A GRUNWALD-WANG TYPE THEOREM FOR ABELIAN VARIETIES

BRENDAN CREUTZ

Abstract. Let A be an abelian variety over a number field k. We show that weak approximation holds in the Weil-Châtelet group, $\mathrm{H}^1(k, A)$. This establishes a conjecture of Lang and Tate which can be seen as an analog of the Grunwald-Wang theorem in class field theory. The methods apply, for the most part, to arbitrary finite Galois modules and so may be of interest in their own right.

1. Introduction

Motivation. Let k be a number field and denote its completion at a prime v by k_v. The Grunwald-Wang theorem is an existence theorem for abelian extensions of k with prescribed local behavior. Namely, given abelian extensions K_v/k_v, for v in some finite set S, with Galois groups H_v, all of which may be embedded in some abelian group H, the theorem asserts that there is an abelian extension K/k with completions K_v. Usually one is also allowed the requirement that $\mathrm{Gal}(K/k)$ can be embedded in H. It is only in a particular set of well understood circumstances that this stronger requirement can fail. For example, the unramified extension of $\mathbb{Q}_2$ of degree 8 cannot be realized by any degree 8 cyclic extension of $\mathbb{Q}$. In general, obstructions can only occur when 8 divides the exponent of H, and then only at primes of k lying above 2.

These global (resp. local) extensions correspond to continuous homomorphisms from the absolute Galois group, G_k (resp. decomposition groups), to H. Considering H as a finite G_k-module with trivial action, we have $\mathrm{H}^1(k, H) = \mathrm{Hom}_{cont}(G_k, H)$ and similarly for the local cohomology groups. So the Grunwald-Wang theorem can be rephrased as a statement about the surjectivity of the restriction map $\mathrm{H}^1(k, H) \to \prod_{v \in S} \mathrm{H}^1(k_v, H)$.

Now let A be an abelian variety over a number field k and n a positive integer. The Weil-Châtelet group, $\mathrm{H}^1(k, A)$, parameterizes torsors under A/k. In [LT, p. 683] Lang and Tate write

Date: January 31, 2012.

2010 *Mathematics Subject Classification.* Primary 11GR34; Secondary 11G99.

Key words and phrases. Galois cohomology, Weil-Châtelet group, Hasse principle.

"In analogy with Grunwald's theorem in class field theory, one may conjecture that if k is an algebraic number field and $\mathfrak{p}$ a given prime, then given $\alpha_{\mathfrak{p}} \in \mathrm{H}^1(k_{\mathfrak{p}}, A)$, there exists $\alpha \in \mathrm{H}^1(k, A)$ restricting to $\alpha_{\mathfrak{p}}$."

For any n, there is a surjective map $\mathrm{H}^1(k, A[n]) \to \mathrm{H}^1(k, A)[n]$ (here $H[n]$ denotes the n-torsion in an abelian group H). One can also ask for analogs of the Grunwald-Wang theorem at finite level.

Question 1.1. *Given an abelian variety A over a number field k, an integer $n \geq 2$ and a finite set of primes S, is the map $\mathrm{H}^1(k, A[n]) \to \prod_{v \in S} \mathrm{H}^1(k_v, A[n])$ surjective?*

Question 1.2. *Given an abelian variety A over a number field k, an integer $n \geq 2$ and a finite set of primes S, is the map $\mathrm{H}^1(k, A)[n] \to \prod_{v \in S} \mathrm{H}^1(k_v, A)[n]$ surjective?*

Perhaps motivating their conjecture, Lang and Tate showed that the answer to these questions is yes when $\mu_n \subset k$ and the action of the Galois group on $A[n]$ is trivial ([LT], see also [Si, Exercise 10.8]). This also follows directly from the Grunwald-Wang theorem. Assuming the finiteness of the Tate-Shafarevich group $Ш(A/k)$, Tate went on to characterize the image of the map $\mathrm{H}^1(k, A) \to \bigoplus_{\text{all } v} \mathrm{H}^1(k_v, A)$ in terms of a kind of reciprocity coming from the dual abelian variety (see [Mi, I.6.26b]). However, this settles neither the conjecture nor the questions above, even under the assumption that $Ш(A/k)$ is finite.

1.1. **Statement of results.** In this paper we prove the conjecture, independently of the finiteness of $Ш(A/k)$. With regard to questions 1.1 and 1.2 we show, in analogy with the Grunwald-Wang theorem, that the answer can be no in general, but generically will be yes.

Theorem 1.3 (weak approximation)**.** *Let A/k be an abelian variety over a number field k and let S be any finite set of primes. Then the map $\mathrm{H}^1(k, A) \to \prod_{v \in S} \mathrm{H}^1(k_v, A)$ is surjective.*

Theorem 1.4. *There exists an abelian variety $A/\mathbb{Q}$ such that, for infinitely many n (including $n = 2$), the map $\mathrm{H}^1(\mathbb{Q}, A)[n] \to \mathrm{H}^1(\mathbb{Q}_2, A)[n]$ is not surjective.*

Theorem 1.5. *Let A/k be an abelian variety over a number field k. There exists a constant $c = c(A, k)$ such that if n is an integer divisible by no prime less than c and S is any finite set of primes, then the map $\mathrm{H}^1(k, A[n]) \to \prod_{v \in S} \mathrm{H}^1(k_v, A[n])$ is surjective.*

The Grunwald-Wang theorem shows that while weak approximation does not always hold for $\mathrm{H}^1(k, \mathbb{Z}/n\mathbb{Z})$, it does hold outside some finite set of primes. Along these lines we prove the following.

Theorem 1.6 (weak weak approximation)**.** *Let A/k be an abelian variety over a number field k and n an integer. Let S be any set of primes containing all primes of bad reduction and all primes dividing n. Let $Ш(k, A[n], S^c)$ denote the subgroup of $\mathrm{H}^1(k, A[n])$ consisting of classes that are locally trivial on S. The restriction map $Ш(k, A[n], S^c) \to \prod_{v \notin S} \mathrm{H}^1(k_v, A[n])$ has dense image in the product of the discrete topologies.*

A slightly weaker form of this result (with $Ш(k, A[n], S^c)$ replaced by $\mathrm{H}^1(k, A[n])$) can be deduced rather easily from [Mi, Lemma I.9.8]. In [Cr] this stronger form is used to show that the p-torsion in the Tate-Shafarevich group of any principally polarized abelian variety over a number field is unbounded as one ranges extensions of degree $\mathcal{O}(p)$, the implied constant depending only on the dimension of the abelian variety.

As we show below, these results are closely related to various local-global properties of the group $\mathrm{H}^1(k, A[n])$. More generally, Dvornicich and Zannier have studied the local-global principle in $G(k)/nG(k)$ and $\mathrm{H}^1(k, G[n])$, for a commutative algebraic group G (see [DZ1, DZ2, DZ3]). Their results and ideas play a large role in the development below. On the other hand, it seems the related problem of weak approximation has only been addressed in the case of linear algebraic groups (for example [Mi, Theorem I.9.10] and the Grunwald-Wang theorem itself).

1.2. **Organization.** Section 2 contains a quick review of Potiou-Tate duality and other results in Galois cohomology of number fields needed in what follows. In section 3 we study various local-global 'principles' for cohomology groups of finite G_k-modules. Much of this section is influenced by the ideas in [DZ1, DZ3]. In section 4 we use Poitou-Tate duality to characterize (weak) weak approximation in terms of the local-global principles of the previous section. The main result here is proposition 4.6, which gives a broad generalization of theorem 1.6. All of this is then applied to the particular case of abelian varieties in section 5, where the proofs of theorems 1.3, 1.4 and 1.5 are given.

2. Preliminaries

We recall several well known results in Galois cohomology that will be used below. For details we refer the reader to [Se4, Section II.5-6] or [CoN, Chapters VII-VIII].

Throughout the paper we adopt the following notation: k is a number field, G_k denotes its absolute Galois group, M is a finite G_k-module of exponent n and $M^\vee = \mathrm{Hom}(M, \mu_n)$ is its dual. We use $\mathrm{H}^i(k, -)$ and $\mathrm{H}^i(k_v, -)$ to denote global and local Galois cohomology groups. Our convention for indexing (co)products will be that if no index set is specified, then the (co)product is to be taken over all primes v of k. Similarly, an expression such as $\prod_{v \notin S}$ is understood to run over all primes of k not in the set S. When we say something holds almost everywhere or almost everywhere locally, this means at all but a finite number of primes of k.

For each prime v of k, duality and the cup-product induce a nondegenerate bilinear pairing (the Tate pairing)

$$(\ ,\ )_v : \mathrm{H}^1(k_v, M) \times \mathrm{H}^1(k_v, M^\vee) \to \mathrm{Br}(k_v)[n]\,. \tag{2.1}$$

For almost all v, the unramified subgroups of $\mathrm{H}^1(k_v, M)$ and $\mathrm{H}^1(k_v, M^\vee)$ are exact annihilators with respect to this pairing.

We denote the global pairing induced by the cup product and duality by

$$(\ ,\ ) : \mathrm{H}^1(k, M) \times \mathrm{H}^1(k, M^\vee) \to \mathrm{Br}(k)[n]\,.$$

This pairing is no longer nondegenerate, but it is compatible with the local pairings via the restriction maps. For this reason we will often denote the Tate pairings as defined on global classes as well (i.e. for $\xi \in \mathrm{H}^1(k, M)$, we may write $(\xi, -)_v$ to mean $(\mathrm{res}_v(\xi), -)_v$ and similarly for classes in $\mathrm{H}^1(k, M^\vee)$).

For nonarchimedean primes v, there is a canonical isomorphism $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ (in the archimedean case a canonical injection). The groups $\mathrm{H}^1(k_v, M)$ and $\mathrm{H}^1(k_v, M^\vee)$ are finite, and the Tate pairing identifies $\mathrm{H}^1(k_v, M)$ and $\mathrm{H}^1(k_v, M^\vee)$ as Pontryagin duals of one another (i.e. $\mathrm{H}^1(k_v, M^\vee) = \mathrm{H}^1(k_v, M)^* := \mathrm{Hom}(\mathrm{H}^1(k_v, M), \mathbb{Q}/\mathbb{Z})$).

The Brauer group of k satisfies a local-global principle expressed by the exactness of

$$0 \to \mathrm{Br}(k) \xrightarrow{\prod \mathrm{res}_v} \bigoplus \mathrm{Br}(k_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0\,.$$

This gives rise to a product rule for global classes. Namely,

$$\sum \mathrm{inv}_v(\xi, \eta)_v = 0 \text{ for all } \xi \in \mathrm{H}^1(k, M) \text{ and } \eta \in \mathrm{H}^1(k, M^\vee). \tag{2.2}$$

Note that since any global class is unramified almost everywhere, this sum is in fact finite.

Given $(\xi_v) \in \prod \mathrm{H}^1(k_v, M)$, there are two obvious necessary conditions for the existence of a lift of (ξ_v) to a global cocycle. First, (ξ_v) must be unramified outside of some finite set of primes. Second, (ξ_v) must obey the aforementioned product rule. In fact these conditions are already sufficient. This is expressed by the (middle third of the) Poitou-Tate exact sequence

$$\mathrm{H}^1(k, M) \to \prod{}' \mathrm{H}^1(k_v, M) \to \mathrm{H}^1(k, M^\vee)^* . \tag{2.3}$$

Here the product is the restricted product taken with respect to unramified subgroups. The map on the right is given by

$$(\xi_v) \mapsto \Big(\eta \mapsto \sum \mathrm{inv}_v(\xi_v, \eta)\Big) \in \mathrm{Hom}\big(\mathrm{H}^1(k, M^\vee), \mathbb{Q}/\mathbb{Z}\big) .$$

As a set, the restricted product consists of all families (ξ_v) such that ξ_v is in the unramified subgroup for almost all v. It is endowed with a natural topology making it into a locally compact group. The topology is defined by specifying a neighborhood base of 0 to be the family of all subgroups $\big(\prod_{v\in T} 0\big) \times \big(\prod_{v\notin T} \mathrm{H}^1_{nr}(k_v, M)\big)$, as T ranges over the finite sets of primes of k containing all primes where M is ramified.

3. Local-global principles

Definition 3.1. Let M be a finite G_k-module and $V \subset \mathrm{H}^1(k, M)$ a subgroup.

(1) For a set T of primes of k, we define $Ш(V, T)$ to be the kernel of the restriction map $V \to \prod_{v\notin T} \mathrm{H}^1(k_v, M)$.
(2) We say that the *Hasse principle* holds for V if $Ш(V, \emptyset) = 0$.
(3) We say that the *strong Hasse principle* holds for V if $Ш(V, T) = 0$, for every finite set of primes T.
(4) For a finite set of primes T, we say that V is *T-singular* if the image of the map $Ш(V, T) \to \prod_{v\in T} \mathrm{H}^1(k_v, M)$ is not trivial.
(5) We say that V is *nonsingular* if it is not T-singular for any finite set of primes T.

Remark 3.2. One easily sees that the strong Hasse principle holds for V if and only if V is nonsingular and the Hasse principle holds. We will see below that the Hasse principle and nonsingularity are, however, independent.

If $\xi \in Ш(V, T)$ for some finite set of primes T, we will say that ξ is *finitely supported*. If in addition $\xi \notin Ш(V, \emptyset)$ we say that ξ is *T-singular* (or simply *singular*). When $V = \mathrm{H}^1(k, M)$ we will use the abbreviation $Ш(k, M, T)$

for $Ш(\mathrm{H}^1(k,M),T)$. For a profinite group G and finite G-module M, let $\mathrm{H}^1_*(G,M)$ denote the kernel of the map $\mathrm{H}^1(G,M) \to \prod_Z \mathrm{H}^1(Z,M)$, where the product runs over all closed cyclic subgroups of G. For a Galois extension K/k we will also write $\mathrm{H}^1_*(K/k,M)$ to denote $\mathrm{H}^1_*(\mathrm{Gal}(K/k),M)$. This group was introduced by Tate (see [Se1] and [Mi, Section I.9]). This group is also used by by Dvornicich and Zannier to study the Hasse principle for divisibility in commutative algebraic groups, see [DZ1, DZ3]. The following lemma is basically well known (see also [Mi, Lemma I.9.3]).

Lemma 3.3. *Let M be a finite G_k-module and let K/k denote the minimal Galois extension over which the action on M is trivial. The strong Hasse principle holds for $\mathrm{H}^1(k,M)$ if and only if $\mathrm{H}^1_*(K/k,M)=0$.*

Proof: Let T be any finite set of primes of k and let U be the set of primes of K which lie above some prime in T. The inflation and restriction maps give a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^1(K/k,M) & \xrightarrow{\inf_{K/k}} & \mathrm{H}^1(k,M) & \xrightarrow{\mathrm{res}_{K/k}} & \mathrm{H}^1(K,M) \\ & & \downarrow \prod \mathrm{res}_w & & \downarrow \prod \mathrm{res}_v & & \downarrow \prod \mathrm{res}_w \\ 0 & \longrightarrow & \prod_{w\notin U} \mathrm{H}^1(K_w/k_v,M) & \longrightarrow & \prod_{w\notin U} \mathrm{H}^1(k_v,M) & \longrightarrow & \prod_{w\notin U} \mathrm{H}^1(K_w,M) \end{array}$$

(In the bottom row v always denotes the prime of k lying under w). The kernel of the middle vertical map is $Ш(k,M,T)$, while the kernel of the vertical map on the left is $Ш(\mathrm{H}^1(K/k,M),T)$ (we are considering $\mathrm{H}^1(K/k,M)$ as a subgroup of $\mathrm{H}^1(k,M)$ via the inflation map). The groups on the right consist of continuous homomorphisms. It follows from Chebotarëv's density theorem that the vertical map on the right is injective. So the kernels of the other two vertical maps are isomorphic.

It thus suffices to show that $\mathrm{H}^1_*(K/k,M)=0$ if and only if the subgroup $\mathrm{H}^1(K/k,M) \overset{\inf_{K/k}}{\subset} \mathrm{H}^1(k,M)$ satisfies the strong Hasse principle. This also follows from Chebotarëv's density theorem. For all but finitely many primes (namely those where K/k is ramified) the decomposition groups are cyclic and every cyclic subgroup occurs as the decomposition group at a positive density set of primes. So $\mathrm{H}^1_*(K/k,M)$ consists entirely of finitely supported classes and every finitely supported class in $\mathrm{H}^1(K/k,M)$ is contained in $\mathrm{H}^1_*(K/k,M)$. The proof is completed by noting that the strong Hasse principle holds if and only if every finitely supported class is trivial.

□

Corollary 3.4. *Let M and K/k be as in the proposition.*

(1) *The Hasse principle holds for* $\mathrm{H}^1(k, M)$ *if and only if* $\mathrm{H}^1_*(K/k, M) \cap Ш(K/k, M, \emptyset) = 0$.
(2) $\mathrm{H}^1(k, M)$ *is nonsingular if and only if* $\mathrm{H}^1_*(K/k, M) \subset Ш(K/k, M, \emptyset)$.

PROOF: As noted in the proof above, every finitely supported class in $\mathrm{H}^1(k, M)$ is contained in (the image under the inflation map of) $\mathrm{H}^1_*(K/k, M)$. The intersection in (1) is trivial if and only if there is no nontrivial class in $\mathrm{H}^1(k, M)$ with trivial support. Similarly the containment in (2) holds if and only if every finitely supported class has trivial support. □

From the proof we also extract the following useful observation.

Corollary 3.5. *Let* M *be a finite* G_k*-module and* S *the finite set of primes consisting of all primes where the decomposition group in* $\mathrm{Gal}(K/k)$ *is not cyclic. Let* V *be a subgroup of* $\mathrm{H}^1(k, M)$ *and* T *any finite set of primes. Then*

(1) $Ш(V, T) \subset Ш(V, S)$.
(2) *if* $T \cap S = \emptyset$, *then* $Ш(V, T) = 0$.

Remark 3.6. Note that the set S in the corollary is contained in the finite set of primes where M is ramified.

3.1. **Local-global principles for** $\mathrm{H}^1(k, \mu_n)$**.** In the case $M = \mu_n$, one can give a complete description of the finitely supported classes in $\mathrm{H}^1(k, \mu_n)$. Recall that Hilbert's theorem 90 gives an isomorphism $\mathrm{H}^1(k, \mu_n) \simeq k^\times / k^{\times n}$, so this can be interpreted as the study of local-global properties of divisibility in $\mathbb{G}_m$. We summarize with the following theorem. For the proof we refer the reader to [CoN, IX.1]. The Grunwald-Wang theorem can be derived as a consequence using, for example, theorem 4.1 below.

Theorem 3.7. *Let* T *be a finite set of primes of* k, $n = 2^r n'$ *be a positive integer with* n' *odd and let* κ *be the kernel of the map* $k^\times / k^{\times n} \to \prod_{v \notin T} k_v^\times / k_v^{\times n}$. *Then*

(1) κ *has order dividing* 2.
(2) κ *is nontrivial if and only if* $k(\mu_{2^r})/k$ *is not cyclic and* T *contains all primes* v *which do not decompose in* $k(\mu_{2^r})$
(3) *If* n *is even, then* κ *is contained in* $k^{\times(n/2)} / k^{\times n} \subset k^\times / k^{\times n}$.

Remark 3.8. Since $k(\mu_4) = k(\sqrt{-1})$ is cyclic, the κ can be nontrivial only when $r \geq 3$, i.e. $8 \mid n$. Suppose $k(\mu_{2^r})/k$ is not cyclic and let S be the set of primes of k which do not decompose in $k(\mu_{2^r})/k$. Then S consists entirely of 2-adic primes. Indeed, all other primes are unramified, so the decomposition groups are cyclic, but $k(\mu_{2^r})|k$ is not.

By way of example, consider $V := \mathrm{H}^1(\mathbb{Q}, \mu_8) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 8}$. For a finite set of primes T, the kernel of the map $\mathbb{Q}^\times/\mathbb{Q}^{\times 8} \to \prod_{v\notin T} \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 8}$ is nontrivial if and only if $2 \in T$. Thus the Hasse principle holds for V, and the singular sets for V are the finite sets of primes containing 2. When $2 \in T$, the nontrivial class in the kernel is represented by 16. In other words 16 is a v-adic 8-th power if and only if $v \neq 2$. Adjoining a square root of 7 to $\mathbb{Q}_2$ gives a ramified extension in which 16 is an 8-th power. However, 16 is not an 8-th power in $\mathbb{Q}(\sqrt{7})^\times$. Thus $\mathrm{H}^1(\mathbb{Q}(\sqrt{7}), \mu_8)$ is nonsingular but the Hasse principlie fails. Note that, in agreement with theorem 3.7(3), 16 is a 4-th power.

4. Weak approximation

Suppose $\xi \in Ш(k, M, T)$ is a class supported entirely on some finite set of primes T. Consider its image $\mathrm{res}_T(\xi) \in \prod_{v\in T} \mathrm{H}^1(k_v, M)$. It follows from the product rule (2.2) that the image of $\mathrm{res}_T^\vee : \mathrm{H}^1(k, M^\vee) \to \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$ must be orthogonal to $\mathrm{res}_T(\xi)$ with respect to the nondegenerate pairing

$$(\ ,\ )_T : \prod_{v\in T} \mathrm{H}^1(k_v, M) \times \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee) \to \mathbb{Q}/\mathbb{Z}\,,$$

given by $\sum_{v\in T} \mathrm{inv}_v(\ ,\ )_v$. In fact, this is the only restriction on the image of $\mathrm{res}_T^\vee$.

Theorem 4.1. *Let M be a finite G_k-module with dual $M^\vee$ and T a finite set of primes. An element $(\xi_v) \in \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$ is in the image of $\mathrm{res}_T^\vee$ if and only if it is orthogonal to $\mathrm{res}_T\ Ш(k, M, T)$ with respect to the pairing $(\ ,\ )_T$.*

The theorem is a special case of proposition 4.6. The more technical version below will allow us to determine also the image of $\mathrm{res}_T^\vee$ modulo arbitrary subgroups of $\prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$. This in turn will be used to characterize weak approximation in the n-torsion of the Weil-Châtelet group of an abelian variety, and ultimately to prove that weak approximation holds in the Weil-Châtelet group. First we give two corollaries. The second, together with the criterion of Neron-Ogg-Shafarevich, implies theorem 1.6.

Corollary 4.2. *The map $\mathrm{res}_T^\vee : \mathrm{H}^1(k, M^\vee) \to \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$ is surjective if and only if $\mathrm{H}^1(k, M)$ is not T-singular. In particular, weak approximation holds for $\mathrm{H}^1(k, M^\vee)$ if and only if $\mathrm{H}^1(k, M)$ is nonsingular.*

Proof: This follows from the fact that $(\ ,\ )_T$ is nondegenerate. □

Corollary 4.3. *Let S be the finite set of primes consisting of primes where M is ramified. The map* $\mathrm{res}_S^\vee : Ш(k, M^\vee, S) \to \prod_{v\notin S} \mathrm{H}^1(k_v, M^\vee)$ *has dense image in the product of the discrete topologies.*

PROOF: Suppose T is any finite set of primes and $(\eta_v) \in \prod_{v\in T\cup S} \mathrm{H}^1(k_v, M^\vee)$ with $\eta_v = 0$, for all v in S. We need to show that (η_v) is orthogonal to $\mathrm{res}_{T\cup S}\ Ш(k, M, T \cup S)$. Clearly (η_v) is orthogonal to $\mathrm{res}_{T\cup S}\ Ш(k, M, S)$. The result then follows from Corollary 3.5 which implies that $Ш(k, M, T \cup S) \subset Ш(k, M, S)$. □

4.1. **Weak approximation for abelian extensions.**

Theorem 4.4 (Grunwald-Wang)**.** *Let T be a finite set of primes and, for each $v \in T$, let K_v/k_v be an abelian extension. There exists an abelian extension K/k with completions K_v.*

PROOF: Choose an abelian group A for which we can find, for each $v \in T$, an embedding $f_v : \mathrm{Gal}(K_v/k_v) \to A$. It suffices to find an abelian group $B \supset A$ such that (f_v) is in the image of the map $\mathrm{Hom}_{cont}(G_k, B) \to \prod_{v\in T} \mathrm{Hom}_{cont}(G_{k_v}, B)$. We reduce to the case that B and, hence, A are cyclic. Suppose $A = \mathbb{Z}/n\mathbb{Z}$ and let $B = \mathbb{Z}/2n\mathbb{Z}$. Let $\xi \in Ш(k, \mu_{2n}, T)$. The dual of B is μ_{2n}, so by theorem 4.1, it suffices to show that $(f_v)_{v\in T}$ is orthogonal to $\mathrm{res}_T(\xi) \in \prod_{v\in T} \mathrm{H}^1(k_v, \mu_{2n})$. By theorem 3.7, ξ lies in the subgroup $n\,\mathrm{H}^1(k, \mu_{2n})$. On the other hand, the f_v are n-torsion and the pairing $(\ ,\ )_T$ is bilinear. The result follows. □

Remark 4.5. If every cyclic factor $\mathbb{Z}/n\mathbb{Z}$ of A is such that $\mathrm{H}^1(k, \mu_n)$ is nonsingular, then one can take $B = A$ in the proof above. Precisely when this can be done is determined by theorem 3.7. Taken together these two results give what is commonly known as the Grunwald-Wang theorem (see [CoN, IX.2]).

4.2. **Weak approximation modulo open subgroups.** Let U be an open subgroup of the restricted product $\prod' \mathrm{H}^1(k_v, M)$. U is a product of subgroups $U_v \subset \mathrm{H}^1(k_v, M)$. If U is a proper subgroup, then all but finitely many of these are equal to the unramified subgroup. If $U_v^\perp$ denotes the exact annihilator of U_v with respect to the Tate pairing, then $U^\perp := \prod U_v^\perp$ is an open subgroup of $\prod' \mathrm{H}^1(k, M^\vee)$. Note that when $U = 0$, $U^\perp$ is the entire restricted product and conversely.

Let us use V_U and $V_{U^\perp}$ to denote the subgroups of global classes which map into U and $U^\perp$, repsectively (i.e.

$$V_U = \{\xi \in \mathrm{H}^1(k, M) \,|\, \forall v,\, \mathrm{res}_v(\xi) \in U_v\},\ \text{and}$$
$$V_{U^\perp} = \{\eta \in \mathrm{H}^1(k, M^\vee) \,|\, \forall v,\, \mathrm{res}_v(\eta) \in U_v^\perp\}\,).$$

Let T denote any finite set of primes and let $I' = (\mathrm{res}_T\ Ш(V_U, T))^\perp \subset \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$ be the orthogonal complement of $\mathrm{res}_T\ Ш(V_U, T)$ with respect to the pairing $(\ ,\ )_T$. Let I denote the image of I' under the quotient map $q : \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee) \to \prod_{v\in T} \frac{\mathrm{H}^1(k_v, M^\vee)}{U_v^\perp}$.

Proposition 4.6. *The composition*

$$\mathrm{H}^1(k, M^\vee) \xrightarrow{\mathrm{res}_T^\vee} \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee) \xrightarrow{q} \prod_{v\in T} \frac{\mathrm{H}^1(k_v, M^\vee)}{U_v^\perp}$$

maps $\mathrm{H}^1(k, M^\vee)$ *surjectively onto* I*. In particular,* $q \circ \mathrm{res}_T^\vee$ *is surjective if and only if* V_U *is not* T*-singular.*

Our proof of this proposition is based on (the discussion leading up to) [CoN, Theorem 9.2.3]. Theorem 4.1 follows by taking U to be the entire restricted product $\prod' \mathrm{H}^1(k_v, M)$ so that $V_U = \mathrm{H}^1(k, M)$, $U^\perp = 0$ and I is the orthogonal complement of $\mathrm{res}_T(\ Ш(k, M, T))$. We start with a couple lemmas.

Lemma 4.7. *I is a proper subgroup of $\prod_{v\in T} \frac{\mathrm{H}^1(k_v, M^\vee)}{U_v^\perp}$ if and only if V_U is T-singular.*

Proof: Suppose there is some nonzero element $\xi_T \in \mathrm{res}_T\ Ш(V_U, T)$. Since the pairing $(\ ,\ )_T$ is nondegenerate, this will be the case if and only if there exists some $\eta_T \in \prod_{v\in T} \mathrm{H}^1(k_v, M^\vee)$ pairing nontrivially with ξ_T. This means $\eta_T \notin I'$. Since $\prod_{v\in T} U_v^\perp$ pairs trivially with $\mathrm{res}_T\ Ш(V_U, T)$, this is equivalent to requiring that the class of η_T modulo $\prod_{v\in T} U_v^\perp$ does not lie in I. □

Lemma 4.8. *The Pontryagin dual of I is canonically isomorphic to $\frac{\prod_{v\in T} U_v}{\mathrm{res}_T\ Ш(V_U, T)}$.*

Proof: For finite abelian groups $A_1 \subset A_2 \subset A_3$, with character groups A_i^*, let $A_i^\perp$ denote the orthogonal complement of A_i in A_3^* with respect to the natural pairing. One checks that (A_2/A_1) and $A_1^\perp/A_2^\perp$ are canonically identified as duals. The result follows by applying this with

$$A_1 = \mathrm{res}_T\ Ш(V_U, T) \subset A_2 = \prod_{v\in T} U_v \subset A_3 = \prod_{v\in T} \mathrm{H}^1(k_v, M)\,,$$

since by definition, $I = \frac{\left(\mathrm{res}_T\ Ш(V_U, T)\right)^\perp}{\prod_{v\in T} U_v^\perp}$. □

Proof of Proposition 4.6: The discussion leading up to theorem 4.1 shows that the image of $\mathrm{res}_T^\vee$ is contained in the set I'. As I is the image of I' under q, the image of the composition in the proposition is contained in I.

By definition $V_{U^\perp}$ is contained in the kernel of $q \circ \mathrm{res}_T^\vee$. Let $\mathcal{C}$ be the cokernel of $q \circ \mathrm{res}_T^\vee$. Taking Pontryagin duals, we have an exact sequence

$$0 \to \mathcal{C}^* \to I^* \to \Big(\frac{\mathrm{H}^1(k, M^\vee)}{V_{U^\perp}}\Big)^*.$$

Our goal is to show that $\mathcal{C}^*$ is trivial.

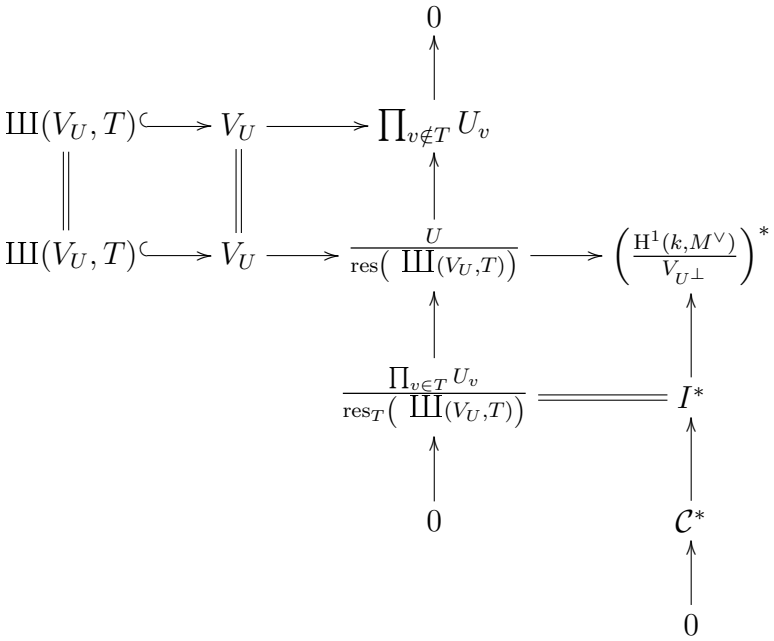
The Poitou-Tate exact sequence (2.3) expresses the fact that an element of U is obtained by restriction of some global class (necessarily in V_U) if and only if it is trivial as an element of $\mathrm{H}^1(k, M^\vee)^*$. Since U pairs trivially with $V_{U^\perp}$ we have an exact sequence

$$V_U \to U \to \Big(\frac{\mathrm{H}^1(k, M^\vee)}{V_{U^\perp}}\Big)^*.$$

This induces an exact sequence

$$V_U \to \frac{U}{\mathrm{res}\,(\,Ш(V_U, T))} \to \Big(\frac{\mathrm{H}^1(k, M^\vee)}{V_{U^\perp}}\Big)^*.$$

Fitting all of this together, we have a commutative and exact diagram



The non-tautological equality here is the identification given by lemma 4.8. It follows by a simple chase in the diagram above that $\mathcal{C}^* \simeq Ш(V_U, T)/\,Ш(V_U, T) = 0$. □

5. Application to abelian varieties

5.1. **Local-global principles for $\mathrm{H}^1(k, A[n])$.** Let A and $A^\vee$ be dual abelian varieties over k and $n \geq 2$. The following theorem summarizes some of the results of [DZ1, DZ3] regarding the strong Hasse principle in the group $\mathrm{H}^1(k, A[n])$. Together with corollary 4.2 this proves theorem 1.5.

Theorem 5.1 (Dvornicich-Zannier)**.** *The strong Hasse principle holds for $\mathrm{H}^1(k, A[n])$ if any one of the following hold.*

(1) A is an elliptic curve and n is prime.
(2) A is an elliptic curve over $\mathbb{Q}$ and $n = p^e$ is any power of a sufficiently large prime (independent of A).
(3) $n = p^e$ is any power of a sufficiently large prime (depending on A and k).

Proof: Parts (1) and (2) are shown in [DZ1] and [DZ3, Theorem 1], respectively. The argument for (3) is given for elliptic curves in [DZ3] (see also [DZ1, Remark 2.6]). It is not particularly difficult to deduce the same for arbitrary abelian varieties. This goes as follows.

Let K/k be the minimal Galois extension over which the Galois action on $A[p^e]$ is trivial. *Suppose* there exists an element $\sigma \in G := \mathrm{Gal}(K/k)$ which acts on $A[p^e]$ as a homothety in $(\mathbb{Z}/p^e\mathbb{Z})^\times \subset \mathrm{Aut}(A[p^e])$ which has no nontrivial fixed points. In other words $\sigma \in G$ lies in the center of G and $P \mapsto \sigma(P) - P$ is an automorphism of $A[p^e]$. It follows from Sah's lemma (see [La, Theorem V.5.1]), that $\mathrm{H}^1_*(G, A[p^e]) \subset \mathrm{H}^1(G, A[p^e]) = 0$. Then, by lemma 3.3, the strong Hasse principle holds for $\mathrm{H}^1(k, A[p^e])$.

The existence of such a σ follows from a result of Serre [Se3] (see also [McQ, Corollary 2.1.7]). There exists a constant $d = d(A, k)$ depending only on A and k, such that, for any n, all d-th powers in $(\mathbb{Z}/n\mathbb{Z})^\times$ arise as homotheties via the action of G_k on $A[n]$. For any prime $p > d + 1$ there exists a nontrivial d-th power in $\mathbb{F}_p^\times$. Hence, there exists an element $\sigma \in G_k$ which acts on $A[p^e]$ as multiplication by some integer $m_\sigma \neq 1 \mod p$. This implies that σ does not fix any nontrivial element of $A[p^e]$. □

5.2. **Weak approximation for abelian varieties.** We apply the results of the previous section to characterize weak approximation in $\mathrm{H}^1(k, A[n])$ and $\mathrm{H}^1(k, A)[n]$. For primes v of k, we make the convention that $\mathrm{H}^0(k_v, A)$ denotes Tate's modified cohomology group; if v is nonarchimedean then $\mathrm{H}^0(k_v, A) = A(k_v)$, if v is archimedean $\mathrm{H}^0(k_v, A)$ is the component group

of $A(k_v)$ (i.e. the quotient of $A(k_v)$ by the connected component containing the identity).

Proposition 5.2. *The map* $\mathrm{H}^1(k, A^\vee[n]) \to \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee[n])$ *is surjective if and only if* $\mathrm{H}^1(k, A[n])$ *is not* T*-singular. The map* $\mathrm{H}^1(k, A^\vee)[n] \to \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n]$ *is surjective if and only if the* n*-Selmer group of* A *is not* T*-singular. In particular, weak approximation holds in* $\mathrm{H}^1(k, A^\vee[n])$ *if and only if* $\mathrm{H}^1(k, A[n])$ *is nonsingular while weak approximation holds in* $\mathrm{H}^1(k_v, A^\vee)[n]$ *if and only if* $\mathrm{Sel}^{(n)}(A/k)$ *is nonsingular.*

Remark 5.3. This implies that weak approximation holds if any of the conditions in theorem 5.1 are met.

Proof: The statements about $\mathrm{H}^1(k, A[n])$ follow from the corollaries to theorem 4.1. The statement for $\mathrm{H}^1(k, A)[n]$ will follow by taking V_U in proposition 4.6 to be the n-Selmer group of A.

For any n, one has a Kummer sequence,

$$\mathrm{H}^0(k_v, A) \xrightarrow{n} \mathrm{H}^0(k_v, A) \xrightarrow{\delta_v} \mathrm{H}^1(k_v, A[n]) \to \mathrm{H}^1(k, A)[n] \to 0\,,$$

and similarly for $A^\vee$. The subgroup $U := \prod \mathrm{Image}(\delta_v) \subset \prod \mathrm{H}^1(k_v, A[n])$ is known to be an open subgroup of the restricted product (the claim is that the image of δ_v is equal to the unramified subgroup at almost all primes). By definition, the subgroup $V_U \subset \mathrm{H}^1(k, A[n])$ of classes restricting into U is the n-Selmer group of A.

Tate's local duality theorems (e.g. [Mi, Corollary 3.4]) show that the orthogonal complement of $\mathrm{Image}(\delta_v)$ is equal to the image of $\mathrm{H}^0(k_v, A^\vee)$ under the connecting homomorphism in the Kummer sequence for the dual abelian variety. So proposition 4.6 implies that the diagonal map in the commuative diagram below is surjective if and only the n-Selmer group of A is not T-singular.

$$\begin{array}{ccccccc}
\mathrm{H}^1(k, A^\vee[n]) & \longrightarrow & \frac{\mathrm{H}^1(k, A^\vee)}{\delta(\mathrm{H}^0(k, A^\vee))} & = & \mathrm{H}^1(k, A^\vee)[n] & \longrightarrow & 0 \\
\downarrow & \searrow & \downarrow & & \downarrow & & \\
\prod_{v\in T} \mathrm{H}^1(k_v, A^\vee[n]) & \longrightarrow & \prod_{v\in T} \frac{\mathrm{H}^1(k_v, A^\vee)}{\delta_v(\mathrm{H}^0(k_v, A^\vee))} & = & \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n] & \longrightarrow & 0
\end{array}$$

Clearly the same is true of the vertical map on the right. This is what we wanted to prove. □

For any n, Tate has defined a bilinear pairing

$$\langle\,,\,\rangle : \mathrm{H}^0(k, A)/n\,\mathrm{H}^0(k, A) \times \mathrm{H}^1(k, A^\vee)[n] \to \mathrm{Br}(k)\,.$$

This pairing is compatible with the pairing

$$(\ ,\ ) : \mathrm{H}^1(k, A[n]) \times \mathrm{H}^1(k, A^\vee[n]) \to \mathrm{Br}(k)$$

via the Kummer sequences of A and $A^\vee$. Namely, for any $P \in \mathrm{H}^0(k, A)/n\,\mathrm{H}^0(k, A)$ and $\eta \in \mathrm{H}^1(k, A^\vee)[n]$, $\langle P, \eta\rangle = (\delta(P), \tilde{\eta})$, where $\delta(P)$ denotes the image of P under the connecting homomorphism and $\tilde{\eta}$ denotes any lift of η to $\mathrm{H}^1(k, A^\vee[n])$. The same is true locally and $\langle\ ,\ \rangle_v$ indentifies $\mathrm{H}^0(k_v, A)/n\,\mathrm{H}^0(k_v, A)$ and $\mathrm{H}^1(k_v, A^\vee)[n]$ as Pontryagin duals.

For any finite set of primes T,

$$\langle\ ,\ \rangle_T := \sum_{v\in T} \mathrm{inv}_v \langle\ ,\ \rangle_v$$

defines a nondegenerate pairing

$$\langle\ ,\ \rangle_T : \prod_{v\in T} \frac{\mathrm{H}^0(k_v, A)}{n\,\mathrm{H}^0(k_v, A)} \times \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n] \to \mathbb{Q}/\mathbb{Z}\,.$$

Since, for any v, $\mathrm{res}_v\left(\mathrm{Sel}^{(n)}(A/k)\right)$ is contained in the image of $\mathrm{H}^0(k_v, A)/n\,\mathrm{H}^0(k_v, A)$ under the connecting homomorphism, this also gives a pairing

$$\langle\ ,\ \rangle_T : \mathrm{Sel}^{(n)}(A/k) \times \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n]) \to \mathbb{Q}/\mathbb{Z}\,.$$

Combining proposition 4.6 with the proof above readily yields the following.

Proposition 5.4. *Let T be a finite set of primes. An element $\eta_T \in \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n]$ is in the image of the restriction map $\mathrm{H}^1(k, A^\vee)[n] \to \prod_{v\in T} \mathrm{H}^1(k_v, A^\vee)[n]$ if and only if*

$$\langle \xi, \eta_T\rangle_T = 0, \text{ for every } \xi \in Ш(\mathrm{Sel}^{(n)}(A/k), T)\,.$$

5.3. **Counter-examples to weak approximation.** Using proposition 5.2 we can give examples where weak approximation fails for $\mathrm{H}^1(k, A[n])$ and $\mathrm{H}^1(k, A)[n]$.

Dvornicich and Zannier [DZ2] have shown that the point $(1561/12^2, 19459/12^3)$ on the curve $E : y^2 = (x + 15)(x - 5)(x - 10)$ is divisible by 4 in $E(\mathbb{Q}_v)$ if and only if $v \neq 2$. This provided one of the first examples of the failure of the strong Hasse principle for n-divisibility on an elliptic curve. Under the connecting homomorphism, the point gives rise to a $\{2\}$-singular class in $\mathrm{Sel}^{(4)}(\mathbb{Q}, E) \subset \mathrm{H}^1(\mathbb{Q}, E[4])$. Weak approximation fails for both $\mathrm{H}^1(\mathbb{Q}, E)[4]$ and 4-coverings of E since, by proposition 5.2, $\mathrm{H}^1(\mathbb{Q}, E)[4] \to \mathrm{H}^1(\mathbb{Q}_2, E)[4]$

cannot be surjective.

Prior to the example above, Cassels and Flynn [CF, p. 61] constructed an abelian surface A over $\mathbb{Q}$ for which the Hasse principle for 2-divisibility fails. We briefly describe their example. Let $C : Y^2 = P(X)Q(X)R(X)$ where P, Q, R are irreducible polynomials of degree 2 with coefficients in $\mathbb{Q}$ and constant term equal to 1, splitting over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(\sqrt{34})$, respectively. The point $a = (0, 1) \in C(\mathbb{Q})$ gives rise to the point $\mathfrak{a} = \{a, a\} \in A(\mathbb{Q})$, where A is the Jacobian of C. It follows from their lemma 6.5.1 that $\mathfrak{a} \notin 2A(\mathbb{Q})$. However, for any $v \leq \infty$, at least one of P, Q, R has a root r_v in $\mathbb{Q}_v$. Then the point $\mathfrak{b} = \{a, (r_v, 0)\} \in A(\mathbb{Q}_v)$ is such that $2\mathfrak{b} = \mathfrak{a}$.

Using the same idea, we can construct an example where weak approximation for $\mathrm{H}^1(\mathbb{Q}, A)[2]$ fails. Let C be the hyperelliptic curve of genus 2 given by

$$y^2 = -(x^2 + 1)(x^2 + 5)(x^2 - 5)\,.$$

We have a point $(0, 5) \in C(\mathbb{Q})$. One can check that this gives a $\mathbb{Q}$-point of infinite order $\mathfrak{a} = \{(0, 5), (0, 5)\}$ on the Jacobian $A = \mathrm{Jac}(C)$. One easily checks that at least one of the quadratic polynomials defining C has a root in $\mathbb{Q}_v$ if and only if $v \neq 2$. So as above we see that $\mathfrak{a}$ is divisible by 2 over $\mathbb{Q}_v$ if and only if $v \neq 2$. So the image of $\mathfrak{a}$ in $\mathrm{Sel}^{(2)}(\mathbb{Q}, A) \subset \mathrm{H}^1(\mathbb{Q}, A[2])$ is $\{2\}$-singular.

The next proposition illustrates how the counterexamples above propagate to higher level.

Proposition 5.5. *Suppose that weak approximation fails for* $\mathrm{H}^1(k, A)[n]$. *Then weak approximation fails for* $\mathrm{H}^1(k, A)[mn]$ *for infinitely many* m.

Proof: We prove the statement for the dual abelian variety. By assumption there is a singular class $\xi \in \mathrm{Sel}^{(n)}(A/k)$. For any positive integer m and any prime v, the map $i : A[n] \to A[mn]$ induces a commutative diagram

$$\begin{array}{ccc} \mathrm{Sel}^{(n)}(A/k) & \xrightarrow{i_*} & \mathrm{Sel}^{(mn)}(A/k) \\ \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} \\ A(k_v)/nA(k_v) & \xrightarrow{m} & A(k_v)/mnA(k_v) \end{array}$$

If $\mathrm{res}_v(\xi) = 0$, then $\mathrm{res}_v(i_*\xi) = 0$. So, since ξ is finitely supported, $i_*(\xi)$ is finitely supported. By assumption there exists v such that $\mathrm{res}_v(\xi) \neq 0$. Choose $Q_v \in A(k_v)$ representing $\mathrm{res}_v(\xi) \in A(k_v)/nA(k_v)$. Then $\mathrm{res}_v(i_*(\xi))$ is represented by mQ_v. Now suppose $\mathrm{res}_v(i_*(\xi)) = 0$. Then there exists some

$P_v \in A(k_v)$ such that $m(Q_v - nP_v) = 0$. Thus $Q_v - nP_v \in A(k_v)[m]$. The torsion subgroup of $A(k_v)$ is finite, so there are infinitely many m for which this cannot happen. For such m we have that $i_*(\xi)$ is singular. The result follows from proposition 5.2. □

Remark 5.6. In a similar fashion, Paladino has shown that a counterexample to the Hasse principle in $A(k)/p^nA(k)$ can lead to counterexamples in $A(k)/p^{n+s}A(k)$ for all $s \geq 0$ [Pa2]. She has also given examples where the Hasse principle fails for divisibility by 9 in elliptic curves over $\mathbb{Q}$ [Pa1]. Similar methods give rise to examples of singular classes and the failure of weak approximation in $\mathrm{H}^1(k, A)[9]$.

5.4. **The conjecture of Lang and Tate.** We now come to the proof of theorem 1.3. Since $\mathrm{H}^1(k, A)$ is torsion, the Bézout identity shows that it will suffice to prove the following theorem.

Theorem 5.7. *For any prime number p, weak approximation holds in $\mathrm{H}^1(k, A)[p^\infty]$.*

Here $\mathrm{H}^1(k, A)[p^\infty]$ denotes the subgroup consisting of elements of p-powered order. Since we will be working only with p-th powers, we use the notation $S^{(n)}(A/k)$ to denote the p^n-Selmer group, $\mathrm{Sel}^{(p^n)}(A/k)$. For any positive integers m and n, multiplication by p^m induces an exact sequence

$$0 \to A[p^m] \xrightarrow{i_*} A[p^{m+n}] \xrightarrow{p^m} A[p^n] \to 0\,,$$

and consequently a map $p^m_* : S^{(m+n)}(A/k) \to S^{(n)}(A/k)$. Let $S(A/k)$ denote the projective limit of the groups $S^{(n)}(A/k)$ with respect to these maps and use $\phi_n : S(A/k) \to S^{(n)}(A/k)$ for the canonical map. One knows that $S(A/k)$ satisfies the strong Hasse principle [Mi, Proposition I.6.22]. Using this we deduce the following.

Lemma 5.8. *For every $n > 0$, there exits m such that the image of any finitely supported class in $S^{(m+n)}(A/k)$ under the map to $S^{(n)}(A/k)$ is trivial.*

Proof: We will show below that, for any nontrivial finitely supported class in $S^{(n)}(A/k)$, there exists some m_0 such that, for any $m \geq m_0$, no lift of ξ to $S^{(m+n)}(A/k)$ is finitely supported. Using this we prove the lemma as follows. Take M_0 to be the maximum of the m_0's as we range over the finitely many nontrivial finitely supported classes in $S^{(n)}(A/k)$ (recall that the n-Selmer group is itself finite). Let $M \geq M_0$ and consider a finitely supported class in $S^{(M+n)}(A/k)$. Its image in $S^{(n)}(A/k)$ cannot be equal to any nontrivial

finitely supported class. On the other hand, its image is finitely supported. It follows that its image must be trivial.

To establish the claim above, let $L_\xi \subset S(A/k)$ be the set of elements which map to ξ in $S^{(n)}(A/k)$. For each $\zeta \in L_\xi$, define $m(\zeta)$ to be the least positive integer such that $\phi_{m(\zeta)+n}(\zeta)$ is not finitely supported. This is well defined since $S(A/k)$ satisfies the strong Hasse principle. Set $m_0 = \sup_{\zeta \in L_\xi} m(\zeta)$. If this supremum is finite the claim follows. So suppose this is not the case. Then we can find a sequence $\{\zeta_i\}_{i=1}^{\infty} \subset L_\xi$ such that, for each i, $\phi_{n+i}(\zeta_i) \in S^{(n+i)}(A/k)$ is finitely supported. Note that $S(A/k)$ is sequentially compact (being a profinite group, it is compact and first countable). So, replacing with a subsequence if necessary, we may assume that the sequence ζ_i converges to some $\zeta \in S(A/k)$. Clearly $\phi_n(\zeta) = \xi \neq 0$. Our claim will be established if we can show that ζ is finitely supported, for this will contradict the strong Hasse principle for $S(A/k)$.

Let S be the finite set of primes consisting of primes of bad reduction for A and primes dividing p. By the criterion of Neron-Ogg-Shafarevich $A[p^e]$ is unramified outside S. Suppose $\mathrm{res}_v(\zeta) \neq 0$ for some $v \notin S$. Then there exists some M such that $\mathrm{res}_v(\phi_{M+n}(\zeta)) \neq 0$. Since ζ is the limit of the ζ_i, we can choose $i > M$ such that $\phi_{M+n}(\zeta_i) = \phi_{M+n}(\zeta)$ in $S^{(M+n)}(A/k)$. Now $i > M$ and $\phi_{i+n}(\zeta_i)$ is finitely supported, so $\phi_{M+n}(\zeta_i)$ must be as well. By corollary 3.5 it follows that $\phi_{M+n}(\zeta) = \phi_{M+n}(\zeta_i)$ is supported on S. This contradiction shows that ζ is supported on S, which is a finite set of primes. This is what we intended to show. □

Proof of Theorem 5.7: We will prove the statement for the dual abelian variety. Let T be any finite set of primes and $\eta_T := (\eta_v)_{v \in T} \in \prod_{v \in T} \mathrm{H}^1(k_v, A^\vee)[p^\infty]$. Let n be a positive integer such that, for all $v \in T$, η_v is killed by p^n. Choose m as in lemma 5.8 and let ξ be any finitely supported class in the p^{m+n}-Selmer group of A. We may consider η_T as an element in $\prod_{v \in T} \mathrm{H}^1(k_v, A^\vee)[p^{n+m}]$. Using proposition 5.4, the theorem will follow if we can show that η_T is orthogonal to ξ with respect to the pairing

$$\langle\ ,\ \rangle_T : S^{(n+m)}(A/k) \times \prod_{v \in T} \mathrm{H}^1(k_v, A^\vee)[p^{n+m}] \to \mathbb{Q}/\mathbb{Z}\,.$$

We have the commutative diagram

$$\begin{array}{ccc} S^{(m+n)}(A/k) & \longrightarrow & S^{(n)}(A/k) \\ \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v \\ \prod_{v \in T} \frac{\mathrm{H}^0(k_v, A)}{p^{m+n}\,\mathrm{H}^0(k_v, A)} & \longrightarrow & \prod_{v \in T} \frac{\mathrm{H}^0(k_v, A)}{p^{n}\,\mathrm{H}^0(k_v, A)} \end{array}$$

By assumption, the image of ξ in the upper-right hand corner is trivial, so this is also true of its image in the lower-right corner. From commutativity it follows that there exists some $P_T \in \prod_{v\in T} \mathrm{H}^0(k_v, A)$ such that $\mathrm{res}_T(\xi) \equiv p^n P_T \mod \prod_{v\in T} p^{m+n}\,\mathrm{H}^0(k_v, A)$. The pairing $\langle\ ,\ \rangle_T$ is bilinear, so

$$\langle \xi, \eta_T\rangle_T = \langle p^n P_T, \eta_T\rangle_T = \langle P_T, p^n\eta_T\rangle_T = \langle P_T, 0\rangle_T = 0\,.$$

This is what we wanted to show. □

Remark 5.9. Corollary 3.5 shows that any finitely supported class in $\mathrm{H}^1(k, A[n])$ is unramified outside the set of primes of bad reduction and the primes above n. It follows that there can only be finitely many singular classes. The strong Hasse principle is also valid for the projective limit of the groups $\mathrm{H}^1(k, A[n])$. The proof of 5.8 carries over for $\mathrm{H}^1(k, A[n])$ in place of $\mathrm{Sel}^{(n)}(A/k)$. A similar argument to that in the proof above then shows that weak approximation holds for the direct limit of the groups $\mathrm{H}^1(k, A[n])$ with respect to the maps induced by the obvious inclusion $A[n] \to A[mn]$.

Aknowledgements. I would like to thank Michael Stoll for comments on a preliminary version of this paper and would like to appologize to Roberto Dvornicich and Umberto Zannier for having failed to properly attribute their results in an earlier draft of this paper.

References

[CF] J.W.S Cassels and V. Flynn: Prolegomena to a middlebrow arithmetic of curves of genus 2, *London Mathematical Society Lecture Note Series* **230**, Cambridge University Press, 1996.

[Cr] B. Creutz: Potential Ш for abelian varieties, *J. Number Theory*, **131** (2011) 2162-2174.

[DZ1] R. Dvornicich and U. Zannier: Local-global divisibility of rational points in some commutative algebraic groups, *Bull. Soc. Math. France* **129** (2001) 317-338.

[DZ2] — An analogue for elliptic curves of the Grunwald-Wang example, *C. R. Acad. Sci. Paris* **I 338** (2004) 47-50.

[DZ3] — On a local-global prinicple for the divisibility of a rational point by a positive integer, *Bull. London Math. Soc.* **39** (2007) 27-34.

[La] S. Lang: Elliptic curves: Diophantine analysis, *Springer-Verlag*, Berlin and New York, 1978.

[LT] S. Lang and J. Tate: Principal homogeneous spaces over abelian varieties, *Amer. Journal of Math.* **80** (1958) 659-684.

[McQ] M. McQuillen: Division points on semi-abelian varieties, *Invent. Math.* **120** (1995) 143-159.

[Mi] J.S. Milne: Arithmetic duality theorems. *Perspectives in Mathematics* **1**, Academic Press, Boston, 1986.

[CoN] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of number fields (second edition). *Grundlehren der math. Wissenschaften* **323**, Springer-Verlag, Berlin, 2000.

[Pa1] L. Paladino: Elliptic curves with $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9, *Jour. de Théorie des Nombres de Bordeaux*, **22** (2010) 139-160.

[Pa2] — On counterexamples to local-global divisibility in commutative algebraic groups, *Acta Arithmetica*, **148** (2011) 21-29.

[Se1] J.P. Serre: Sur les groupes de congruence des variétés abéliennes, *I. Izv. Akad. Nauk SSSR, Ser. Mat.*, **28** (1964) 3-20; ibid., **35** (1971) 731-737.

[Se3] — Quelques propriétes des groupes algébriques commutatifs, Appendix in Astérisque **69-70** (1979) 191-202.

[Se4] — Galois cohomology, *Springer Monographs in Mathematics*, Springer-Verlag, 2002.

[Si] J.H. Silverman: The arithmetic of elliptic curves. *Graduate Texts in Mathematics* **106**, Springer-Verlag, 1986.

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

E-mail address: brendan.creutz@sydney.edu.au