

RELATIVE BRAUER GROUPS OF GENUS 1 CURVES*

BY

MIRELA CIPERIANI

*Department of Mathematics, University of Texas at Austin
Austin, TX 78712, USA
e-mail: mirela@math.utexas.edu*

AND

DANIEL KRASHEN

*Department of mathematics, University of Georgia, Athens
Athens, GA 30602, USA
e-mail: dkrashen@math.uga.edu*

ABSTRACT

In this paper we develop techniques for computing the relative Brauer group of curves, focusing particularly on the case where the genus is 1. We use these techniques to show that the relative Brauer group may be infinite (for certain ground fields) as well as to determine this group explicitly for certain curves defined over the rational numbers. To connect to previous descriptions of relative Brauer groups in the literature, we describe a family of genus 1 curves, which we call “cyclic type” for which the relative Brauer group can be shown to have a particularly nice description. In order to do this, we discuss a number of formulations of the pairing between the points on an elliptic curve and its Weil–Chat et group into the Brauer group of the ground field, and draw connections to the period-index problem for genus 1 curves.

* The authors would like to thank Brian Conrad and Adrian Wadsworth for helpful conversations and suggestions during the writing of this paper. Thanks also to Peter Clark for many valuable suggestions and corrections. Finally, we would like to thank the anonymous referee for a number of helpful comments and corrections. Received August 27, 2010 and in revised form July 11, 2011

1. Introduction

Let X be a smooth projective curve of genus 1 over a field k . The main objects of study in this paper are the elements of the Brauer group of k which are split by the function field of X , i.e., the kernel of the natural homomorphism $\text{Br}(k) \rightarrow \text{Br}(k(X))$. These elements form a subgroup which we call the relative Brauer group of X . This group is of interest both from the point of view of studying the curve X as well as from the point of view of field arithmetic and the structure of division algebras. From the perspective of the curve X , one may interpret the relative Brauer group as an obstruction to the existence of a rational point, related to the so-called “elementary obstruction.” In addition, it is closely related to the period-index problem. From the point of view of field arithmetic and division algebras, this type of splitting information for function fields, and more generally index reduction formulas as in [MPW96], play an important role in constructing examples and counterexamples (such as Merkurjev’s construction of fields with various u -invariants [Lam89]). Unfortunately, such information is only known for very special varieties at this point, such as for projective homogeneous varieties under a linear algebraic group. In particular, in the case of curves, until recently, one only had a complete description of the relative Brauer group when the genus was 0. In [Han03], the relative Brauer groups of certain genus 1 hyperelliptic curves were described in a surprisingly tractable way.

In this paper we introduce tools for computing these relative Brauer groups, and we introduce the notion of a curve of “cyclic type” in order to explain when particularly nice descriptions of the relative Brauer group may be given as in [Han03]. The present paper has been used in [HHW10] to obtain explicit descriptions of the relative Brauer group for certain plane cubic curves, and in [Kuo], which uses generalized Clifford algebra constructions to study a somewhat more general class of curves. These tools are also applied to the period-index problem and the elementary obstruction.

A main ingredient in this paper is a number of reformulations of the pairing of Tate relating to points on an elliptic curve and the elements of its Tate–Shafarevich group. Some of these results appear in the literature, and we cite results of Bashmakov [Baš72] and Lichtenbaum [Lic69] to obtain some of these. Although we don’t make the claim that the other reformulations in this paper are necessarily new, we were unable to obtain references in the literature after

talking to experts in the area, and in any case, we believe that it is of value to collect some of these results together as we do here.

The contents of this paper are as follows. Section 2 presents the basic relationship between the relative Brauer group, the Picard variety and the period-index problem in terms of a surjective map

$$\mathbf{a}_X : \mathbf{Pic}(X)(k) \rightarrow \text{Br}(k(X)/k)$$

for a smooth projective variety X over k . In Section 3 we give a number of different interpretations of the map \mathbf{a}_X in terms of pairings and in Section 4 we use these to give a number of applications: In Section 4.1 we show that if X is a homogeneous space for an elliptic curve E of cyclic type (Definition 4.2) with respect to the subgroup $T \subset E$, then we have an exact sequence (generalizing [Han03]), where $E' = E/T$,

$$E'(k) \xrightarrow{\phi} E(k) \xrightarrow{\mathbf{a}_X} \text{Br}(k(X)/k) \longrightarrow 0,$$

and where ϕ is dual to the isogeny with kernel T . We further give an interpretation of the map \mathbf{a}_X in terms of a natural cup product. In Section 4.2, we give a generalization of a result of Cassels ([Cas62]) that the period and index must coincide for an element of the Tate–Shafarevich group. In Section 4.3 we relate the relative Brauer group to the elementary obstruction (see Definition 1.4) and prove

THEOREM 4.9: *Suppose X is a homogeneous space for an elliptic curve E defined over k and $X(k) = \emptyset$. Then $\text{Br}(X_{k(E)}/k(E)) \neq 0$ — i.e., the relative Brauer group must be nontrivial when one extends scalars to the function field of E .*

It follows from this (see Corollary 4.10) that if $X(k) \neq \emptyset$ for X as above, then there exists a field extension K/k such that the elementary obstruction for X_K is nontrivial. In Section 4.4 we show that the relative Brauer group of any smooth projective variety X is always finite when k is local or finitely generated over a prime field (Proposition 4.11), however we construct in Theorem 4.12 certain fields k , and genus 1 curves X/k , such that the relative Brauer group $\text{Br}(k(X)/k)$ is infinite.

Finally, in Section 5 we show that the relative Brauer group may be computed algorithmically. The algorithms described in this section have been implemented (in certain cases) as a Macaulay2 [M2] package “Relative Brauer,” freely available at the second author’s webpage [Kra07]. This package uses pari as well [par], and may be used to produce examples of relative Brauer groups for certain homogeneous spaces of elliptic curves defined over \mathbb{Q} . Some of the examples in this paper were produced using this program.

Although this paper is concerned principally with the computation of relative Brauer groups, one is often also interested in the more precise question of how to calculate the index of $\alpha_{k(X)}$ for a general class α in the Brauer group of k . In [KL08], the second author jointly with M. Lieblich has shown that this more general problem of index reduction for a genus 1 curve may be entirely reduced to the problem discussed in this paper of computing the relative Brauer group.

1.1. DEFINITIONS AND NOTATION. Throughout the paper we will consider an arbitrary ground field k , and we will denote by k^{sep} a fixed separable closure. We denote the absolute Galois group $\text{Gal}(k^{sep}/k)$ by G . Unless specified otherwise, all cohomology groups should be interpreted as étale cohomology, and in particular, $H^i(k, A)$ coincides with the Group cohomology $H^i(G, A)$.

Definition 1.1: For a k -scheme X , we define the **index** of X to be

$$\text{ind}(X) = \gcd\{[E : k] \mid E/k \text{ is a finite field extension and } X(E) \neq \emptyset\}.$$

In the case that X is a genus 1 curve, it follows from [Lic68] that this coincides with the same gcd taken only over degrees of separable field extensions.

For a smooth proper variety X , we denote its Picard group by $\text{Pic}(X)$. We define **Pic**(X) to be the sheafification of the *fppf*-presheaf

$$S \mapsto \text{Pic}(X \times_k S).$$

This is represented by a k -group scheme (see [Mur64, II.15]), which, by abuse of notation, we also denote by **Pic**(X). This is projective in case X is (see [FGI+05, Chap. 9, Thm. 9.5.4]). We let $\text{Pic}^0(X)$ denote the subgroup of $\text{Pic}(X)$ consisting of those divisor classes which are algebraically equivalent to 0, and we recall that the Picard variety of X , denoted **Pic**⁰(X), is the corresponding subscheme of **Pic**(X). We recall that **Pic**(X) is an abelian variety if X is either a curve [FGI+05, Chap. 9, Ex. 9.5.23, pages 289, 309] or an abelian variety

[Mum70, III.13]. Since X has a point after some finite separable field extension [Lan72, Prop. 10, page 76], it follows from [FGI+05, Chap. 9, Thm. 9.2.5] that $\mathbf{Pic}(X)$ may be considered also as the étale sheafification of the above presheaf. In particular, we may describe the k -points of $\mathbf{Pic}(X)$ as $\mathbf{Pic}(X)(k) = (\mathbf{Pic}(X_{k^{sep}}))^G$. For every G -fixed element of the Neron–Severi group $\lambda \in \mathbf{NS}(X_{k^{sep}})^G$, we may consider the subscheme $\mathbf{Pic}^\lambda(X) \subset \mathbf{Pic}(X)$ of divisors of X in the class λ . These are principal homogeneous spaces for the abelian variety $\mathbf{Pic}^0(X)$. Note that in the case of a curve, we may identify $\mathbf{NS}(X) = \mathbf{NS}(X_{k^{sep}})^G \cong \mathbb{Z}$ by the degree map on divisors, and hence we may denote classes by integers. We recall that the collection of all principal homogeneous spaces for an abelian variety A/k may be identified with the torsion abelian group $H^1(k, A)$, which is also called the Weil–Châtelet group of A .

Definition 1.2: Let X be a smooth projective curve over k . We define the **period** of X to be the order of the class $[\mathbf{Pic}^1(X)]$ in $H^1(k, \mathbf{Pic}^0(X))$.

For a k -scheme X , we let $\mathrm{Br}(X)$ denote the Brauer group of equivalence classes of Azumaya algebras, and for a ring R , we write $\mathrm{Br}(R)$ for $\mathrm{Br}(\mathrm{Spec}(R))$. In the case X is a smooth and quasi-projective variety, we may identify $\mathrm{Br}(X) = H^2(X, \mathbb{G}_m)$ by the result of Gabber/de Jong (see [dJ]), and we have an injection $\mathrm{Br}(X) \hookrightarrow \mathrm{Br}(k(X))$ (see [Gro68a, Gro68b, Gro68c]).

Definition 1.3: Given a morphism of schemes $Y \rightarrow X$, we define the **relative Brauer group**, written $\mathrm{Br}(Y/X)$, as the kernel of the pullback map $\mathrm{Br}(X) \rightarrow \mathrm{Br}(Y)$.

We will frequently abuse notation and write $\mathrm{Br}(Y/R)$ if $X = \mathrm{Spec}(R)$ is affine, or $\mathrm{Br}(S/R)$ if $Y = \mathrm{Spec}(S)$, and so on.

We recall the definition of the elementary obstruction:

Definition 1.4 ([CTS87, Defn. 2.2.1]): Let X be a smooth geometrically integral variety over k , and consider the exact sequence of Galois modules

$$0 \rightarrow (k^{sep})^* \rightarrow k^{sep}(X)^* \rightarrow k^{sep}(X)^*/(k^{sep})^*.$$

The elementary obstruction $ob(X)$ is by definition the class of this extension of G modules in $\mathrm{Ext}_G^1(k^{sep}(X)^*/(k^{sep})^*, (k^{sep})^*)$.

PROPOSITION 1.5 ([CTS87, Prop. 2.2.2(a)]): *Suppose X is a smooth geometrically integral variety over a field k and $X(k) \neq \emptyset$. Then $ob(X)$ vanishes.*

2. The Picard variety, the period and the index

If X is a smooth projective variety over a field k , there is a well-known natural surjective map

$$\alpha_X : \mathbf{Pic}(X)(k) \rightarrow \text{Br}(k(X)/k)$$

which will be a critical tool in our description of the relative Brauer group. Particularly important will also be the restriction of this map to the divisor classes algebraically equivalent to 0.

We define the map α_X as follows. Consider the short exact sequence of G -modules

$$(1) \quad 0 \longrightarrow k^{sep}(X)^*/(k^{sep})^* \longrightarrow \text{Div}(X_{k^{sep}}) \longrightarrow \text{Pic}(X_{k^{sep}}) \longrightarrow 0.$$

Since $k^{sep}(X)/k(X)$ is a G -Galois extension, we may use Hilbert’s Theorem 90 to identify

$$\begin{aligned} H^1(G, k^{sep}(X)^*/(k^{sep})^*) &\cong \ker(\text{Br}(k) \rightarrow \text{Br}(k(X))) \\ &= \text{Br}(k(X)/k) = \text{Br}(X/k). \end{aligned}$$

Using this, the long exact sequence in cohomology from sequence 1 gives the desired map:

$$\alpha_X : \mathbf{Pic}(X) \rightarrow \text{Br}(k).$$

We now investigate the restriction of this map to the divisor classes of degree 0. Let $\text{NS}(X)$ be the Nerón–Severi group $\text{Div}(X)/\text{Div}^0(X)$, where $\text{Div}^0(X)$ is the group of divisors which are algebraically equivalent to 0. The group $\text{NS}(X_{k^{sep}})$ comes with an action of the Galois group G , and the short exact sequence

$$0 \longrightarrow \text{Pic}^0(X_{k^{sep}}) \longrightarrow \text{Pic}(X_{k^{sep}}) \longrightarrow \text{NS}(X_{k^{sep}}) \longrightarrow 0$$

gives rise to a boundary map

$$\text{NS}(X_{k^{sep}})^G \rightarrow H^1(k, \mathbf{Pic}^0(X)(k^{sep})).$$

Note that $\text{Div}(X_{k^{sep}})^G = \text{Div}(X)$. We define in $\text{NS}(X_{k^{sep}})^G$ two subgroups $i(X)$ and $p(X)$ as follows:

$$\begin{aligned} i(X) &= \text{im}(\text{Div}(X) \rightarrow \text{NS}(X_{k^{sep}})^G) = \text{im}(\text{NS}(X) \rightarrow \text{NS}(X_{k^{sep}})^G), \\ p(X) &= \ker(\text{NS}(X_{k^{sep}})^G \rightarrow H^1(k, \mathbf{Pic}(X))). \end{aligned}$$

These groups have been defined and studied independently by Peter Clark (see [Cla]).

THEOREM 2.1: *Let X be a smooth projective variety over k . Then we have exact sequences*

$$\begin{aligned}
 0 &\longrightarrow \text{Pic}(X) \longrightarrow \mathbf{Pic}(X)(k) \xrightarrow{\alpha_X} \text{Br}(X/k) \longrightarrow 0, \\
 0 &\longrightarrow \text{Pic}^0(X) \longrightarrow \mathbf{Pic}^0(X)(k) \xrightarrow{\alpha_X} \text{Br}(X/k) \longrightarrow p(X)/i(X) \longrightarrow 0.
 \end{aligned}$$

Remark 2.2: If X is a smooth projective curve, this is in essence done by Lichtenbaum in [Lic69]. In this case, we note that $NS(X_{k^{sep}})$ is simply isomorphic to \mathbb{Z} by associating to every divisor its degree. In particular, we observe in this case $i(X) = \text{ind}(X)\mathbb{Z}$. Further, it follows from [Lic69] that the boundary map $NS(X_{k^{sep}})^G \cong \mathbb{Z} \rightarrow H^1(k, \mathbf{Pic}(X))$ sends 1 to the class of the homogeneous space $\mathbf{Pic}^1(X)$, and so we obtain $p(X) = \text{per}(X)\mathbb{Z}$. We therefore see that the failure of surjectivity of $\alpha_X|_{\mathbf{Pic}^0(X)(k)}$ exactly describes the obstruction for the period and index of the curve X to coincide.

COROLLARY 2.3: *Suppose X is a curve with $\text{ind}(X) = \text{per}(X)$. Then the map α is surjective.*

Proof of Theorem 2.1. Identifying $\text{Pic}(X)$ with the image in $\mathbf{Pic}(X)(k) = \text{Pic}(X_{k^{sep}})^G$ of $\text{Div}(X)$, we obtain from the long exact sequence in cohomology from sequence 1

$$0 \rightarrow \text{Pic}(X) \rightarrow \mathbf{Pic}(X)(k) \rightarrow \text{Br}(k) \rightarrow \text{Br}(X),$$

which immediately gives us the first part of the theorem.

For the second part, let $\text{Br}_0(X/k) = \alpha_X(\mathbf{Pic}^0(X)(k))$. Using the morphism of exact sequences:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & k^{sep}(X)^*/(k^{sep})^* & \longrightarrow & \text{Div}^0(X_{k^{sep}}) & \longrightarrow & \text{Pic}^0(X_{k^{sep}}) \longrightarrow 0 \\
 & & \parallel & & \downarrow & & \downarrow \\
 0 & \longrightarrow & k^{sep}(X)^*/(k^{sep})^* & \longrightarrow & \text{Div}(X_{k^{sep}}) & \longrightarrow & \text{Pic}(X_{k^{sep}}) \longrightarrow 0
 \end{array}$$

We obtain an inclusion of short exact sequences:

$$(2) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \text{Pic}^0(X) & \longrightarrow & \mathbf{Pic}^0(X)(k) & \longrightarrow & \text{Br}_0(X/k) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Pic}(X) & \longrightarrow & \mathbf{Pic}(X)(k) & \longrightarrow & \text{Br}(X/k) \longrightarrow 0 \end{array}$$

Using the long exact sequence associated to the sequence

$$0 \longrightarrow \text{Pic}^0(X_{k^{sep}}) \longrightarrow \text{Pic}(X_{k^{sep}}) \longrightarrow \text{NS}(X_{k^{sep}}) \longrightarrow 0$$

we may identify

$$p(X) = \text{coker}(\mathbf{Pic}^0(X) \rightarrow \mathbf{Pic}(X)),$$

and using the sequence

$$0 \longrightarrow \text{Div}^0(X_{k^{sep}}) \longrightarrow \text{Div}(X_{k^{sep}}) \longrightarrow \text{NS}(X_{k^{sep}}) \longrightarrow 0$$

together with the fact that the map $\text{Div}(X) = \text{Div}(X_{k^{sep}})^G \rightarrow \text{NS}(X_{k^{sep}})^G$ factors through the surjective map $\text{Div}(X) \rightarrow \text{Pic}(X)$, we may also identify

$$i(X) = \text{coker}(\text{Pic}^0(X)(k) \rightarrow \text{Pic}(X)(k)).$$

Therefore, applying the snake lemma to sequence 2 gives an exact sequence of cokernels:

$$0 \rightarrow i(X) \rightarrow p(X) \rightarrow \frac{\text{Br}(X/k)}{\text{Br}_0(X/k)} \rightarrow 0,$$

which gives, via the definition of $\text{Br}_0(X/k)$,

$$0 \rightarrow \text{Pic}^0(X) \rightarrow \mathbf{Pic}^0(X)(k) \rightarrow \text{Br}(X/k) \rightarrow p(X)/i(X) \rightarrow 0,$$

as desired. ■

3. Pairings and the map \mathfrak{a}_X

In this section we show that the map \mathfrak{a}_X constructed above may be interpreted in a number of ways in terms of pairings. We will afterwards use these different interpretations to prove new results concerning relative Brauer groups in section 4.

Throughout, we will abuse notation and write \mathfrak{a}_γ instead of \mathfrak{a}_X in the case that X is a genus 1 curve corresponding to a cohomology class $\gamma \in H(k, E)$ for an elliptic curve E .

3.1. THE TATE PAIRING.

THEOREM 3.1 ([Lic68]): *Let A be an abelian variety over a field k , and consider the Tate pairing*

$$\langle \cdot, \cdot \rangle : H^1(k, A) \times \mathbf{Pic}^0(A)(k) \rightarrow \text{Br}(k).$$

In the case A is an elliptic curve, we have $\langle \gamma, p \rangle = \mathfrak{a}_\gamma(p)$.

Proof. This may be found in [Lic68, pages 1213–1216]. Since it is not explicitly stated as a theorem in this paper, we note that on page 1213 of [Lic68], Lichtenbaum defines the pairing due to Tate, on page 1215 he defines the pairing coming from \mathfrak{a} , and in pages 1215–1216 he proves that these coincide. ■

For future reference, let us also recall the definition of the Tate pairing. Let A be an abelian variety over k . Denote by $Z(A)$ the group of 0-dimensional cycles on $A_{k^{sep}}$ of degree 0, and by $Y(A)$ the Albanese kernel of A defined by the exact sequence

$$0 \rightarrow Y(A) \rightarrow Z(A) \rightarrow A(k^{sep}) \rightarrow 0.$$

Let $D \subset A \times \mathbf{Pic}^0(A)$ be a Poincaré divisor and let π_1, π_2 be the projection maps from $A \times \mathbf{Pic}^0(A)$ to A and $\mathbf{Pic}^0(A)$, respectively. We define $Z(A)_D$ (respectively $Y(A)_D$) to be the subgroup of $Z(A)$ (resp. $Y(A)$) of elements α , such that $\pi_1^{-1}(|\alpha|)$ transversely intersects D , where $|\alpha|$ is the support of α . Note that we have a well defined map

$$\pi_2 (\pi_1^{-1}(\cdot) \cap D) : Z(A)_D \rightarrow \text{Div}(\mathbf{Pic}^0(A)_{k^{sep}}).$$

Since this agrees with the cycle theoretic map $(\pi_2)_*(\pi_1^*(\alpha \cdot D))$, and since the elements of $Y(A)$ are rationally equivalent to 0, it follows that the image of this map is always a principal divisor, giving us actually a map

$$\pi_2 (\pi_1^{-1}(\cdot) \cap D) : Y(A)_D \rightarrow k^{sep}(A)^*/(k^{sep})^*.$$

To define the **Tate pairing**, we start with a class $\gamma \in H^1(k, A(\bar{k}))$, and let $\alpha \in H^2(k, Y(A))$ be its image under the connecting homomorphism. Choose a representative cochain $\bar{\alpha}$ for α and choose a Poincaré divisor D transversal to $|\bar{\alpha}|$. Consider the $k^{sep}(A)^*/k^{sep*}$ -valued cocycle $\beta = \pi_2 (\pi_1^{-1}(\bar{\alpha}) \cap D)$. Since $A(k) \neq \emptyset$, the elementary obstruction for A vanishes (Proposition 1.5), and consequently, we may lift the class of β to a class $\tilde{\beta} \in H^2(k, k^{sep}(A)^*)$ which turns out to be unramified — i.e., an element of $H^2(A, \mathbb{G}_m) = \text{Br}(A)$. By

changing $\tilde{\beta}$ by a constant class from $\text{Br}(k)$, we may assume that $\tilde{\beta}$ is trivial when specialized to the identity $0 \in A(k)$. The pairing is then defined by $\langle \gamma, p \rangle = \tilde{\beta}|_p$.

3.2. PAIRING VIA SPECIALIZATIONS OF BRAUER CLASSES. Let X be a smooth projective variety over k with a rational point $x \in X(k)$. Recall that the group $\text{Br}(X_{k^{sep}}/X, x)$ is defined to be the subgroup of $\text{Br}(X_{k^{sep}}/X)$ consisting of those Brauer classes α such that the specialization of α at x is trivial.

LEMMA 3.2: *We have an isomorphism*

$$\begin{array}{ccc}
 H^1(k, \mathbf{Pic}(X)) & \xrightarrow{\sim} & \text{Br}(X_{k^{sep}}/X, x) \\
 \gamma \longmapsto & & \mathcal{A}_\gamma,
 \end{array}$$

defined as follows. Consider the exact sequence

$$(3) \quad 0 \longrightarrow k^{sep}(X)^*/(k^{sep})^* \longrightarrow \text{Div}(X_{k^{sep}}) \longrightarrow \mathbf{Pic}(X)(k^{sep}) \longrightarrow 0.$$

For $\gamma \in H^1(k, \mathbf{Pic}(X))$, take the image of γ under the connecting homomorphism in the first exact sequence. This is an element $\tilde{\gamma} \in H^2(k, \text{Prin}(X)) = H^2(k, k^{sep}(X)^*/(k^{sep})^*)$. Any lift of this class to $H^2(k, k^{sep}(X)^*)$ will be an element of the unramified Brauer group of X , and we define \mathcal{A}_γ to be the unique class in $H^2(k, k^{sep}(X)^*)$ lifting it which is unramified and is trivial when specialized to the point x .

Remark 3.3: Note that we abuse notation here in that \mathcal{A}_γ depends on a particular choice of point x . In the case which will be especially useful to us, X will be an abelian variety, and in this case, we will always take the point x to be the identity $0 \in X(k)$.

Remark 3.4: We will often wish to consider classes γ in $H^1(k, \mathbf{Pic}^0(X))$. We abuse notation in this case and write \mathcal{A}_γ to denote the Brauer class associated to the image of γ in $H^1(k, \mathbf{Pic}(X))$.

We will use this lemma to prove the following alternate formulation of the Tate pairing:

THEOREM 3.5: *Let A be an abelian variety over k , and $B = \mathbf{Pic}^0(A)$ its dual. Let $\alpha \in H(k, B(k^{sep}))$, and choose X_α a homogeneous space in the class α .*

Then for each $p \in A(k)$ we have

$$\langle \alpha, p \rangle = \mathbf{a}_{X_\alpha}(p) = \mathcal{A}_\alpha|_p.$$

We now give a proof of the lemma, followed by a proof of this theorem.

Proof of Lemma 3.2. Since $\text{Div}(X_{k^{sep}})$ has a basis which is permuted by the Galois group, it follows that $H^1(k, \text{Div}(X_{k^{sep}})) = 0$ (see for example [Sal99, Lemma 12.3]). We therefore obtain from (3) an exact sequence

$$(4) \quad 0 \rightarrow H^1(k, \mathbf{Pic}(X)) \rightarrow H^2(k, k^{sep}(X)^*/(k^{sep})^*) \rightarrow H^2(k, \text{Div}(\overline{X})).$$

Using Proposition 1.5, we see that since $X(k) \neq \emptyset$, we have a split exact sequence

$$0 \rightarrow (k^{sep})^* \rightarrow k^{sep}(X)^* \rightarrow k^{sep}(X)^*/(k^{sep})^* \rightarrow 0,$$

and therefore we obtain an exact sequence

$$(5) \quad 0 \rightarrow \text{Br}(k) \rightarrow \text{Br}(k^{sep}(X)/k(X)) \rightarrow H^2(k, k^{sep}(X)^*/(k^{sep})^*) \rightarrow 0.$$

The map $k^{sep}(X) \rightarrow \text{Div}(X_{k^{sep}})$ induces a map

$$\text{ram} : \text{Br}(k^{sep}(X)/k(X)) \rightarrow H^2(k, \text{Div}(X_{k^{sep}}))$$

called the ramification map¹, and $\ker(\text{ram}) = \text{Br}(X)$. Let us denote the kernel of the map

$$H^2(k, k^{sep}(X)^*/(k^{sep})^*) \rightarrow H^2(k, \text{Div}(X_{k^{sep}}))$$

by $H^{2, nr}(k, k^{sep}(X)^*/(k^{sep})^*)$. Using sequence (5) we find we have an exact sequence

$$0 \rightarrow \text{Br}(k) \rightarrow \text{Br}(X_{k^{sep}}/X) \rightarrow H^{2, nr}(k, k^{sep}(X)^*/(k^{sep})^*) \rightarrow 0$$

and an identification $H^{2, nr}(k, k^{sep}(X)^*/(k^{sep})^*) = H^1(k, \mathbf{Pic}(X))$. Again using the fact that X has a rational point, we may use specialization of Brauer classes at the point x to split the map $\text{Br}(k) \rightarrow \text{Br}(X)$, yielding an isomorphism

$$\text{Br}(X_{k^{sep}}/X, x) \cong H^1(k, \mathbf{Pic}(X)),$$

as desired. ■

¹ Although this is perhaps not the standard definition of the ramification map, this definition is shown to be equivalent in [GS06] to the standard one, as defined, for example, in [Sal99, Chapter 10]. Here our map is given in [GS06, Section 6.6] equation (6), page 152, and is reformulated on the following page as being equivalent to (the sum of) the standard ramification maps over all closed points.

Remark 3.6: We note that it follows from this proof that in fact we may express the relative Brauer group $\text{Br}(X_{k^{sep}}/X)$ as a product

$$\text{Br}(X_{k^{sep}}/X) \cong \text{Br}(k) \times H^1(k, \mathbf{Pic}(X)).$$

Further, in the case that X is a curve, $H^1(k, \mathbf{Pic}(X)) = H^1(k, \mathbf{Pic}^0(X))$, which follows from the fact that

$$0 \rightarrow \mathbf{Pic}^0(X)(k^{sep}) \rightarrow \mathbf{Pic}(X)(k^{sep}) \rightarrow \mathbb{Z} \rightarrow 0$$

is split exact (since $X(k) \neq \emptyset$), and $H^1(k, \mathbb{Z}) = 0$.

Proof of Theorem 3.5. It is not hard to check that the operation $\pi_B(\cdot \cap D)$ gives a commutative diagram of sets:

$$\begin{array}{ccccccc}
 (6) & 0 & \longrightarrow & \text{Prin}(B) & \longrightarrow & \text{Div}^0(B) & \longrightarrow & A(k^{sep}) & \longrightarrow & 0 \\
 & & & \uparrow & & \uparrow & & \parallel & & \\
 & & & Y(A)_D & \longrightarrow & Z(A)_D & \longrightarrow & A(k^{sep}) & & \\
 & & & \downarrow & & \downarrow & & \parallel & & \\
 & 0 & \longrightarrow & Y(A) & \longrightarrow & Z(A) & \longrightarrow & A(k^{sep}) & \longrightarrow & 0
 \end{array}$$

where the top and bottom rows are exact sequences of abelian groups with Galois action. The pairing of Tate is obtained by the composition of the connecting homomorphism from the bottom of diagram (6) on elements which lie in the middle row followed by the upwards vertical map, while the pairing using \mathcal{A} uses the connecting homomorphism on the top of the diagram. The result therefore follows immediately from commutativity of the diagram and equality of the rightmost terms. ■

3.3. PAIRINGS VIA TORSION POINTS. For an elliptic curve E over k and an integer n prime to the characteristic of k , we will let e_n denote the Weil pairing $E[n] \otimes_{\mathbb{Z}} E[n] \rightarrow \mu_n$. We let $\delta_n : E(k) \rightarrow H^1(k, E[n])$ denote the boundary map from the Kummer sequence:

$$(7) \quad 0 \rightarrow E[n] \rightarrow E \xrightarrow{n} E \rightarrow 0.$$

THEOREM 3.7: *Let E be an elliptic curve over k , let $p \in E(k)$ and $\gamma \in H^1(k, E[n])$, and let X_γ be a homogeneous space in the class γ . Then*

$$\langle \bar{\gamma}, p \rangle = e_n(\gamma \cup \delta_n p) = \mathfrak{a}_{X_\gamma}(p) = \mathcal{A}_\gamma|_p,$$

where $\bar{\gamma}$ is the image of γ in $H(k, E)$.

Proof. It follows from [Baš72, Prop. 9] that $\langle \overline{\gamma}, p \rangle = e_n(\gamma \cup \delta_n p)$. The remaining assertions follow from Theorem 3.5. ■

4. Applications

4.1. PAIRINGS VIA CYCLIC ISOGENIES. Let E be an elliptic curve, and suppose we are given a finite Galois submodule $T \subset E$. We obtain an isogeny, uniquely defined up to isomorphism [Sil92, III.§4, Prop. 4.12]:

$$(8) \quad 0 \rightarrow T \rightarrow E \xrightarrow{\phi} E' \rightarrow 0,$$

for an elliptic curve E' and a dual isogeny, also unique up to isomorphism [Sil92, III.§6, Thm. 6.1]:

$$(9) \quad 0 \rightarrow T' \rightarrow E' \xrightarrow{\phi'} E \rightarrow 0.$$

We say that $T \subset E$ is cyclic if its points defined over a separable closure are cyclic as an abstract group. In other words, T is a closed reduced subscheme of E such that $T(k^{sep})$ is a cyclic subgroup of $E(k^{sep})$.

PROPOSITION 4.1: *Suppose that $T \subset E$ is a cyclic submodule of order n with n prime to the characteristic of k , and let E', T' be as above. Then there is a natural isomorphism of G -modules:*

$$T \otimes_{\mathbb{Z}} T' \cong \mu_n.$$

Further, if $i : T \rightarrow E[n]$ is the inclusion and $p = \phi|_{E[n]}$, then this isomorphism is given by $t \otimes t' \mapsto e_n(it, p^{-1}t')$.

Proof. If $i : T \rightarrow E[n]$ is the natural inclusion, it is easy to see that we obtain a commutative diagram with exact rows:

$$(10) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & T & \longrightarrow & E & \xrightarrow{\phi} & E' & \longrightarrow & 0 \\ & & \downarrow i & & \parallel & & \downarrow \phi' & & \\ 0 & \longrightarrow & E[n] & \longrightarrow & E & \xrightarrow{n} & E & \longrightarrow & 0 \\ & & \downarrow p & & \downarrow \phi & & \parallel & & \\ 0 & \longrightarrow & T' & \longrightarrow & E' & \xrightarrow{\phi'} & E & \longrightarrow & 0 \end{array}$$

which by the snake lemma (applied to the bottom two sequences) gives a short exact sequence

$$(11) \quad 0 \rightarrow T \xrightarrow{i} E[n] \xrightarrow{p} T' \rightarrow 0,$$

where i is induced by the natural inclusion and p is induced by the map ϕ . Consider the Weil pairing

$$e_n : E[n] \otimes_{\mathbb{Z}} E[n] \rightarrow \mu_n.$$

Since this pairing is alternating, we have $e_n(T, T) = 0$, and so we have an induced non-degenerate pairing $T \otimes_{\mathbb{Z}} E[n]/T \rightarrow \mu_n$. But by equation (11), we obtain a non-degenerate pairing $T \otimes_{\mathbb{Z}} T' \rightarrow \mu_n$. Since this is clearly an isomorphism ignoring the Galois action, this gives an isomorphism of Galois modules $T \otimes_{\mathbb{Z}} T' \cong \mu_n$ as desired. ■

Definition 4.2: Let X be a homogeneous space for E of period $n = \text{per}(X)$. We say that X **has cyclic type** if its cohomology class in $H^1(k, E)$ may be represented as the image of a cocycle $\gamma \in H^1(k, T)$, where $T \subset E$ is a cyclic submodule of order n .

The following observation shows that cyclic homogeneous spaces are somewhat special:

PROPOSITION 4.3: *Suppose X is a cyclic homogeneous space for E . Then $\text{per}(X) = \text{ind}(X)$.*

Proof. Choose a particular Galois cocycle $\bar{\gamma} \in Z^1(G, T)$ representing X . Via Galois descent, we may describe X as given by the curve $E_{k^{sep}}$ equipped with the new Galois action $\sigma \cdot p = \sigma(p) \oplus \bar{\gamma}(\sigma)$. Let $\phi : E \rightarrow E'$ be the isogeny with kernel T . Consider the isogeny $\phi_X : X_{k^{sep}} \rightarrow E'_{k^{sep}}$ given after the above identification by $\phi \times_k k^{sep}$. We claim that this descends to give a morphism $X \rightarrow E'$. To see this we need to check $\sigma(\phi(p)) = \phi(\sigma \cdot p)$. But since $\bar{\gamma}(\sigma) \in T = \ker(\phi)$, we have

$$\phi(\sigma \cdot p) = \phi(\sigma(p) \oplus \bar{\gamma}(\sigma)) = \phi(\sigma(p)) \oplus \phi(\bar{\gamma}(\sigma)) = \phi(\sigma(p)) = \sigma(\phi(p)).$$

Now, since we have a n to 1 étale cover $X \rightarrow E'$, the preimage of the origin in E' gives a separable point in X of degree n over k , and therefore $\text{ind}(X)|n = \text{per}(X)$. But since $\text{per}(X)|\text{ind}(X)$ holds for any curve X , these must be equal. ■

LEMMA 4.4: Let $E, E', T, T', \phi, \phi'$ be as above. Let

$$\delta_{\phi'} : E(k) \rightarrow H^1(k, T')$$

be the boundary map of the exact sequence (8), and let

$$\delta_n : E(k) \rightarrow H^1(k, E[n])$$

be the boundary map from the Kummer sequence (7). Then we have for $\gamma \in H^1(k, T)$ and $x \in E(k)$ (and via the identification of Lemma 4.1)

$$\gamma \cup \delta_{\phi'} x = e_n(i\gamma \cup \delta_n x).$$

Before proving this lemma, we will derive the following consequence, generalizing aspects of the descriptions of the relative Brauer group obtained in [Han03]:

THEOREM 4.5: Let $E, E', T, T', \phi, \phi', \delta'_\phi$ be as above. Let X be a genus 1 curve coming from a cocycle $\gamma \in H^1(k, T)$ of order n as above. Then we have a surjective map

$$E(k) \xrightarrow{\mathbf{a}_X} \text{Br}(k(X)/k)$$

with $\phi' : E'(k) \rightarrow E(k)$ mapping into the kernel of \mathbf{a}_X and with \mathbf{a}_X given by the formula: $\mathbf{a}_X(x) = \gamma \cup \delta_{\phi'} x$, where we identify $T \otimes_{\mathbb{Z}} T' \cong \mu_n$ as in Lemma 4.1.

Remark 4.6: For certain cases of T , one may show that the resulting algebras $\mathbf{a}_X(x)$ are cyclic as follows:

If $T \cong \mathbb{Z}/n$, then an element $\gamma \in H^1(k, T)$ corresponds to a cyclic extension of degree n splitting $\mathbf{a}_X(x)$. Such an algebra is therefore represented by a cyclic algebra of degree n .

In the case that T has odd order, and that there exists a quadratic extension L/k such that $T_L \cong \mathbb{Z}/n$, and such that, after setting M/L to be the cyclic extension corresponding to $\gamma \in H^1(k_L, T_L)$, we have that M/k is Galois with Galois group $\text{Gal}(M/L) \rtimes \text{Gal}(L/k)$, then in the case that k contains a primitive n th root of unity, it follows from [RS82] that $\mathbf{a}_X(x)$ may be represented by a cyclic algebra of degree n . More generally, it follows from [HKRT96, Prop. 2.8] that the same result holds even in the case that μ_n is contained in any quadratic extension of k .

In the case that n is a prime and $T \cong \mu_n$, $\gamma \in H^1(k, T)$ corresponds to a Kummer extension splitting $\mathbf{a}_X(x)$, and in this case it follows from Albert's result [Jac96, Thm. 2.11.12, page 82] that $\mathbf{a}_X(x)$ is a cyclic algebra.

Proof of Lemma 4.4. Choose $x \in E(k)$ and $\gamma \in H^1(k, T)$ and choose $y \in E(k^{sep})$ with $[n]y = x$. By the commutativity of diagram (10), $z = \phi(y)$ satisfies $\phi'(z) = x$. Therefore we have $\delta_{\phi'}(x)(\sigma) = \sigma(z) - z, \delta_n(x)(\sigma) = \sigma(y) - y$ for $\sigma \in \text{Gal}(k)$. We now compute

$$\begin{aligned} -\gamma \cup \delta_{\phi'}(x)(\sigma, \tau) &= (\sigma z - z) \otimes \sigma(\gamma(\tau)) \\ &= (\sigma(\phi y) - \phi y) \otimes \sigma(\gamma(\tau)) \\ &= \phi(\sigma y - y) \otimes \sigma(\gamma(\tau)) \\ &= p(\sigma y - y) \otimes \sigma(\gamma(\tau)). \end{aligned}$$

Considering the isomorphism of Proposition 4.1, this gives

$$\begin{aligned} -\gamma \cup \delta_{\phi'}(x)(\sigma, \tau) &= e_n((\sigma y - y) \otimes i\sigma(\gamma(\tau))) \\ &= e_n((\sigma y - y) \otimes \sigma(i\gamma(\tau))) \\ &= -e_n(\delta_n x \cup i\gamma)(\sigma, \tau). \quad \blacksquare \end{aligned}$$

Proof of Theorem 4.5. We start with the sequence

$$0 \longrightarrow \text{Pic}^0(X) \longrightarrow \mathbf{Pic}^0(X)(k) \xrightarrow{\mathbf{a}_X} \text{Br}(X/k) \longrightarrow p(X)/i(X) \longrightarrow 0$$

of Theorem 2.1, and identify $E = \mathbf{Pic}^0(X)$. Using Theorem 3.7, we see that we may represent the map \mathbf{a}_X as a cup product from the torsion points of the elliptic curve E . Using Lemma 4.4, we may further interpret this as coming from the pairing coming from the pair of dual isogenies with kernels T and T' . By Proposition 4.3, we have that the period and the index of X must coincide, and therefore by Corollary 2.3, the map \mathbf{a}_X is surjective. \blacksquare

4.2. PERIOD AND INDEX. Since the Hasse principle holds for elements of $\text{Br}(k)$ for k global, we obtain information about $i(X)$ and $p(X)$ from local data (see section 2 for the definitions of these invariants). In particular, we have a simple generalization of a result of Cassels (see [Cas62], [O’N02], see also [Cla06]), the proof being an adaptation of the ideas of [O’N02] and [Cla06] to the present context. This may also be seen as a “divisorial” analog to [Ols70, Cor. 16].

THEOREM 4.7: *Suppose k is a global field, and let X/k be a smooth projective variety. Then if $X_v(k_v) \neq \emptyset$ for all but possibly one valuation v on k , then $p(X) = i(X)$.*

Proof. It suffices to see that these conditions force the relative Brauer group of X to be trivial. If $\alpha \in \text{Br}(X/k)$, we note that $\alpha_{k_v} \in \text{Br}(X_{k_v}/k_v)$ for every valuation v . By the hypothesis and by Corollary A.3 in Appendix A, we have $\alpha_{k_v} = 0$. This means that all except possibly one of the Hasse invariants of α vanishes. But by reciprocity, the sum of the Hasse invariants is 0, implying that $\alpha = 0$. ■

This immediately implies the result of Cassels [Cas62]:

COROLLARY 4.8: *If E is an elliptic curve and $[X] \in \text{III}(E)$, then $\text{per}(X) = \text{ind}(X)$.*

4.3. THE ELEMENTARY OBSTRUCTION. The following result says that a non-trivial homogeneous space may always be detected by its relative Brauer group, at least after extending the ground field:

THEOREM 4.9: *Suppose X is a homogeneous space for an elliptic curve E defined over k and $X(k) = \emptyset$. Then $\text{Br}(X_{k(E)}/k(E)) \neq 0$ — i.e., the relative Brauer group must be nontrivial when one extends scalars to the function field of E .*

Proof. Let $[X]$ denote the class of X in $H^1(k, E)$, and let $\mathcal{A} = \mathcal{A}_{[X]}$. It follows from Theorem 3.5 that if we consider the generic point $\eta \in E(k(E))$, then $\alpha_X(\eta) = \mathcal{A}|_\eta$ is an element of the relative Brauer group $\text{Br}(X_{k(E)}/k(E))$. Further, since the isomorphism of Lemma 3.2 maps the class $[X]$ to the algebra \mathcal{A} , it follows that \mathcal{A} is a nontrivial Brauer class. Since restriction to the generic point gives an injection $\text{Br}(E) \rightarrow \text{Br}(k(E))$, it also follows that \mathcal{A}_η is nontrivial. Therefore $\text{Br}(X_{k(E)}/k(E)) \neq 0$ as claimed. ■

COROLLARY 4.10: *Let X be a curve of genus 1 over k and suppose $X(k) \neq \emptyset$. Then there exists a field extension K/k such that the elementary obstruction for X_K is nontrivial.*

Proof. For this, we simply let $K = k(E)$ where E is the Jacobian of X . In this case it follows from Theorem 4.9 that the relative Brauer group $\text{Br}(K(X)/K)$ is nontrivial. But this implies that the elementary obstruction must also be nontrivial: arguing by contradiction, assume $ob(X_K) = 0$. In this case there exists a splitting $K^{sep}(X)^* \rightarrow (K^{sep})^*$, and in particular, the morphism

$$\text{Br}(K) = H^2(K, (K^{sep})^*) \rightarrow H^2(K, K^{sep}(X)^*) = \text{Br}(K(X))$$

is also split injective. But this implies that its kernel $\text{Br}(K(X)/K)$ must be trivial, yielding a contradiction. ■

4.4. HOW BIG IS THE RELATIVE BRAUER GROUP? The following result is a consequence of our results combined with the theorem of Lang and Néron [LN59], and is known by the experts.

PROPOSITION 4.11: *Suppose that X is a smooth projective variety defined over a field k which is local or finitely generated over \mathbb{Q} . Then $\text{Br}(k(X)/k)$ is finite.*

Proof. In the case that k is local this is immediate from [Roq66, Thm. 1]. If k is finitely generated over its prime field, we consider the map

$$\mathfrak{a}_X : \mathbf{Pic}^0(X)(k) \rightarrow \text{Br}(k(X)/k),$$

which has finite cokernel by Theorem 2.1. Further, since the Brauer group is torsion, it is enough to show that $\mathbf{Pic}^0(X)(k)$ is finitely generated. But, since in this case $\mathbf{Pic}^0(X)$ is an abelian variety over k , this follows from the work of Lang and Néron [LN59]. ■

THEOREM 4.12: *Suppose that E is an elliptic curve defined over a field k , and suppose X is a nontrivial homogeneous space over E . Then there exists a field extension L/k such that the relative Brauer group $\text{Br}(L(X)/L)$ is infinite.*

LEMMA 4.13: *Suppose X is a nontrivial homogeneous space for an elliptic curve E . Then if $L = k(E)$, there is a Brauer class $0 \neq \alpha \in \text{Br}(X_L/L)$ and an injection $\text{Br}(X/k) \oplus \langle \alpha \rangle \hookrightarrow \text{Br}(X_L/L)$.*

Proof. Let $\eta \in E(L)$ be the generic point, and let $\alpha = \mathfrak{a}_X(\eta)$. By Lemma A.1, the map $\text{Br}(k) \rightarrow \text{Br}(L)$ is injective. By Theorem 3.5 and Theorem 4.9, the element α is the restriction of the Brauer class $\mathcal{A}(X) \in \text{Br}(E, 0_E) \subset \text{Br}(E)$ to the generic point $\eta \in E$, and $\alpha \neq 0$.

Using Lemma 3.2, we may write $\text{Br}(E, 0_E) \oplus \text{Br}(k) = \text{Br}(E) \hookrightarrow \text{Br}(L)$. In particular, since $\alpha \in \text{Br}(E, 0_E)$ and $\text{Br}(X/k) \subset \text{Br}(k)$, the groups $\langle \alpha \rangle$ and $\text{Br}(X/k)$ do not intersect considered as subgroups of $\text{Br}(X_L/L) \subset \text{Br}(L)$. In particular, we obtain an injection $\text{Br}(X/k) \oplus \langle \alpha \rangle \hookrightarrow \text{Br}(X_L/L)$ as claimed. ■

Proof of Theorem 4.12. Suppose X is a homogeneous space of index n . We will begin by reducing to the case that n is prime. This is not essential for the result, but helps the exposition of the proof. Let p be a prime divisor of n , and let F'/k

be a prime to p closure of k . Note that $X(F') = \emptyset$ still with $\text{ind}(X'_F) = p^k$. Since every field extension has degree a power of p , we have

$$\text{ind}(X_{F'}) = \gcd\{[E : F'] \mid X(E) \neq \emptyset\} = \min\{[E : F'] \mid X(E) \neq \emptyset\}.$$

Consequently, there is a field E/F' of degree p^k with $X(E) \neq \emptyset$. Since F' is prime to p -closed, it follows that there is an intermediate field extension $F' \subset F \subset E$ with $[F : F'] = p^{k-1}$. Consequently, X_F has index exactly p .

We will construct a chain of field extensions of F ,

$$F = L_0 \subset L_1 \subset L_2 \subset \dots,$$

such that $(\mathbb{Z}/p)^i \subset \text{Br}(X_{L_i}/L_i)$, and $\text{Br}(X_{L_{i-1}}/L_{i-1})$ injects into $\text{Br}(X_{L_i}/L_i)$. Assuming that this has been done for $i - 1$; we define L_i to be the function field $L_{i-1}(X)$. By Lemma 4.13, there is an $\alpha \in \text{Br}(L_i(X)/L_i)$ such that $\text{Br}(L_{i-1}(X)/L_{i-1}) \oplus \langle \alpha \rangle \hookrightarrow \text{Br}(L_i(X)/L_i)$. Since the index of X_{L_i} is p , $\langle \alpha \rangle \cong \mathbb{Z}/p$, and the induction step follows from the fact that $(\mathbb{Z}/p)^{i-1} \subset \text{Br}(L_{i-1}(X)/L_{i-1})$.

Let $L = \varinjlim L_i = \bigcup_i L_i$. Clearly the natural restriction map $\text{Br}(L_i) \rightarrow \text{Br}(L)$ maps $\text{Br}(L_i(X)/L_i)$ to $\text{Br}(L(X)/L)$. I claim that this map is injective. Arguing by contradiction, let us suppose there is an $\alpha \in \text{Br}(L_i(X)/L_i)$ with $\alpha_L = 0$. If A is a central simple algebra in the class of α , then this says that the Severi–Brauer variety SB_A has an L -rational point [Sal99]. With respect to some projective embedding of the variety SB_A , this point has a finite number of coordinates, which must therefore lie in some field L_j , for a sufficiently large integer j . But this means $SB_A(L_j) \neq \emptyset$ and so L_j splits A . This implies that $\alpha_{L_i} = 0$. But this contradicts the injectivity of $\text{Br}(X_{L_{i-1}}/L_{i-1}) \rightarrow \text{Br}(X_{L_i}/L_i)$.

We therefore have $\bigcup \text{Br}(L_i(X)/L_i) \subset \text{Br}(L(X)/L)$, which implies $(\mathbb{Z}/p)^\infty \subset \text{Br}(L(X)/L)$, as desired. ■

5. An explicit description of α_X for genus 1 curves

Let E be an elliptic curve over k given on an affine patch by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let L/k be a G -Galois extension (which is no longer assumed to be the entire absolute Galois group), and let $\gamma \in Z^1(G, E(L))$ be a 1-cocycle (crossed homomorphism) representing a homogeneous space X/k for E/k . That is to say,

as G varieties, X_L is isomorphic to E_L with the Galois action $\sigma^\gamma = \bigoplus_{\gamma(\sigma)} \circ \sigma$, where by \bigoplus_p we mean the automorphism of the elliptic curve given by addition by $p \in E$. This means, for example, that for $p \in E(L)$, we have $\sigma^\gamma(p) = \gamma(\sigma) \oplus \sigma(p)$. With this in mind, we represent points in $X(L)$ by points in $E(L)$, just with a different G -module structure.

For a function $f \in L(X)$, where X is a G -variety, we have an action of $\sigma \in G$ on f by $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$, where the σ^{-1} is the action on X and the σ is induced by the action on L . In particular, if we identify $L(X)$ with $L(E)$ with a twisted action, we may write our action of $\sigma \in G$ on $f \in L(X)$ via

$$(12) \quad \sigma^\gamma(f)(p) = \sigma \circ f \circ (\sigma^\gamma)^{-1}(p) = \sigma \circ f \circ \sigma^{-1}(p \oplus \gamma(\sigma)).$$

5.1. COMPUTATIONS. The goal of this section is to explicitly describe the map $\alpha_X : E(k) \rightarrow \text{Br}(X/k)$ described above in Theorem 2.1. Given an element $p \in E(k)$, this works in the following steps:

- (1) Represent p as an element in $(\text{Pic}^0(X_L))^G$.
- (2) Pull this element back to an element in $D_p \in \text{Div}^0(X_L)$.
- (3) Compute the coboundary ∂D_p as a 1-cocycle with values in $\text{Div}^0(X_L)$.
- (4) Realize these values as lying in principal divisors on X , i.e., for each p, σ , find a function $f_{p,\sigma} \in L(X)$ whose divisor is $\partial D_p(\sigma)$. This gives a 1-cochain $f_p(\sigma) = f_{p,\sigma}$.
- (5) Let $\tilde{c}_p = \partial f_p$, and note that we may consider this as a 2-cocycle with values in L^* (i.e., values are constant). That is to say, choosing $q \in X(L)$, we have a 2-cocycle $c_p(\sigma, \tau) = \tilde{c}_p(\sigma, \tau)(q)$. This is our Brauer group element.

It will be useful to have an explicit way to show that certain divisors are principal. We begin with the following definition:

Definition 5.1: Suppose $p, q \in E(L)$. Define the function $l_{p,q} \in L(E)$ in the following way

- If $p = q = \infty$, then $l_{p,q} = 1$.
- If $p \neq q = \infty$, $p = (x_1, y_1)$, then $l_{p,q} = x - x_1$.
- If $p, q \neq \infty$, $p = q = (x_1, y_1)$, then

$$l_{p,q} = (y - y_1)(2y_1 + a_1x_1 + a_3) - (x - x_1)(3x_1^2 + 2a_2x_1 + a_4 - a_1y_1).$$

- If $p, q \neq \infty$, $p \neq q$, $p = (x_1, y_1)$, $q = (x_2, y_2)$, then

$$l_{p,q} = (y_2 - y_1)x - (x_2 - x_1)y + x_2y_1 - x_1y_2.$$

LEMMA 5.2: Let $p_1, p_2 \in E(L)$, and let $q = p_1 \oplus p_2$. Then

$$\left(\frac{l_{p_1, p_2}}{l_{q, \ominus q}} \right) = p_1 + p_2 - q - 0_E.$$

Proof. This is a routine verification. Note that $l_{p,q}$ is the equation of a line in \mathbb{A}^2 which passes through the points p, q . ■

We now go through the above steps in sequence:

1. For $p \in E(k)$, we represent p by the class of the divisor $p - 0_E \in (\text{Pic}^0(X_L))^G$.
2. This is done already. The divisor is $D_p = p - 0_E$.
3. Set $d_p = \partial(D_p)$. Explicitly, we have

$$\begin{aligned} d_p(\sigma) &= \sigma^\gamma(p - 0_E) - (p - 0_E) \\ &= \gamma(\sigma) \oplus \sigma(p) - (\gamma(\sigma) + p) + 0_E. \end{aligned}$$

Since $p \in E(k)$, $\sigma(p) = p$, and so we have

$$d_p(\sigma) = \gamma(\sigma) \oplus p + 0_E - \gamma(\sigma) - p.$$

4. By Lemma 5.2, if we set

$$f_{p,\sigma} = \frac{l_{\gamma(\sigma) \oplus p, \ominus \gamma(\sigma) \oplus p}}{l_{\gamma(\sigma), p}},$$

we have

$$(13) \quad (f_{p,\sigma}) = \gamma(\sigma) \oplus p + 0_E - \gamma(\sigma) - p = d_p(\sigma),$$

so $f_p(\sigma) = f_{p,\sigma}$ which gives a 1-cochain with values in $L(X)$.

5. Let $\tilde{c}_p = \partial f_p$. By standard arguments, we in fact know that this function has values in L . Explicitly we have

$$c_p(\sigma, \tau) = \frac{f_{p,\sigma} \sigma^\gamma f_{p,\tau}}{f_{p,\sigma\tau}} = \frac{(f_{p,\sigma})(\ominus \gamma(\sigma) f_{p,\tau}^\sigma)}{f_{p,\sigma\tau}}.$$

Remark 5.3: The only relevant issue about the functions $f_{p,\sigma}$ is that their associated principal divisor is described as in equation (13). In particular, we may change the functions $f_{p,\sigma}$ by any constants and get an equivalent 2-cocycle describing c_p .

THEOREM 5.4: Suppose $p \in E(k)$. Then with the above notation

$$\mathfrak{a}_p = (L/k, G, c_p),$$

where c_p is given as

$$c_p(\sigma, \tau) = \frac{(f_{p,\sigma})(\ominus_{\gamma(\sigma)} f_{p,\tau})}{f_{p,\sigma\tau}}.$$

We gather these facts in the following application:

COROLLARY 5.5: *Suppose X is a genus 1 curve with Jacobian E and suppose $\text{ind}(X) = \text{per}(X)$. Let L/k be a Galois extension with group G and suppose $X(L) \neq \emptyset$. Then the relative Brauer group $\text{Br}(X/k)$ is given by*

$$(14) \quad \{[(L/k, G, c_p)] \mid p \in E(k)\},$$

where

$$(15) \quad c_p(\sigma, \tau) = \frac{(f_{p,\sigma})(\ominus_{\gamma(\sigma)} f_{p,\tau})}{f_{p,\sigma\tau}},$$

and where the function $f_{p,\sigma} \in L(E)$ is defined by the expression

$$f_{p,\sigma} = \frac{l_{\gamma(\sigma) \oplus p, \ominus_{\gamma(\sigma)} \oplus p}}{l_{\gamma(\sigma), p}},$$

and the functions l_{p_1, p_2} are given in Definition 5.1.

Remark 5.6: In the case that the cocycle $\gamma \in H^1(L, E(L))$ has values in $E(k)$, we may simplify our expression for the cocycle c_p above by noting that the functions $f_{p,\sigma}$ are in $k(E)$ (using their explicit description above), and hence are Galois invariant. We may therefore write in this case

$$c_p(\sigma, \tau) = \frac{f_{p,\sigma}(\ominus_{\gamma(\sigma)} f_{p,\tau})}{f_{p,\sigma\tau}}.$$

Remark 5.7: In the case that $G = \langle \sigma \mid \sigma^m \rangle$ is a cyclic group with generator σ of order m , and the values of the cocycle are in $E(k)$, we may simplify our formula for c_p significantly. Using the fact that c_p is a cocycle with values in k^* , one may check explicitly that in this case c_p is cohomologous to c'_p , where for $0 \leq i, j < n$ we have

$$c'_p(\sigma^i, \sigma^j) = \begin{cases} 1, & i + j < m, \\ c_p(1, 1)c_p(2, 1) \cdots c_p(m - 1, 1), & i + j \geq m. \end{cases}$$

In particular, the central simple algebra represented by c_p is the cyclic algebra

$$(L, \sigma, c_p(1, 1)c_p(2, 1) \cdots c_p(m - 1, 1)).$$

5.2. EXAMPLES.

5.2.1. *A hyperelliptic curve.* We demonstrate this formula for the relative Brauer group by reproducing an example of I. Han [Han03]. Let X be the hyperelliptic genus 1 curve given by the affine equation $y^2 = ax^4 + b$, and suppose $X(k) = \emptyset$. The Jacobian E of this curve is given by the Wierstrauss equation $y^2 = x^3 - 4abx$. Let $L = k(\beta)$, where $\beta^2 = b$. We have $(0, \pm\beta) \in X(L)$, and so the index of X is 2 and hence is also equal to the period of X . Let the order 2 group $G = \langle \sigma \mid \sigma^2 \rangle$ be the Galois group of L/k .

Note that the (non-identity) 2-torsion points of E are exactly those points with y coordinate 0. These are

$$t_0 = (0, 0), \quad t_+ = (0, 2\lambda), \quad t_- = (0, -2\lambda),$$

where $\lambda^2 = 4ab$. In particular, we have three possibilities: $\lambda \in k$, $\lambda \in L \setminus k$, or $\lambda \notin L$. We will assume the second possibility holds, i.e., $ab \in (L^*)^2 \setminus (k^*)^2$.

LEMMA 5.8: *Define a 1-cocycle $\gamma \in H^1(G, E(L))$ via $\gamma(id) = 1, \gamma(\sigma) = t_0$. Then γ corresponds to X viewed as a homogeneous space over E .*

Proof. This is exactly [Sil92, Example 3.7, pages 293–295]. ■

We will consider the case where $rk(E) = 0$. In this case, since the image of \mathfrak{a} is entirely 2-torsion, $im(\mathfrak{a}) = \mathfrak{a}(E(k)_2)$, where $E(k)_2$ is the 2-power torsion part of $E(k)$. On the other hand, since the only k -rational non-identity 2-torsion point is t_0 , if there are other points in $(k)_2$, there must be at least a 4-torsion point. An explicit computation quickly shows, however, that this would contradict the fact that ab is not a square (the line from t_0 to the 4-torsion point would have to be tangent at the 4-torsion point, and therefore its slope would have to be a fourth root of $16ab$). Consequently, we have

$$Br(X/k) = \langle \mathfrak{a}_{t_0} \rangle.$$

By Corollary 5.5, we have

$$A = \mathfrak{a}_{t_0} = (L/k, G, c_{t_0}),$$

with $c = c_{t_0}$ described as above. For this example we compute explicitly

$$f_{t_0, id} = \frac{l_{0_E \oplus t_0, \ominus \gamma(id) \ominus t_0}}{l_{\gamma(\sigma), t_0}} = \frac{l_{t_0, t_0}}{l_{0_E, t_0}} = \frac{x}{x} = 1,$$

and

$$f_{t_0, \sigma} = \frac{l_{\gamma(\sigma) \oplus t_0, \ominus \gamma(\sigma) \ominus t_0}}{l_{\gamma(\sigma), t_0}} = \frac{l_{0_E, 0_E}}{l_{t_0, t_0}} = \frac{1}{x}.$$

Using $q = t_+$ in formula (14) in Corollary 5.5, and using the fact that $\sigma(t_+) = t_-$, we have

$$c(id, id) = c(id, \sigma) = c(\sigma, id) = 1,$$

$$c(\sigma, \sigma) = -\frac{1}{4ab}.$$

Therefore, the relative Brauer group $\text{Br}(X/k)$ is generated by the algebra

$$A = (L/k, \sigma, -1/4ab) = (L/k, \sigma, -ab)$$

$$= (b, -ab)_{-1} = (b, a)_{-1} + (b, -b)_{-1} = (a, b)_{-1}$$

and so $\text{Br}(X/k) = \{1, (a, b)_{-1}\}$.

5.2.2. *A curve of index 5.* Let E be the elliptic curve over \mathbb{Q} given by the equation

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

One may check (for example, using Pari [par]) that the torsion subgroup of this curve is $\mathbb{Z}/5\mathbb{Z}$, generated by $g = (5, 5)$, and that its rank is 0. Let L/\mathbb{Q} be any cyclic degree 5 extension, say $G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma \mid \sigma^5 \rangle$. Let $\gamma \in H^1(G, E(L))$ be given by $\gamma(\sigma) = g$. The element γ corresponds to a homogeneous space X for E , which is isomorphic to E if and only if γ is trivial. We will show:

Example 5.9: The relative Brauer group $\text{Br}(X/\mathbb{Q})$ of the curve X is cyclic generated by the cyclic algebra $(L/\mathbb{Q}, \sigma, 11)$. In particular, if 11 is not a norm from L , then X is not split.

Proof. This follows from direct computation with the above formulas. In particular, since for our curve $E(\mathbb{Q}) = \langle g \rangle$, one need only check the 2-cocycle in the image of the point g .

One may check that for our curve, we may use the functions f_{g, σ^i} given by

$$f_{g, id} = 1, \quad f_{g, \sigma} = \frac{x - 16}{5x - y - 20}, \quad f_{g, \sigma^2} = \frac{x - 16}{6x + y - 35},$$

$$f_{g, \sigma^3} = \frac{x - 5}{-5x + y + 20}, \quad f_{g, \sigma^4} = \frac{1}{x - 5}.$$

Using Remark 5.6, we may express our cocycle c_g as

$$c_g(\sigma^i, \sigma^j) = \frac{f_{g, \sigma^i}(\ominus_{g^i} f_{q, \sigma^j})}{f_{q, \sigma^{i+j}}}.$$

With the aid of computational software ([par], [M2]), we may determine the functions $\ominus_{g^i} f_{q, \sigma^j}$. In particular, we have

$$\begin{aligned} \ominus_g f_{g, \sigma} &= \frac{5x - y - 20}{6x + y - 35}, & \ominus_{g^2} f_{g, \sigma} &= \frac{5x + y - 19}{6x - y - 36}, \\ \ominus_{g^3} f_{g, \sigma} &= \frac{x - 5}{-5x - y + 19}, & \ominus_{g^4} f_{g, \sigma} &= \frac{5 - x}{11}. \end{aligned}$$

and by using Remark 5.7, we may find a cohomologous cocycle

$$c'_g(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < 5, \\ 1/11 & \text{if } i + j \geq 5. \end{cases} \quad \blacksquare$$

5.2.3. *An example with noncyclic relative Brauer group.* Using the computer package [Kra07], we may construct other interesting examples by using curves of rank 0 with interesting torsion subgroups. The following is the result of output from this program:

Let E be the elliptic curve defined over \mathbb{Q} by the affine equation

$$y^2 + xy + y = x^3 + x^2 - 10x - 10.$$

Let L/\mathbb{Q} be a cyclic Galois extension with generator σ of order 4. Given a torsion point $t \in E(k)$ of order n dividing 4, we may use it to define a homomorphism $\text{Gal}(L/k) \rightarrow E(k)$ by sending the generator $\sigma \in \text{Gal}(L/\mathbb{Q})$ to the torsion point t . Via the map $\text{Hom}(\text{Gal}(L/\mathbb{Q}), E(k)) \rightarrow H^1(\mathbb{Q}, E)$, this defines a principal homogeneous space X_t .

For the elliptic curve E , pari/gp tells us that E is rank 0 with torsion subgroup generated by the points $(8, 18)$ of order 4 and $(-1, 0)$ of order 2.

For the homogeneous space defined by $t = \ominus(8, 18)$, the relative Brauer group is isomorphic to $\mathbb{Z}/4 \times \mathbb{Z}/2$, generated by the cyclic algebras:

$$\begin{aligned} \mathfrak{a}_{X_t}(8, 18) &= (L/k, \sigma, 405) = (L/k, \sigma, 5), \\ \mathfrak{a}_{X_t}(-1, 0) &= (L/k, \sigma, -81) = (L/k, \sigma, -1). \end{aligned}$$

Appendix A. Rational points over function fields

The following lemma is due to Nishimura [Nis55]:

LEMMA A.1: *Suppose X and Y are schemes over k such that Y is proper, $Y(k) = \emptyset$, X is irreducible and $x \in X(k)$ is a smooth point. Then $Y(k(X)) = \emptyset$.*

Proof. The proof proceeds by induction on $\dim(X)$. Suppose that $Y(k(X)) \neq \emptyset$. Then there is a rational morphism $\phi : X \dashrightarrow Y$. If $\dim(X) = 0$, then $x = X$ and ϕ gives an element of $Y(k)$, contradicting our hypothesis $Y(k) = \emptyset$. For the general induction step, let \tilde{X} be the blowup of X at the point x and let $E \subset \tilde{X}$ be the exceptional divisor. Since the map ϕ may be defined in a set of codimension at least 2 and, in particular, by restricting this morphism to E , we obtain a rational map $E \dashrightarrow Y$. Since $E \cong \mathbb{P}^{\dim(X)-1}$, E contains a smooth k -point and is irreducible. Therefore, by letting E take the role of X , the induction hypothesis implies $Y(k) \neq \emptyset$, contradicting our hypothesis and completing the proof. ■

One consequence of this fact is that the index of projective varieties is not changed by such field extensions:

COROLLARY A.2: *Suppose Y is a projective variety, and X is a variety with a smooth rational k -point. Then $\text{ind } Y = \text{ind } Y_{k(X)}$.*

Proof. For a positive integer n , let $Y^{[n]}$ be the Hilbert scheme of n points on Y . Since this is a projective scheme, Lemma A.1 tells us that $Y^{[n]}(k) \neq \emptyset$ if and only if $Y^{[n]}(k(X)) \neq \emptyset$. Since the index of Y may be thought of as the gcd of the set of positive integers n such that $Y^{[n]}$ has a rational point, we obtain $\text{ind } Y = \text{ind } Y_{k(X)}$. ■

In particular, we obtain

COROLLARY A.3: *Suppose X is a scheme defined over k with a smooth point $x \in X(k)$. Then the restriction map $\text{Br}(k) \rightarrow \text{Br}(k(X))$ is injective.*

Proof. Recall that for a central simple algebra A over a field F , A is split if and only if the associated Severi–Brauer variety SB_A has an F -point [Sal99]. Therefore, if A is a central simple k algebra with $[A] \neq 0$ in $\text{Br}(k)$, then the variety SB_A has no k -points. If the algebra is split by $k(X)$, then this implies SB_A does

have a point over $k(X)$. Since SB_A is a proper variety, this would contradict Lemma A.1. Therefore, we must have $SB_A(k(X)) = \emptyset$ and $[A]_{k(X)} \neq 0$. ■

References

- [Baš72] M. I. Bašmakov, *Cohomology of Abelian varieties over a number field*, Uspehi Matematicheskikh Nauk **27** (1972), 25–66. English translation: Russian Mathematical Surveys **27** (1972), 6, 25–70.
- [Cas62] J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, Journal für die Reine und Angewandte Mathematik **211** (1962), 95–112.
- [Cla] P. L. Clark, *The period-index problem in WC-groups. II*, preprint, <http://math.uga.edu/~pete/wc2.pde>.
- [Cla06] P. L. Clark, *There are genus one curves of every index over every number field*, Journal für die Reine und Angewandte Mathematik **594** (2006), 201–206.
- [CTS87] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles. II*, Duke Mathematical Journal **54** (1987), 375–492.
- [dJ] A. Johan de Jong, *A Result of Gabber*, <http://www.math.columbia.edu/~dejong/papers/2-gabber.pdf>.
- [FGI⁺05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure and A. Vistoli, *Fundamental Algebraic Geometry*, Mathematical Surveys and Monographs, Vol. 123, American Mathematical Society, Providence, RI, 2005. Grothendieck's FGA explained.
- [Gro68a] A. Grothendieck, *Le groupe de Brauer. I. Algèbres d'Azumaya et interprétations diverses*, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam, 1968, pp. 46–66.
- [Gro68b] A. Grothendieck, *Le groupe de Brauer. II. Théorie cohomologique*, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam, 1968, pp. 67–87.
- [Gro68c] A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam, 1968, pp. 88–188.
- [GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Volume 101 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2006.
- [Hai84] D. E. Haile, *On the Clifford algebra of a binary cubic form*, American Journal of Mathematics **106** (1984), 1269–1280.
- [Hai89] D. Haile, *On Clifford algebras, conjugate splittings, and function fields of curves*, in *Ring Theory 1989 (Ramat Gan and Jerusalem, 1988/1989)*, Israel Mathematical Conference Proceedings, Vol. 1, Weizmann, Jerusalem, 1989, pp. 356–361.
- [Hai92] D. E. Haile, *When is the Clifford algebra of a binary cubic form split?*, Journal of Algebra **146** (1992), 514–520.
- [Han03] I. Han, *Relative Brauer groups of function fields of curves of genus one*, Communications in Algebra **31** (2003), 4301–4328.

- [HHW10] D. E. Haile, I. Han and A. R. Wadsworth, *Curves C that are Cyclic Twists of $Y^2 = X^3 + c$ and the Relative Brauer Groups $Br(k(C)/k$* , ArXiv e-prints, April 2010. 1004.0714.
- [HKRT96] D. E. Haile, M.-A. Knus, M. Rost and J.-P. Tignol, *Algebras of odd degree with involution, trace forms and dihedral extensions*, Israel Journal of Mathematics **96** (part B)(1996), 299–340.
- [HT88] D. Haile and S. Tesser, *On Azumaya algebras arising from Clifford algebras*, Journal of Algebra **116** (1988), 372–384.
- [HT89] T. J. Hodges and S. B. Tesser, *Representing Clifford algebras as crossed-products*, Journal of Algebra **123** (1989) 500–505.
- [Jac96] N. Jacobson, *Finite-Dimensional Division Algebras over Fields*, Springer-Verlag, Berlin, 1996.
- [KL08] D. Krashen and M. Lieblich, *Index reduction for Brauer classes via stable sheaves*, Interanational Mathematics Research Notices (8):Art. ID rnn010, 31, 2008.
- [Kra07] D. Krashen, *Relative Brauer*, 2007, Computer package for Macaulay2 using pari, <http://www.math.uga.edu/~dkrashen/relbr/>.
- [Kuo] J.-M. Kuo, *On an algebra associated to a ternary cubic curve*, Journal of Algebra **330** (2011), 86–102.
- [Lam89] T. Y. Lam, *Fields of u -invariant 6 after A. Merkurjev [A. S. Merkur'ev]*, in *Ring Theory 1989 (Ramat Gan and Jerusalem, 1988/1989)*, Israel Mathematical Conference Proceedings, Vol. 1, Weizmann, Jerusalem, 1989, pp. 12–30.
- [Lan72] S. Lang, *Introduction to Algebraic Geometry*, Addison-Wesley, Reading, Mass., 1972. Third printing, with corrections.
- [Lic68] S. Lichtenbaum, *The period-index problem for elliptic curves*, American Journal of Mathematics **90** (1968), 1209–1223.
- [Lic69] S. Lichtenbaum, *Duality theorems for curves over p -adic fields*, Inventiones Mathematicae **7** (1969), 120–136.
- [LN59] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*, American Journal of Mathematics **81** (1959), 95–118.
- [M2] Macaulay 2, Computer program, <http://www.math.uiuc.edu/Macaulay2/>.
- [MPW96] A. S. Merkurjev, I. A. Panin and A. R. Wadsworth, *Index reduction formulas for twisted flag varieties. I*, *K-Theory* **10** (1996), 517–596.
- [Mum70] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Tata Institute of Fundamental Research, Bombay, 1970.
- [Mur64] J. P. Murre, *On contravariant functors from the category of pre-schemes over a field into the category of abelian groups (with an application to the Picard functor)*, Publications Mathématiques. Institut de Hautes Études Scientifiques **23** (1964), 5–43.
- [Nis55] H. Nishimura, *Some remarks on rational points*, Memoires of the College of Science, University of Kyoto. Series A. Mathematics **29** (1955), 189–192.
- [Ols70] L. D. Olson, *Galois cohomology of cycles and applications to elliptic curves* American Journal of Mathematics **92** (1970), 75–85.
- [O'N02] C. O'Neil, *The period-index obstruction for elliptic curves*, Journal of Number Theory **95** (2002), 329–339.

- [par] Pari-gp, Computer program, <http://www.parigp-home.de/>.
- [Roq66] P. Roquette, *Splitting of algebras by function fields of one variable*, Nagoya Mathematical Journal **27** (1966), 625–642.
- [RS82] L. H. Rowen and D. J. Saltman, *Dihedral algebras are cyclic*, Proceedings of the American Mathematical Society **84** (1982), 162–164.
- [Sal99] D. J. Saltman, *Lectures on Division Algebras*, American Mathematical Society, Providence, RI, 1999.
- [Sil92] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1992.