A METHOD OF COMPUTING THE CONSTANT FIELD OBSTRUCTION TO THE HASSE PRINCIPLE FOR THE BRAUER GROUPS OF GENUS ONE CURVES

ILSEOP HAN

Abstract. Let $k$ be a global field of characteristic unequal to two. Let $C : y^2 = f(x)$ be a nonsingular projective curve over $k$, where $f(x)$ is a quartic polynomial over $k$ with nonzero discriminant, and $K = k(C)$ be the function field of $C$. For each prime spot $p$ on $k$, let $\hat{k}_p$ denote the corresponding completion of $k$ and $\hat{k}_p(C)$ the function field of $C \times_k \hat{k}_p$. Consider the map

$$h : \text{Br}(K) \rightarrow \prod_p \text{Br}(\hat{k}_p(C)),$$

where $p$ ranges over all the prime spots of $k$. In this paper, we explicitly describe all the constant classes (coming from Br($k$)) lying in the kernel of the map $h$, which is an obstruction to the Hasse principle for the Brauer groups of the curve. The kernel of $h$ can be expressed in terms of quaternion algebras with their prime spots. We also provide specific examples over $\mathbb{Q}$, the rationals, for this kernel.

1. Introduction

Let $k$ be a global field with char($k$) $\neq 2$ and let Br($k$) denote the Brauer group of $k$. Let $C$ be a geometrically irreducible nonsingular projective curve over $k$ and $K = k(C)$ be the function field of $C$ over $k$. For the scalar extension map $\theta : \text{Br}(k) \rightarrow \text{Br}(K)$ given by $[A] \mapsto [A \otimes_k K]$, a class $[B] \in \text{Br}(K)$ is called a constant class in Br($K$) if $[B] = \theta([A])$ for some $[A] \in \text{Br}(k)$. We denote the relative Brauer group of $K$ over $k$, i.e., ker($\theta$), by Br($K/k$).

For each prime spot $p$ on $k$, let $\hat{k}_p$ denote the corresponding completion of $k$ and $\hat{k}_p(C)$ the function field of $C \times_k \hat{k}_p$. Consider the map

$$h : \text{Br}(K) \rightarrow \prod_p \text{Br}(\hat{k}_p(C)),$$

Received September 20, 2015; Revised January 4, 2016.

2010 Mathematics Subject Classification. 16K20, 16K50, 14H05, 14H45.

Key words and phrases. Brauer groups, Hasse principle, function fields of genus 1.

©2016 Korean Mathematical Society

1431
where \( p \) ranges over all the prime spots of \( k \) (including real infinite prime spots). The nontrivial Brauer classes in \( \ker(h) \) are the obstruction to the Hasse principle for the Brauer groups of function fields of curves.

Now, let \( J \) be the Jacobian of the curve \( C \) and let \( \mathfrak{V}(J) \) be the Shafarevich-Tate group of \( J \). Assume that \( C \) has a \( k \)-rational point. Recall then the well-known fact (cf. e.g. [5, p. 561]) that

\[
\ker(\text{Br}(K) \to \prod_p \text{Br}(\hat{k}_p(C))) \cong \mathfrak{V}(J).
\]

Furthermore, R. Parimala and R. Sujatha showed in [5] that

\[
\ker(\text{W}(K) \to \prod_p \text{W}(\hat{k}_p(C))) \cong 2^2 \mathfrak{V}(J),
\]

where \( \text{W}(F) \) is the Witt group of a field \( F \) and \( 2^2 \mathfrak{V}(J) \) is the 2-torsion subgroup of \( \mathfrak{V}(J) \). (For the isomorphisms in (2) and (3), it turns out that the condition of \( C \) having a \( k \)-rational point plays an essential role.) Utilizing this fact, they studied the correspondence between the obstruction to the Hasse principle for Witt groups of function fields and elements of \( 2^2 \mathfrak{V}(J) \) when the Jacobian \( J \) is an elliptic curve \( E \). This enabled them to describe the 2-torsion subgroup of \( \ker(h) \), where \( h \) is the map in (1), for the case of elliptic curves over \( \mathbb{Q} \) of the form \( E : y^2 = x^3 - ax \), given an element of \( 2^2 \mathfrak{V}(E) \). In particular, when \( E \) is the elliptic curve defined by \( y^2 = x^3 + px \) over \( \mathbb{Q} \) where \( p \equiv 1 \pmod{8} \) and 2 is not a quartic residue mod \( p \), they showed in [5, Theorem 3.3] that

\[
2\ker(h) = \langle [(1, x/\mathbb{Q})], [(2, x/\mathbb{Q})] \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.
\]

In this paper, we consider the curve over \( k \) of the form \( C : y^2 = f(x) \) where \( f(x) \) is any quartic polynomial with nonzero discriminant. This \( C \) is a hyperelliptic curve of genus 1. Unlike the work in [5], we do not assume that \( C \) possesses a \( k \)-rational point. Thus the isomorphisms in (2) and (3) are not available here.

The main purpose of the paper is to provide a method of computation so as to give precise description of all the constant classes existing in the kernel of the map \( h \) in (1). To facilitate calculation, we will investigate the kernel of the map \( \text{Br}(k) \to \prod_p \text{Br}(\hat{k}_p(C)) \) as well as the relative Brauer group \( \text{Br}(K/k) \), and then combine these results. Every constant class of \( \ker(h) \) can be expressed as the class of a quaternion algebra \( Q \), which is completely determined by the prime spots where \( Q \) doesn’t split. At the end of Sections 3 and 5, we illustrate how to construct explicit examples over \( \mathbb{Q} \).

2. Preliminary

In this section, we introduce notations and definitions, and briefly review some basic facts which will be needed in later sections.

Let \( k \) be a field (with \( \text{char}(k) \neq 2 \) throughout). Let \( C \) be a nonsingular projective curve, or simply a curve, over \( k \) and \( K = k(C) \) be the function field
of \( C \), which is an algebraic function field in one variable over \( k \) where \( k \) is algebraically closed in \( K \).

When the curve \( C \) possesses a rational point over \( k \), in short, \( C(k) \neq \emptyset \), the following lemma is easily deducible from the existence of a specialization map corresponding to the rational point (cf. [4, p. 175]).

**Lemma 2.1.** Let \( k \) be any field. Let \( K = k(C) \) be the function field of a curve \( C \) over \( k \). If \( C(k) \neq \emptyset \), then \( \text{Br}(K/k) = \{0\} \).

Let \( k \) be a global field. By a prime spot on \( k \), we mean an equivalence class of discrete valuations on \( k \) or an equivalence class of archimedean absolute values on \( k \). Define
\[
P(k) = \{ \mathfrak{p} \mid \mathfrak{p} \text{ is a prime spot of } k \},
\]
and for each \( \mathfrak{p} \in P(k) \), let \( \hat{k}_p \) denote the corresponding completion of \( k \). It is obvious that if \( C(k) \neq \emptyset \), then \( C(\hat{k}_p) \neq \emptyset \) for every \( \mathfrak{p} \in P(k) \) (but not conversely). Thus, if \( C(\hat{k}_p) = \emptyset \) for some \( \mathfrak{p} \in P(k) \), then \( C(k) = \emptyset \).

For \( a, b \in k^* = k - \{0\} \), let \( Q = (a, b/k) \) denote a quaternion algebra over \( k \) with \( k \)-base \( 1, i, j, ij \), such that \( i^2 = a, \ j^2 = b, \) and \( ij = -ji \). When \( k \) is a global field, define the support of \( Q \) as follows:
\[
supp(Q) = \{ \mathfrak{p} \in P(k) \mid Q \otimes_k \hat{k}_p \text{ is nonsplit} \}.
\]

We next recall a useful tool especially to represent quaternion algebras over a global field.

**Lemma 2.2 (Hilbert’s Reciprocity Law).** Let \( k \) be a global field. For a quaternion algebra \( Q \) over \( k \), the set \( supp(Q) \) is finite with even cardinality. Further, given any finite subset \( N \) of \( P(k) \) with even cardinality, there is a unique quaternion algebra \( Q \) over \( k \) with \( supp(Q) = N \).

According to Hilbert’s Reciprocity Law, \( Q \) is split if and only if \( supp(Q) \) is the empty set. Furthermore, we define
\[
Q_{\{p_1, \ldots, p_{2n}\}}
\]
to be the quaternion algebra over \( k \) with support \( \{p_1, \ldots, p_{2n}\} \subseteq P(k) \). For example, if 2 is the dyadic prime spot (that is, the characteristic of the corresponding residue field is 2) and \( \infty \) is the real infinite prime spot over \( Q \), then
\[
Q_{(2, \infty)} = (-1, -1/Q).
\]

Now, let \( C_0 \) be the projective conic curve over a field \( k \) defined by the homogeneous equation \( ax^2 + by^2 - z^2 = 0 \), where \( a, b \in k^* \). Plainly, \( C_0 \) is nonsingular as \( \text{char}(k) \neq 2 \). Then the function field \( K = k(C_0) \) is the quotient field of \( k[x, z]/(ax^2 + b - z^2) \) and so \( K \) has the form \( k(x, \sqrt{ax^2 + b}) \). This \( K \) has genus 0.

The following lemma can be verified by a direct computation (or see [4, Proposition 1.3.2]), which will be used in Section 3.
Lemma 2.3. Let $k$ be any field. For $Q = (a, b/k)$ and $C_0$ as above, the quaternion algebra $Q$ is split if and only if $C_0(k) \neq \emptyset$.

When the genus is zero, the Hasse Principle (or alternatively, Lemma 2.2 together with Lemma 2.3) tells us that $C_0(k) \neq \emptyset$ if and only if $C_0(\hat{k}_p) \neq \emptyset$ for every $p \in P(k)$.

Finally, when $k$ is a local field, recall that there exists a unique nonsplit quaternion algebra over $k$. P. Roquette (see [6, Theorem 1]) showed:

Lemma 2.4. Let $k$ be a local field. Let $C$ be a curve over $k$ and $K = k(C)$. If $d$ is the smallest positive integer which is the degree of a divisor of $K$ over $k$, then

$$\text{Br}(K/k) \cong \mathbb{Z}/d\mathbb{Z}.$$  

In particular, let $C$ be the curve of the form $y^2 = f(x)$, where $f(x) \in k[x]$ is square-free. If $C(k) = \emptyset$, then

$$\text{Br}(K/k) = \{ 0, [D] \}$$

where $D$ is the unique nonsplit quaternion algebra over $k$.

3. The kernel of the map $\text{Br}(k) \rightarrow \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C))$

Let $k$ be a global field and $f(x) \in k[x]$ be a polynomial of degree $n$. We assume that $\text{disc}(f) \neq 0$, so $f$ has no repeated roots in its splitting field. Consider the curve $C: y^2 = f(x)$. This is a nonsingular affine curve but its projective closure is singular at the point at infinity whenever $n \geq 4$. By blowing up the singular point, we obtain an associated nonsingular projective curve $C'$ in which the affine curve $C$ is dense and $k(C) = k(C')$. Hence, although we write $C$, we actually mean $C'$.

For the curve $C: y^2 = f(x)$ as above, we want to describe in this section the kernel of the map

$$g : \text{Br}(k) \rightarrow \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C)).$$

We are especially interested in the case where $f$ has degree 4 (so $C$ is a hyperelliptic curve of genus 1). We will also consider the case of degree 2 below (so the associated curve is a conic curve of genus 0) since there is a connection between the two in certain circumstances.

To begin, let us define $S_C$ to be the set of prime spots such that the curve $C$ has no rational point locally over $\hat{k}_p$, that is,

$$S_C = \{ p \in P(k) \mid C(\hat{k}_p) = \emptyset \}.$$  

Note that $S_C$ is finite by the Hasse-Weil bound. Then, we have:
Proposition 3.1. Let $k$ be a global field and let $C$: $y^2 = f(x)$ be a curve over $k$. Then one has

$$\ker(g) = \begin{cases} [Q] & \text{if } Q \text{ is a quaternion algebra over } k \text{ with } \text{supp}(Q) \subseteq S_C \\ \emptyset & \text{otherwise} \end{cases},$$

where $g$ is the map in (4). Further, if $S_C = \emptyset$, then $\ker(g)$ is trivial. If $S_C \neq \emptyset$, then $\ker(g)$ has $2^{|S_C|-1}$ elements.

Proof. The map $g$ can be viewed as the composition of the maps

$$\begin{align*}
\text{Br}(k) & \xrightarrow{i} \prod_{p \in P(k)} \text{Br}(\hat{k}_p) \\
& \xrightarrow{j} \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C)).
\end{align*}$$

The map $i$ in (6) is injective by the local-global principle for central simple algebras over global fields and $\ker(j)$ is 2-torsion since each component in the direct product has a 2-torsion kernel. This tells us that $\ker(g)$ is 2-torsion and hence, for each nontrivial class $[Q] \in \ker(g)$, the exponent of $Q$ is 2. Since $k$ is a global field, it follows that $\text{ind}(Q) = \exp(Q)$, which is 2. Therefore $\ker(g)$ consists of classes of quaternion algebras over $k$. Next, assume that there exists a quaternion algebra $Q$ such that $\text{supp}(Q) \nsubseteq S_C$. Then, we can take a $p \in P(k)$ such that $p \in \text{supp}(Q)$ but $p \notin S_C$. For this $p$, note that $C(\hat{k}_p) \neq \emptyset$. It follows from Lemma 2.1 that $\text{Br}(\hat{k}_p(C)/\hat{k}_p) = 0$. Hence, $Q \otimes_k \hat{k}_p(C)$ is nonsplit and therefore $[Q] \notin \ker(g)$. In other words, if $[Q] \in \ker(g)$, then $Q$ must be a quaternion algebra with $\text{supp}(Q) \subseteq S_C$.

Conversely, assume that $Q$ is a quaternion algebra with $\text{supp}(Q) \subseteq S_C$. We show that $[Q] \in \ker(g)$. First, if $p \notin \text{supp}(Q)$, then $Q \otimes_k \hat{k}_p$ is split and so is $Q \otimes_k \hat{k}_p(C)$. Secondly, if $p \notin \text{supp}(Q)$, then $C(\hat{k}_p) = \emptyset$ since $\text{supp}(Q) \subseteq S_C$. It follows from Lemma 2.4 that $[Q \otimes_k \hat{k}_p] \in \text{Br}(\hat{k}_p(C)/\hat{k}_p)$. This shows that $Q \otimes_k \hat{k}_p(C)$ is split for all $p \in P(k)$ and hence $[Q] \in \ker(g)$ as claimed.

Counting the cardinality of the kernel of $g$ is immediate by Lemma 2.2. This completes the proof. □

Now, for a quartic polynomial $f$, we want to describe $\ker(g)$ obtained in Proposition 3.1. For efficient calculations, let us first begin with the quadratic polynomials.

- Quadratic Case

Let $C_0$ be a conic curve over a field $k$ of the form

$$C_0: y^2 = ax^2 + bx + c = a(x + \frac{b}{2a})^2 - \frac{b^2 - 4ac}{4a}.$$ 

Put

$$D := b^2 - 4ac \quad (= \text{disc}(f))$$

and consider the quaternion algebra $Q = (a, -\frac{D}{4a}/k)$. Notice then that $Q \cong (a, D/k)$ since $(a, -4a/k)$ is split. Hence, the function field $k(C_0)$ is in fact determined by the quaternion algebra $(a, D/k)$. Further, it follows from Lemma 2.3 that $(a, D/k)$ is split if and only if $C_0(k) \neq \emptyset$. 

\[\text{A METHOD OF COMPUTING THE CONSTANT FIELD OBSTRUCTION} \quad 1435\]
Define the map
\[
g_a : \text{Br}(k) \longrightarrow \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C_0)).
\]

**Corollary 3.2.** Let \( C_0 : y^2 = ax^2 + bx + c \) be a conic curve over a global field \( k \). Let \( Q = (a, D/k) \) where \( D = b^2 - 4ac \). For the map \( g_a \) in (7), one has
\[
\ker(g_a) = \left\{ [Q'] \middle| \begin{array}{l}
Q' \text{ is a quaternion algebra over } k \\
\text{with supp}(Q') \subseteq \text{supp}(Q)
\end{array} \right\}.
\]
The cardinality of this set is \( 2^{n-1} \) where \( n = |\text{supp}(Q)| \).

**Proof.** Observe that \( p \in \text{supp}(Q) \) if and only if \( Q \otimes_k \hat{k}_p \) is nonsplit if and only if \( C_0(\hat{k}_p) = \emptyset \) if and only if \( p \in SC_0 \). The second 'iff' statement comes from Lemma 2.3. Hence, we have \( SC_0 = \text{supp}(Q) \) and apply Proposition 3.1. \( \square \)

**Example 3.3.** Consider the conic curve \( C_0 : y^2 = -x^2 + 17x - 361 \) over \( \mathbb{Q} \). Then \( D = b^2 - 4ac = -1155 = -3 \cdot 5 \cdot 7 \cdot 11 \) and thus the corresponding quaternion algebra is \( Q = (-1, -1155/\mathbb{Q}) \) with \( \text{supp}(Q) = \{3, 7, 11, \infty\} \). For \( p \in \{3, 7, 11\} \), observe that \( (-1, -p/\mathbb{Q}) \cong Q(p, \infty) \). Hence, by Corollary 3.2, we have
\[
\ker(g_a) = \langle [(-1, -3/\mathbb{Q})], [(-1, -7/\mathbb{Q})], [(-1, -11/\mathbb{Q})] \rangle \cong \bigoplus_{i=1}^{3} \mathbb{Z}/2\mathbb{Z}.
\]

- **General Quartic Case**

We now consider the quartic case: Let \( f(x) = \sum_{i=0}^{4} a_i x^i \) be a polynomial of degree 4 (with \( \text{disc}(f) \neq 0 \)). We may assume that \( a_4 = 0 \) by substituting \((x - \frac{a_3}{4a_4})\) for \( x \). For convenience, let us use different letters for coefficients. For the curve
\[
C : y^2 = f(x) = ax^4 + bx^2 + cx + d,
\]
we define
\[
S = \{ p \in P(k) \mid C \text{ has a bad reduction at } p \} \cup \mathcal{D} \cup \mathcal{R},
\]
where \( \mathcal{D} \) is the set of all dyadic spots and \( \mathcal{R} \) is the set of real infinite prime spots of \( k \).
If $\Delta$ represents the discriminant of $f$ in (8), recall that $\Delta$ is the resultant of $f$ and its derivative $f'$ divided by the leading coefficient $a$, that is,

\[
\Delta = \frac{1}{a} \det \begin{pmatrix}
a & 0 & b & c & d & 0 & 0 \\
0 & a & 0 & b & c & d & 0 \\
0 & 0 & a & 0 & b & c & d \\
4a & 0 & 2b & c & 0 & 0 & 0 \\
0 & 4a & 0 & 2b & c & 0 & 0 \\
0 & 0 & 4a & 0 & 2b & c & 0 \\
0 & 0 & 0 & 4a & 0 & 2b & c \\
\end{pmatrix}
\]

(10)

\[
= a(-4b^3c^2 - 27ac^4 + 16b^4d + 144abc^2d - 128ab^2d^2 + 256a^2d^3).
\]

For the curve $C$, we now want to describe the kernel of the map $g$ in (4). According to Proposition 3.1, it suffices to determine the set $S_C$ in (5). The following proposition allows us to do only a finite amount of computation to determine this $S_C$.

Proposition 3.4. Let $C$ be the quartic curve as above over a global field $k$. For $S$ in (9), if $p \notin S$, then $C(\kbar_p) \neq \emptyset$. In other words, $S_C \subseteq S$.

Proof. For each (non-nyadic finite) prime spot $p \notin S$, the curve $C$ has good reduction at $p$ from the definition of $S$. Note then that the reduction of $C$ has a point over the corresponding finite field because any genus 1 curve has at least one point over the finite field by the Hasse-Weil bound. Since this point can be lifted to a $p$-adic point over $\kbar_p$ by Hensel’s lemma, we have $C(\kbar_p) \neq \emptyset$. □

- Special Quartic Case

Next, consider the case in which the coefficient of $x$ in (8) is 0. That is, $C: y^2 = ax^4 + bx^2 + c$.

The discriminant of this quartic polynomial is

\[
\Delta = 16ac(b^2 - 4ac)^2.
\]

In this case, there is a connection between this genus 1 curve $C$ and the genus 0 curve $C_0: y^2 = ax^2 + bx + c$, which reduces a certain amount of work for computing $S_C$ in (5).

Proposition 3.5. Let $C: y^2 = ax^4 + bx^2 + c$ be a curve over a global field $k$. Let $Q = (a, D/k)$ where $D = b^2 - 4ac$. If $p \in \text{supp}(Q)$, then $C(\kbar_p) = \emptyset$. Hence, one has

\[
\text{supp}(Q) \subseteq S_C \subseteq S.
\]

Proof. We first note that if the affine piece of $C: y^2 = ax^4 + bx^2 + c$ contains a rational point, say $(r, s)$, over $k$, then so does $C_0: y^2 = ax^2 + bx + c$ by taking the rational point $(r^2, s)$ over $k$. On the other hand, if $C$ contains nonsingular $k$-rational points at infinity, then the leading coefficient $a$ of $f$ must be a square in $k$ (cf. [8, Theorem 2.5.2]). If this is the case, then the quaternion algebra
$Q$ is split and so $C_0(k) \neq \emptyset$ by the arguments right above (7). To sum up, if $C(k) \neq \emptyset$, then $C_0(k) \neq \emptyset$.

Now, if $p \in \text{supp}(Q)$, then $Q \otimes_k \hat{k}_p$ is nonsplit. This is equivalent to saying that $C_0(\hat{k}_p) = \emptyset$ by Lemma 2.3. It follows from the above arguments that $C(\hat{k}_p) = \emptyset$. Therefore, we obtain $\text{supp}(Q) (= S_{C_0}) \subseteq S_C$. This completes the proof since we already observed that $S_C \subseteq S$ by Proposition 3.4. \hfill \Box

Remark 3.6. Notice that

$$k(C_0) = k(x, \sqrt{ax^2+bx+c}) \cong k(x^2, \sqrt{ax^4+bx^2+c}) \subseteq k(x, \sqrt{ax^4+bx^2+c}) = k(C).$$

This induces a Brauer group map $\text{Br}(k(C_0)) \rightarrow \text{Br}(k(C))$. Moreover, when $k$ is a global field, there exists a map $\text{Br}(\hat{k}_p(C_0)) \rightarrow \text{Br}(\hat{k}_p(C))$ for each $p \in P(k)$. Hence, there is a commutative diagram

$$
\begin{array}{ccc}
\text{Br}(k) & \xrightarrow{g_0} & \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C_0)) \\
\Downarrow & & \Downarrow \\
\text{Br}(k(C)) & \xrightarrow{g} & \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C)).
\end{array}
$$

From this, it is clear that $\ker(g_0)$ is a subset of $\ker(g)$.

Before closing this section, we give specific examples of $\ker(g)$ when $C$ is a quartic curve. Example 3.7(a) below should be compared with the associated conic case in Example 3.3.

**Example 3.7.** (a) Consider the curve

$$C: y^2 = -x^4 + 17x^2 - 361.$$  

Recall then that $D = -1155$ and the corresponding quaternion algebra is $Q = (-1, -1155/Q)$ with $\text{supp}(Q) = \{3, 7, 11, \infty\}$ as shown in Example 3.3. Since the equation of $C$ has discriminant

$$\Delta = 7705328400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 19^2,$$

it follows that $S = \{2, 3, 5, 7, 11, 19, \infty\}$. To determine $S_C$, observe that the equation in (12) has no solution (mod 2$^2$) and the leading coefficient $-1$ of $f$ is not a square 2-adically. This tells us $C(Q_2) = \emptyset$. On the other hand, the reduction of $C$ in (12) contains nonsingular points $(0, 2) \pmod{5}$ and $(1, 4) \pmod{19}$, which can be lifted to $C(Q_5)$ and $C(Q_{19})$ respectively. Using Proposition 3.5, we conclude that $S_C = \{2, 3, 7, 11, \infty\}$ and therefore

$$\ker(g) = \langle [Q_{(2,\infty)}], [Q_{(3,\infty)}], [Q_{(7,\infty)}], [Q_{(11,\infty)}] \rangle \cong \bigoplus_{i=1}^4 \mathbb{Z}/2\mathbb{Z}.$$
A METHOD OF COMPUTING THE CONSTANT FIELD OBSTRUCTION 1439

(b) (General case) Consider the curve

\[ C: y^2 = -3x^4 - 4x^2 + x - 4. \]

Since the equation of \( C \) has discriminant

\[ \Delta = 216333 = 3^2 \cdot 13 \cdot 43^2, \]

it follows that \( S = \{ 2, 3, 13, 43, \infty \} \). To determine \( S_C \), observe that the equation in (13) has no solution (mod \( 3^2 \)) and \(-3\) is not a square 3-adically. This tells us \( C(\mathbb{Q}_3) = \emptyset \). On the other hand, it can be shown that the reduction of \( C \) in (13) contains nonsingular points \((1, 0)\) (mod 2), \((0, 3)\) (mod 13), and \((3, 8)\) (mod 43), which can be lifted to \( C(\mathbb{Q}_2), C(\mathbb{Q}_{13}) \) and \( C(\mathbb{Q}_{43}) \) respectively.

Finally, since \(-3x^4 - 4x^2 + x - 4 < 0\) for all \( x \in \mathbb{R} \) and the leading coefficient of \( f \) is negative, we conclude that \( S_C = \{ 3, \infty \} \) and therefore

\[ \ker(g) = \langle [\mathbb{Q}_{(3, \infty)}] \rangle \cong \mathbb{Z}/2\mathbb{Z}. \]

4. Relative Brauer groups of genus one curves

Let \( C: y^2 = f(x) \), where \( f \) is a quartic polynomial, be a nonsingular projective curve over a field \( k \). In this section, we briefly review recent results on the relative Brauer group \( Br(k(C)/k) \). (See [3] and [1] for details.)

- General Quartic Case

Let \( C: y^2 = f(x) \), where

\[ f(x) = ax^4 + bx^2 + cx + d \]

is a quartic polynomial with \( \text{disc}(f) \neq 0 \). Then the Jacobian \( E \) of \( C \) has the form

\[ E: y^2 = x^3 - 2bx^2 + (b^2 - 4ad)x + ac^2. \]

Note here that \((0, 0)\) is a \( k \)-rational point on \( E \) if and only if \( c = 0 \) in (15) since \( a \neq 0 \). This special case will be covered separately in a more detailed setting later.

If \( E(k) \) denotes the group of rational points over \( k \), then there exists a surjective homomorphism (cf. [1, Propositions 9 and 11])

\[ E(k) \twoheadrightarrow Br(k(C)/k) \text{ given by} \]

\[ O \mapsto 0 \]

\[ (0, 0) \mapsto [(a, b^2 - 4ad/k)] \]

\[ (0, s) \mapsto 0 \quad \text{if } s \neq 0 \]

\[ (r, s) \mapsto [(a, r/k)] \quad \text{if } r \neq 0. \]

If \( c \neq 0 \), notice that \((0, s), s \neq 0 \), is a \( k \)-rational point if and only if \( a \in k^{*2} \). If this happens, the relative Brauer group \( Br(k(C)/k) \) is trivial. Hence, we have:
Proposition 4.1. Let $C: y^2 = ax^4 + bx^2 + cx + d$ be a quartic curve over a field $k$. Then one has

$$\text{Br}(k(C)/k) = \{ [(a, r/k)] \mid (r, s) \in E(k) \} \cup \{0\}.$$ 

In order to provide specific examples with $k = \mathbb{Q}$ when $c \neq 0$, we utilize SAGE (Software for Algebra and Geometry Experimentation; see [7]) as there seems to be no reasonable ways of finding generators of $E(\mathbb{Q})$ by hand. SAGE can compute the ranks of elliptic curves over $\mathbb{Q}$ together with generators of infinite order. This allows us to describe the relative Brauer group $\text{Br}(K/\mathbb{Q})$.

- Special Quartic Case

We now consider the case of (14) in which the coefficient of $x$ becomes zero. That is, let $C: y^2 = f(x)$, where $f(x) = ax^4 + bx^2 + c$. Then the Jacobian $E$ of $C$ has the form

$$E: y^2 = x^3 - 2bx^2 + Dx,$$

where $D = b^2 - 4ac$. Notice that $D \neq 0$ since $\Delta$ in (11) is assumed to be nonzero. Then there exists a group homomorphism (cf. [8, p. 302])

$$\alpha: E(k) \to k^*/k^{*2}$$

defined by

$$\alpha(P) = \begin{cases} 1 \pmod{k^{*2}} & \text{if } P = O, \text{ the point at infinity,} \\ D \pmod{k^{*2}} & \text{if } P = (0,0), \\ r \pmod{k^{*2}} & \text{if } P = (r,s) \text{ with } r \neq 0. \end{cases}$$

For convenience, if we write $t$ for $t \pmod{k^{*2}}$, then Proposition 4.1 above can be rewritten as below:

Corollary 4.2. Let $C: y^2 = ax^4 + bx^2 + c$ be a quartic curve over $k$. Then one has

$$\text{Br}(k(C)/k) = \{ [(a, t/k)] \mid t \in \text{im}(\alpha) \},$$

where $\alpha$ is the map in (18).

If $k$ is a global field, recall then that $E(k)$ is a finitely generated abelian group by the Mordell-Weil Theorem. Since $k^*/k^{*2}$ is 2-torsion, it follows that $\text{im}(\alpha)$ is finite and so is $\text{Br}(k(C)/k)$. Furthermore, with the isogenous curve

$$E': y^2 = x^3 + bx^2 + acx,$$

we can also consider the map

$$\alpha': E'(k) \to k^*/k^{*2}$$

analogous to $\alpha$ for $E$ over $k$. (The map $\alpha'$, likewise $\alpha$, is in fact the connecting homomorphism $H^0(k, E) \to H^1(k, \mu_2)$ arising from an exact sequence $0 \to$...
A METHOD OF COMPUTING THE CONSTANT FIELD OBSTRUCTION

If \( \mu_2 \rightarrow E \rightarrow E' \rightarrow 0 \). If \( r \) denotes the rank of \( E(k) \), then we utilize a well-known formula (cf. [9, p. 91], or see [2, Lemma 5.1] for a more general formula):

\[
\frac{|\text{im}(\alpha)\cdot|\text{im}(\alpha')|}{4} = 2^r
\]

to facilitate computation of \( \text{im}(\alpha) \) and therefore of \( \text{Br}(k(C)/k) \).

5. Obstructions to the Hasse principle for the Brauer groups

Let \( K = k(C) \) be a function field of a curve \( C \) over a global field \( k \). For the scalar extension map \( \theta : \text{Br}(k) \rightarrow \text{Br}(K) \), a class \([B] \in \text{Br}(K)\) is said to be a constant class in \( \text{Br}(K) \) if \([B] = \theta([A])\) for some \([A] \in \text{Br}(k)\). As in (1), for the map

\[
h : \text{Br}(K) \rightarrow \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C)),
\]

let \( \ker_c(h) \) denote the set of all constant classes in the \( \ker(h) \). The nontrivial \( \ker_c(h) \) is the obstruction to the Hasse principle for the Brauer groups of function fields of curves. In this section, we determine all the constant classes that are in \( \ker(h) \) when the curve \( C \) has genus 1 and provide examples.

Proposition 5.1. Let \( k \) be a global field and let \( C : y^2 = f(x) \) where \( f \) is a quartic polynomial over \( k \). Then one has

\[
\ker_c(h) = \left\{ [Q \otimes_k K] \mid Q \text{ is a quaternion algebra over } k \text{ with supp}(Q) \subseteq S_C \right\},
\]

where \( S_C \) is the set in (5). Furthermore, for the map \( g \) in (4), \( \text{Br}(K/k) \) is a subgroup of \( \ker(g) \) and

\[
|\ker_c(h)| = \frac{|\ker(g)|}{|\text{Br}(K/k)|}.
\]

Proof. There is a commutative diagram with the maps as before

\[
\begin{array}{ccc}
\text{Br}(k) & \longrightarrow & \text{Br}(K) \\
i & & |h| \\
\prod_{p \in P(k)} \text{Br}(\hat{k}_p) & \longrightarrow & \prod_{p \in P(k)} \text{Br}(\hat{k}_p(C)).
\end{array}
\]

Since the map \( g \) is the composition of the maps \( i \) and \( j \), we first notice that \( \text{Br}(K/k) \) is a subgroup of \( \ker(g) \). Now, let \([B] \in \ker_c(h)\). Then, by definition, there exists \([A] \in \text{Br}(k)\) such that \([A \otimes_k K] = [B]\). From the commutative diagram, it is apparent that \([A] \in \ker(g)\). By Proposition 3.1, \([A]\) is the class of a quaternion algebra over \( k \) with supp(\(A\)) \subseteq S_C. Finally, it is obvious that \( \ker(g) \) is finite and \(|\ker(g)| = |\text{Br}(K/k)||\ker_c(h)|. \]

It follows immediately from Proposition 5.1 that if \(|S_C| \leq 1\), then \( \ker(g) \) is trivial and so are \( \text{Br}(K/k) = 0 \) and \( \ker_c(h) = 0 \).
Corollary 5.2. If $|S_C| \leq 1$, then $\ker_c(h) = 0$.

Corollary 5.3. If $C$ has a rational point over $k$, then $\ker_c(h) = 0$.

As pointed out earlier in the introduction, the examples of [5] have no non-trivial constant classes in the kernel since the curve $C$ there has a $k$-rational point.

Remark 5.4. If $C$: $y^2 = f(x)$ is an elliptic curve (so deg$(f) = 3$), then $C$ has a nonsingular rational point at infinity. Moreover, if $f(x)$ has odd degree $\geq 5$, then the curve $C$ contains one nonsingular rational point at infinity after realizing $C$ as a projective curve covered by two affine pieces $y^2 = f(x)$ and $x^2 = u^{2g+2} f(\overline{u})$ where $g$ is the genus of the curve $C$. Accordingly, if deg$(f)$ is odd, then $C$ always contains a nonsingular rational point over $k$ and therefore $\ker_c(h)$ is trivial by Corollary 5.3.

We finally provide explicit examples of $\ker_c(h)$ when $k = \mathbb{Q}$. The examples below are immediate consequences of Examples 3.8 together with Proposition 4.1, Corollary 4.2, and Proposition 5.1. Although it is possible to derive by a direct calculation, we instead use SAGE to speed up our computations.

Example 5.5. (a) Let
$$K = \mathbb{Q}(C) = \mathbb{Q}(x, \sqrt{-x^4 + 17x^2 - 361}).$$
Then the corresponding quaternion algebra is $Q = (-1, -1155/\mathbb{Q})$ with supp$(Q) = \{3, 7, 11, \infty\}$. It can be checked that the Jacobian $E$ of $C$ has form
$$E: y^2 = x^4 - 2 \cdot 17x^2 - 3 \cdot 5 \cdot 7 \cdot 11x$$
with rational points $(0, 0), (21, 0), (55, 0)$. Applying (20), we obtain the isogenous curve of the form $E': y^2 = x^4 + 17x^2 + 361x$, which obviously contains a rational point $(0, 0)$. This is sufficient to determine $\text{Br}(K/\mathbb{Q})$. Thus, we have
$$\overline{-3 \cdot 5 \cdot 7 \cdot 11}, \overline{-3 \cdot 7}, \overline{5 \cdot 11} \in \text{im}(\alpha) \quad \text{and} \quad 361 = \overline{19^2} \in \text{im}(\alpha').$$
Moreover, computer calculation shows that $E(\mathbb{Q})$ has rank $0$. Applying formula (21), we have $\text{im}(\alpha) = \langle -3 \cdot 7, 5 \cdot 11 \rangle$. Hence, it follows from (19) that
$$\text{Br}(K/\mathbb{Q}) = \langle \langle [Q_{(2, 3, 7, \infty)}], [Q_{(2, 11)}] \rangle \rangle \cong \bigoplus_{i=1}^{2} \mathbb{Z}/2\mathbb{Z},$$
since supp$(-1, -21/\mathbb{Q}) = \{2, 3, 7, \infty\}$ and supp$(-1, 55/\mathbb{Q}) = \{2, 11\}$. By Example 3.7(a), we see
$$\ker(g) = \langle \langle [Q_{(2, \infty)}], [Q_{(3, \infty)}], [Q_{(7, \infty)}], [Q_{(11, \infty)}] \rangle \rangle \cong \bigoplus_{i=1}^{4} \mathbb{Z}/2\mathbb{Z},$$
and therefore by Proposition 5.1, we conclude that
$$\ker_c(h) = \langle \langle [Q_{(2, \infty)}] \otimes_{\mathbb{Q}} K], [Q_{(3, \infty)}] \otimes_{\mathbb{Q}} K]\rangle \cong \bigoplus_{i=1}^{2} \mathbb{Z}/2\mathbb{Z}. $$
(b) (General case) Let
\[ K = \mathbb{Q}(C) = \mathbb{Q}(x, \sqrt{-3x^4 - 4x^2 + x - 4}) \]
Then the Jacobian of \( C \) has the form
\[ E: y^2 = x^3 + 8x^2 - 32x - 3. \]
Using SAGE, we see that the curve \( E \) has rank 1 with a generator of infinite order \((-1, 6)\). To find rational points of finite order, it can be checked that \( \tilde{E}(\mathbb{F}_5) = 6 \) and \( \tilde{E}(\mathbb{F}_{17}) = 20 \). This tells us that there exists at most one rational point of finite order (with order 2) other than the point at infinity. Since the \( y \)-coordinate of a rational point of order 2 is 0, we see that \((3, 0)\) is the rational point of order 2. So we have \( E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \). Now, observe that \((-3, 3/\mathbb{Q})\) is split but \((-3, -1/\mathbb{Q})\) is nonsplit with \( \text{supp}(-3, -1/\mathbb{Q}) = \{3, \infty\} \). Hence, we have
\[ \text{Br}(K/\mathbb{Q}) = \langle [\mathbb{Q}_{3, \infty}] \rangle \cong \mathbb{Z}/2\mathbb{Z}. \]
By Example 3.7(b), we see
\[ \ker(g) = \langle [\mathbb{Q}_{3, \infty}] \rangle \cong \mathbb{Z}/2\mathbb{Z} \]
and therefore by Proposition 5.1
\[ \ker_c(h) = 0. \]

Acknowledgment. The author would like to thank Prof. A. R. Wadsworth for reviewing and contributing to this paper.

References
[1] D. Haile, and I. Han, *On an algebra determined by a quartic curve of genus one*, J. Algebra 313 (2007), no. 2, 811–823.
[2] D. Haile, I. Han, and A. R. Wadsworth, *Curves \( C \) that are cyclic twists of \( Y^3 = X^3 + c \) and the relative Brauer groups \( \text{Br}(k(C)/k) \)*, Trans. Amer. Math. Soc. 364 (2012), no. 9, 4875–4908.
[3] I. Han, *Relative Brauer Groups of Function Fields of Curves of Genus One*, Comm. Algebra 31 (2003), no. 9, 4301–4328.
[4] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, Cambridge, 2006.
[5] R. Parimala and R. Sujatha, *Hasse principle for Witt groups of function fields with special reference to elliptic curves*, Duke Math. J. 85 (1996), no. 3, 555–582.
[6] P. Roquette, *Splitting of algebras by function fields of one variable*, Nagoya Math. J. 27 (1966), 625–642.
[7] SAGE Mathematical Software, Version 2.6, http://www.sagemath.org.
[8] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[9] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.

Ilseop Han
Department of Mathematics
California State University, San Bernardino
San Bernardino, CA 92407, USA
E-mail address: ihan@csusb.edu