E. Gazaki and I. Leal (2022) "Zero Cycles on a Product of Elliptic Curves Over a p-adic Field,"
International Mathematics Research Notices, Vol. 2022, No. 14, pp. 10586–10625
Advance Access Publication March 27, 2021
https://doi.org/10.1093/imrn/rnab020

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Zero Cycles on a Product of Elliptic Curves Over a p-adic Field

Evangelia Gazaki[1,*] and Isabel Leal[2]

[1]Department of Mathematics, University of Virginia, Kerchof Hall, 141 Cabell Drive, Charlottesville, VA 22904, USA and [2]Courant Institute of Mathematical Sciences, New York University, New York City, NY 10012, USA

*Correspondence to be sent to: e-mail: eg4va@virginia.edu

We consider a product $X = E_1 \times \cdots \times E_d$ of elliptic curves over a finite extension K of $\mathbb{Q}_p$ with a combination of good or split multiplicative reduction. We assume that at most one of the elliptic curves has supersingular reduction. Under these assumptions, we prove that the Albanese kernel of X is the direct sum of a finite group and a divisible group, extending work by Raskind and Spiess to cases that include supersingular phenomena. Our method involves studying the kernel of the cycle map $CH_0(X)/p^n \to H^{2d}_{\text{ét}}(X, \mu_{p^n}^{\otimes d})$. We give specific criteria that guarantee this map is injective for every $n \geq 1$. When all curves have good ordinary reduction, we show that it suffices to extend to a specific finite extension L of K for these criteria to be satisfied. This extends previous work by Yamazaki and Hiranouchi.

1 Introduction

Let X be a smooth, projective, and geometrically integral variety over a field K having a K-rational point. We consider the group $CH_0(X)$ of zero cycles on X modulo rational equivalence and let $A_0(X)$ be the subgroup of zero cycles of degree zero. There is an abelian variety, Alb_X, called the *Albanese variety* of X, universal for maps from X to abelian varieties, and an induced homomorphism,

$$A_0(X) \to \text{Alb}_X(K),$$

Received February 15, 2018; Revised December 18, 2020; Accepted January 22, 2021

© The Author(s) 2021. Published by Oxford University Press. All rights reserved. For permissions, please e-mail: journals.permission@oup.com.

called the *Albanese map* of X. When X is a curve, the group $A_0(X)$ coincides with $\mathrm{Pic}^0(X)$ and the Abel–Jacobi theorem tells us that the above map is an isomorphism. In higher dimensions, however, the situation is far more mysterious and the Albanese map can have a very significant kernel, which we denote by $T(X)$.

When K is an algebraic number field, the fascinating Bloch–Beilinson conjectures predict that the Albanese kernel $T(X)$ is a torsion group. At the same time, the group $CH_0(X)$ is expected to be a finitely generated abelian group, so $T(X)$ must be finite. On the other hand, the Albanese kernel is expected to be enormous for varieties with positive geometric genus over large fields like $\mathbb{C}$ or $\mathbb{Q}_p$.

In this work, the case of interest to us is that of a p-adic base field K. In this case, the expected structure of $T(X)$ is given by the following conjecture.

Conjecture 1.1. Let X be a smooth projective and geometrically integral variety over a finite extension of $\mathbb{Q}_p$. The Albanese kernel $T(X)$ is the direct sum of a finite group and a divisible group.

A 1st version of this conjecture was formulated by Colliot-Thélène ([4]), and a later one by Raskind and Spiess ([18]). In fact, Raskind and Spiess established the conjecture for a product $X = C_1 \times \cdots \times C_d$ of smooth projective curves all of whose Jacobians have a mixture of split multiplicative and good ordinary reduction.

More recently, S. Saito and K. Sato ([20]) proved a weaker form of this conjecture. Namely, if k is the residue field of the p-adic field K, they established that, when X has a regular projective flat model $\mathcal{X}$ over the ring of integers, $\mathcal{O}_K$, on which the reduced subscheme of the divisor $\mathcal{X} \otimes_{\mathcal{O}_K} k$ has simple normal crossings, the group $A_0(X)$ is the direct sum of a finite group and a group that is m-divisible for every integer m coprime to the residue characteristic. The result has since been extended ([4]) to every smooth projective variety X over a p-adic field. Conjecture 1.1 is still very open though and we do not have any general method to prove that the quotients $T(X)/p^n$ are "small."

In this paper we focus on the case of a product $X = E_1 \times \cdots \times E_d$ of elliptic curves over a p-adic field K. Following the method introduced by Raskind and Spiess in [18], we manage to extend their result to include also supersingular reduction phenomena. Our 1st result is a proof of Conjecture 1.1 in the following case.

Theorem 1.2. Let $E_1, \cdots, E_d$ be elliptic curves over a p-adic field K with either good or split multiplicative reduction. We assume that at most one of the curves has supersingular reduction. Then the Albanese kernel, $T(X)$, of the product $X = E_1 \times \cdots \times E_d$ is the direct sum of a finite group and a divisible group.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

1.1 The cycle map

An essential tool for the study of zero cycles on varieties defined over arithmetic fields is the study of the cycle map to étale cohomology,

$$CH_0(X)/n \xrightarrow{c_n} H^{2d}_{ét}(X, \mu_n^{\otimes d}),$$

where $d = \dim(X)$. The map c_n is in general neither injective nor surjective. When X is a smooth surface over a p-adic field and n is coprime to p, Esnault and Wittenberg ([6]) give some far reaching computations of the kernel. However, when n is a power of p, still very little is known.

Our primary goal in this paper is to describe as much as possible the kernel of the cycle map c_{p^n} in the context of Theorem 1.2 and for every $n \geq 1$. Unlike Theorem 1.2 that was already known when all the curves have good ordinary or split multiplicative reduction, the injectivity of c_{p^n} was previously known only in very limited cases. Under the assumptions of Theorem 1.2, it has been established by Raskind and Spiess ([18]) and Hiranouchi ([8]) that the map c_{p^n} is injective under the additional assumption that $E_i[p^n] \subset E_i(K)$ for every $i \in \{1, \cdots, d\}$. The only result independent of $n \geq 1$ is due to Yamazaki ([29]), who proved injectivity of c_n for every $n \geq 1$, for a product $X = C_1 \times \cdots \times C_d$ of Mumford curves, that is, higher genus analogues of Tate curves.

In this article we focus on removing the strong K-rationality assumption, $E_i[p^n] \subset E_i(K)$, and pass to the limit for p^n. For a product $X = E_1 \times E_2$ of two elliptic curves not both having supersingular reduction, we give sufficient criteria for the injectivity of c_{p^n}, for every $n \geq 1$. These criteria depend heavily on the reduction type of E_1, E_2 (Theorem 3.14, Proposition 3.21, Proposition 3.25) and when they are satisfied, they give us very sharp results. Namely, Theorem 1.2 gives us a decomposition, $T(X) \simeq D \oplus F$, where D is a divisible group and F a finite group. Our method often allows us to fully compute the finite group F, which to our knowledge is the 1st result in this direction.

Example 1.3. Let $X = E \times E$ be the self-product of an elliptic curve over K with good ordinary reduction. Under some mild assumptions, the cycle map c_{p^n} is injective for every $n \geq 1$ and we have an isomorphism, $T(X) \simeq D \oplus \mathbb{Z}/p^n$, if $E[p^n] \subset E(K)$ for some $n \geq 1$ and n is the largest with this property. If $n = 0$, the Albanese kernel $T(X)$ is divisible.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

When the criteria for injectivity are not satisfied, we show that an obstruction to injectivity is very possible to exist (Proposition 3.15, Proposition 3.22). However, when all the curves have good ordinary reduction, we show that the obstruction goes away after extending to a tower of finite extensions of K. Namely, we prove the following theorem.

Theorem 1.4. Let $E_1, \cdots, E_d$ be elliptic curves over K with good ordinary reduction. Let $X = E_1 \times \cdots \times E_d$. Then there exists a finite extension L of K such that the cycle map

$$CH_0(X \times_K L)/p^n \xrightarrow{c_{p^n}} H^{2d}_{\acute{e}t}(X \otimes_K L, \mu_{p^n}^{\otimes d}),$$

is injective for every $n \geq 1$.

1.2 A corollary over global fields

One special case when we get sharp results is when the elliptic curves have complex multiplication by an imaginary quadratic field. In this case we get the following global-to-local corollary for a product X of elliptic curves defined over an algebraic number field.

Corollary 1.5. Let $X = E \times E$ be the self-product of an elliptic curve over an algebraic number field K. Assume that E has complex multiplication by an imaginary quadratic field M. Let $X_v = X \otimes_K K_v$ be the base change to a completion of K at a finite place v. Then the Albanese kernel, $T(X_v)$, is divisible for almost all ordinary reduction places v of K.

1.3 Outline of our method

In this paper we use a method introduced by Raskind and Spiess in [18] and continued by more authors ([29], [17], [9], [8]).

Relation to the Somekawa K-group

Raskind and Spiess reduced the study of the Albanese kernel $T(X)$ on a product of curves to the study of the Somekawa K-group $K(K; A_1, \cdots, A_r)$ attached to abelian varieties $A_1, \cdots, A_r$ over K. This group is a generalization of the Milnor K-group, $K^M_r(K)$ of the field K. It is a quotient of the group

$$\bigoplus_{L/K \text{ finite}} A_1(L) \otimes \cdots \otimes A_r(L)$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

first by a relation similar to the *projection formula* of $CH_i(X)$ and then by a 2nd relation coming from function fields of curves, known as *Weil reciprocity*.

The big advantage of this method is that the group $K(K; A_1, \cdots, A_r)$ has specific generators and relations. More importantly, when working over a p-adic field K, the projection formula is easy to use and in most cases it gives already enough relations that guarantee that the quotients $T(X)/p^n$ are small.

The Galois symbol

Similarly to the case of the Milnor K-groups, for an integer $n \geq 1$ invertible in K, there is a map to Galois cohomology, known as *the generalized Galois symbol*,

$$K(K; A_1, \cdots, A_r)/n \xrightarrow{s_n} H^r(K, A_1[n] \otimes \cdots \otimes A_r[n]).$$

This map is constructed similarly to the Galois symbol of the Bloch–Kato conjecture, and it is conjectured by Somekawa ([25]) to always be injective. Nonetheless, a counterexample has been found in [26], not for abelian coordinates but for the group $K(K; T, T)$ attached to two copies of a certain non-split torus over a 2-dimensional local field K.

Coming to the question of injectivity of the cycle map c_{p^n} for products of curves over p-adic fields all having a K-rational point, this question has been reduced by Yamazaki to verifying the Somekawa conjecture for abelian varieties.

For elliptic curves $E_1, \cdots, E_r$ over a p-adic field K satisfying the assumptions of Theorem 1.4, the conjecture has been established ([18], [8]) under the assumption that $E_i[p^n] \subset E_i(K)$, for $i = 1, \cdots, r$. This is the assumption we would like to remove. When $E_i[p] \subset E_i(K)$ for every $i = 1, \cdots, d$, we introduce a new method to pass to the limit for p^n. Roughly speaking, our method is based on the following principle. "When $E_i[p] \subset E_i(K)$, the K-group $K(K; E_1, E_2)/p$ is generated by p^N torsion points for sufficiently large $N \geq 1$." When this is not achieved over K, we construct a tower, $K \subset L_1 \subset \cdots \subset L_r$ of finite extensions so that this condition is achieved in the tower. When the curve E_i has either good ordinary or split multiplicative reduction, we even manage to remove the assumption $E_i[p] \subset E_i(K)$ by using the theory of p-adic uniformization of elliptic curves.

We note that in all our computations we use a group larger than $K(K; E_1, \cdots, E_r)$. Namely, in the definition of the Somekawa K-group we forget the relations coming from function fields of curves. For this larger group, we show that most of our conditions become necessary for injectivity. This, however, does not disprove the Somekawa conjecture.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Some corollaries

As a byproduct of our proofs, we obtain some important corollaries. First, in the context of Theorem 1.2, we get a decomposition $T(X) \simeq F \oplus D$, with the finite group F generated by K-rational points. We hope that this corollary could have potential applications over global fields.

Moreover, using computations of Yamazaki ([29]), we obtain a corollary about the Brauer–Manin pairing, $CH_0(X) \times Br(X) \to \mathbb{Q}/\mathbb{Z}$, where by $Br(X)$ we denote the Brauer group of X (Corollary 3.29).

We wish our methods could be used to establish Theorem 1.2 for any product of elliptic curves. Unfortunately, there is a very serious obstruction for a product $E_1 \times E_2$ of two curves with supersingular reduction. Namely, in this case, the easy projection formula of the Albanese kernel does not seem to give us enough relations that guarantee the quotient $T(E_1 \times E_2)/p$ is finite.

Notation

Unless otherwise specified, all cohomology groups considered in this paper will be over the étale site. In particular, for a field K, we will denote by $H^i(K, -)$ the Galois cohomology groups of K. Moreover, we will denote the separable closure of a field F by $\overline{F}$.

If L/K is an extension of fields and X is a variety over K, we will denote the base change $X \otimes_K L$ by X_L.

2 Mackey Functors and Somekawa K-Groups

In this section we review the definition of the Somekawa K-group $K(K; A_1, \cdots, A_r)$ for abelian varieties $A_1, \cdots, A_r$ over a perfect field K. We start by reviewing the definition of a Mackey functor.

Let K be a perfect field. A Mackey functor $\mathcal{F}$ over K is a presheaf on the category of étale K-schemes having the following additional property. For every finite morphism $X \xrightarrow{f} Y$ of étale K-schemes, in addition to the restriction map $\mathcal{F}(Y) \xrightarrow{f^\star} \mathcal{F}(X)$, there is also a push-forward map, $\mathcal{F}(X) \xrightarrow{f_\star} \mathcal{F}(Y)$. The maps $f^\star$ and $f_\star$ satisfy certain functoriality conditions, for example, for a composition $X \xrightarrow{f} Y \xrightarrow{g} Z$, we have an equality, $(f \circ g)_\star = f_\star \circ g_\star$. Moreover, there is a decomposition $\mathcal{F}(X_1 \sqcup X_2) = \mathcal{F}(X_1) \oplus \mathcal{F}(X_2)$. Therefore, $\mathcal{F}$ is fully determined by its value $\mathcal{F}(L) := \mathcal{F}(\mathrm{Spec} L)$ at every finite extension L over K. For a more detailed discussion on the properties of Mackey functors we refer to [18, page 13, 14].

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Notation

From now, if $K \overset{f}{\hookrightarrow} L$ is a finite extension of perfect fields, we will denote the restriction map by $\mathrm{res}_{L/K} : \mathcal{F}(K) \to \mathcal{F}(L)$ and the push-forward map by $N_{L/K} : \mathcal{F}(L) \to \mathcal{F}(K)$ and call it *the norm*.

Example 2.1. Let A be an abelian variety over K. Then A induces a Mackey functor by assigning to a finite extension L/K, $A(L) := \mathrm{Hom}(\mathrm{Spec}L, A)$. For a finite extension F/L, the push-forward is the norm map on abelian varieties, $N_{F/L} : A(F) \to A(L)$.

Kahn proved in [11] that the category MF_K of Mackey functors on $(\mathrm{Spec}K)_{\text{ét}}$ is an *abelian category with a tensor product* $\otimes^M$. For abelian varieties $A_1, \cdots, A_r$ over K, we review the definition of $A_1 \otimes^M \cdots \otimes^M A_r$ below. The definition is in fact very similar for general Mackey functors $\mathcal{F}_1, \cdots, \mathcal{F}_r$, but here we only need the abelian variety case.

Definition 2.2. Let $A_1, \cdots, A_r$ be abelian varieties over a perfect field K. The Mackey product $A_1 \otimes^M \cdots \otimes^M A_r$ is defined at a finite extension L over K as follows:

$$(A_1 \otimes^M \cdots \otimes^M A_r)(L) := \left(\bigoplus_{F/L \text{ finite}} A_1(F) \otimes \cdots \otimes A_r(F) \right) / R_1.$$

Here R_1 is the subgroup generated by elements of the form

$$a_1 \otimes \cdots \otimes N_{F'/F}(a_i) \otimes \cdots \otimes a_r - \mathrm{res}_{F'/F}(a_1) \otimes \cdots \otimes a_i \otimes \cdots \otimes \mathrm{res}_{F'/F}(a_r),$$

where $F' \supset F \supset L$ is a tower of finite extensions of K, $a_i \in A_i(F')$ for some $i \in \{1, \cdots, r\}$, and $a_j \in A_j(F)$ for every $j \neq i$.

Notation 2.3. From now on we will be using the standard symbol notation for the generators of $(A_1 \otimes^M \cdots \otimes^M A_r)(L)$, namely $\{a_1, \cdots, a_r\}_{F/L}$ for $a_i \in A_i(F)$.

Norm and restriction

Since $A_1 \otimes^M \cdots \otimes^M A_r$ is a Mackey functor, there are norm and restriction maps corresponding to any finite extension L/K. Namely,

$$\mathrm{res}_{L/K} : (A_1 \otimes^M \cdots \otimes^M A_r)(K) \to (A_1 \otimes^M \cdots \otimes^M A_r)(L),$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

and

$$N_{L/K} : (A_1 \otimes^M \cdots \otimes^M A_r)(L) \to (A_1 \otimes^M \cdots \otimes^M A_r)(K).$$

Moreover, we have the relation $N_{L/K} \circ \mathrm{res}_{L/K} = [L : K]$.

Remark 2.4. We note that the symbol $\{a_1, \cdots, a_r\}_{F/L} \in (A_1 \otimes^M \cdots \otimes^M A_r)(L)$ is nothing but $N_{F/L}(\{a_1, \cdots, a_r\}_{F/F})$. The defining relation R_1 is classically referred to as *projection formula*. We rewrite it using the symbolic notation:

$$\{a_1, \cdots, N_{F/L}(a_i), \cdots, a_r\}_{L/L} = N_{F/L}(\{\mathrm{res}_{F/L}(a_1), \cdots, a_i, \cdots, \mathrm{res}_{F/L}(a_r)\}_{F/F}). \tag{2.5}$$

2.1 The Somekawa K-group

We are now ready to review the definition of the K-group $K(K; A_1, \cdots, A_r)$ attached to abelian varieties over a perfect field K.

Definition 2.6. The Somekawa K-group $K(K; A_1, \cdots, A_r)$ is defined as

$$K(K; A_1, \cdots, A_r) = (A_1 \otimes^M \cdots \otimes^M A_r)(K)/R_2,$$

where the subgroup R_2 is generated by the following family of elements. Let C be a smooth complete curve over K endowed with morphisms $g_i : C \to A_i$ for $i = 1, \cdots, r$. Then for every function $f \in k(C)^\times$ we require

$$\sum_{x \in C} \mathrm{ord}_x(f)\{g_1(x), \cdots, g_r(x)\}_{\kappa(x)/K} \in R_2.$$

The above definition was given by Somekawa ([25]), following a suggestion of K. Kato. Somekawa defined more generally a K-group $K(K; G_1, \cdots, G_r)$ attached to semi-abelian varieties over a field K, that in the special case when $G_i = \mathbb{G}_m$ for every i, it turns out to be isomorphic to the Milnor K-group, $K_r^M(K)$. Recently this definition has been generalized to include more general coordinates. We refer to [10] and [12] for more details.

Remark 2.7. In most of this paper we will be using the Mackey product $(A_1 \otimes^M \cdots \otimes^M A_r)(K)$ for our calculations. From now on we will use the same symbolic notation,

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

$\{a_1, \cdots, a_r\}_{L/K}$, for the generators of both the Mackey product and the Somekawa K-group. To avoid confusion, we will always clarify which group we are using.

Galois symbol

Let $A_1, \cdots, A_r$ be abelian varieties over a perfect field K and n be an integer invertible in K. The Kummer maps, $A_i(L)/n \hookrightarrow H^1(L, A_i[n])$, together with the cup product and the norm map of Galois cohomology (i.e., the corestriction map) induce a generalized Galois symbol,

$$s_n : K(K; A_1, \cdots, A_r)/n \to H^r(K, A_1[n] \otimes \cdots \otimes A_r[n]).$$

Conjecture 2.8. ([25]) The generalized Galois symbol s_n is always injective.

This conjecture is the analogue of the Bloch–Kato conjecture for the Somekawa K-groups. It is still very open in general and as already mentioned in the introduction, a counterexample has been found ([26]) for non-abelian coordinates.

2.2 Relation to zero cycles

For a product $X = E_1 \times \cdots \times E_d$ of elliptic curves over a field K, Raskind and Spiess ([18, Corollary 2.4.1]) constructed a finite decreasing filtration $F^0 \supset F^1 \supset \cdots \supset F^N \supset 0$ of $CH_0(X)$ such that the successive quotients F^i/F^{i+1} are isomorphic to Somekawa K-groups of the form $K(K; E_{i_1}, \cdots, E_{i_r})$, for $1 \leq i_1 < \cdots < i_r \leq d$. More precisely, they proved an isomorphism (We note that the construction of Raskind and Spiess was a lot more general, for a product of smooth complete and geometrically connected curves all having a K-rational point, and the filtration was constructed using the Somekawa K-groups attached to their Jacobian varieties.)

$$CH_0(X) \simeq \mathbb{Z} \oplus \bigoplus_{1 \leq \nu \leq d} \bigoplus_{1 \leq i_1 < \cdots < i_\nu \leq d} K(K; E_{i_1}, \ldots, E_{i_\nu}).$$

Additionally, the subgroups F^1 and F^2 coincide with $A_0(X)$ and $T(X)$, respectively, ([18, Remark 2.4.2 (b)], [29, Example 2.2]).

Yamazaki then showed ([29, Proposition 2.4]) that in the above set-up, the injectivity of the cycle map

$$CH_0(X)/n \xrightarrow{c_n} H^{2d}_{\acute{e}t}(X, \mu_n^{\otimes d})$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

can be reduced to verifying the Somekawa conjecture for all the Galois symbols

$$K(E_{i_1}, \cdots, E_{i_r})/n \xrightarrow{s_n} H^{2r}(K; E_{i_1}[n] \otimes \cdots \otimes E_{i_r}[n]).$$

2.3 Injectivity in the p-adic case

From now on we focus on the case of a p-adic field K. In fact we make the following convention.

Convention 2.9. From now on, unless specified otherwise, we assume that K is a p-adic field with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{m}_K$, and residue field k. Moreover, we assume that all the elliptic curves considered in this paper have *split semistable reduction*.

We give an overview of the status of Conjecture 2.8.

When n is coprime to p

In this case the problem is easier to handle. When at least two of the abelian varieties $A_1, \cdots, A_r$ have good reduction, the injectivity of s_n follows from the following stronger result.

Theorem 2.10. (Raskind and Spiess [18, Theorem 3.5]) If n is coprime to p and at least two of the abelian varieties $A_1, \cdots, A_r$ have good reduction, the group $K(K; A_1, \cdots, A_r)$ is n-divisible. In particular the Galois symbol vanishes, $s_n = 0$.

When n is a power of p

Proving injectivity of s_{p^n} for $n \geq 1$ over a p-adic field K is a mixed characteristic problem of great difficulty. Raskind and Spiess described a general method that could be used to establish injectivity, under the additional assumption that $\mu_{p^n} \subset K$ and $A_i[p^n] \subset A_i(K)$, for $i = 1, \cdots, r$. We briefly review this method only for two elliptic curves E_1, E_2 over K, to keep the notation simple.

The main idea is to relate the generalized Galois symbol s_{p^n} to the classical Galois symbol of the Bloch–Kato conjecture,

$$K_2^M(K)/p^n \xrightarrow{g_{p^n}} H^2(K, \mu_{p^n}^{\otimes 2}).$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

When $\mu_{p^n} \subset K$, the latter has a concrete description in terms of central simple algebras. Moreover, for a symbol $\{x, y\}$ the following equivalence is known.
tcbcol@upper

$$g_{p^n}(\{x,y\}) = 0 \Leftrightarrow \ x \in N_{K(\sqrt[p^n]{y})/K}(K(\sqrt[p^n]{y})^\times) \Leftrightarrow \ y \in N_{K(\sqrt[p^n]{x})/K}(K(\sqrt[p^n]{x})^\times).$$

The steps of the method are as follows:

- Because of the K-rationality assumption, we can fix an isomorphism $E_i[p^n] \simeq (\mu_{p^n})^{\oplus 2}$, for $i = 1, 2$. This in turn gives us isomorphisms

$$H^2(K, E_1[p^n] \otimes E_2[p^n]) \simeq \bigoplus^4 H^2(K, \mu_{p^n}) \simeq \bigoplus^4 Br(K)[p^n] \simeq \bigoplus^4 \mathbb{Z}/p^n.$$

- The next step is to describe realizations of the Mackey functors E_1/p^n and E_2/p^n as subfunctors of $\mathbb{G}_m/p^n$. If such realizations exist and are compatible with the Kummer map, $E_i(L)/p^n \hookrightarrow H^1(L, E_i[p^n])$, for every finite extension L of K, then this description can be used in order to compute the image of

$$(E_1/p^n \otimes^M E_2/p^n)(K) \xrightarrow{s_{p^n}} H^2(K, E_1[p^n] \otimes E_2[p^n]),$$

  using known facts about the classical Galois symbol.
- After computing the image, one could try to show an isomorphism,

$$\begin{array}{ccc} (E_1/p^n \otimes^M E_2/p^n)(K) & \xrightarrow{\simeq} & \mathrm{Im}(s_{p^n}) \\ \downarrow & \nearrow_{s_{p^n}} & \\ K(K; E_1, E_2)/p^n. & & \end{array}$$

  This would imply that the projection $(E_1/p^n \otimes^M E_2/p^n)(K) \twoheadrightarrow K(K; E_1, E_2)/p^n$ is an equality and in particular the diagonal s_{p^n} is an isomorphism as well.

Following the above method, Raskind and Spiess established injectivity of s_{p^n} for abelian varieties with a mixture of good ordinary and split multiplicative reduction under the above K-rationality assumption. Their work has since been generalized by Yamazaki ([29]) who managed to remove the assumption but only for abelian varieties with split multiplicative reduction. More recently Hiranouchi ([8]) extended the original computation to include also supersingular reduction elliptic curves. We will review his

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

result in the next section. See also [17] for an alternative proof for the self-product $E \times E$ of an ordinary reduction elliptic curve.

Remark 2.11. We note that for elliptic curves $E_1, \cdots, E_r$ over the p-adic field K with $r \geq 3$, proving Conjecture 2.8 amounts to showing the K-group $K(K; E_1, \cdots, E_r)$ is divisible. As we will see later in the paper Corollary 3.28, this usually follows as an easy corollary after proving the conjecture for the product of two elliptic curves.

Remark 2.12. Raskind and Spiess imagined that the Mackey functor relation should be enough to establish injectivity when working with abelian varieties over p-adic fields, while the function field relation of $K(K; A_1, \cdots, A_r)$ is expected to be crucial for varieties over number fields. We will show in the forthcoming sections, however, that without the K-rationality assumption, injectivity is not always guaranteed by the Mackey functor relations, even over p-adic fields.

2.4 Decomposing the Mackey functor E/p for an elliptic curve E

Let E be an elliptic curve over K such that $E[p] \subset E(K)$. In this subsection we review the aforementioned realization of the Mackey functor E/p as a subfunctor of $\mathbb{G}_m/p$. We first need some information about the filtration of $K^\times$ arising from the groups of units, $\mathcal{O}_K^\times \supset U_K^1 \supset U_K^2 \supset \cdots$, where $U_K^i = 1 + \mathfrak{m}_K^i$.

The unit groups as Mackey functors

We assume $\mu_p \subset K$. We define the following filtration of the group $K^\times/p := K^\times/(K^\times)^p$. For $i \geq 0$,

$$\overline{U}_K^i := \mathrm{Im}(U_K^i \to K^\times/p).$$

Note that the assumption $\mu_p \subset K$ implies that $p-1$ divides the absolute ramification index e_K. We denote $e_0(K) := \frac{e_K}{p-1}$. The graded quotients $\overline{U}_K^i/\overline{U}_K^{i+1}$ are known to satisfy the following.

Lemma 2.13. ([15, Lemma 2.1.4]) Assume $\mu_p \subset K$.

(a) If $0 \leq i < pe_0(K)$ and i is coprime to p, then $\overline{U}_K^i/\overline{U}_K^{i+1} \simeq k$.
(b) If $0 \leq i < pe_0(K)$ and i is divisible by p, then $\overline{U}_K^i/\overline{U}_K^{i+1} \simeq 1$.
(c) If $i = pe_0(K)$, then $\overline{U}_K^i/\overline{U}_K^{i+1} \simeq \mathbb{Z}/p$.
(d) If $i > pe_0(K)$, then $\overline{U}_K^i = 1$.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Definition 2.14. For every $i \geq 0$, we define a Mackey functor, $\overline{U}^i$ as follows. If L is a finite extension of K, then

$$\overline{U}^i(L) := \overline{U}_L^{ie(L/K)}.$$

For a finite extension F/L, the norm $N_{F/L}$ and restriction maps $\mathrm{res}_{F/L}$ are induced by the norm and restriction on $\mathbb{G}_m$.

Theorem 2.15. ([15], [27]) Let E be an elliptic curve over K with split semistable reduction such that $E[p] \subset E(K)$. The Mackey funtor E/p is calculated as follows:

$$E/p = \begin{cases} \mathbb{G} : m/p, & \text{if E is a Tate curve} \\ \overline{U}^0 \oplus \overline{U}^{pe_0(K)}, & \text{if E has ordinary reduction} \\ \overline{U}^{pt} \oplus \overline{U}^{p(e_0(K)-t)}, & \text{if E has supersingular reduction.} \end{cases}$$

For the case of a supersingular reduction elliptic curve, there is an invariant t that appears in the above decomposition. This invariant is defined as follows.

Definition 2.16. For an elliptic curve E over K with supersingular reduction such that $E[p] \subset E(K)$, the invariant t is defined to be

$$t := \max\{i \geq 0 : P \in \hat{E}(\mathfrak{m}_K^i), \text{ for every } P \in E[p]\}.$$

The fact that E has supersingular reduction yields that $t \geq 1$. Moreover, $t < pe_0(K)$. This is because for every $j \geq pe_0(K)$ the group $\hat{E}(\mathfrak{m}_K^j)$ is known to be torsion free ([23]).

Remark 2.17. We note that the decomposition given in Theorem 2.15 is constructed using the image of the Kummer map, $E(L)/p \hookrightarrow H^1(L, E[p])$, for L a finite extension of K. In fact, the assumption $E[p] \subset E(L)$ for every such extension L gives an isomorphism between $H^1(L, E[p])$ and $L^\times/p \oplus L^\times/p$, so via the Kummer map we may view $E(L)/p$ as subgroup of $L^\times/p \oplus L^\times/p$. This compatibility allows us to use the above decomposition for the generalized Galois symbol, $(E_1 \otimes^M E_2)/p(K) \to H^2(K, E_1[p] \otimes E_2[p])$.

Example 2.18. Assume for example that E_1 is an elliptic curve with good ordinary reduction and E_2 is a Tate curve, with $E_i[p] \subset E_i(K)$ for $i = 1, 2$. Let $a \in E_1(K)$ and $b \in E_2(K)$ be two closed points. Under the decomposition given by Theorem 2.15, the

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

image of $b \in E_2(K)/p$ can be thought of as the class of a point $b \in K^\times/p$. Moreover, the image of $a \in E_1(K)/p$ is of the form (a_1, a_2) with $a_1 \in \overline{U}_K^0$ and $a_2 \in \overline{U}_K^{pe_0(K)}$. Then,

$$s_p(\{a,b\}_{K/K}) = (g_p(\{a_1,b\}), g_p(\{a_2,b\})) \in \mathbb{Z}/p \oplus \mathbb{Z}/p,$$

where $g_p : K_2^M(K)/p \to Br(K)[p] \simeq \mathbb{Z}/p$ is the classical Galois symbol.

3 The Main Theorems

We make the following assumption for the rest of this section.

Assumption 3.1. Unless otherwise specified, E_1, E_2 *shall denote elliptic curves over the p-adic field K, both with split semistable reduction, and such that at least one of them does not have supersingular reduction*. Moreover, if E is an elliptic curve over K with good reduction, we will denote by $\mathcal{E}$ its Néron model, (which is an abelian scheme over $\mathrm{Spec}(\mathcal{O}_K)$) and by $\overline{E} := \mathcal{E} \otimes_{\mathcal{O}_K} k$ the special fiber (which is an elliptic curve over the residue field k).

We consider the local Galois symbol

$$s_{p^n} : K(K; E_1, E_2)/p^n \to H^2(K, E_1[p^n] \otimes E_2[p^n]).$$

We recall the following result.

Theorem 3.2. (Hiranouchi, [8]) If $E_i[p^n] \subset E_i(K)$ for $i = 1, 2$, the map s_{p^n} is injective.

Hiranouchi used an involved argument to prove injectivity of s_p. The injectivity of s_{p^n} follows by diagram chasing and induction. Theorem 3.2, together with the computation of the image of s_p by Hiranouchi and Hirayama ([9, Theorem 3.4]), yield the following theorem.

Theorem 3.3. (Hiranouchi [8], Hiranouchi–Hirayama [9]) Assume that $E_i[p^n] \subset E_i(K)$ for $i = 1, 2$. Then

$$\frac{K(K; E_1, E_2)}{p^n} \simeq \frac{E_1 \otimes^M E_2}{p^n}(K) \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } E_1, E_2 \text{ have the same reduction type} \\ \mathbb{Z}/p^n \oplus \mathbb{Z}/p^n, & \text{if } E_1, E_2 \text{ have different reduction type} \end{cases}$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Remark 3.4. It is important to note that, while proving injectivity of s_p, Hiranouchi showed that the group $(E_1 \otimes^M E_2)/p$ can be generated by symbols of the form $\{a, b\}_{K/K}$.

Our 1st goal is to remove the strong assumption $E_i[p^n] \subset E_i(K)$ and pass to the limit for p^n. Starting with the case when $E_i[p] \subset E_i(K)$, for $i = 1, 2$, the following quite general lemma provides a sufficient criterion that guarantees injectivity of s_{p^n} for every $n \geq 1$.

Lemma 3.5. Let E_1, E_2 be elliptic curves over K. Assume that $E_i[p^n] \subset E_i(K)$, $i = 1, 2$, for some $n \geq 1$, which is the largest with this property. Further, assume that the Galois symbol s_p is injective. If $K(K; E_1, E_2)/p$ can be generated by symbols of the form $\{a, b\}_{K/K}$ with either $a \in E_1[p^n]$ or $b \in E_2[p^n]$, then the group $p^n K(K; E_1, E_2)$ is p-divisible, that is, $p^n K(K; E_1, E_2) = p^s K(K; E_1, E_2)$, for every $s > n$. In particular, the Galois symbol s_{p^m} is injective for every $m \geq 1$.

Proof. Let $x \in p^n K(K; E_1, E_2)$. We may write $x = p^n y$ for some $y \in K(K; E_1, E_2)$. We consider the image of y in $K(K; E_1, E_2)/p$. By the assumption of the lemma, we may write y in the following form,

$$y = \sum_i \{a_i, b_i\}_{K/K} + pz, \tag{3.6}$$

where $z \in K(K; E_1, E_2)$ and either $a_i \in E_1[p^n]$ or $b_i \in E_2[p^n]$. We conclude that the element $p^n y$ is p-divisible.

Notice that this implies that the Galois symbol s_{p^m} is injective for every $m \geq 1$. For, if $m \leq n$, the injectivity follows from Theorem 3.2. On the other hand, if $x \in \ker(s_{p^s})$ for some $s > n$, a simple induction and diagram chasing shows that $x \in p^n K(K; E_1, E_2)$ and the claim follows by the p-divisibility of $p^n K(K; E_1, E_2)$. ∎

Remark 3.7. It is clear that if the elliptic curves E_1, E_2 satisfy Lemma 3.5, then Theorem 1.2 holds for the product $X = E_1 \times E_2$. Indeed, if D is the maximal p-divisible subgroup of $K(K; E_1, E_2)$, then we can write $K(K; E_1, E_2) \simeq D \oplus F$ for some subgroup F. The lemma together with the fact that $K(K; E_1, E_2)/p^i$ is a finite group for every $i \geq 1$ imply that subgroup F is finite. In many cases, we won't be able to verify the assumptions of Lemma 3.5. However, very often we will be able to show the weaker condition that the group $p^N K(K; E_1, E_2)$ is p-divisible for some $N \geq n$, by showing that the K-group $K(K; E_1, E_2)/p$ can be generated by symbols of the form $\{a, b\}_{K/K}$, with either $a \in E_1[p^N](K)$ or $b \in E_2[p^N](K)$, for some $N > n$.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Remark 3.8. We note that if either Lemma 3.5 or the weaker condition of Remark 3.7 holds, we can show that the finite summand F of $K(K;E_1,E_2)$ can be generated by symbols $\{x,y\}_{K/K}$ defined over K, as long as this is true for the group $K(K;E_1,E_2)/p$. This follows inductively using the exact sequence $K(K;E_1,E_2)/p \xrightarrow{p^m} K(K;E_1,E_2)/p^{m+1} \longrightarrow K(K;E_1,E_2)/p^m \longrightarrow 0$. When E_1,E_2 satisfy Assumption 3.1, this has been proved by Hiranouchi (see Remark 3.4).

3.1 The product of two elliptic curves with ordinary reduction

Our 1st computation will be for the product $E_1 \times E_2$ of two elliptic curves over K, both having good ordinary reduction. We start with a preliminary discussion, which includes some background on elliptic curves of such reduction type.

The connected-étale exact sequence

Let E be an elliptic curve over K with good ordinary reduction, and $n \geq 1$ a positive integer. The G_K-module $E[p^n]$ has a one-dimensional G_K-invariant submodule. Namely, we have a short exact sequence of G_K-modules,

$$0 \to E[p^n]^\circ \to E[p^n] \to E[p^n]^{et} \to 0, \tag{3.9}$$

where $E[p^n]^\circ := \hat{E}[p^n]$ are the p^n-torsion points of the formal group $\hat{E}$ of E.

If we further assume that $E[p^{n-1}] \subset E(K)$, then after a finite unramified extension L_0/K of degree coprime to p, this sequence becomes

$$0 \to \mu_{p^n} \to E[p^n] \to \mathbb{Z}/p^n \to 0. \tag{3.10}$$

The short exact sequence (3.9) is known as the *connected-étale exact sequence* for $E[p^n]$. The reason for the name is that this exact sequence can be obtained from the exact sequence of *finite flat group schemes* over $\mathrm{Spec}(\mathcal{O}_K)$,

$$0 \to \mathcal{E}[p^n]^\circ \to \mathcal{E}[p^n] \to \mathcal{E}[p^n]^{et} \to 0,$$

by extending to the generic fiber. Here we denoted by $\mathcal{E}$ the Néron model of E.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

The Serre–Tate parameter

We next assume that $\mu_p \subset K$ and that we have a non-splitting short exact sequence of finite flat group schemes over $\mathrm{Spec}(\mathcal{O}_K)$,

$$0 \to \mu_p \to \mathcal{E}[p] \to \mathbb{Z}/p \to 0. \tag{3.11}$$

This in particular means that $\hat{E}[p] \subset \hat{E}(\mathcal{O}_K)$. Notice that $\mathcal{E}[p]$ defines in this case a non-trivial element of $\mathcal{E}xt^1_{\mathcal{O}_K}(\mathbb{Z}/p, \mu_p) \simeq H^1_{fppf}(\mathcal{O}_K, \mu_p)$. This group is isomorphic to $\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ and therefore the extension $\mathcal{E}[p]$ (or equivalently the Galois module $E[p]$) corresponds to a unit $u \in \mathcal{O}_K^\times$ that is not a pth power. That is, the sequence (3.11) becomes split after extending to the finite extension $K(\sqrt[p]{u})$. The unit u is known as the Serre–Tate parameter of E. For more information we refer to [14, Chapter 8, Section 9].

Next we want to give a new interpretation of this unit u that will be more helpful for our purposes. We first need some information about the Mackey functor $\hat{E}/[p]$, where $\hat{E}$ is the formal group of E and $[p] : \hat{E} \to \hat{E}$ is the multiplication by p isogeny. Because we assumed that E has ordinary reduction, the isogeny $[p]$ has height one. Recall that $\hat{E}$ induces a Mackey functor that is defined at a finite extension L/K as $\hat{E}(L) := \hat{E}(\mathcal{O}_L)$ with the obvious norm and restriction maps.

Proposition 3.12. Let E be an elliptic curve over K with good ordinary reduction, and $\hat{E}$ be its formal group. Assume that $\hat{E}[p] \subset \hat{E}(\mathcal{O}_K)$ and $\mu_p \subset K$. Then we have an isomorphism of Mackey functors, $\hat{E}/[p] \simeq \overline{U}^1 \simeq \overline{U}^0$.

Proof. The 1st isomorphism follows directly from [15, Theorem 2.1.6, Corollary 2.1.7], if we apply it to the height 1 isogeny, $[p] : \hat{E} \to \hat{E}$. To make this more precise, for every finite extension L/K, we have an isomorphism, $\hat{E}(\mathcal{O}_L)/[p]\hat{E}(\mathcal{O}_L) \simeq \overline{U}_L^{p(e_0(L)-t(L))+1}$, where the invariant $t(L)$ is defined as

$$t(L) = \max\{i \geq 0 : P \in \hat{E}(\mathfrak{m}_L^i), \text{ for every } P \in \hat{E}[p]\}.$$

We claim that $t(L) = e_0(L)$. Since for every finite extension L'/L we have equalities, $t(L') = e(L'/L)t(L)$ and $e_0(L') = e(L'/L)e_0(L)$, it suffices to prove this equality after extending to $L(E[p])$. But then the result follows from Theorem 2.15. The 2nd isomorphism follows from Lemma 2.13. ∎

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

We next consider the short exact sequence of abelian groups,

$$0 \to \hat{E}(\mathcal{O}_K) \xrightarrow{j} E(K) \xrightarrow{r} \overline{E}(k) \to 0, \tag{3.13}$$

where $E(K) \xrightarrow{r} \overline{E}(k)$ is the reduction map. By tensoring (3.13) with $\mathbb{Z}/p$ and using Proposition 3.12 we get an exact sequence,

$$\overline{U}_K^0 \xrightarrow{j} E(K)/p \xrightarrow{r} \overline{E}(k)/p \to 0.$$

The claim is that the map $\overline{U}_K^0 \xrightarrow{j} E(K)/p$ is not injective. Namely there is a unit $u \in \overline{U}_K^0$ that generates the kernel and this unit is the Serre–Tate parameter of E. To construct u, we proceed as follows. Let $b \in \overline{E}[p](k)$ be a p-torsion point with $b \neq 0$. Such a point exists because $\overline{E}[p] \simeq E^{et}[p] \simeq \mathbb{Z}/p$. Since the reduction map is surjective, we may choose a lift $\tilde{b}$ of b in $E(K)$. We claim that $r(p\tilde{b}) = pb = 0$, but $p\tilde{b}$ is nonzero. Indeed, if $p\tilde{b} = 0$, then $\tilde{b}$ would be a K-rational p-torsion point of E, which would contradict the non-splitting of the short exact sequence (3.11). Next, the exactness of the sequence (3.13) yields the existence of a unit $u \in \mathcal{O}_K^\times$ such that $j(u) = p\tilde{b}$. The class of $u \in \mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ is independent of the choice of lift. To finish the claim, we need to verify that $u \notin K^{\times p}$. Assume to the contrary that u is a pth power, that is, $u = v^p$ for some v in $K^\times$. Then the equation $pj(v) = p\tilde{b}$ yields that $\tilde{b} - j(v)$ is a non-zero p-torsion point of E. Since $r(\tilde{b}) = b \neq 0$, this would imply that $E[p] \subset E(K)$, which is a contradiction.

Injectivity in the wild case

In this subsection we consider the question of injectivity of the Galois symbol for two elliptic curves E_1, E_2 with ordinary reduction. We will often work with the Mackey product, $(E_1 \otimes^M E_2)(K)/p^n$ instead of the Somekawa K-group $K(K; E_1, E_2)/p^n$. To distinguish between the two groups, we will call the map

$$(E_1 \otimes^M E_2)(K)/p^n \xrightarrow{s_{p^n}} H^2(K, E_1[p^n] \otimes E_2[p^n])$$

the *Mackey functor Galois symbol*. Recall that the latter has the same image as the actual Galois symbol

$$K(K; E_1, E_2)/p^n \xrightarrow{s_{p^n}} H^2(K, E_1[p^n] \otimes E_2[p^n]),$$

but it might have a larger kernel.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Theorem 3.14. Assume $\mu_p \subset K$. Let E_1, E_2 be elliptic curves over K with good ordinary reduction and let $n \geq 0$ be the largest integer such that $E_i[p^n] \subset E_i(K)$, for $i = 1, 2$. Assume:

- The extension $L = K(E_1[p^{n+1}], E_2[p^{n+1}])$ has wild ramification.
- For $i = 1, 2$ we have short exact sequences of G_K-modules,

$$0 \to \mu_{p^{n+1}} \to E_i[p^{n+1}] \to \mathbb{Z}/p^{n+1} \to 0.$$

Then the Galois symbol $s_{p^m} : K(K; E_1, E_2)/p^m \to H^2(K, E_1[p^m] \otimes E_2[p^m])$ is injective for every $m \geq 1$. In particular, if $n = 0$, the K-group $K(K; E_1, E_2)$ is p-divisible.

Proof. We first prove injectivity when $n \geq 1$, which implies $E_i[p] \subset E_i(K)$ for $i = 1, 2$. Without loss of generality assume that $K(E_1[p^{n+1}])/K$ is wildly ramified. Then there exists a p^n-torsion point $w \in E_1[p^n]$ such that the extension $L_w = K(\frac{1}{p}w)$ is wildly ramified over K. We will show that the assumption of Lemma 3.5 holds, more precisely, that $K(K; E_1, E_2)/p$ is generated by symbols of the form $\{w, y\}_{K/K}$ with $y \in E_2(K)$.

By Theorem 3.2 we get that the Galois symbol s_p is injective and can be computed by the following composition,

$$K(K; E_1, E_2)/p \simeq (\overline{U}^0 \otimes^M \overline{U}^0)(K) \xrightarrow{g_p} Br(K)[p] \simeq \mathbb{Z}/p,$$

where g_p is the classical Galois symbol. Moreover, recall (2.15) that we have a decomposition, $E_1(K)/p \simeq \overline{U}^0_K \oplus \overline{U}^{pe_0(K)}_K$. We consider the image of $w = (w_1, w_2)$ under this decomposition. Since L_w/K is wildly ramified, we necessarily have $w_1 \neq 0$ and even stronger, that $w_1 \in \overline{U}^i_K \setminus \overline{U}^{i+1}_K$ for some i coprime to p. To prove the claim, it suffices therefore to show that there exists some $y \in \overline{U}^0(K) \subset E_2(K)/p$ such that $g_p(\{w_1, y\}) \neq 0$. Equivalently, it suffices to show that there exists a unit $y \in \overline{U}^0(K)$ such that $y \notin N_{K(\sqrt[p]{w})/K}(K(\sqrt[p]{w})^\times)$. The existence of such a y follows by [21, page 86, Corollary 7].

Now we prove injectivity when $n = 0$. In this case, either $E_1[p] \not\subset E_1(K)$ or $E_2[p] \not\subset E_2(K)$. We will show that $(E_1 \otimes^M E_2)/p = 0$, which in particular implies that the K-group $K(K; E_1, E_2)$ is p-divisible.

We have that $\mu_p \subset K$, and for $i = 1, 2$, there are short exact sequences of G_K modules

$$0 \to \mu_p \to E_i[p] \to \mathbb{Z}/p \to 0.$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Without loss of generality, assume that $K(E_1[p])/K$ is wildly ramified. In particular, the extension $0 \to \mu_p \to E_1[p] \to \mathbb{Z}/p \to 0$ does not split, and the corresponding Serre–Tate parameter u has the property that $K(\sqrt[p]{u})/K$ is a totally ramified degree p extension.

Recall that the category of Mackey functors is abelian with a tensor product. The short exact sequence of abelian groups (3.13) induces a short sequence of Mackey functors,

$$0 \to \hat{E}_i \to E_i \to [E_i/\hat{E}_i] \to 0,$$

where $[E_i/\hat{E}_i]$ is the Mackey functor defined as follows. For a finite extension F/K, denote the residue field of F by k_F, and let $[E_i/\hat{E}_i](F) := \overline{E}_i(k_F)$. Moreover, the restriction $\mathrm{res}_{F/K} : [E_i/\hat{E}_i](K) \to [E_i/\hat{E}_i](F)$ is the usual restriction, $\overline{E}_i(k) \xrightarrow{\mathrm{res}_{F/K}} \overline{E}_i(k_F)$, while the norm $N_{F/K} : [E_i/\hat{E}_i](F) \to [E_i/\hat{E}_i](K)$ is the map $e(F/K) \cdot N_{F/K} : \overline{E}_i(k_F) \to \overline{E}_i(k)$. The fact that $[E_i/\hat{E}_i]$ is a Mackey functor has been shown by Raskind and Spiess ([18, page 15]). We consider the sequence for $i = 2$ and we apply the right exact functor, $\otimes\mathbb{Z}/p$. Using Proposition 3.12, we obtain an exact sequence of Mackey functors,

$$\overline{U}^0 \otimes^M \overline{U}^0 \xrightarrow{j} \overline{U}^0 \otimes^M E_2/p \xrightarrow{r} \overline{U}^0 \otimes^M [E_2/\hat{E}_2]/p \to 0.$$

We claim that $\overline{U}^0 \otimes^M [E_2/\hat{E}_2]/p = 0$. Indeed, consider a symbol $\{x, y\}_{F/K}$, where F is some finite extension of K, $x \in \overline{U}^0(F)$, and $y \in [E_2/\hat{E}_2](F)$. There is $y' \in [E_2/\hat{E}_2](\overline{F})$ such that $py' = y$; more precisely, for some finite unramified extension F'/F, we can find $y' \in [E_2/\hat{E}_2](F')$ such that $py' = y$. But, since F'/F is unramified, the norm map $N_{F'/F} : \overline{U}^0(F') \to \overline{U}^0(F)$ is surjective ([21, page 81, Proposition 1]), so the claim follows. We conclude that there is an exact sequence $\overline{U}^0 \otimes^M \overline{U}^0 \xrightarrow{j} \overline{U}^0 \otimes^M E_2/p \to 0$.

Using a similar argument, we obtain an exact sequence of Mackey functors,

$$\overline{U}^0 \otimes^M E_2/p \xrightarrow{j} E_1/p \otimes^M E_2/p \xrightarrow{r} [E_1/\hat{E}_1]/p \otimes^M E_2/p \to 0.$$

We can again conclude that $[E_1/\hat{E}_1]/p \otimes^M E_2/p = 0$, because the elliptic curve E_2 has good reduction, and hence for every finite unramified extension F'/F, the norm map $N_{F'/F} : E_2(F') \to E_2(F)$ is surjective ([16, Corollary 4.4]). Finally, the two exact sequences induce a surjection,

$$\overline{U}^0 \otimes^M \overline{U}^0 \xrightarrow{j} E_1/p \otimes^M E_2/p \to 0.$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Evaluating at Spec(K), we get a surjection,

$$(\overline{U}^0 \otimes^M \overline{U}^0)(K) \xrightarrow{j} (E_1/p \otimes^M E_2/p)(K) \to 0.$$

The group $(\overline{U}^0 \otimes^M \overline{U}^0)(K)$ is isomorphic via the classical Galois symbol to $\mathbb{Z}/p$ ([8, Lemma 3.3]). It suffices therefore to show that some non-zero element of $(\overline{U}^0 \otimes^M \overline{U}^0)(K)$ is mapped to zero under j. But this now is easy, using the description of the Serre–Tate parameter u described in the beginning of this section. Namely, by our assumption, the extension $K(\sqrt[p]{u})$ is totally ramified of degree p over K, and hence there exists a unit $b \in \overline{U}^0(K)$ such that $g_p(\{u,b\}_{K/K}) \neq 0$. Thus we get a generator $\{u,b\}_{K/K}$ of $(\overline{U}^0 \otimes^M \overline{U}^0)(K)$, which is clearly mapped to zero under j. ■

Possible kernel in the unramified case

We will now show that if the assumption of Theorem 3.14 does not hold, the Mackey functor Galois symbol has a nontrivial kernel. We emphasize that this does not disprove Conjecture 2.8, since the group $(E_1/p \otimes^M E_2/p)(K)$ could in general be larger than the Somekawa K-group $K(K; E_1, E_2)/p$.

Proposition 3.15. Let E_1, E_2 be elliptic curves over K with good ordinary reduction. We assume that $\mu_p \subset K$ and the G_K modules $E_i[p]$ fit into short exact sequences,

$$0 \to \mu_p \to E_i[p] \to \mathbb{Z}/p \to 0.$$

Suppose that the extension $K(E_1[p], E_2[p])$ is nontrivial and unramified over K. Then the Galois symbol s_p vanishes, while $(E_1/p \otimes^M E_2/p)(K) \simeq \mathbb{Z}/p$. In particular, the Mackey functor $E_1/p \otimes^M E_2/p$ is isomorphic to $\overline{U}^0 \otimes^M \overline{U}^0$.

Proof. First we show that $(E_1/p \otimes^M E_2/p)(K) \simeq \mathbb{Z}/p$. This follows similarly to the proof of Theorem 3.14. Without loss of generality, we assume that the extension $K(E_1[p])$ is nontrivial and unramified over K. We have an exact sequence of Mackey functors,

$$0 \to \langle u \rangle \to \overline{U}^0 \xrightarrow{j} E_1/p \to [E_1/\hat{E}_1]/p \to 0,$$

where u is the Serre–Tate parameter of E_1. Here we denoted by $\langle u \rangle$ the Mackey subfunctor of $\overline{U}^0$ generated by u. Note that for a finite extension L of K, $\langle u \rangle(L)$ is either 0 or $\mathbb{Z}/p$ depending on whether u is a pth power in L or not. When we apply $\otimes^M \overline{U}^0$ to

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

the above sequence, the Mackey functor $\langle u\rangle \otimes^M \overline{U}^0$ vanishes. If L/K is a finite extension such that $u \notin L^{\times p}$, then the extension $L(\sqrt[p]{u})$ is unramified over L and therefore the norm map $\overline{U}^0_L \to \overline{U}^0_K$ is surjective. We conclude that in this case the surjection $\overline{U}^0 \otimes^M \overline{U}^0 \xrightarrow{j} E_1/p \otimes^M E_2/p \to 0$ is an isomorphism, and hence $(E_1/p \otimes^M E_2/p)(K) \simeq \mathbb{Z}/p$.

Next we show that $s_p = 0$. To show this, we use local Tate duality. The local Tate duality pairing for the finite G_K-module $E_1[p] \otimes E_2[p]$ and for $i = 0, 1, 2$ is a perfect pairing,

$$\langle \cdot, \cdot \rangle : H^i(K, E_1[p] \otimes E_2[p]) \times H^{2-i}(K, \mathrm{Hom}(E_1[p] \otimes E_2[p], \mu_p)) \to \mathbb{Z}/p.$$

Using the Weil pairing and the fact that elliptic curves are self-dual abelian varieties, the above pairing for $i = 2$ becomes,

$$\langle \cdot, \cdot \rangle : H^2(K, E_1[p] \otimes E_2[p]) \times \mathrm{Hom}_{G_K}(E_1[p], E_2[p]) \to \mathbb{Z}/p.$$

According to the main theorem of [7, Theorem 1.1], the orthogonal complement under $\langle \cdot, \cdot \rangle$ of the image of s_p consists precisely of those homomorphisms $f : E_1[p] \to E_2[p]$ that extend to a homomorphism $\tilde{f} : \mathcal{E}_1[p] \to \mathcal{E}_2[p]$ of finite flat group schemes over $\mathrm{Spec}(\mathcal{O}_K)$, where $\mathcal{E}_i$ is the Néron model of E_i for $i = 1, 2$. Since both elliptic curves have ordinary reduction, the above subgroup of $\mathrm{Hom}_{G_K}(E_1[p], E_2[p])$ has a simpler description. Namely, according to [7, Proposition 8.8], the orthogonal complement of $\mathrm{Im}(s_p)$ is the subgroup

$$H = \{f \in \mathrm{Hom}_{G_K}(E_1[p], E_2[p]) : f(E_1[p]^\circ) \subset E_2[p]^\circ\}.$$

We will show that every G_K-homomorphism $f : E_1[p] \to E_2[p]$ lies in H, which will imply that $s_p = 0$. By the assumption of the proposition, $E_i[p]^\circ \simeq \mu_p$, for $i = 1, 2$, and the G_K action on $E_i[p]$ is upper triangular of the form $\begin{pmatrix} 1 & \alpha_i(\sigma) \\ 0 & 1 \end{pmatrix}$, for $\sigma \in G_K$, where $\alpha_i : G_K \to \mathrm{Hom}(\mathbb{Z}/p, \mu_p)$. Since we assumed that the extension $K(E_1[p], E_2[p])$ is nontrivial, at least one of the two characters α_i is nonzero of order exactly p.

Let $f : E_1[p] \to E_2[p]$ be a G_K-homomorphism. After we consider splittings as abelian groups (and not as G_K-modules), $E_i[p] \simeq \mu_p \oplus \mathbb{Z}/p$, we can write f in a matrix

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

form $f = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$. We want to show that the function $f_3 : E_1[p]^\circ \xrightarrow{f} E_2[p] \to E_2[p]^{et}$ vanishes. This follows by the equality of matrices,

$$\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}\begin{pmatrix} 1 & \alpha_1(\sigma) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_2(\sigma) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix},$$

which yields $\alpha_2(\sigma)f_3 = f_3\alpha_1(\sigma) = 0$, for every $\sigma \in G_K$. ■

Corollary 3.16. Theorem 1.4 holds for a product $X = E_1 \times E_2$ of elliptic curves with good ordinary reduction.

Proof. As usual, let $n \geq 0$ be the largest integer such that $E_i[p^n] \subset E_i(K)$ for $i = 1, 2$. By extending to a finite extension if necessary, we may assume that $\mu_p \subset K$ and for $i = 1, 2$ we have short exact sequences of G_K-modules,

$$0 \to \mu_{p^{n+1}} \to E_i[p^{n+1}] \to \mathbb{Z}/p^{n+1} \to 0.$$

The only case when we need to extend the base field is when the extension

$$L_1 := K(E_1[p^{n+1}], E_2[p^{n+1}])$$

is unramified over K. After extending to L_1 we examine whether the extension $L_2 := K(E_1[p^{n+2}], E_2[p^{n+2}])$ has wild ramification over L_1. After repeating this process finitely many times, we get an extension L_{r+1}/L_r, for some $r \geq 1$, that has wild ramification. Indeed, there is a largest integer $N > n$ such that $\mu_{p^N} \subset K$, so L_{r+1}/K has wild ramification for some $r \geq 1$. Choosing r the smallest with that property, we have that L_{r+1}/L_r has wild ramification and injectivity holds over L_r. ■

Structural results

We next consider the Albanese kernel, $T(E_1 \times E_2)$. Recall that by the work of Raskind and Spiess ([18]) we have an isomorphism,

$$T(E_1 \times E_2) \simeq K(K; E_1, E_2) \simeq T(E_1 \times E_2)_{\mathrm{div}} \oplus (\text{finite}),$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

where we denoted by $T(E_1 \times E_2)_{\text{div}}$ the maximal divisible subgroup of the Albanese kernel. Theorem 3.14 and Proposition 3.15 allow us in most cases to fully determine the finite summand of $T(E_1 \times E_2)$.

Corollary 3.17. Let $X = E_1 \times E_2$ be the product of two elliptic curves over K with good ordinary reduction. Let $n \geq 0$ be the largest nonnegative integer such that $E_i[p^n] \subset E_i(K)$ for $i = 1, 2$. Assume that the extension $K(E_1[p^{n+1}], E_2[p^{n+1}])$ has wild ramification. Then we have an isomorphism for the Albanese kernel,

$$T(X) \simeq \begin{cases} T(X)_{\text{div}} \oplus \mathbb{Z}/p^n, & \text{if } n \geq 1 \\ T(X)_{\text{div}}, & \text{if } n = 0. \end{cases}$$

Proof. Case 1: Assume that $n \geq 1$. We consider first the special case when for $i = 1, 2$ we have short exact sequences of G_K-modules,

$$0 \to \mu_{p^{n+1}} \to E_i[p^{n+1}] \to \mathbb{Z}/p^{n+1} \to 0.$$

In this case the corollary follows directly from Theorem 3.14 and Theorem 3.3, since we already know by the computations of Hiranouchi (Theorem 3.3) that

$$K(K; E_1, E_2)/p^n \simeq \mathbb{Z}/p^n.$$

For the general case, let L/K be the smallest finite extension such that the special case holds for the product $E_{1,L} \times E_{2,L}$. It suffices to show that for every $m \geq 1$ the norm map,

$$N_{L/K} : K(L; E_{1,L}, E_{2,L})/p^m \to K(K; E_1, E_2)/p^m$$

is surjective. For, the surjectivity of the norm together with Theorem 3.14 will imply that for every $s > n$ the K-group $p^s K(K; E_1, E_2)$ is p-divisible. At the same time Theorem 3.3 gives us an isomorphism, $K(K; E_1, E_2)/p^n \simeq \mathbb{Z}/p^n$, and hence the norm will in fact be an isomorphism, from which the claim follows.

The surjectivity of the norm follows easily, since L/K is a finite unramified extension. For such extensions, the norm map $N_{L/K} : E_1(L) \to E_1(K)$ is surjective [16, Corollary 4.4]. Using the projection formula (2.5) of the Somekawa K-group, we can easily show that $N_{L/K} : K(L; E_{1,L}, E_{2,L}) \to K(K; E_1, E_2)$ is also surjective.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Case 2: Assume that $n = 0$. Let L/K be the smallest finite extension such that $\mu_p \subset L$ and the G_L-modules $E_i[p]$ fit into short exact sequences,

$$0 \to \mu_p \to E_i[p] \to \mathbb{Z}/p \to 0. \tag{3.18}$$

The assumption of Theorem 3.17 implies that for at least one $i \in \{1,2\}$ the sequence (3.18) does not split. More importantly, it corresponds to a non-trivial Serre–Tate parameter $u \in \mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$, which is such that the extension $L(\sqrt[p]{u})/L$ is totally ramified. In this case, the argument is exactly the same as when $n \geq 1$. Namely, Theorem 3.14 gives us that the K-group $K(L; E_{1,L}, E_{2,L})$ is p-divisible. The general case follows again by the surjectivity of the norm map,

$$K(L; E_{1,L}, E_{2,L})/p \xrightarrow{N_{L/K}} K(K; E_1, E_2)/p.$$

Note that in this case we have a tower, $K \subset L_0 \subset L$ with L_0/K unramified and L is at most $L_0(\mu_p)$. Since the latter is an extension of degree coprime to p, the norm map N_{L/L_0} is surjective. ∎

The case of complex multiplication

We close the story of two ordinary reduction elliptic curves by considering a very special case, the one of a product $X = E_1 \times E_2$ of two elliptic curves both having complex multiplication by an imaginary quadratic field. We note that this case is only partially covered by Corollary 3.17. Namely, if $E_i[p] \subset E_i(K)$ for $i = 1,2$, then we can apply Theorem 3.14 and Corollary 3.17 for X.

The reason we cannot apply Corollary 3.17 when $E_i[p] \not\subset E_i(K)$ for at least one i is the following. After extending to a tower, $K \subset L_0 \subset L$, such that L_0/K is unramified and L is at most $L_0(\mu_p)$, the G_L-module $E_i[p]$ fits into a short exact sequence,

$$0 \to \mu_p \to E_i[p] \to \mathbb{Z}/p \to 0.$$

This sequence splits over L, that is, the corresponding Serre–Tate parameter is trivial. This follows by [22, A.2.4]. We therefore have an isomorphism,

$$T(E_1 \times E_2 \times L) \simeq \mathbb{Z}/p \oplus T(E_1 \times E_2 \times L)_{\mathrm{div}}.$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Question 3.19. What happens over K? Is $T(X)$ divisible? Or is its finite summand isomorphic to $\mathbb{Z}/p$?

We do not have a method to answer this question in great generality, but we can say something when K is unramified over $\mathbb{Q}_p$. This case is of particular importance, as it will give us global-to-local applications (see Section 4).

Proposition 3.20. Let $X = E_1 \times E_2$ be the product of two elliptic curves over K with good ordinary reduction. Assume that K is unramified over $\mathbb{Q}_p$ and that the elliptic curves E_1, E_2 have complex multiplication by an imaginary quadratic field. Then $T(E_1 \times E_2)$ is divisible.

Proof. By the usual surjectivity of the norm argument, we may reduce to the case when

$$L := K(E_1[p], E_2[p]) = K(\mu_p).$$

By Theorem 3.14, we have an isomorphism, $K(L; E_{1,L}, E_{2,L})/p \simeq \mathbb{Z}/p$ and this K-group can be generated by symbols of the form $\{w, b\}_{L/L}$ with $w \in E_1[p](L)$. We can even choose $w \in \hat{E}_1[p](\mathcal{O}_L)$. We will show that the norm,

$$N_{L/K} : K(L; E_{1,L}, E_{2,L})/p \to K(K; E_1, E_2)/p$$

vanishes. Since it is also surjective, this will imply that $K(K; E_1, E_2)$ is p-divisible. Since $K(L; E_{1,L}, E_{2,L})/p$ is cyclic, it suffices to show that $N_{L/K}(\{w, b\}_{L/L}) = 0$ for some nontrivial symbol $\{w, b\}_{L/L}$. Recall from Proposition 3.12 that the p-torsion point w satisfies

$$w \in \hat{E}_1(\mathfrak{m}_L^{e_0(L)}) \setminus \hat{E}_1(\mathfrak{m}_L^{e_0(L)+1}).$$

Since we assumed that K is unramified over $\mathbb{Q}_p$, we have $e_0(L) = 1$ and hence $w \in \hat{E}_1(\mathfrak{m}_L^1) \setminus \hat{E}_1(\mathfrak{m}_L^2)$. By [15, Theorem 2.1.6] we get that the image of w in $\overline{U}_L^0$ lies in $\overline{U}_L^1 \setminus \overline{U}_L^2$. This means that the jump of the ramification filtration of $L(\frac{1}{p}w)/L$ is exactly at $p-1$. Coming to the symbol $\{w, b\}_{L/L}$, we can write $b = (b_1, b_2)$ for the image of b in $E_2(L)/p \simeq \overline{U}_L^0 \oplus \overline{U}_L^p$. We therefore conclude that if $\{w, b\}_{L/L} \neq 0$, then $b_1 \in \overline{U}_L^{p-1}$.

We next consider the restriction map,

$$\mathrm{res}_{L/K} : \hat{E}_2(\mathcal{O}_K)/[p]\hat{E}_2(\mathcal{O}_K) \to \hat{E}_2(\mathcal{O}_L)/[p]\hat{E}_2(\mathcal{O}_L).$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

Since $e(L/K) = p-1$, we can easily see that the image of $\mathrm{res}_{L/K}$ lies in the subgroup $\hat{E}_2(\mathfrak{m}_L^{p-1})/([p]\hat{E}_2(\mathcal{O}_L) \cap \mathfrak{m}_L^{p-1})$. Because L/K is totally ramified, the image in fact equals this subgroup. Using [15, Theorem 2.1.6] once more we conclude that the image of

$$\hat{E}_2(\mathcal{O}_K)/[p]\hat{E}_2(\mathcal{O}_K) \xrightarrow{\mathrm{res}_{L/K}} \hat{E}_2(\mathcal{O}_L)/[p]\hat{E}_2(\mathcal{O}_L) \xrightarrow{\simeq} \overline{U}_L^0$$

is exactly $\overline{U}_L^{p-1}$. Thus, we can find a generator of the K-group $K(L; E_{1,L}, E_{2,L})/p$ of the form $\{w, \mathrm{res}_{L/K}(b')\}_{L/L}$ for some $b' \in E_2(K)$. The projection formula (2.5) yields an equality,

$$N_{L/K}(\{w, \mathrm{res}_{L/K}(b')\}_{L/L}) = \{N_{L/K}(w), b'\}_{K/K}.$$

But the latter symbol is zero. For, w is a p-torsion point of $E_1(L)$. Since the norm is a homomorphism, the same is true for $N_{L/K}(w)$. But the formal group $\hat{E}_1(\mathcal{O}_K)$ is torsion-free, and hence $N_{L/K}(w) = 0$. ∎

3.2 The product of two elliptic curves, one with ordinary and the other with supersingular reduction

In this subsection, we consider the product of two elliptic curves E_1 and E_2 over K, and we assume E_1 has ordinary reduction and E_2 has supersingular reduction. We recall that, when $E_i[p] \subset E_i(K)$ for $i = 1, 2$, we have an isomorphism

$$s_p : K(K; E_1, E_2)/p \xrightarrow{\simeq} (E_1 \otimes^M E_2)/p \xrightarrow{\simeq} \mathbb{Z}/p \oplus \mathbb{Z}/p.$$

We proceed similarly to the case of two ordinary reduction elliptic curves, considering first some cases when the injectivity of s_{p^n} can be verified for every $n \geq 1$.

Proposition 3.21. Let E_1, E_2 be elliptic curves with good reduction over K, where E_1 has ordinary reduction, and E_2 has supersingular reduction. The Galois symbol s_{p^n} is injective for every $n \geq 1$ in each of the following cases.

(1) When $E_i[p^n] \subset E_i(K)$ for $i = 1, 2$ and some $n \geq 1$, which is the largest with this property, and there is some $w \in E_1[p^n]$ such that under the decomposition $E_1(K)/p \xrightarrow{\simeq} \overline{U}_K^0 \oplus \overline{U}_K^{pe_0(K)}$, w can be written in the form $w = (w_1, w_2)$ with $w_1 \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$ for some i coprime to p and such that

$$i \leq \min\{pt(K), p(e_0(K) - t(K))\}.$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

(2) When $E_2[p] \subset E_2(K)$, and the G_K-module $E_1[p]$ fits into a short exact sequence of the form (3.10) having a non-trivial Serre–Tate parameter u such that $u \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$ for some i coprime to p with $i \leq \min\{pt(K), p(e_0(K) - t(K))\}$. In this case the K-group $K(K; E_1, E_2)$ is p-divisible.

Proof. Note that the assumption $E_2[p] \subset E_2(K)$ implies $\mu_p \subset K^\times$. Recall that we have a decomposition as Mackey functors,

$$E_2/p \xrightarrow{\simeq} \overline{U}^{p(e_0(K)-t(K))} \oplus \overline{U}^{pt(K)},$$

where $t(K)$ is the invariant of E_2 defined in section 2.

We first consider case (1). From Lemma 3.5, it is enough to prove that the K-group $K(K; E_1, E_2)/p$ can be generated by symbols of the form $\{a, b\}_{K/K}$ with either $a \in E_1[p^n]$ or $b \in E_2[p^n]$. The key idea is to show that there exist elements $b_1 \in \overline{U}_K^{p(e_0(K)-t(K))}$ and $b_2 \in \overline{U}_K^{pt(K)}$ such that $s_p(\{w, (b_1, 0)\}_{K/K}) \neq 0$ and $s_p(\{w, (0, b_2)\}_{K/K}) \neq 0$, and therefore, by injectivity of s_p, elements of the form $\{w, (b_1, 0)\}_{K/K}$ and $\{w, (0, b_2)\}_{K/K}$ generate $K(K; E_1, E_2)/p$.

We have that $w_1 \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$ for some $i < pe_0(K)$ coprime to p that satisfies

$$i \leq \min\{pt(K), p(e_0(K) - t(K))\}.$$

If $i + pe_0(K) - pt(K) \leq pe_0(K)$, then, from the computations in [8, Lemma 3.4], we can find $b_1 \in \overline{U}_K^{p(e_0(K)-t(K))}$ such that $\{w, (b_1, 0)\}_{K/K} \neq 0$; on the other hand, if $i + pt(K) \leq pe_0(K)$, then we can find $b_2 \in \overline{U}_K^{pt(K)}$ such that $\{w, (0, b_2)\}_{K/K} \neq 0$. The 1st case occurs if $i \leq pt(K)$, while the 2nd one occurs if $i \leq p(e_0(K) - t(K))$. Since we have $i \leq \min\{pt(K), p(e_0(K) - t(K))\}$, we get the result.

We now consider case (2). As usual, using Proposition 3.12 we get a surjection of Mackey functors,

$$\overline{U}^0 \otimes^M E_2/p \xrightarrow{j} (E_1 \otimes^M E_2)/p \to 0.$$

The 1st Mackey functor is isomorphic to $(\overline{U}^0 \otimes^M \overline{U}^{pt(K)}) \oplus (\overline{U}^0 \otimes^M \overline{U}^{p(e_0(K)-t(K))})$. [8, Lemma 3.4] gives that the group $\overline{U}^0 \otimes^M \overline{U}^{pt(K)} \oplus \overline{U}^0 \otimes^M \overline{U}^{p(e_0(K)-t(K))}(K)$ is isomorphic via the classical Galois symbol to $\mathbb{Z}/p \oplus \mathbb{Z}/p$. Moreover, because we assumed that $u \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$ with i coprime to p and $i \leq \min\{pt(K), p(e_0(K) - t(K))\}$, the same lemma [8, Lemma 3.4] together with the discussion preceding it imply that there exist $b_1, b_2 \in E_2(K)/p$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

such that $\{u, b_1\}_{K/K}$ and $\{u, b_2\}_{K/K}$ generate $(\overline{U}^0 \otimes^M E_2/p)(K)$. But both these symbols are mapped to zero under j. We conclude that $(E_1 \otimes^M E_2)(K)/p = 0$ and in particular that the K-group $K(K; E_1, E_2)$ is p-divisible. ■

Similarly to the case of two ordinary reduction elliptic curves, we can show that if some of the assumptions of Proposition 3.21 are not satisfied, the Mackey functor Galois symbol has a non-trivial kernel. This is the purpose of the next proposition.

Proposition 3.22. Let E_1, E_2 be elliptic curves with good reduction over K, where E_1 has ordinary reduction, and E_2 has supersingular reduction. We assume that $E_2[p] \subset E_2(K)$, and the G_K-module $E_1[p]$ fits into a short exact sequence of the form (3.10) having a non-trivial Serre–Tate parameter u. Suppose that $u \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$ for some integer i such that $i > \min\{pt(K), p(e_0(K) - t(K))\}$. Then the Galois symbol s_p vanishes, while the group $(E_1/p \otimes^M E_2/p)(K)$ contains $\mathbb{Z}/p$.

Proof. The proof is very analogous to the proof of Proposition 3.15, so we give a less detailed analysis of the argument. All the cases to consider are similar, so without loss of generality we assume that $pt(K) < i < p(e_0(K) - t(K))$. In this case we will show that $s_p = 0$, while the Mackey functor $E_1/p \otimes^M E_2/p$ is isomorphic to $\overline{U}^0 \otimes^M \overline{U}^{p(e_0(K)-t(K))}$.

We consider the exact sequence of Mackey functors,

$$\langle u \rangle \otimes^M E_2/p \to \overline{U}^0 \otimes^M E_2/p \xrightarrow{j} E_1/p \otimes^M E_2/p \to 0,$$

where $\langle u \rangle$ is the Mackey functor defined in the proof of Theorem 3.14. We have a decomposition $\langle u \rangle \otimes^M E_2/p \simeq (\langle u \rangle \otimes^M \overline{U}^{pt(K)}) \oplus (\langle u \rangle \otimes^M \overline{U}^{p(e_0(K)-t(K))})$. Similarly to the proof of Proposition 3.21, because we assumed $i < p(e_0(K) - t(K))$, we can find $x \in \overline{U}_K^{pt(K)}$ such that the symbol $\{u, x\}_{K/K} \in (\langle u \rangle \otimes^M \overline{U}^{pt(K)})(K) \subset (\overline{U}^0 \otimes^M \overline{U}^{pt(K)})(K)$ is non-trivial. On the other hand, the inequality $i > pt(K)$ implies that $\langle u \rangle \otimes^M \overline{U}^{p(e_0(K)-t(K))} = 0$. We conclude that $E_1/p \otimes^M E_2/p \simeq \overline{U}^0 \otimes^M \overline{U}^{p(e_0(K)-t(K))}$.

Next we show that $s_p = 0$. We consider the orthogonal complement of $\mathrm{Im}(s_p)$ under local Tate duality. According to [7, Proposition 8.11], the complement in this case coincides with the following subgroup of $\mathrm{Hom}_{G_K}(E_1[p], E_2[p])$,

$$\{f \in \mathrm{Hom}_{G_K}(E_1[p], E_2[p]) : f(E_1[p]^\circ) = 0\}.$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

The G_K-action on $E_1[p]$ is of the form $\begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & 1 \end{pmatrix}$, for $\sigma \in G_K$, where $\alpha : G_K \to \mathrm{Hom}(\mathbb{Z}/p, \mu_p)$ is a non-trivial character. Let $f \in \mathrm{Hom}_{G_K}(E_1[p], E_2[p])$. Once again we may write f in a matrix form, $f = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$. We have a matrix equality,

$$\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} \begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & 1 \end{pmatrix},$$

which yields $f_1\alpha(\sigma) = f_3\alpha(\sigma) = 0$, for every $\sigma \in G_K$ and hence $f_1 = f_3 = 0$. This means exactly that f vanishes when restricted to $E_1[p]^\circ$. ■

Our main goal now is to show that when the assumptions of Proposition 3.21 do not hold, we can construct a tower $K \subset K_1 \cdots \subset K_r$ of finite extensions of K so that the weaker criterion described in Remark 3.7 holds over K_r. This will imply that there exists a large enough integer $N \geq 1$ such that the K-group $p^N K(K; E_1, E_2)$ is p-divisible. In particular Theorem 1.2 holds for $E_1 \times E_2$. We start with the following lemma.

Lemma 3.23. Let K be a p-adic field containing a primitive p^2th root of unity, ζ_{p^2}. Let $u \in \overline{U}_K^0$ be such that $u \in \overline{U}_K^i \setminus \overline{U}_K^{i+1}$, where $0 < i < pe_0(K)$ and i is coprime to p. Let $L = K(\sqrt[p]{u})$. Write $v = \sqrt[p]{u}$. Then $v \in \overline{U}_L^i \setminus \overline{U}_L^{i+1}$.

Proof. We have $v \in \overline{U}_L^j \setminus \overline{U}_L^{j+1}$ for some j. We will show that $j = i$. Write $M = L(\sqrt[p]{v})$, and we therefore have a tower $K \subset L \subset M$ of totally ramified degree p extensions. Using Takemoto's computation of the Hasse–Herbrand function ([27, Lemma 2.2 (2)]), we have

$$\psi_{L/K}(t) = \begin{cases} t, & 0 \leq t \leq pe_0(K) - i \\ pt - pe_K + (p-1)i, & pe_0(K) - i \leq t, \end{cases}$$

$$\psi_{M/K}(t) = \begin{cases} t, & 0 \leq t \leq pe_0(K) - i \\ pt - pe_K + (p-1)i, & pe_0(K) - i \leq t \leq pe_0(K) + e_K - i \\ p^2t - 2p^2e_K + (p^2-1)i, & pe_0(K) + e_K - i \leq t \end{cases}$$

and

$$\psi_{M/L}(t) = \begin{cases} t, & 0 \leq t \leq p^2e_0(K) - j \\ pt - p^2e_K + (p-1)j, & p^2e_0(K) - j \leq t \end{cases}$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

The function $\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}$ is non-differentiable at two points in $(0, \infty)$; one corresponds to the unique point where $\psi_{L/K}$ is non-differentiable, $pe_0(K) - i$, and the other corresponds to the unique point where $\psi_{M/L}$ is non-differentiable. On one hand, the 2nd point where $\psi_{M/K}$ is non-differentiable is $\tilde{t} = pe_0(K) + e_K - i$. On the other hand, $\psi_{M/L}$ is non-differentiable at $p^2 e_0(K) - j$, so we have

$$\psi_{L/K}(\tilde{t}) = p^2 e_0(K) - j.$$

Using Takemoto's formula for $\psi_{L/K}$ and the fact that $\tilde{t} > pe_0(K) - i$, we get

$$\begin{aligned} p^2 e_0(K) - j &= \psi_{L/K}(pe_0(K) + e_K - i) \\ &= p(pe_0(K) + e_K - i) - pe_K + (p-1)i \\ &= p^2 e_0(K) - i. \end{aligned}$$

Hence we conclude that $i = j$. ∎

Theorem 3.24. Let E_1, E_2 be elliptic curves with good reduction over K, where E_1 has ordinary reduction, and E_2 has supersingular reduction. There exists a positive integer $N \geq 1$ such that the group $p^N K(K; E_1, E_2)$ is p-divisible. In particular, the Albanese kernel of the product $X = E_1 \times E_2$ is the direct sum of a finite group and a divisible group.

Proof. We start by extending the base field K to a finite extension K_1, which is such that,

- $E_i[p] \subset E_i(K_1)$, for $i = 1, 2$,
- $\mu_{p^2} \subset K_1$,
- $\hat{E}_1[p^n] \subset \hat{E}_1(\mathcal{O}_{K_1})$ for some $n \geq 1$ and n is the largest with this property.

We consider a p^n-torsion point $w_0 \in \hat{E}_1[p^n]$ such that w_0 does not lie in the image of $[p] : \hat{E}_1(\mathcal{O}_{K_1}) \to \hat{E}_1(\mathcal{O}_{K_1})$. Simply speaking, $\frac{1}{p} w_0 \notin E_1(K_1)$. We consider the decomposition $E_1(K_1)/p \simeq \overline{U}^0_{K_1} \oplus \overline{U}^{pe_0(K_1)}_{K_1}$ and we write $w_0 = (w_{0,1}, w_{0,2})$. Assume that $w_{0,1} \in \overline{U}^i_{K_1} \setminus \overline{U}^{i+1}_{K_1}$ for some $0 \leq i \leq pe_0(K_1)$. Let $t = t(K_1)$ be the t-invariant of the elliptic curve E_2 over K_1. If $i \leq \min\{pt(K_1), p(e_0(K_1) - t(K_1))\}$, then we can imitate the method of Proposition 3.21 to find elements $b_1, b_2 \in E_2(K_1)/p$ such that $\{w_0, b_1\}_{K_1/K_1}$ and $\{w_0, b_2\}_{K_1/K_1}$ generate $K(K_1; E_1, E_2)/p$. Using Remark 3.7, in this case, we get that the group $p^n K(K_1; E_1, E_2)$ is p-divisible.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

If the index i does not satisfy the above inequality, we perform the following algorithmic process. By extending the base field if necessary, we may assume that the extension $L_1 = K_1(\frac{1}{p}w_0)/K_1$ has wild ramification. This in particular means that the index i is coprime to p. Note that this will always happen eventually (see Corollary 3.16). We fix an element $w_1 \in \hat{E}_1(\mathcal{O}_{L_1})$ such that $[p]w_1 = w_0$. Moreover we write $w_1 = (w_{1,1}, w_{1,2}) \in E_1(L_1)/p$. The claim is that $w_{1,1} \in \overline{U}^i_{L_1} \setminus \overline{U}^{i+1}_{L_1}$. This follows by Lemma 3.23. Note that in order to apply this lemma, we needed to assume $\mu_{p^2} \subset K_1$.

Next, notice that $e_0(L_1) = pe_0(K_1)$ and $t(L_1) = pt(K_1)$. We check again whether

$$i \leq \min\{p^2 t(K_1), p^2(e_0(K_1) - t(K_1))\}.$$

If not, we repeat the process, adding more torsion points of the formal group until we find a finite extension L_r such that $i \leq \min\{p^{r+1}t(K_1), p^{r+1}(e_0(K_1) - t(K_1))\}$. We conclude that for some $r \geq 0$ the group $p^{n+r}K(L_r; E_1, E_2)$ is p-divisible.

To finish the argument, we need to show that Theorem 1.2 holds for the product $X = E_1 \times E_2$. Let $s = [L_r : K] = p^l \cdot m$, where m is coprime to p. Let $x \in K(K; E_1, E_2)$. We have, $s \cdot x = N_{L_r/K}(\mathrm{res}_{L_r/K}(x))$. Set $y = m \cdot x$ and $v = \mathrm{res}_{L_r/K}(x) \in K(L_r; E_1, E_2)$, so that we have an equality $p^l y = N_{L_r/K}(v)$. By the previous step, we get

$$p^{l+n+r}y = N_{L_r/K}(p^{n+r}v) \equiv 0 \bmod p^{l+n+r+1}N_{L_r/K}(K(L_r; E_1, E_2)).$$

Since the K-group $K(K; E_1, E_2)$ is m-divisible ([18, Theorem 3.5]), the above relation holds for every $y \in K(K; E_1, E_2)$. We can therefore set $N = l + n + r$ to make the statement of the theorem true. ■

3.3 When one curve is a Tate elliptic curve

In this section we extend our computations to the case when at least one of the two curves is a Tate elliptic curve. When both E_1, E_2 are Tate curves, the injectivity of $K(K; E_1, E_2)/n \to H^2(K, E_1[n] \otimes E_2[n])$ has been proved by Yamazaki ([29]), for every $n \geq 1$. We therefore assume that E_1 is a Tate elliptic curve and E_2 has good reduction.

We want to proceed as in the previous subsections, giving sufficient (and for the Mackey functor necessary) criteria for the map

$$K(K; E_1, E_2)/p^n \xrightarrow{s_{p^n}} H^2(K, E_1[p^n] \otimes E_2[p^n])$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

to be injective. In this case it suffices to consider only the injectivity of s_p when $\mu_p \subset K$ and the q-invariant of E_1 is not a pth power. Indeed, if $q = q'^{p^n}$ for some $q' \in \mathfrak{m}_K$ that is not a pth power and some $n \geq 1$, we can replace E_1 with the isogenous elliptic curve $E_1' = \mathbb{G}_m/q'^{\mathbb{Z}}$. Namely, the p^n-power map gives an isogeny, $E_1' \xrightarrow{\phi} E_1$, which induces a map on K-groups,

$$K(K; E_1', E_1) \xrightarrow{\phi} K(K; E_1, E_2).$$

The image of ϕ is exactly the subgroup $p^n K(K; E_1, E_2)$. We conclude that proving that the group $p^n K(K; E_1, E_2)$ is p-divisible is equivalent to proving that the K-group $K(K; E_1', E_2)$ is p-divisible.

We start by fixing a uniformizer π_K of K. The analogue of Theorem 3.14 and Proposition 3.21 in this case is given by the following proposition.

Proposition 3.25. Let E_1, E_2 be elliptic curves over K such that E_1 is a Tate curve and E_2 has good reduction. Assume $\mu_p \subset K$ and $\hat{E}_2[p] \subset E_2(K)$. Moreover, suppose that E_1 has invariant $q \in \mathfrak{m}_K$ such that $\sqrt[p]{q} \notin K$.

(1) If E_2 has ordinary reduction, then a necessary and sufficient condition for the injectivity of the Mackey functor Galois symbol

$$(E_1 \otimes^M E_2)(K)/p \xrightarrow{s_p} H^2(K, E_1[p] \otimes E_2[p])$$

is that $q \in \mathfrak{m}_K^i \setminus \mathfrak{m}_K^{i+1}$ for some i coprime to p.

(2) If E_2 has supersingular reduction with $E_2[p] \subset E_2(K)$ and E_2 has invariant $t(K)$, then a necessary and sufficient condition for the injectivity of the Mackey functor Galois symbol s_p is that q can be written as $q = \pi_K^i u$, with either i coprime to p, or $u \in \overline{U}_K^j \setminus \overline{U}_K^{j+1}$ with $j \leq \min\{pt(K), p(e_0(K) - t(K))\}$.

In the above cases, the K-group $K(K; E_1, E_2)$ is p-divisible.

Proof. The two cases are very similar, therefore we only prove the proposition when E_2 has ordinary reduction. We first prove that, if $q \in \mathfrak{m}_K^i \setminus \mathfrak{m}_K^{i+1}$ for some i coprime to p, then $K(K; E_1, E_2)$ is p-divisible.

We have an exact sequence of Mackey functors $\mathbb{G}_m/p \xrightarrow{\varepsilon} E_1/p \to 0$. Since the functor $\otimes^M E_2/p$ is right exact, we get a surjection, $(\mathbb{G}_m/p \otimes^M E_2/p)(K) \xrightarrow{\varepsilon} (E_1/p \otimes^M E_2/p)(K)$. We want to show that the group $(E_1/p \otimes^M E_2/p)(K)$ vanishes. Since we assumed that $\sqrt[p]{q} \notin K$, the above map ε has a kernel generated by the image of q. We can proceed

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

similarly to the proof of the 2nd part of Theorem 3.14. Namely, we will show that the group $(\mathbb{G}_m/p \otimes^M E_2/p)(K)$ is generated by symbols of the form $\{q, x\}_{K/K}$ with $x \in E_2(K)$. Since we assumed that $\hat{E}_2[p] \subset E(K)$, we have an exact sequence of Mackey functors,

$$\overline{U}^0 \to E_2/p \to [E_2/\hat{E}_2]/p \to 0,$$

where $[E_2/\hat{E}_2]$ is the Mackey functor defined in Theorem 3.14. Since $\mathbb{G}_m/p\otimes^M$ is right exact, we obtain an exact sequence

$$\mathbb{G} : m/p \otimes^M \overline{U}^0 \to \mathbb{G} : m/p \otimes^M E_2/p \to \mathbb{G} : m/p \otimes^M [E_2/\hat{E}_2]/p \to 0. \tag{3.26}$$

It suffices therefore to show that the groups $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$ and $(\mathbb{G}_m/p \otimes^M [E_2/\hat{E}_2]/p)(K)$ can be generated by symbols of the form $\{q, x\}_{K/K}$ with $x \in \overline{U}^0_K$ and $x \in [E_2/\hat{E}_2]/p(K)$, respectively.

By [8, Lemma 3.3], $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$ is isomorphic to $\mathbb{Z}/p$ via the classical Galois symbol g_p. Since we assumed that $q \in \mathfrak{m}_K^i \setminus \mathfrak{m}_K^{i+1}$ for some i coprime to p, we can write $q = \pi_K^i v$, for some unit $v \in U_K^0$. We consider the extension $L = K(\sqrt[p]{\pi_K})$. According to [27, Lemma 2.2 (1)], this extension is totally ramified of degree p whose Galois group $\mathrm{Gal}(L/K)$ has a jump at the ramification filtration at $pe_0(K)$. By [21, page 86, Corollary 7], there exists $x \in U_K^{pe_0(K)}$ such that $g_p(\{\pi_K, x\}_{K/K}) \neq 0$. Therefore, $\{\pi_K, x\}_{K/K}$ generates $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$. We claim that $\{q, x\}_{K/K}$ also generates $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$. Indeed, observe that $\{q, x\}_{K/K} = i\{\pi_K, x\}_{K/K} + \{v, x\}_{K/K}$, and, since $K(\sqrt[p]{x})/K$ is unramified, $\{v, x\}_{K/K} = 0$. Since i is coprime to p and $\{\pi_K, x\}_{K/K} \neq 0$, we get $\{q, x\}_{K/K} \neq 0$. It follows that $\{q, x\}_{K/K}$ generates $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$.

The computation for $(\mathbb{G}_m/p \otimes^M [E_2/\hat{E}_2]/p)(K)$ is similar, so we omit it.

We next want to show that the condition on the invariant q is necessary for the injectivity of s_p at the level of the Mackey product, $(E_1/p \otimes^M E_2/p)(K)$. We assume that $q = \pi_K^{p^s} v$, for some $s \geq 1$ and some unit $v \in \mathcal{O}_K^\times$ that is not a pth power. In this case we claim that the group $(E_1 \otimes^M E_2)/p$ contains $\mathbb{Z}/p$, while $s_p = 0$. The proof is very similar to the proofs of Proposition 3.15 and Proposition 3.22, so we only sketch the argument here.

The 1st claim follows by the sequence (3.26). Namely, we can show that the map

$$(\langle q \rangle \otimes^M E_2/p)(K) \to (\mathbb{G} : m/p \otimes^M [E_2/\hat{E}_2]/p)(K)$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

vanishes. On the other hand, the group $(\mathbb{G}_m/p \otimes^M \overline{U}^0)(K)$ can be generated by a symbol of the form $\{q, x\}_{K/K}$, unless the unit v is in $\overline{U}_K^{pe_0(K)}$.

To show that the map s_p vanishes, we need to compute again the orthogonal complement of $\mathrm{Im}(s_p)$ under Tate duality. We claim that this complement coincides with the following subgroup of $\mathrm{Hom}_{G_K}(E_1[p], E_2[p])$, $\{f \in \mathrm{Hom}_{G_K}(E_1[p], E_2[p]) : f(\mu_p) = 0\}$. The claim follows by the following commutative diagram,

$$\begin{array}{ccc} (\mathbb{G}_m/p \otimes^M E_2/p)(K) & \xrightarrow{s_p} & H^2(K, \mu_p \otimes E_2[p]) \\ \downarrow \varepsilon & & \downarrow \\ (E_1/p \otimes^M E_2/p)(K) & \xrightarrow{s_p} & H^2(K, E_1[p] \otimes E_2[p]) \end{array}$$

We already saw that the map ε is surjective. Note that the top s_p is also surjective. This follows by [2, Theorem 2.9]. The rest of the argument is the same as in Proposition 3.2. ■

We end this section with the analogue of Theorem 3.24.

Corollary 3.27. Let E_1 be a Tate curve and E_2 a supersingular reduction elliptic curve. Then the Albanese kernel of the product $X = E_1 \times E_2$ is the direct sum of a finite group and a divisible group.

Proof. By [18, Theorem 3.5] we have an isomorphism, $T(E_1 \times E_2) \simeq D \oplus F$, where D is a group that is m-divisible for every integer m coprime to p and F is a finite group. Let M be the order of F. It suffices to show that the group $M \cdot T(E_1 \times E_2)$ is the direct sum of a p-divisible group and a finite group. To do this we imitate the proof of Theorem 3.24, which applies almost verbatim. In fact it becomes even easier, since we can construct a tower of finite extensions, $L_r \supset \cdots \supset L_1 \supset K$, by attaching roots of unity, $\{\zeta_{p^n} : n_0 \leq n \leq n_0 + r\}$, which are considered as torsion points of the Tate curve E_1. Lemma 3.23 reassures that after attaching a finite number of roots of unity the assumptions of Proposition 3.25 will eventually hold over L_r. The rest of the proof is exactly the same as Theorem 3.24 but now applied to the m-divisible group D. ■

3.4 The product of more than two curves

To finish the proof of theorems (1.2) and (1.4), we need to consider also the case of the K-group $K(K; E_1, \cdots, E_r)$ attached to more than two elliptic curves. Everything will follow

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

from the next corollary, which generalizes previous computations of Raskind and Spiess ([18, Theorem 4.5, Remark 4.4.5]) and Hiranouchi ([8, Proposition 4.3]).

Corollary 3.28. Let $E_1, \cdots, E_r$ be elliptic curves over K with split semistable reduction. Assume that E_1 does not have supersingular reduction and if E_i has supersingular reduction for some $i \geq 2$, then $E_i[p] \subset E_i(K)$. If $r \geq 3$, the K-group $K(K; E_1, \cdots, E_r)$ is p-divisible.

Proof. We will show that the Mackey product, $(E_1/p \otimes^M \cdots \otimes^M E_r/p)(K) = 0$. Using associativity of the product, it suffices to prove the claim when $r = 3$. Moreover, using the surjectivity of the norm, we may assume that $\mu_p \subset K$ and if E_i has ordinary reduction for some $i \in \{2, 3\}$, then $\hat{E}_i[p] \subset E_i(K)$.

We will prove the corollary in the following two specific cases to illustrate the method. Any other case can be proved in a very analogous way.

- Assume that all three curves have good ordinary reduction. Imitating the proof of Theorem 3.14, we can prove a surjection of Mackey functors,

$$\overline{U}^0 \otimes^M \overline{U}^0 \otimes^M \overline{U}^0 \to (E_1 \otimes^M E_2 \otimes^M E_3)/p \to 0.$$

  The claim then follows after we observe that the functor $\overline{U}^0 \otimes^M \overline{U}^0 \otimes^M \overline{U}^0$ vanishes by [18, Lemma 4.2.1].
- Assume that E_1 has ordinary reduction and E_2, E_3 have supersingular reduction. Since we assumed that $E_i[p] \subset E_i(K)$ for $i = 2, 3$, we can use Theorem 2.15 to compute the Mackey functors E_i/p. We consider the product $(E_1 \otimes^M E_2)/p$. By Proposition 3.21 and Proposition 3.22 we get that this product is either 0 or isomorphic to a direct sum of Mackey functors of the form $\overline{U}^0 \otimes^M \overline{U}^s$ for some $s > 0$. By [8, Lemma 3.3] we get an isomorphism,

$$\overline{U}^0 \otimes^M \overline{U}^s \simeq (\mathbb{G} : m \otimes^M \mathbb{G} : m)/p \simeq \overline{U}^0 \otimes^M \overline{U}^0.$$

  Therefore the Mackey functor, $(E_1 \otimes^M E_2 \otimes^M E_3)/p$ can be decomposed in direct pieces that look like $\overline{U}^0 \otimes^M \overline{U}^0 \otimes^M E_3/p$. By imitating the argument for the product $\overline{U}^0 \otimes^M E_3/p$, the claim follows once again by [18, Lemma 4.2.1]. ∎

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

3.5 The Brauer–Manin pairing

We close this section by discussing a corollary about the Brauer–Manin pairing,

$$CH_0(X) \times Br(X) \to \mathbb{Q}/\mathbb{Z}$$

between the group $CH_0(X)$ and the Brauer group, $Br(X)$ of X. This corollary follows directly by the work by Yamazaki ([29, Theorem 1.2]).

Corollary 3.29. Let $E_1, \cdots, E_r$ be elliptic curves over a p-adic field K with good reduction and such that at least one does not have supersingular reduction. Let $X = E_1 \times \cdots \times E_r$. There is a finite extension L of K such that the left kernel of the Brauer–Manin pairing

$$CH_0(X \times_K L) \times Br(X \times_K L) \to \mathbb{Q}/\mathbb{Z}$$

is the maximal divisible subgroup of $CH_0(X \times_K L)$.

Proof. Yamazaki showed the left kernel of the pairing

$$CH_0(X) \times Br(X) \to \mathbb{Q}/\mathbb{Z}$$

is the maximal divisible subgroup of $CH_0(X)$ if and only if the cycle map c_{p^n} is injective for every $n \geq 1$. The corollary then follows by Theorem 1.4. ■

4 Applications Over Number Fields

We close this paper by suggesting a conjecture for varieties defined over algebraic number fields. In this section, K shall denote a number field. We will denote by Ω the set of all places of K.

Conjecture 4.1. Let X be smooth projective geometrically connected variety over a number field K such that X has a K-rational point. Let $X_v := X \times_K K_v$ be the base change to the completion, K_v, at a finite place v of K. If the Albanese kernel, $T(X_v)$, is the direct sum of a divisible group, D_v, and a finite group, F_v, then $T(X_v)$ is divisible for almost all finite places v of K, that is $F_v = 0$ for almost all places v.

We already saw that even the local picture has only been established in very few cases. However, we saw that for $X = E_1 \times \cdots \times E_d$ a product of elliptic curves over a

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

p-adic field K_v, Conjecture 1.1 has been established in most cases. We will focus on this case to provide two pieces of evidence towards Conjecture 4.1.

Complex multiplication

The 1st evidence comes from Theorem 3.14. In fact, the following is a direct corollary of Proposition 3.20

Corollary 4.2. Let $X = E \times E$ be the self-product of an elliptic curve over an algebraic number field K. Assume that E has complex multiplication by an imaginary quadratic field M. Then the Albanese kernel, $T(X_v)$, is divisible for almost all ordinary reduction places v of K.

Proof. Let v be an ordinary reduction place of X. Assume that v lies above a rational prime p. The corollary follows immediately from Proposition 3.20 after we observe that for all but finitely many v the extension $K_v/\mathbb{Q}_p$ is unramified. ■

Local-to-global expectations

Our 2nd motivation for Conjecture 4.1 comes from a local-to-global conjecture for zero cycles and its compatibility with a famous conjecture of Beilinson ([1]) and Bloch ([3]). The latter predict that for a smooth projective geometrically connected variety X over a number field K, the Albanese kernel $T(X)$ is a finite group. On the other hand, the Brauer–Manin pairing gives rise to a complex

$$\widehat{A_0(X)} \xrightarrow{\Delta} \widehat{A_{0,\mathbf{A}}(X)} \to \mathrm{Hom}(Br(X)/Br(K), \mathbb{Q}/\mathbb{Z}),$$

where for an abelian group M we denote by $\widehat{M} := \varprojlim_n M/nM$. The *adelic Chow group*, $A_{0,\mathbf{A}}(X)$, is defined to be $\prod_{v \text{ finite}} A_0(X_v)$ when K is a totally imaginary number field. In the general case it has a more complicated expression. It was originally proposed by Colliot-Thélène and Sansuc ([5, Section 4]) that for geometrically rational varieties the above complex is exact. This conjecture was later generalized to arbitrary varieties by blackKato and Saito ([13, 7.6.2], see also [19, page 394]). For more information on the local-to-global conjecture we refer to [4, Conjéctures 1.5] and [28, Section 2.6].

From now on suppose $X = E_1 \times E_2$ is the product of two elliptic curves over K. Restricting the above complex to the Albanese kernel gives rise to a complex,

$$K(\widehat{K; E_1}, E_2) \xrightarrow{\Delta} K(K; \widehat{E_{1v}}, E_{2v}) \to \mathrm{Hom}(Br(X)/Br_1(X), \mathbb{Q}/\mathbb{Z}),$$

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

where $Br_1(X) := \ker(Br(X) \to Br(X_{\overline{K}}))$. By a result of Skorobogatov and Zarhin ([24]) the quotient $Br(X)/Br_1(X)$ is finite. Assuming Conjecture 1.1 is true for X, it implies that the middle term of the complex is an infinite product of finite groups. The only way that all three conjectures are compatible with each other is if in the group $K(K;\widehat{E_{1v}, E_{2v}})$ only finitely many places give nontrivial contribution. That is, the group $K(K;E_{1v},E_{2v})$ should be divisible for all but finitely many places v of K.

Acknowledgments

We would like to express our sincere gratitude to Professors Bhargav Bhatt, Spencer Bloch, Jean-Louis Colliot-Thélène, Toshiro Hiranouchi, Kazuya Kato, Shuji Saito, and Takao Yamazaki for their interest in our work and their helpful comments and suggestions. We are particularly grateful to T. Yamazaki for pointing out a mistake in an earlier version of this paper. Finally, we would like to thank our referees for pointing out inaccuracies and providing many useful suggestions that helped improve significantly the paper. The first author was partially supported by the NSF grant DMS-2001605.

References

[1] Beilinson, A. A. "Higher Regulators and Values of L-Functions." *Current Problems in Mathematics*, vol. 24, Itogi Nauki i Tekhniki. 181, 1984–238. Moscow: Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform.

[2] Bloch, S. "Algebraic K-theory and classfield theory for arithmetic surfaces." *Ann. Math. (2)* 114 (1981): 229–65.

[3] Bloch, S. "Algebraic cycles and values of L-functions." *J. Reine Angew. Math.* 350 (1984): 94–108.

[4] Colliot-Thélène, J.-L. "L'arithmétique du groupe de Chow des zéro-cycles." *J. Théor. Nombres Bordeaux* 7 (1995): 51–73. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[5] Colliot-Thélène, J.-L. and J.-J. Sansuc. "On the Chow groups of certain rational surfaces: a sequel to a paper of S." *Bloch. Duke Math. J.* 48 (1981): 421–47.

[6] Esnault, H. and O. Wittenberg. "On the cycle class map for zero-cycles over local fields." *Ann. Sci. Éc. Norm. Supér. (4)* 49 (2016): 483–520. With an appendix by Spencer Bloch.

[7] Gazaki, E. "A finer Tate duality theorem for local Galois symbols." *J. Algebra* 509 (2018): 337–85.

[8] Hiranouchi, T. "Milnor K-groups attached to elliptic curves over a p-adic field." *Funct. Approx. Comment. Math.* 54 (2016): 39–55.

[9] Hiranouchi, T. and S. Hirayama. "On the cycle map for products of elliptic curves over a p-adic field." *Acta Arith.* 157 (2013): 101–18.

[10] Ivorra, F. and K. Rülling. "K-groups of reciprocity functors." *J. Algebraic Geom.* 26 (2017): 199–278.

[11] Kahn, B. "Nullité de certains groupes attachés aux variétés semi-abéliennes sur un corps fini; application." *C. R. Math. Acad. Sci. Paris Sér. I* 314 (1992): 1039–42.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023

[12] Kahn, B. and T. Yamazaki. "Voevodsky's motives and Weil reciprocity." *Duke Math. J.* 162 (2013): 2751–96.

[13] Kato, K. and S. Saito. "Global Class Field Theory of Arithmetic Schemes." *Applications of Algebraic K-Theory to Algebraic Geometry and Number Theory, Part I, II (Boulder, Colo., 1983)*, vol. 55 of Contemp. Math. 255–331. Providence, RI: Amer. Math. Soc., 1986.

[14] Katz, N. M. and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1985.

[15] Kawachi, M. "Isogenies of degree p of elliptic curves over local fields and Kummer theory." *Tokyo J. Math.* 25 (2002): 247, 12–59.

[16] Mazur, B. "Rational points of abelian varieties with values in towers of number fields." *Invent. Math.* 18 (1972): 183–266.

[17] Murre, J. and D. Ramakrishnan. "Local Galois Symbols on E x E." *Motives and Algebraic Cycles*, vol. 56 of Fields Inst. Commun. 257–91. Providence, RI: Amer. Math. Soc., 2009.

[18] Raskind, W. and M. Spiess. "Milnor K-groups and zero-cycles on products of curves over p-adic fields." *Compos. Math.* 121 (2000): 1–33.

[19] Saito, S. "Some observations on motivic cohomology of arithmetic schemes." *Invent. Math.* 98 (1989): 371–404.

[20] Saito, S. and K. Sato. "A finiteness theorem for zero-cycles over p-adic fields." *Ann. Math. (2)* 172 (2010): 1593–639. With an appendix by Uwe Jannsen.

[21] Serre, J.-P. *Local fields*, vol. 67 of Graduate Texts in Mathematics. 1979.

[22] Serre, J.-P. "Abelian l-adic representations and elliptic curves," vol. 7 of *Research Notes in Mathematics*. Wellesley, MA: A K Peters, Ltd, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[23] Silverman, J. H. "The Arithmetic of Elliptic Curves," vol. 106 of Graduate Texts in Mathematics, 2nd edn. Dordrecht: Springer, 2009.

[24] Skorobogatov, A. N. and Y. G. Zarhin. "The Brauer group and the Brauer–Manin set of products of varieties." *J. Eur. Math. Soc. (JEMS)* 16 (2014): 749–68.

[25] Somekawa, M. "On Milnor K-groups attached to semi-abelian varieties." *K-Theory* 4 (1990): 105–19.

[26] Spiess, M. and T. Yamazaki. "A counterexample to generalizations of the Milnor–Bloch–Kato conjecture." *J. K-Theory* 4 (2009): 77–90.

[27] Takemoto, T. *Zero-Cycles on Products of Elliptic Curves Over p-adic Fields*. 2007.

[28] Wittenberg, O. "Rational Points and Zero-Cycles on Rationally Connected Varieties Over Number Fields." *Algebraic Geometry: Salt Lake City 2015*, vol. 97 of Proc. Sympos. Pure Math. 597–635. Providence, RI: Amer. Math. Soc., 2018.

[29] Yamazaki, T. "On Chow and Brauer groups of a product of Mumford curves." *Math. Ann.* 333 (2005): 549–67.

Downloaded from https://academic.oup.com/imrn/article/2022/14/10586/6175325 by University of Virginia Library user on 22 February 2023