K)_{\mathrm{tors}}$. The regulator is defined as

$$R_A = |\det(\langle a_i, \mathcal{L}_j\rangle)|.$$

It is *non-zero* as we know that after tensoring with $\mathbf{R}$ on the source, the canonical height pairing is non-degenerate on K-points (ultimately by arguments with the geometry of numbers).

To examine the effect of an isogeny on the regulator, pick bases $\{b_i\}$ and $\{\mathcal{L}'_j\}$ for $B(K)/B(K)_{\text{tors}}$ and $\widehat{B}(K)/\widehat{B}(K)_{\text{tors}}$. The collection $\{f(a_i)\}$ is linearly independent in $B(K)/B(K)_{\text{tors}}$ respectively. We wish to understand the index, or equivalently $h(f_{\text{free}})$ where f_{free} is the induced (injective) map between these Mordell–Weil lattices.

Applying the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)_{\text{tors}} & \longrightarrow & A(K) & \longrightarrow & A(K)/A(K)_{\text{tors}} & \longrightarrow & 0 \\ \downarrow & & \downarrow f_{\text{tors}} & & \downarrow f(K) & & \downarrow f_{\text{free}} & & \downarrow \\ 0 & \longrightarrow & B(K)_{\text{tors}} & \longrightarrow & B(K) & \longrightarrow & B(K)/B(K)_{\text{tors}} & \longrightarrow & 0 \end{array}$$

gives a six term exact sequence with *finite* terms. The Euler characteristic is therefore 1, so $h(f(K)) = h(f_{\text{tors}}) \cdot h(f_{\text{free}})$. Looking at the regulator, we see that

$$R_B = |\det(\langle b_i, \mathcal{L}'_j\rangle)| = |\det(\langle f(a_i), \mathcal{L}'_j\rangle)| h(f_{\text{free}}) = |\det(\langle f(a_i), \mathcal{L}'_j\rangle)| h(f(K)) \frac{\#B(K)_{\text{tors}}}{\#A(K)_{\text{tors}}}$$

using the multi-linearity of the determinant for the second equality.

Applying the same argument to $\widehat{f}$, we see that

$$R_A = |\det(\langle a_i, f^*(\mathcal{L}'_j)\rangle)| h(\widehat{f}(K)) \frac{\#\widehat{A}(K)_{\text{tors}}}{\#\widehat{B}(K)_{\text{tors}}}$$

The functoriality of the pairing shows that the determinant terms on the right sides of these formulas for R_A and R_B are the same for each ij-entry in the matrices, and hence the determinants coincide. Thus, upon dividing R_A by R_B these mystery determinants cancel out and we get:

$$\frac{R_A}{\#A(K)_{\text{tors}} \cdot \#\widehat{A}(K)_{\text{tors}}} = \frac{h(f(K))}{h(\widehat{f}(K))} \frac{R_B}{\#B(K)_{\text{tors}} \cdot \#\widehat{B}(K)_{\text{tors}}}. \tag{2.3}$$

Put this in the fridge too. Note how the mysterious torsion terms in the BSD coefficients pleasantly appear here alongside the regulator terms! Hence, we will not need to grapple directly with torsion (whose behavior under an isogeny is unpredictable).

2.3. **The Volume Term.** We now analyze how Ω_A and Ω_B are related. First we recall the definition from [L3, §6], say for A. Pick a nonzero $\omega \in \Omega^{\text{top}}_{A/K}(A)$ and a Haar measure μ on $\mathbf{A}_K$. Representing μ as a restricted tensor product $\prod' \mu_v$, for each v we get a Haar measure on $A(K_v)$ defined by

$$m_{A,v} = \lambda_v |\omega|_v \mu_v^{\dim(A)}$$

where λ_v is a "covergence factor" defined to be 1 for archimedean v and $L_v(1/q_v)^{-1}$ for non-archimedean v. Provided that $v \notin S$ and ω extends to a v-integral generator of the line of top-degree global differential forms on the Néron model at v (as is the case for all but finitely many v, by considering the relative cotangent space of the Néron model over $\mathcal{O}_{K,S}$ as a finitely generated $\mathcal{O}_{K,S}$-module), we saw in [L3] that this measure assigns volume 1 to $A(K_v)$. Thus, it makes sense to form the product measure

$$m_{A,\mu} = \prod m_{A,v}$$

as a measure on $A(\mathbf{A}_K)$; as such it independent of the choice of ω due to the product formula.

We also have the quotient measure $\overline{m}_\mu$ on $\mathbf{A}_K/K$ induced by μ on $\mathbf{A}_K$ and counting measure on its discrete closed subgroup K. The *Tamagawa measure*

$$m_A = \overline{m}_\mu(\mathbf{A}_K/K)^{-\dim(A)} m_{A,\mu}$$

is independent of the choice of μ as well. Finally, we can define

$$\Omega_A = m_A(A(\mathbf{A}_K))$$

which is independent of the choice of μ and ω.

Because we defined the Tamagawa measure independent of choices, it is easy to see the effect of the isogeny, as follows. First, note that the convergence factors λ_v are isogeny invariant since they're defined in terms of the local L-function at each non-archimedean place. We claim that for *every* place v (including real and complex places),

$$m_{A,v}(A(K_v)) = \#\ker(f(K_v))m_{B,v}(f(A(K_v))).$$

The key point is that since $f : A \to B$ is an étale K-isogeny, the Zariski-local structure of étale morphisms and the K_v-analytic inverse function theorem imply that $f(K_v) : A(K_v) \to B(K_v)$ has open image onto which it is a local analytic isomorphism. Being a homomorphism of K_v-analytic groups, it is a $\ker(f(K_v))$-torsor onto its compact open image.

Fix a choice of ω_B for constructing the Tamagawa measure for B (along with a fixed adelic measure $\mu = \prod' \mu_v$), and then use $\omega_A := f^*(\omega_B)$ and μ to build the Tamagawa measure for A. By working over a small open subset $\Delta_v \subset f(A(K_v)) \subset B(K_v)$ over which the preimage in $A(K_v)$ is a disjoint union of $\#\ker(f(K_v))$ open subsets which each map analytically isomorphically onto Δ_v, it follows from the K_v-analytic Change of Variables formula that the pushforward Haar measure $f(K_v)_*(m_{A,v})$ on $f(A(K_v))$ is equal to $\#\ker(f(K_v)) \cdot m_{B,v}|_{f(A(K_v))}$ (as we can compare these Haar measures by evaluating each on Δ_v). Now evaluating the volume of the entire image $f(A(K_v))$, we get

$$m_{A,v}(A(K_v)) = \#\ker(f(K_v))m_{B,v}(f(A(K_v))).$$

Since the index of the compact open subgroup $f(A(K_v))$ in $B(K_v)$ is $\#\mathrm{coker}(f(K_v))$, we finally obtain:

$$\mu_{A,v}(A(K_v)) = \mu_{B,v}(B(K_v))h(f(K_v)).$$

Both of the volume terms here are equal to 1 provided $v \notin S$ and ω_A and ω_B generate the top-degree v-integral differential forms, so for such v we have $h(f(K_v)) = 1$ as well. Enlarge S to include all the places where this does not happen, so now for $v \notin S$ we have $h(f(K_v)) = 1$. The Tamagawa measure is the product of the local measures up to dividing by an overall adelic volume factor that is the same for A and B (depending on each only through their common dimension), so we conclude that

$$\Omega_A = \Omega_B \prod_{v \in S} h(f(K_v)). \tag{2.4}$$

This completes our analysis of the change of factors of the BSD coefficient under the K-isogeny f.

3. Results on Galois Cohomology

In this section we collect important facts about local and global duality in Galois cohomology, illustrate them with examples, and discuss Tate local duality for abelian varieties.

3.1. Local Duality.

We recall a few facts about Galois cohomology of local fields; all may be found in [Mil06, §I.2] or [NSW08, Chapter VII]. Let L be a finite extension of $\mathbf{Q}_p$ with absolute Galois group G_L, and let M be a finite discrete G_L-module.

Fact 3.1 (Finiteness)**.** *The cohomology groups $H^i(G_L, M)$ are finite.*

Fact 3.2 (Local Tate Duality)**.** *The cup product pairing combined with evaluation $M \times M^D \to \overline{L}^\times$ gives a perfect pairing*

$$H^i(L, M) \times H^{2-i}(L, M^D) \to \mathrm{Br}(L) \simeq \mathbf{Q}/\mathbf{Z}$$

for $0 \leq i \leq 2$.

Remark 3.3. There is also a version of this for archimedean places using modified Tate cohomology groups: see [Mil06, Theorem I.2.13].

Let $I_L \subset G_L$ be the inertia group. We define the *unramified* Galois cohomology group

$$H^1_{\mathrm{un}}(L, M) := H^1(G_L/I_L, M^{I_L}) \subset H^1(L, M).$$

Fact 3.4. *$H^1_{\mathrm{un}}(L, M)$ and $H^1_{\mathrm{un}}(L, M^D)$ are exact annihilators of each other under this pairing.*

Let M have order m, and define the Euler characteristic

$$\chi(M) = \frac{\#H^0(L, M)\#H^2(L, M)}{\#H^1(L, M)}.$$

Fact 3.5 (Local Euler Characteristic)**.** *We have $\chi(M) = \|m\|_L$ where $\|\cdot\|_L$ is the normalized valuation on L (i.e., $\chi(M) = (\#\mathcal{O}_L/m\mathcal{O}_L)^{-1} = p^{-[L:\mathbf{Q}_p]v_p(m)}$).*

Example 3.6. Consider the case $M = \mu_m$, so

$$H^i(L, \mu_m) = \begin{cases} \mu_m(L), & i = 0 \\ L^\times/(L^\times)^m & i = 1 \\ \mathbf{Z}/m\mathbf{Z}, & i = 2 \\ 0, & i > 2 \end{cases}$$

On the other hand, $M^D = \mathrm{Hom}_{G_L}(\mu_n, L^\times) = \mathbf{Z}/n\mathbf{Z}$, so

$$H^i(L, \mathbf{Z}/n\mathbf{Z}) = \begin{cases} \mathbf{Z}/m\mathbf{Z}, & i = 0 \\ \mathrm{Hom}(G_L, \mathbf{Z}/m\mathbf{Z}), & i = 1 \\ \mu_m(L), & i = 2 \\ 0, & i > 2 \end{cases}$$

In particular, for $i = 1$ we have a duality between $\mathrm{Hom}(G_L, \mathbf{Z}/m\mathbf{Z})$ and $L^\times/(L^\times)^m$. After identifying $\mathrm{Hom}(G_L, \mathbf{Z}/m\mathbf{Z})$ with $\mathrm{Hom}(L^\times, \mathbf{Z}/m\mathbf{Z})$ using local class field theory, one can check the cup-product duality becomes evaluation (up to an inversion, depending on conventions for the local Artin map).

This also illustrates the local Euler characteristic formula (and in fact is the essential explicit calculation in the proof of that formula). For example, if $p \nmid m$ then the group $1 + \mathfrak{m}_L$ is m-divisible, so $\#L^\times/(L^\times)^m = \#\mu_m(L) \cdot m$ since for the *finite* residue field k_L the cokernel and kernel of $t^m : k_L^\times \to k_L^\times$ have the same size. Thus, the Euler characteristic in this case is

$$\frac{\#\mu(L) \cdot m}{\#\mu_m(L) \cdot m} = p^0 = 1 = \|m\|_L$$

as desired.

3.2. **Tate Local Duality for Abelian Varieties.**

Next we present a duality between the Galois cohomology of an abelian variety and its dual.

Fact 3.7. *Let L be a local field of characteristic zero and A be an abelian variety over L. There is a canonical pairing*

$$\widehat{A}(L) \times H^1(L, A) \to \mathbf{Q}/\mathbf{Z}$$

that identifies each as the Pontryagin dual of the other (vieweing $\widehat{A}(L)$ with its natural compact topology and $H^1(L, A)$ with the discrete topology).

This is a combination of results in algebraic geometry and number theory. We will not give a complete proof, but will explain how to define the pairing and how to relate $\widehat{A}(L)$ to $\mathrm{Ext}^1_L(A, \mathbf{G}_m)$.

The first part is algebraic geometry, as follows. Let A be an abelian scheme over a base S, and $\widehat{A}$ be the dual abelian scheme (which always exists by a deep theorem of Raynaud and Deligne whose proof involves a detour through algebraic spaces, or assume projectivity as over fields so that the dual is provided by Grothendieck's work with Picard schemes). For an S-scheme T we claim that as groups

$$\widehat{A}(T) = \mathrm{Ext}^1(A_T, \mathbf{G}_m)$$

naturally in T. The group $\mathrm{Ext}^1(A_T, \mathbf{G}_m)$ can be interpreted either as classifying extensions of T-group schemes (exactness for the fppf topology) or in terms of homological algebra as classifying extensions in the category of abelian sheaves on the fppf site: the two notions coincide because $\mathbf{G}_m$-torsor sheaves for the fppf topology over a scheme are always representable (ultimately by effectivity of fpqc descent for affine morphisms).

Remark 3.8. Let us describe how this "relative Weil Barsotti formula" is proved; we only need it in the classical setting where T is the spectrum of a field, but the relative case is very important in one of the conceptual approaches to the definition of the Cassels–Tate pairing that we will study in a later lecture. Given an extension of A_T by $\mathbf{G}_m$ as T-group schemes, we get a line bundle on A_T by forgetting the group structure, and it is trivialized over the identity section of A_T via the identification of the kernel with $\mathbf{G}_m$; as such this lies in $\widehat{A}(T)$. The hard part to show that every element of $\widehat{A}(T)$ arises in this way from such a group extension that is moreover unique up to isormorphism. The full proof is discussed in [Oor66, §18]. Oort uses the result over an algebraically closed field as input, which is addressed in [Ser88, VII.16, Theorem 6]. With a bit of care, it is not necessary to use the classical case; see the Appendix for how this is done.

Given this, working in the derived category of abelian sheaves on the fppf site of S we have

$$\widehat{A}(S) = \mathrm{Ext}^1(A, \mathbf{G}_m) = \mathrm{Hom}(A, \mathbf{G}_m[1]) \quad \text{and} \quad H^1(S, A) = \mathrm{Ext}^1(\mathbf{Z}_S, A) = \mathrm{Hom}(\mathbf{Z}_S, A[1]).$$

Then by composing, we obtain a "Yoneda Ext-pairing"

$$H^1(S, A) \times \widehat{A}(S) = \mathrm{Hom}(\mathbf{Z}_S, A[1]) \times \mathrm{Hom}(A, \mathbf{G}_m[1]) \to \mathrm{Hom}(\mathbf{Z}_S, \mathbf{G}_m[2]) = H^2(S, \mathbf{G}_m) =: \mathrm{Br}(S).$$

That is the algebraic geometry, and the number-theoretic input is that for $S = \mathrm{Spec}(L)$ with L a non-archimedean local field, local class field theory identities $\mathrm{Br}(L)$ with $\mathbf{Q}/\mathbf{Z}$, thereby defining the desired pairing.

If we make $\widehat{A}(L)$ into a compact Hausdorff group using the topology on L, and view $H^1(L, A)$ as a discrete group, Fact 3.7 is the assertion that this pairing is a Pontryagin duality. The statement is [Mil06, Corollary I.3.4], and the proof occupies [Mil06, Ch. I, §3].

Remark 3.9. There is one important detail omitted in the proof in [Mil06, Ch. I, §3]: in the proof of [Mil06, Ch. I, Thm. 3.2] it is asserted that a certain diagram commutes, and this is both non-obvious and underlie the entire mechanism by which the proof of the duality theorem in characteristic 0 can be reduced to Tate local duality for finite Galois modules. More specifically, by using [Mil06, Ch. I, Lemma 3.1] to rewrite Ext's in terms of group cohomology, the commutativity of the right square in the proof with $r = 2$ asserts the commutativity of

$$\begin{array}{ccc} H^1(K, \widehat{A}[n]) & \longrightarrow & H^1(K, \widehat{A})[n] \\ \downarrow & & \downarrow \\ H^1(K, A[n])^* & \longrightarrow & (H^0(K, A)^*)[n] \end{array}$$

in which the rows come from the sequence $0 \to A[n] \to A \xrightarrow{n} A \to 0$ and its $\widehat{A}$-analogue, the left side is Tate local dualuty via the identification of $A[n]$ as Cartier dual to $\widehat{A}[n]$, and the right map expresses the local duality pairing for A over L. The fact that this commutes is subtle, and a proof using derived categories is given in [MO].

Remark 3.10. The abstract definition of the pairing makes it easy to see the functoriality of local duality for abelian varieties, which is to say the commutativity of:

$$\begin{array}{ccccc} \widehat{B}(L) & \times & H^1(L,B) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \Big\downarrow \widehat{f} & & \Big\uparrow f & & \Big\| \\ \widehat{A}(L) & \times & H^1(L,A) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \end{array}$$

3.3. **Global Duality.** Now we recall some results about global Galois cohomology: standard references are [Mil06, §I.4] and [NSW08, Chapter VIII], while [L4] deduces them from a modification of étale cohomology. Let K be a number field and S a finite set of places of K containing the archimedean places. Let M be a finite discrete G_S-module such that $\#M$ is an S-unit.

Fact 3.11 (Finiteness)**.** *The cohomology groups $H^i(G_S, M)$ are finite.*

For a place v of K, choosing an inclusion $G_{K_v} \to G_K$ we can study $H^i(K_v, M) := H^i(G_{K_v}, M)$. If v is non-archimedean, we set $\widetilde{H}^i(K_v, M) = H^i(K_v, M)$. If v is archimedean, we set $\widetilde{H}^i(K_v, M) = H^i_T(K_v, M)$ (Tate cohomology). Define the finite product

$$P^i_S(K, M) = \prod_{v \in S} \widetilde{H}^i(K_v, M),$$

so there is a map $H^i(G_S, M) \to P^i_S(K, M)$ given by restriction.

Using local duality, there is an identification $P^i_S(K, M) \simeq P^{2-i}_S(K, M^D)^*$. This also gives maps $P^i_S(K, M^D) \to H^{2-i}(G_S, M)^*$.

We also define

$$Ш^i_S(K, M) = \ker(H^i(G_S, M) \to P^i_S(K, M)).$$

Fact 3.12. *The groups $Ш^1_S(K, M)$ and $Ш^2_S(K, M^D)$ are finite and there is a canonical non-degenerate pairing*

$$Ш^1_S(K, M) \times Ш^2_S(K, M^D) \to \mathbf{Q}/\mathbf{Z}.$$

Furthermore, there is an exact sequence

$$\begin{array}{ccccccc} 0 \longrightarrow & H^0(G_S, M) & \longrightarrow & P^0_S(K, M) & \longrightarrow & H^2(G_S, M^D)^* & \\ & & & & & \Big\downarrow & \\ & H^1(G_S, M^D)^* & \longleftarrow & P^1_S(K, M) & \longleftarrow & H^1(G_S, M) & \\ & \Big\downarrow & & & & & \\ & H^2(G_S, M) & \longrightarrow & P^2_S(K, M) & \longrightarrow & H^0(G_S, M^D)^* & \longrightarrow 0 \end{array}$$

The exact sequence can be viewed as an local cohomology sequence in étale cohomology: see [L4]. This also gives a nice description of the pairing.

Remark 3.13. The vertical arrows are defined using the perfect duality between $Ш^1_S$ and $Ш^2_S$: dualzing the exact sequence

$$P^0_S(K, M) \xrightarrow{\gamma} H^2(G_S, M^D)^* \to \text{coker}(\gamma) \to 0$$

gives that $\text{coker}(\gamma)^* = Ш^2_S(K, M^D)^*$, and this has a natural map to $Ш^1_S(K, M) \subset H^1(G_S, M)$. The other vertical map is defined similarly.

Example 3.14. The $Ш^i_S(K, M)$ are interesting to study. For example, for S a finite set of primes and $M = \mathbf{Z}/m\mathbf{Z}$ with m invertible in $\mathcal{O}_{K,S}$,

$$Ш^1_S(K, \mathbf{Z}/m\mathbf{Z}) \simeq \mathrm{Hom}(\mathrm{Cl}_S(K), \mathbf{Z}/m\mathbf{Z}).$$

Here $\mathrm{Cl}_S(K)$ is the S-class group. By class field theory, it is isomorphic to the Galois group of the maximal abelian extension of K inside K_S at which all primes of S split completely. Therefore $\mathrm{Hom}(\mathrm{Cl}_S(K), \mathbf{Z}/m\mathbf{Z})$ parametrizes cyclic extensions of K unramified outside S with degree dividing m in which the primes of S split completely.

Example 3.15. Another example is the Grunwald–Wang theorem. In this case one actually wants to take S to be the set of *all* places of K (so strictly speaking we need to define $P^i_S(K, M)$ as an infinite restricted product with respect to $H^i_{\mathrm{un}}(K_v, M)$'s for all but finitely many v and need to revisit how the 9-term exact sequence is defined) and we consider whether there is a local-to-global principle for being an mth-power in K. In other words, is $\alpha \in K^\times$ is an mth power if $\alpha \in K_v^\times$ is an mth power for all places v?

This is not always true (e.g., 16 is a local 8th power at all places of $\mathbf{Q}(\sqrt{7})$), and the obstruction is measured by $Ш^1_S(K, \mu_m)$. Indeed, the Kummer exact sequence and Hilbert 90 show that $H^1(G_K, \mu_m) = K^\times/(K^\times)^m$, so

$$Ш^1_S(K, \mu_m) = \ker\left(K^\times/(K^\times)^m \to \prod_{v \in S} K_v^\times/(K_v^\times)^m\right).$$

The theorem of Grunwald–Wang is that this group is usually trivial, except in specific special cases with $8|m$ (depending on how K interacts with 2-power cyclotomic fields and on certain properties of the 2-adic places in S) for which it has order 2.

For global cohomology groups, there is also a global Euler–Poincaré characteristic formula.

Fact 3.16 (Global Euler–Poincaré Characteristic)**.** *We have*

$$\frac{\#H^0(G_S, M) \cdot \#H^2(G_S, M)}{\#H^1(G_S, M)} = \prod_{v\,\mathrm{arch}} \frac{\#H^0(G_v, M)}{|\#M|_v} = \prod_{v\,\mathrm{arch}} \frac{\#H^0_T(G_v, M^D)}{\#H^0(G_v, M^D)}$$

where $|\cdot|_v$ is the normalized absolute value on K_v (the square of the usual absolute value when v is complex).

Remark 3.17. This is not actually an Euler characteristic in general, as higher cohomology groups might be non-zero when K is a real place and $\#M$ is even.

Example 3.18. Let $p \neq 2$ be prime. Let us consider the case $M = \mu_p$ with $S = S_p \cup S_\infty$ consisting of the primes above p and the archimedean places. Furthermore, suppose K does not contain non-trivial pth roots unity. From the Kummer exact sequence, we obtain short exact sequences

$$1 \to \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \to H^1(G_S, \mu_p) \to \mathrm{Cl}_S(K)[p] \to 1$$
$$1 \to \mathrm{Cl}_S(K)/p\,\mathrm{Cl}_S(K) \to H^2(G_S, \mu_p) \to \mathrm{Br}(\mathcal{O}_{K,S})[p] \to 1$$

Let us check the global Euler–Poincaré characteristic formula in this case.

There are no pth roots of unity $\mathcal{O}_{K,S}^\times$, and the rank is $\#S - 1$. Thus $\#\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p = p^{\#S-1}$. By Grothendieck's work on Brauer groups for regular schemes (applied to $\mathcal{O}_{K,S}$), $\mathrm{Br}(\mathcal{O}_{K,S})$ is the part of the Brauer group of K unramified outside of S. Finallly, we have the exact sequence from class field theory

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

We see that

$$\operatorname{Br}(\mathcal{O}_{K,S})[p] = \ker\left(\bigoplus_{v\in S}\operatorname{Br}(K_v) \to \mathbf{Q}/\mathbf{Z}\right)[p] = \ker\left(\bigoplus_{v\in S_p}\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}\right)$$

This has size $p^{\#S_p-1}$.

As $\#\operatorname{Cl}(\mathcal{O}_{K,S})[p] = \#\operatorname{Cl}(\mathcal{O}_{K,S})/p\operatorname{Cl}(\mathcal{O}_{K,S})$, we obtain

$$\frac{\#H^0(G_S,\mu_p)\#H^2(G_S,\mu_p)}{\#H^1(G_S,\mu_p)} = p^{\#S_p-1-(\#S-1)} = p^{-\#S_\infty}$$

On the other hand, for each real place v complex conjugation acts non-trivially on μ_p, so $\#H^0(G_v,\mu_p) = 1$, while $|\#\mu_p|_v = p$. For a complex place, $\#H^0(G_v,\mu_p) = p$ and $|\#\mu_p|_v = p^2$. Thus,

$$\prod_v \frac{\#H^0(G_v,\mu_p)}{|\#\mu_p|_v} = p^{-\#S_\infty}.$$

This verifies the formula for μ_p.

Remark 3.19. A similar calculation is the foundation of the proof of the global Euler–Poincaré characteristic formula.

4. A Calculation Using Galois Cohomology

Let $f : A \to B$ be a K-isogeny of abelian varieties over K, and let S be a finite set of places of K as in Section 2. Thus S contains all archimedean places, all primes dividing $\deg(f)$, and all primes of bad reduction for A (same as for B). Our previous work shows that the isogeny invariance of the Birch and Swinnerton-Dyer conjecture is equivalent to the following:

Proposition 4.1. *We have*

$$\prod_{v\in S} h(f(K_v)) = \frac{\#\ker Ш(\widehat{f})}{\#\ker Ш(f)}\frac{h(f(K))}{h(\widehat{f}(K))}.$$

Let $M = \ker(f)(K_S)$. We use $H^1(G_S, A)[f]$ to denote the kernel of the map on cohomology induced by f. The following commutative diagram is the key to the proof.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(G_S,M) & \longrightarrow & P^0_S(K,M) & & & & \\
 & & & & \downarrow & & & & \\
 & & & & H^2(G_S,M^D)^* & & & & \\
 & & & & \downarrow & & & & \\
0 & \longrightarrow & \operatorname{coker}(f(K)) & \longrightarrow & H^1(G_S,M) & \longrightarrow & H^1(G_S,A)[f] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\varphi'} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi''} & & \\
0 & \longrightarrow & \bigoplus_{v\in S}\operatorname{coker}(f(K_v)) & \longrightarrow & P^1_S(K,M) & \longrightarrow & \bigoplus_{v\in S} H^1(K_v,A)[f] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\psi'} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi''} & & \\
0 & \longrightarrow & H^1(G_S,\widehat{B})[\widehat{f}]^* & \longrightarrow & H^1(G_S,M^D)^* & \longrightarrow & \left(\operatorname{coker}\widehat{f}(K)\right)^* & \longrightarrow & 0
\end{array}$$

We will see that this is commutative, that the rows and middle column are exact, and that the left and right columns are complexes. The diagram is a combination of multiple exact sequences which include pieces of Proposition 4.1. In particular:

- the first column gives information about $\prod_{v\in S} \#\mathrm{coker} f(K_v)$, $\#\mathrm{coker} f(K)$, and $\#\ker Ш(\widehat{f})$ (as we'll see that $Ш(\widehat{f})$ is dual to $\mathrm{coker}(\psi')$, so they have the same size);
- the second column gives information about $\prod_{v\in S} \#\ker f(K_v)$ and $\#\ker f(K)$;
- applying the snake lemma to the first and second rows gives information about $\#\ker Ш(f)$ (as we'll see that $\ker \varphi'' = \ker Ш(f)$);
- the third row gives information about $\#\mathrm{coker}\widehat{f}(K)$.

However, $\#\ker \widehat{f}(K)$ appears nowhere in the diagram, so we must look for it elsewhere!

Now we turn to defining the diagram.

- The first and second full rows are truncations of the long exact cohomology sequences for the short exact sequences
$$0 \to M \to A(K_S) \xrightarrow{f} B(K_S) \to 0 \quad \text{and} \quad 0 \to M \to A(\overline{K_v}) \xrightarrow{f} B(\overline{K_v}) \to 0.$$
- For the third row, recall that there is a canonical isomorphism between $\ker(\widehat{f})$ and the Cartier dual of $\ker(f)$. Thus $M^D = \mathrm{Hom}(M, K_S^\times)$ is naturally isomorphic to $\ker(\widehat{f})(K_S)$. Then dualize a truncation of the long exact sequence for
$$0 \to M^D \to \widehat{B}(K_S) \xrightarrow{\widehat{f}} \widehat{A}(K_S) \to 0.$$
- The middle column comes from Fact 3.12.
- By Fact 3.7, there is a duality $B(K_v)^* \simeq H^1(K_v, \widehat{B})$. Under this isomorphism, the subgroup $\mathrm{coker}(f(K_v))^*$ is identified with $H^1(K_v, \widehat{B})[f]$ using Remark 3.10. We take ψ' to be the dual of the composite map
$$H^1(G_S, \widehat{B})[\widehat{f}] \to \bigoplus_{v\in S} H^1(K_v, \widehat{B})[\widehat{f}] \simeq \bigoplus_{v\in S} \mathrm{coker}(f(K_v))^*.$$
- Likewise, the map ψ'' is the dual of the composite
$$\mathrm{coker}(\widehat{f}(K)) \to \bigoplus_{v\in S} \mathrm{coker}(\widehat{f}(K_v)) \simeq \bigoplus_{v\in S} H^1(K_v, A)[f]^*.$$

These definitions make it clear that the middle column and rows are exact, and that the right and left columns are complexes because the middle column is exact.

It is mostly elementary to check that this diagram commutes, except for checking the lower squares commute, so we now address that point. We split up the square as

$$\begin{array}{ccc}
\bigoplus_{v\in S} \mathrm{coker}(f(K_v)) & \longrightarrow & \bigoplus_{v\in S} \widetilde{H}^1(K_v, M) \\
\downarrow & & \downarrow \\
\bigoplus_{v\in S} H^1(K_v, \widehat{B})[\widehat{f}]^* & \longrightarrow & \bigoplus_{v\in S} \widetilde{H}^1(K_v, M^D)^* \\
\downarrow & & \downarrow \\
H^1(G_S, \widehat{B})[\widehat{f}]^* & \longrightarrow & H^1(G_S, M^D)^*
\end{array}$$

The bottom obviously commutes, as the vertical maps are just restriction. The fact that the top commutes is the non-obvious compatibility of the duality pairing for abelian varieties with Tate local duality (Remark 3.9!).

For a finite complex of finite abelian groups, the Euler characteristic of the complex equals the Euler characteristic of the cohomology. In particular, for an exact sequence of finite abelian groups the Euler characteristic is 1. We apply this observation to various parts of the diagram:

- *First and Second Row.* We need to know that $\ker(\varphi'') = \ker(Ш(f))$. This is proven in [Mil06, Proposition I.6.5], and the content is to show that the natural map

$$H^1(G_S, A) \to H^1(\mathrm{Gal}(K_v^{\mathrm{un}}/K_v), A)$$

for $v \notin S$ is the zero map. More specifically, an element of $H^1(G_S, A)$ corresponds to an A-torsor X over K_v^{un}, so we must show $X(K_v) \neq \emptyset$; in other words, we claim that an unramified torsor for an abelian variety over K_v with good reduction is necessarily trivial. An argument using Néron models relying on the good reduction of A and Lang's theorem shows this; see [Mil06, Proposition I.3.8]. This argument is also implicit in [L3, §5].

We now apply the snake lemma to the first and second rows: after truncating, we obtain an exact sequence

$$0 \to \ker(\varphi') \to \ker(\varphi) \to \ker(\varphi'') \to \ker(\psi')/\operatorname{Im}(\varphi') \to 0.$$

All of the groups in this diagram are finite, so

$$\frac{\#\ker(\varphi') \cdot \#\ker Ш(f)}{\#\ker(\varphi) \cdot \#(\ker(\psi')/\operatorname{Im}(\varphi'))} = 1$$

- *First Column.* A similar argument shows that $\ker Ш(\widehat{f}) = \operatorname{coker}(\psi')^*$. Then using the duality between $\ker(Ш(\widehat{f}))$ and $\operatorname{coker}(Ш(f))$ (Fact 2.2), we see that $\operatorname{coker}(\psi') = (\ker(Ш(\widehat{f}))^*$. Computing the Euler characteristic of the complex and its cohomology gives that

$$\frac{\#\mathrm{coker}(f(K)) \cdot \#H^1(G_S, \widehat{B})[\widehat{f}]}{\prod_{v\in S} \#\mathrm{coker}(f(K_v))} = \frac{\#\ker(\varphi')\#\ker(Ш(\widehat{f}))}{\#\ker(\psi')/\operatorname{Im}(\varphi')}.$$

- *Third Row.* The row is exact, so $\#H^1(G_S, M^D) = \#\mathrm{coker}(\widehat{f}(K)) \cdot \#H^1(G_S, \widehat{B})[\widehat{f}]$.
- *Middle Column.* By definition $H^0(G_S, M) = \ker f(K)$, so if we truncate the middle column at $\ker(\varphi)$ we obtain

$$1 = \frac{\#\ker(f(K))}{\prod\limits_{v\in S} \#\ker(f(K_v))} \cdot \left(\prod_{v \text{ arch}} \frac{\#H^0(K_v, M)}{\#H^0_T(K_v, M)} \right) \cdot \frac{\#H^2(G_S, M^D)}{\#\ker(\varphi)}.$$

The extra terms at archimedean places is due to using the Tate cohomology group $H^0_T(K_v, M)$ in the definition of $P^0_S(K, M)$ whereas $\#\ker f(K_v) = H^0(K_v, M)$.

Multiply these four equalities with the obvious equality $\#\ker \widehat{f}(K) = \#H^0(G_S, M^D)$ to get

$$\prod_{v\in S} h(f(K_v)) = \frac{\#\ker Ш(\widehat{f})}{\#\ker Ш(f)} \cdot \frac{h(f(K))}{h(\widehat{f}(K))} \cdot \chi(G_S, M^D) \cdot \prod_{v \text{ arch}} \frac{\#H^0(K_v, M)}{\#H^0_T(K_v, M)}. \tag{4.1}$$

Voila, the last two terms cancel by the global Euler–Poincaré characteristic formula (Fact 3.16), so this completes the proof of Proposition 4.1! □

Remark 4.2. The term $\#\ker \widehat{f}(K)$ does not appear in the large diagram, but appears twice in (4.1): once in $\chi(G_S, M^D)$ and once in $h(\widehat{f}(K))$.

Appendix A. Relative Weil–Barsotti Formula and Applications

We want to show that for any scheme S and abelian A-scheme (A, e), there is a natural isomorphism between the group $\mathrm{Ext}^1(A, \mathbf{G}_m)$ of isomorphism classes of commutative extensions of S-groups

$$1 \to \mathbf{G}_m \to E \to A \to 1 \tag{A.1}$$

and the group $\widehat{A}(S)$ of isomorphism classes of pairs (L, i) consisting of a $\mathbf{G}_m$-torsor L over A (equivalently, a line bundle over A) equipped with a trivialization i of $e^*(L)$ such that fiberwise $L_s \in \mathrm{Pic}(A_s)$ is algebraically equivalent to zero (i.e., lies in the identity component of $\mathrm{Pic}_{A_s/k(s)}$). By the Theorem of the Square, the latter is equivalent to saying that

$$m^*(L_s) = (p_1)^*(L_s) + (p_2)^*(L_s)$$

as $\mathbf{G}_m$-torsors (equivalently as line bundles, then using $\otimes$ in place of the "diagonal pushout" construction "+" for torsors) over $A_s \times A_s$; such an isomorphism is ambiguous up to a global unit over A_s, which is to say an element of $k(s)^\times$, so it is unique upon demanding that it respect the evident trivializations on both sides arising from i_s on $e_s^*(L_s)$.

To be precise, given (A.1) we can view E as a $\mathbf{G}_m$-torsor over A, and the group law $E \times E \to E$ over $m : A \times A \to A$ defines a map of $\mathbf{G}_m$-torsors

$$E \times E = (p_1)^*(E) + (p_2)^*(E) \to m^*(A)$$

over $A \times A$, so an isomorphism (as for any map between torsors for any group). Moreover, $e^*(E) = \ker(E \to A) = \mathbf{G}_m$ has an evident trivialization via the global section 1 over S, so the underlying $\mathbf{G}_m$-torsor E really is in $\widehat{A}(S)$. That defines a map

$$\mathrm{Ext}^1(A, \mathbf{G}_m) \to \widehat{A}(S). \tag{A.2}$$

By construction this is clearly natural in A and compatible with base change morphisms in S.

Theorem A.1. *The map* (A.2) *is an isomorphism of groups.*

Proof. The description of the group law on Ext^1 in terms of pushout/pullback makes it easy to check that (A.2) is a homomorphism (e.g., consider the Čech 1-cocycle description of line bundles, and use the *injection* $\widehat{A}(S) \to \mathrm{Pic}(A)$).

To prove injectivity, suppose we are given (A.1) and that $E \to A$ has a section t over S, so the element $t \circ e \in E(S)$ lies over e, which is to say it belong to $\mathbf{G}_m(S)$. Applying to t the action by the inverse element of $\mathbf{G}_m(S)$ brings us to a new t with the property that $t : A \to E$ is an S-map carrying e to the identity 1 of E (same as the the identity of its S-subgroup $\mathbf{G}_m$!). We claim that now t is a homomorphism, so (A.1) is split as an exact sequence of S-groups (and hence is the vanishing class in Ext^1), as desired.

By the relative rigidity lemma [GIT, Prop. 6.1], since A is an abelian S-scheme it suffices to check the homomorphism property on geometric fibers. But over an algebraically closed field it is meaningful (e.g., by arguments as in Borel's book on algebraic groups given in the affine case) to form the "smooth closed algebraic subgroup generated" by a closed subvariety through the identity in a given smooth group variety. The image of $t(A)$ is proper, so the algebraic group it generates inside E is proper and connected, hence an abelian variety, so the homomorphism property comes down to classical rigidity considerations. This completes the proof that the homomorphism (A.2) is injective. Note that this final step did really use a technique specific to working over fields; it replaces the step where the proof in [Oor66, §18] appeals to the Weil–Barsotti theorem over fields.

There remains the most interesting part (as in the classical case), namely surjectivity: for $(L, i) \in \widehat{A}(S)$ (so i identifies $e^*(L)$ with $\mathbf{G}_m$), we must show that L admits an S-group structure making the projection

$$q : L \to A$$

an S-homomorphism and we must identify its kernel $e^*(L)$ with $\mathbf{G}_m$ as S-groups recovering the given trivialization i. For this we will proceed similarly to the classical case over fields. The "Mumford morphism" $\phi_L : A \to \widehat{A}$ between abelian S-schemes vanishes by rigidity since it vanishes on fibers by the classical theorem (i.e., Theorem of the Square as noted above), so we have an isomorphism (equivalently, a morphism!) of $\mathbf{G}_m$-torsors

$$(p_1)^*(L) + (p_2)^*(L) \to m^*(L)$$

over $A \times A$, and it is ambiguous by an element of $\mathbf{G}_m(A) = \mathbf{G}_m(S)$, so we can uniquely choose this isomorphism to respect the evident trivializations on both sides arising from i. But this is exactly the data of an S-morphism

$$\mu : L \times L \to L$$

over $m : A \times A \to A$. The uniqueness controlled by i-compatibility ensures that if we write down the "associativity" diagram then it commutes! Hence, μ is an associative composition law. Likewise, uniqueness controlled by i-compatibility ensures that the global section of $e^*(L)$ defined by i is a 2-sided identity for this composition law (exercise!), and one sees that μ is commutative.

Finally, the equality $\phi_{[-1]^*(L)} = \phi_L$ which we check by rigidity and the classical theory on geometric fibers gives an isomorphism of $\mathbf{G}_m$-torsors

$$L^{-1} \to [-1]^*(L)$$

which moreover is unique upon demanding i-compatibility. But L^{-1} is the pushout of the $\mathbf{G}_m$-torsor $L \to A$ along the inversion automorphism of $\mathbf{G}_m$, which is to say that there is an isomorphism of A-schemes $L \to L^{-1}$ compatible with $\mathbf{G}_m$-actions intertwined through inversion on $\mathbf{G}_m$. This latter isomorphism is uniquely determined upon demanding i-compatibility, so composing gives an A-isomorphism $L \to [-1]^*(L)$, which is to say an isomorphism

$$\mathrm{inv} : L \to L$$

over inversion on A, and by design it is i-compatible. Thus, the same kind of uniqueness considerations resting on i-compatibility as above ensure that inv is a 2-sided inverse for μ relative to the 2-sided identity in $e^*(L)$ arising from i.

We have now built a commutative S-group law on L over the S-group law on A, and its kernel $e^*(L)$ is identified with a commutative S-group law on $\mathbf{G}_m$ having identity section 1 (due to how the identity of μ was built!). It is easy to check by hand that the only S-group law on the pointed scheme $(\mathbf{G}_m, 1)$ over any ring is the usual one (a "rigidity" analogous to that of abelian schemes, which is sufficient to prove over an artin local base since $\mathbf{G}_m$ is affine of finite presentation over S; all is clear over the residue field, and then deduced over the artin local ring via deformation theory of tori over rings such as in SGA3, and surely can also be done by bare hands via length induction in the present circumstances). This gives the desired identification of the kernel with $\mathbf{G}_m$ *in such a way that* the resulting translation-action of the kernel on L recovers the original $\mathbf{G}_m$-torsor structure on L (otherwise the class we just built in Ext^1 wouldnt be hitting what we expect in $\widehat{A}(S)$!). □

An immediate consequence of Theorem A.1 is that the fppf sheaf $\mathscr{E}xt^1(A, \mathbf{G}_m)$ on the category of S-schemes is represented by $\widehat{A}$. Now focusing on sheaves on $S_{\text{ét}}$, consider the local-to-global spectral sequence for Ext:

$$\mathrm{E}_2^{i,j} = \mathrm{H}^i(S, \mathscr{E}xt^j(A, \mathbf{G}_m)) \Rightarrow \mathrm{Ext}^{i+j}(A, \mathbf{G}_m).$$

The terms with $j = 0$ (i.e., the terms along the bottom edge) vanish since the functor $\mathscr{H}om(A, \mathbf{G}_m)$ on S-schemes given by $T \rightsquigarrow \mathrm{Hom}(A_T, \mathbf{G}_{m,T})$ vanishes (i.e., there is no nonzero homomorphism from an abelian scheme to a smooth relatively affine group scheme over any base scheme). Thus, we get a natural homomorphism

$$\mathrm{H}^i(S, \widehat{A}) = \mathrm{H}^i(S, \mathscr{E}xt^1(A, \mathbf{G}_m)) \to \mathrm{Ext}^{i+1}(A, \mathbf{G}_m).$$

In particular, setting $i = 1$, we get a natural homomorphism

$$\mathrm{H}^1(S, \widehat{A}) \to \mathrm{Ext}^2(A, \mathbf{G}_m) = \mathrm{Hom}_{\mathbf{D}(S_{\text{ét}})}(A, \mathbf{G}_m[2]) \tag{A.3}$$

where $\mathbf{D}(S_{\text{ét}})$ is the derived category of abelian sheaves on $S_{\text{ét}}$.

We now apply this in the study of an abelian variety A over a number field K, to give one of the constructions of the *Cassels–Tate pairing*

$$Ш(A) \times Ш(\widehat{A}) \to \mathbf{Q}/\mathbf{Z}.$$

The construction we describe will be rather abstract, but it is cohomologically rather clean (and doesn't involve any messing around with cocycles). The price to pay for cohomological elegance is that many desirable properties of the pairing (such as its interaction with double duality and skew-symmetric relative to polarizations) will not be apparent for this formulation of the constriction.

Let $X := \mathrm{Spec}(\mathcal{O}_K)$, and let $U \subset X$ be any dense open whose complement contains the points of bad reduction, so A extends to an abelian scheme $\mathscr{A}$ over U. Using the cohomological work in [L4] (especially if K has real places), let $\overline{X}$ be the "compactification" of X via real places. Let $j : U_{\text{ét}} \to \overline{X}_{\text{ét}}$ be the natural map of étale sites; recall that by definition $\mathrm{H}^i_c(U, \mathscr{F}) := \mathrm{H}^i(\overline{X}, j_!(\mathscr{F}))$ for any abelian sheaf $\mathscr{F}$ on $U_{\text{ét}}$, and class field theory gives canonical isomorphisms

$$\mathrm{H}^3_c(U, \mathbf{G}_m) \simeq \mathrm{H}^3(\overline{X}, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}.$$

In [L3, §5] there were several descriptions given for $Ш(A)$, or rather for the slightly larger group $Ш(A)' \subset \mathrm{H}^1(K, A)$ in which local triviality at the archimedean places is not imposed (so really just the real places are ignored). The description of $Ш(\widehat{A})'$ provided by [L3, Prop. 5.4] yields the description

$$Ш(\widehat{A}) = \ker(\mathrm{H}^1(U, (\mathscr{A})^\wedge) \to \prod_{x \in \overline{X} - U} \mathrm{H}^1(K_x, \widehat{A})) \tag{A.4}$$

in terms of the dual abelian scheme $(\mathscr{A})^\wedge$ over U.

We will now give an alternative description, for $Ш(A)$, in terms of $\mathrm{H}^1_c(U, \mathscr{A})$. It was explained near the end of [L4, §5] that for any $x \in \overline{X}$ and $i \geq 1$, $\mathrm{H}^i_x(\overline{X}, j_!(\mathscr{G}))$ is equal to $\mathrm{H}^{i-1}(K^{D_x}, \mathscr{G}_K)$ for any $i \geq 1$. (If x is a finite point then K^{D_x} is the fraction field of the henselization of $\mathcal{O}_{X,x}$, whereas if x is a real point then K^{D_x} is a copy of the field of real algebraic numbers.) Thus, the local cohomology sequence on $\overline{X}$ for $\mathscr{F} := j_!(\mathscr{A})$ gives an exact sequence

$$\prod_{x \in \overline{X} - U} A(K^{D_x}) \xrightarrow{\delta} \mathrm{H}^1_c(U, \mathscr{A}) \to \mathrm{H}^1(U, \mathscr{A}) \to \prod_{x \in \overline{X} - U} \mathrm{H}^1(K^{D_x}, A)$$

(and the final map is identified with the natural restrictions). The natural map $\mathrm{H}^1(K^{D_x}, A) \to \mathrm{H}^1(K_x, A)$ to cohomology over the local field K_x is *injective*: this says that A-torsors over K^{D_x} with a K_x-point necessarily having a K^{D_x}-point, and that property follows from the real Nullstellensatz for real x and from considerations with Néron models for unramified torsors when x is finite. Using the A-analogue of (A.4) then yields an analogue of [L3, (5.5)] incorporating real places: a quotient presentation

$$\prod_{x \in \overline{X} - U} A(K^{D_x}) \to \mathrm{H}^1_c(U, \mathscr{A}) \to Ш(A) \to 0.$$

By (A.3), we have a natural pairing

$$\mathrm{H}^1_c(U, \mathscr{A}) \times \mathrm{H}^1(U, (\mathscr{A})^\wedge) \to \mathrm{H}^1_c(U, \mathscr{A}) \times \mathrm{Hom}_{\mathbf{D}(U_{\text{ét}})}(\mathscr{A}, \mathbf{G}_m[2]) \to \mathrm{H}^3_c(U, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z},$$

where the finally arrow is defined via functoriality of $\mathrm{H}^\bullet_c(U, \cdot)$ on the derived category. Restricting to the subgroup $Ш(\widehat{A})$ in the second variable, the resulting pairing composes back to the pairing against $A(K^{D_x})$ in the first variable induced by the $\mathbf{Q}/\mathbf{Z}$-valued Tate local duality pairing for A over $K_x \supset K^{D_x}$. Thus, the local triviality of classes in $Ш(\widehat{A})$ thereby yields a bilinear pairing between $Ш(A)$ and $Ш(\widehat{A})$ valued in $\mathbf{Q}/\mathbf{Z}$; this is seen to be compatible with shrinking U by just unraveling some definitions. The agreement of this construction with others is not at all obvious, and the asymmetric manner in which it treats A and $\widehat{A}$ makes it unclear how this pairing interacts with double duality for abelian varieties.

References

[L3] Brian Conrad, *Neron Models, Tamagawa Factors, and Tate-Shafarevich Groups*, October 2015.

[L2] Brian Conrad and Akshay Venkatesh, *Bloch-Kato Conjecture and Height Pairings*, October 2015.

[L1] ———, *Overview*, September 2015.

[MO] *Why is the Tate local duality pairing compatible with the Cartier duality pairing?*, http://mathoverflow.net/questions/177361/why-is-the-tate-local-duality-pairing-compatible-with-the-cartier-duality-pairin

[L4] Alessandro Masullo, *Global Duality in Galois Cohomology*, October 2015.

[Mil06] J. S. Milne, *Arithmetic Duality Theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006. MR 2261462 (2007e:14029)

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026 (2008m:11223)

[Oor66] F. Oort, *Commutative group schemes*, Lecture Notes in Mathematics, vol. 15, Springer-Verlag, Berlin-New York, 1966. MR 0213365 (35 #4229)

[Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French. MR 918564 (88i:14041)

[L5] Akshay Venkatesh, *BSD Examples*, October 2015.