On the Arithmetic of Hyperelliptic Curves

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citable link</td>
<td><a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:33493477">http://nrs.harvard.edu/urn-3:HUL.InstRepos:33493477</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA">http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA</a></td>
</tr>
</tbody>
</table>
On the Arithmetic of Hyperelliptic Curves

A dissertation presented

by

Jason Charles Bland

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University
Cambridge, Massachusetts

March 2016
© 2016 – Jason Charles Bland
All rights reserved.
On the Arithmetic of Hyperelliptic Curves

Abstract

My research involves answering various number-theoretic questions involving hyperelliptic curves. A hyperelliptic curve is a generalization of elliptic curves to curves of higher genus but which still have explicit equations.

The first part of this thesis involves examining moduli of hyperelliptic curves and in particular, compare their field of moduli with possible fields of definition of the curve. For even genus $g$, a general hyperelliptic curve of genus $g$ cannot be defined over its field of moduli. Meanwhile, in odd genus, this can be done for curves which admit only two automorphisms, but the curve constructed may not be a hyperelliptic curve in the familiar sense.

The second part involves the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. The 2-Selmer group is a subgroup of the Galois cohomology group $H^1(K, J[2])$, and $J[2]$ is preserved by quadratic twists, so one may consider how the 2-Selmer rank varies over quadratic twists. I show that starting with any hyperelliptic curve with a rational Weierstrass point, the 2-Selmer rank is unbounded over quadratic twists.
Part 1. Obstructions to the Field of Definition

1. Introduction

2. Relevant Arithmetic Invariant Theory

2.1. The Twisted Representation

2.2. An Obstruction to Lifting

3. Moduli of Interest

3.1. The Moduli Space of Binary Forms

3.2. The Relative Curve Over Moduli Space

4. Lifts From Moduli Space

4.1. Lifting to Binary Forms

4.2. Lifting to Hyperelliptic Curves

5. Interpretation of $\mathfrak{A}_{2g+2}$

6. Invariants of Systems of Binary Quadratic Forms

7. The Genus 2 Case

7.1. Constructing the Twisted Representation

7.2. Genus 2 Curves With Stabilizer

8. The Moduli Space as an $SL(3)$-Quotient

Part 2. The 2-Selmer Group May be Arbitrarily Large

9. Introduction

10. Cohomology Classes Arising From 2-Torsion

11. Proof of Theorem 9.4

11.1. The Reducible Case

11.2. The Irreducible Case

References
My research involves answering various number-theoretic questions involving hyperelliptic curves. A hyperelliptic curve is a generalization of elliptic curves (genus 1 curves, with a marked point to be more precise) to curves of higher genus but which still have explicit equations. There are two possible ways one may define a hyperelliptic curve:

(1) A curve $C$ with a map $\varphi : C \to \mathbb{P}^1$ of degree 2.

(2) A curve $C$ such that the canonical map $C \to \mathbb{P}^{2g-2}$ has degree 2.

The curves that satisfy definition (1) are described by an equation of the form

\begin{equation}
    y^2 = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1}z + \cdots + a_0z^{2g+2}
\end{equation}

inside the weighted projective space $\mathbb{P}(1, 1, g + 1)$, where $g$ is the genus of $C$. The map $\varphi$ is given by $[x : z]$, and is branched at $2g + 2$ points, which are precisely the Weierstrass points of $C$. The smoothness of the curve amounts to the discriminant of the binary form on the right hand side being nonzero. Often one simply uses affine coordinates and writes $y^2 = f(x)$ where $f$ is a polynomial of degree $2g + 1$ or $2g + 2$.

In genus $g \geq 2$, definition (1) implies (2). Furthermore, the map $\varphi$ is unique up to an automorphism of $\mathbb{P}^1$. Meanwhile, the image of the canonical map has genus zero, so (2) implies (1) over an algebraically closed field, but not necessarily over an arbitrary field. For example, $C$ could be a double cover of a conic which contains no points over the base field. This is possible precisely for odd $g$, and we give constructions in Section 4.

Recall that the divisors of degree zero in $C$ form an abelian variety of dimension $g$, called the Jacobian of $C$ and denoted by $J$ here. If a base point $P_0$ of $C$ is given, then $C$ embeds into $J$ via associating to any point $P$ the divisor $P - P_0$. The study of $J$ is a useful tool to understand $C$. For example, in order to determine the $K$-points of $C$ for a field $K$, one might first try to determine the $K$-points of $J$, and then determine
which such points lie in the image of $C \hookrightarrow J$. The advantage of $J$ is that $J(K)$ is an abelian group, and if $K$ is a number field then this group is finitely generated.

As for the $K$-points of $J$, an important step in determining this group is the 2-Selmer group $S_2(K, J)$ a finite abelian group that will be defined later. The group $S_2(K, J)$ lies inside the cohomology group $H^1(K, J[2])$, for $J[2]$ the 2-torsion subgroup of $J$. $J[2]$ is generated by the differences $P - Q$ where $P$ and $Q$ are Weierstrass points, so when working with $J[2]$ it can be useful for $C$ to have a Weierstrass point over $K$, which we may move to $1$. In this case $a_{2g+2} = 0$ and so $C$ is given by the equation

\[(0.2) \quad y^2 = a_{2g+1}x^{2g+1}z + a_{2g}x^{2g}z^2 + \cdots + a_0 z^{2g+2}.\]

Now for nonzero $d \in K$ we may consider the quadratic twist of $C$ defined by

\[(0.3) \quad dy^2 = a_{2g+1}x^{2g+1}z + a_{2g}x^{2g}z^2 + \cdots + a_0 z^{2g+2}.\]

(The quadratic twist makes sense for arbitrary hyperelliptic curves as well.) This curve is isomorphic to $C$ over the algebraic closure of $K$, but not over $K$ unless $d$ is a square. Also the quadratic twist fixes the Weierstrass points and hence $J[2]$. On the other hand, arithmetic entities such as $S_2(K, J)$ may change. In this way, starting from $C$ we get a family of curves parameterized by $K^\times/(K^\times)^2$, and we might ask what 2-Selmer groups are possible. In Part 2 I show that the size of $S_2$ is unbounded. Unfortunately, this almost certainly will not translate into unboundedness of the rank of $J(K)$, given the difficulty of finding abelian varieties with large rank and the fact that the large sets of 2-Selmer elements constructed are done so without associating them to points of $J(K)$. However, showing that such points do not arise from $K$-points of $J$ would involve a local-to-global obstruction, and is a topic of future research.

Another project I have worked on involves moduli of hyperelliptic curves. In general, the set of isomorphism classes of curves of a fixed genus $g \geq 2$ admits the natural
structure of a quasiprojective variety, called the moduli space of curves of genus $g$. Inside this space we may consider the locus consisting of hyperelliptic curves. The moduli space is an important tool in the understanding of algebraic curves.

One question we might ask is given a point in moduli space, to produce a curve mapping to this point. One measure of the difficulty of such a procedure would be to consider possible fields of definition of such curves. For example, in the case of elliptic curves, the moduli space of elliptic curves is parameterized by a single number, the $j$-invariant. Now it is possible to find an elliptic curve with $j$-invariant $t$ whose coefficients are rational functions of $t$. This automatically shows that a curve may be defined over its field of moduli. On the other hand, any gap between the field of moduli of a curve and its possible fields of definition will introduce complexity into algebraic functions required to construct a curve.

It has been known that the field of moduli is not always a field of definition. Counterexamples have been known both for abelian varieties of even dimension and for curves of genus 2. My work generalizes the genus 2 situation, as all genus 2 curves are hyperelliptic. It turns out that for even genus $g$, a general hyperelliptic curve of genus $g$ cannot be defined over its field of moduli. However, in odd genus, this can be done, at least for those curves which admit only two automorphisms. The caveat is that such curves might not be double covers of $\mathbb{P}^1$ — only of conics in general. In Part I, I give obstructions to defining a hyperelliptic curve over its field of moduli and show what objects can be constructed in their place. It turns out that the genus zero curve given by quotienting $C$ by its hyperelliptic involution can be constructed in the automorphism-free case.

I’ve also looked at one case of curves which have extra automorphisms. Here there are some general tools that can be used, but in order to understand the possible outcomes one needs to have an idea of what curves to look for.
Part 1. Obstructions to the Field of Definition

1. Introduction

Often when dealing with algebraic objects, we want them to be defined over a reasonable field. Fix a field $K$ and let $X$ be an algebraic variety defined over $K^s$, the separable closure of $K$. Then we say $K$ is a field of definition of $X$ if $X$ is $K^s$-isomorphic to $Y \times_K K^s$ for some variety $Y$ defined over $K$.

The most basic obstruction to a field of definition is the field of moduli, which utilizes the action of the Galois group $\text{Gal}(K^s/K)$ on varieties defined over $K^s$. We say an extension $K'$ of $K$ is the field of moduli of $X$ if

$$\sigma X \cong X \iff \sigma \in \text{Gal}(K^s/K').$$

The field of moduli of $X$ depends only on the $K^s$-isomorphism class of $X$. If $X$ is already defined over an extension $L$ of $K$, then for $\sigma \in \text{Gal}(K^s/L)$, $\sigma X$ is identical to $X$. Hence every field of definition of $X$ must contain the field of moduli.

This raises the question of whether a variety may be defined over its field of moduli. This question is related to the problem of explicitly constructing an object from its invariants, or equivalent given its point in a moduli space. If $\mathcal{M}$ is a moduli space over $K$ for objects such as $X$, then $X$ has field of moduli contained in $L$ if and only if $[X] \in \mathcal{M}(L)$. As a result, a construction of $X$ from $[X]$ would limit the gap between a variety’s field of moduli and its possible fields of definition.

A well-known example is the case of elliptic curves. There is an explicit elliptic curve defined over the ring $R = \mathbb{Z}[t, \frac{1}{(t-1728)}]$ (in particular, its discriminant is a unit in $R$) with $j$-invariant $t$. This shows directly that every elliptic curve with $j$-invariant not equal to 0 or 1728 can be defined over its field of moduli. (This statement is still true for the two exceptional $j$-invariants, as shown by the curves $y^2 + y = x^3$ and $y^2 = x^3 - x$.)
On the other hand, it is known that there exist principally polarized abelian varieties of every even dimension which cannot be defined over their field of moduli. This illustrates that the question of whether a variety can be defined over its field of moduli is nontrivial.

We will be interested in the case of hyperelliptic curves. Let $\mathcal{H}_g$ denote the moduli space of hyperelliptic curves of genus $g \geq 2$, and suppose $K$ is a field of characteristic zero (such as a $p$-adic field or a number field). Given a $K$-point of $\mathcal{H}_g$ (or possibly in some compactification of $\mathcal{H}_g$), we would like to know whether this point arises from a curve defined over $K$.

One simple result that follows from this work is:

**Theorem 1.1.** Let $K$ be a $p$-adic field or a number field. Then every hyperelliptic curve of genus $g \geq 2$ with only two automorphisms and field of moduli contained in $K$ admits $K$ as a field of definition if and only if $g$ is odd.

Note that a hyperelliptic curve of genus $g$ is a double cover of $\mathbb{P}^1$ branched at $2g+2$ points, and this double cover is in fact the canonical series. Thus when studying hyperelliptic curves we may instead consider $\mathbb{P}^1$ with specified effective divisors of degree $2g+2$, which in turn are given by binary forms of degree $2g+2$ up to scaling. The advantage of using binary forms is that here the ambient space admits the structure of a vector space, and so we may use representation theory to aid in the description of the orbits.

We expect that much of our work will also apply when $K$ has positive characteristic $p > 2g + 1$.

2. **Relevant Arithmetic Invariant Theory**

Suppose $X$ is a variety defined over $K$, usually $X = V$ a vector space, and $G$ is a reductive group defined over $k$. Let $Y = X//G$ be the quotient. Arithmetic invariant theory seeks to answer the question of what $K$-points on the quotient $Y$ reveal about
K-orbits of X or related objects when K is not separably closed. Letting \( \pi : X \to Y \) be the projection map, we will only consider \( y \in Y \) for which \( G(K^s) \) acts transitively on the fiber \( \pi^{-1}(y) \), and assume this is the case from now on unless stated otherwise.

**Proposition 2.1.** Given \( x \in X(K) \) with \( \pi(x) = y \), the \( G(K) \)-orbits lying within the fiber \( X_y(K) \) are in bijection with the pointed set

\[
\ker \left( \gamma : H^1(K, G_x) \to H^1(K, G) \right)
\]

where \( G_x \) is the stabilizer of \( x \) in \( G \), an algebraic group defined over \( K \).

**Proof.** Suppose \( x' \in X_y(K) \). Since \( G(K^s) \) acts transitively on \( \pi^{-1}(y) \), there exists \( g \in G(K^s) \) with \( x' = gx \), uniquely determined up to right multiplication by \( G_x(K^s) \).

But now for \( \sigma \in \text{Gal}(K^s/K) \), applying \( \sigma \) gives \( x' = \sigma(g)x \), and so \( g^{-1}\sigma(g) \in G_x(K^s) \). Let

\[
c_\sigma = g^{-1}\sigma(g).
\]

Then \( c_\sigma \) is a \( G_x(K^s) \)-valued cochain which is a \( G(K^s) \)-valued coboundary (in particular, a cocycle), so \( c_\sigma \in H^1(K, G_x) \) and \( \gamma(c) = 0 \). If we replace \( g \) by \( gs \) for \( s \in G_x(K^s) \), then \( c_\sigma \) will be replaced by \( s^{-1}c_\sigma s \), so the class of \( c_\sigma \in H^1(K, G_x) \) is independent of \( g \). Also, another point in \( X_y(K) \) in the same \( G(K) \)-orbit as \( x' \) is of the form \( hx' \) for some \( h \in G(K) \), in which case \( hx' = hgx \) and so \( c_\sigma \) is replaced by

\[
(hg)^{-1}\sigma(hg) = (g^{-1}h^{-1})(h\sigma(g)) = g^{-1}\sigma(g) = c_\sigma
\]

and so \( c_\sigma \) only depends on the \( G(K) \)-orbit of \( x' \).

Conversely, given \( c_\sigma \in H^1(K, G_x) \) with \( \gamma(c) = 0 \), we will produce a \( G(K) \)-orbit in \( X_y(K) \). Since \( \gamma(c) = 0 \), \( c_\sigma \) becomes a \( G(K^s) \)-valued coboundary, and so \( c_\sigma = g^{-1}\sigma(g) \).
for some \( g \in G(K^s) \). Letting \( x' = gx \), we have

\[
(2.4) \quad \sigma(x') = \sigma(g)x = g (g^{-1} \sigma(g)) x = gx = x'
\]

and so \( x' \in X(K) \), necessarily in \( X_g(K) \) is \( \pi \) is \( G \)-invariant. A different choice of element \( g' \in G(K^s) \) with \( c_\sigma = (g')^{-1} \sigma(g') \) requires \( \sigma(g') \sigma(g)^{-1} = g'g^{-1} \), and so \( g'g^{-1} \in G(K) \). This means \( g'x \) will be in the same \( G(K) \)-orbit as \( gx = x' \), and so the associated \( G(K) \)-orbit is well-defined.

2.1. **The Twisted Representation.** In the case \( X = V \), we can assign \( K \)-orbits to the remaining elements of \( H^1(K, G_x) \). Elements \( c \in H^1(K, G) \) are called *pure inner forms*. Given \( c \), let \( G^c \) be the inner form associated to the element in \( H^1(K, G^{ad}) \) induced from \( c \). Specifically, \( G^c(K^s) = G(K^s) \) with the Galois action on \( G^c \) given by

\[
(2.5) \quad \sigma^c(g) = c_\sigma \sigma(g) c_\sigma^{-1}.
\]

We also obtain a representation of \( G^c \) from \( V \) as follows: letting \( \rho : G \rightarrow GL(V) \) the the homomorphism corresponding to the \( G \)-action, \( \rho_\sigma(c) \) lies in \( H^1(K, GL(V)) \) and must be trivial. Therefore there exists \( h \in GL(V)(K^s) \) such that

\[
(2.6) \quad \rho(c_\sigma) = h^{-1} \sigma(h).
\]

Given \( h \), we can produce \( \rho_h : G^c(K^s) \rightarrow GL(V)(K^s) \) defined by

\[
(2.7) \quad \rho_h(g) = h \rho(g) h^{-1}
\]

which is compatible with the Galois action, therefore yielding a \( K \)-representation of \( G^c \). Furthermore, a different choice of \( h \) gives an isomorphic representation. So we will write \( V^c \) for the representation of \( G^c \) and call \( V^c \) the *twisted representation* of \( V \) associated to the pure inner form \( c \).
Recall that $Y = X/G = V/G$ and $\pi : V \to Y$ is the natural map. We give a map $\pi^c : V^c \to Y$ which identifies $Y$ with $V^c/G^c$. The map is given by

(2.8) \quad \pi^c(v) = \pi(h^{-1}v).

$\pi^c$ is $G^c$-invariant because

(2.9) \quad \pi^c(g^cv) = \pi^c(gh^{-1}v) = \pi(gh^{-1}v) = \pi(h^{-1}v) = \pi^c(v).

We may now consider the fibers $V_y^c = (\pi^c)^{-1}(y)$ for $y \in Y$, which are preserved by $G^c$. Explicitly,

(2.10) \quad V_y^c(K) = \left\{ v \in V^c(K) = V(K) \middle| \pi^c(v) = y \right\}

(2.11) = V(K) \cap hV_y(K^s).

**Proposition 2.2.** Given $v \in V(K)$ such that $\pi(v) = y$, then for every $c \in H^1(K, G)$, there is a bijection between $\gamma^{-1}(c)$ and the set of $G^c(K)$-orbits in $V_y^c(K)$. Here

(2.12) \quad \gamma : H^1(K, G_v) \to H^1(K, G)

is as before.

**Proof.** This is a generalization of the previous proposition in the case $X = V$. Suppose $w \in V_y^c(K)$. Since $h^{-1}w \in V_y(K^s)$, there exists $g \in G(K^s)$ with $h^{-1}w = gv$, unique up to right multiplication by $G_v(K^s)$. Then $w = hgv$ is fixed by $\text{Gal}(K^s/K)$, so $G_v(K^s)$ contains

(2.13) \quad (hg)^{-1}\sigma(hg) = g^{-1}h^{-1}\sigma(h)\sigma(g) = g^{-1}c_\sigma\sigma(g).

Let $\chi_\sigma$ be this cochain. Then as in the previous proposition, $\chi_\sigma \in H^1(K, G_v)$ is independent modulo coboundary of the choice of $g$, and $\gamma(\chi) = c$. Moreover, $\chi$ only depends on the $G^c(K)$-orbit of $w$; a $w'$ in this orbit has the form $w' = hg'h^{-1}w = \dots$
$hg'gv$ for some $g' \in G^c(K)$, and so $h^{-1}w' = g'gv$. This replaces $g$ by $g'g$, and hence replaces $\chi_\sigma$ by

\begin{align}
(g'g)^{-1}c_\sigma \sigma(g'g) &= g^{-1}(g')^{-1}c_\sigma \sigma(g')\sigma(g) \\
&= g^{-1}(g')^{-1}c_\sigma (c_\sigma^{-1}g'c_\sigma) \sigma(g) \\
&= g^{-1}c_\sigma \sigma(g)
\end{align}

which is still $\chi_\sigma$.

Conversely, given $\chi \in \gamma^{-1}(c)$, we must have $\chi_\sigma = g^{-1}c_\sigma \sigma(g)$ for some $g \in G(K^s)$, and then let $w = hgv$. An argument similar to the previous proposition shows that $w \in V^c_y(K)$, and a different choice of $g$ produces an element in the same $G^c(K)$-orbit. □

2.2. An Obstruction to Lifting. Given $y \in Y(K)$, there may not be an $x \in X(K)$ such that $\pi(x) = y$; in other words, $X_y(K)$ is empty.

One possibility for $X = V$ is that $y$ does have a lift $x' \in V^c_y(K)$ for some $c \in H^1(K,G)$. In this case, associated to $x'$, we obtain a map

\begin{equation}
\gamma' : H^1(K, G^c_y) \to H^1(K, G^c)
\end{equation}

and then we may determine whether $V_y$ contains any $K$-points by considering $V$ as a twisted representation of $V^c$.

Here we describe another obstruction for any $X$, provided the stabilizer of a lift of $y$ (over $K^s$) is abelian. First we show:

**Proposition 2.3.** There is a canonical group scheme $G_y$ defined over $K$ along with isomorphisms $\iota_x : G_y(K^s) \to G_x$ for every $x \in X_y(K^s)$.

**Proof.** If $x \in X_y(K^s)$, then any other element $x' \in X_y(K^s)$ has the form $x' = gx$ for $g$ uniquely determined up to right multiplication by $G_x$. Now $sx' = x'$ if and only if
sgx = gx, or rather $g^{-1}sgx = x$, so $G_{x'} = gG_xg^{-1}$. Furthermore, conjugation by $g$ on $G_x$ is independent of the choice of $g$, since a different choice of $g$ has the form $gt$ for $t \in G_x$, and $G_x$ is abelian, so conjugation by $t$ fixes $G_x$.

We obtain a collection of isomorphisms $G_x \to G_{x'}$ for every $x, x' \in X_y(K^s)$, which are compatible under composition. So we may define the group $G_y$ over $K^s$ along with isomorphisms $\iota_x : G_y \to G_x$, with the property that

\begin{equation}
(2.18) \quad \iota_{gx}(a) = g\iota_x(a)g^{-1}.
\end{equation}

We now define a Galois action on $G_y$, which allows us to descend $G_y$ to $K$. For $\sigma \in \text{Gal}(K^s/K)$ and $x \in X_y(K^s)$, we have $\sigma(x) \in X_y(K^s)$, and if $s \in G_x$, then $\sigma(s) \in G_{\sigma(x)}$. We define our Galois action on $G_y$ by

\begin{equation}
(2.19) \quad \sigma(a) = \iota_{\sigma(x)}^{-1}\left(\sigma(\iota_x(a))\right).
\end{equation}

We need to know that this map $\text{Gal}(K^s/K) \to \text{Aut}(G_y)$ is independent of $x$ and a homomorphism. To see that it is well-defined, a different choice of lift of $y$ has the form $gx$ for some $g \in G(K^s)$, and then

\begin{align}
(2.20) \quad & \iota_{gxa}^{-1}\left(\sigma(\iota_{gx}(a))\right) = \iota_{g(x)}^{-1}\sigma(g\iota_x(a)g^{-1}) \\
(2.21) \quad & = \iota_{g(x)}^{-1}\left(\sigma(g)\sigma(\iota_x(a))\sigma(g)^{-1}\right) \\
(2.22) \quad & = \iota_{\sigma(x)}^{-1}\left(\sigma(\iota_x(a))\right).
\end{align}

To show this is a group action, fix $x \in X_y(K^s)$. Then we have

\begin{equation}
(2.23) \quad \sigma \left(\tau(a)\right) = \sigma \left(\iota_{\tau(x)}^{-1}\left(\tau(\iota_x(a))\right)\right)
\end{equation}
(now using $\tau(x)$ as our lift of $y$ for $\sigma$)

\begin{align*}
(2.24) & \quad = \iota^{-1}_{\sigma(\tau(x))}\left(\sigma\left(\iota^{-1}_{\tau(x)}\left(\iota^{-1}_{\tau(x)}\left(\tau(\iota_x(a))\right)\right)\right)\right) \\
(2.25) & \quad = \iota^{-1}_{\sigma(\tau(x))}\left(\sigma\left(\tau(\iota_x(a))\right)\right) \\
(2.26) & \quad = (\sigma \circ \tau)(a).
\end{align*}

Now we define the obstruction class $d \in H^2(K, G_y)$ as follows: if $x \in X_y(K^s)$, then there exists $g_\sigma \in G(K^s)$ such that $g_\sigma^\sigma x = x$, uniquely determined up to left multiplication by $G_x$. Now $g_\sigma^\sigma g_\tau g_{\sigma \tau}^{-1} \in G_x$, and so we define

\begin{equation}
(2.27) \quad d_{\sigma, \tau} = \iota^{-1}_x \left( g_\sigma^\sigma g_\tau g_{\sigma \tau}^{-1} \right).
\end{equation}

The class $d \in H^2(K, G_y)$ is independent of the choice of $g_\sigma$ for a given $x$ by a standard argument. A different choice of $g_\sigma$ would amount to replacing $g_\sigma$ by $s_\sigma g_\sigma$ for some $s_\sigma \in G_x$. Let $a_\sigma = \iota^{-1}_x(s_\sigma) \in G_y(K^s)$. Then we have

\begin{align*}
(2.28) & \quad (s_\sigma g_\sigma)^\sigma (s_\tau g_\tau)(s_{\sigma \tau} g_{\sigma \tau})^{-1} = s_\sigma g_\sigma^\sigma s_\tau^\sigma g_{\sigma \tau} g_{\sigma \tau}^{-1} s_{\sigma \tau}^{-1} \\
(2.29) & \quad = s_\sigma g_\sigma^\sigma \iota_x(a_\tau)^\sigma g_{\sigma \tau} g_{\sigma \tau}^{-1} s_{\sigma \tau}^{-1} \\
(2.30) & \quad = s_\sigma g_\sigma^\sigma \iota_x(a_\tau)^{\sigma}(a_\tau)^\sigma g_{\sigma \tau} g_{\sigma \tau}^{-1} s_{\sigma \tau}^{-1} \\
\quad \text{(now using $\sigma(x) = g_\sigma^{-1} x$)}
\end{align*}

\begin{align*}
(2.31) & \quad = s_\sigma g_\sigma^\sigma g_{\sigma}^{-1} \iota_x(\sigma a_\tau)g_\sigma^\sigma g_{\sigma \tau} g_{\sigma \tau}^{-1} s_{\sigma \tau}^{-1} \\
(2.32) & \quad = s_\sigma \iota_x(\sigma a_\tau)^\sigma g_\sigma^\sigma g_{\sigma \tau} g_{\sigma \tau}^{-1} s_{\sigma \tau}^{-1}.
\end{align*}
(now using the fact that $G_x$ is abelian)

(2.33) \[ = s_{\sigma}t_x(\sigma a_{\tau})s_{\sigma_{\tau}}^{-1}\left( g_{\sigma}^\sigma g_{\tau} g_{\sigma_{\tau}}^{-1} \right) \]

(2.34) \[ = t_x\left( a_{\sigma}^\sigma a_{\tau} a_{\sigma_{\tau}}^{-1} \right) g_{\sigma}^\sigma g_{\tau} g_{\sigma_{\tau}}^{-1} \]

and so $d_{\sigma,\tau}$ is changed only by the $G_y$-valued coboundary $a_{\sigma}^\sigma a_{\tau} a_{\sigma_{\tau}}^{-1}$. The class $d$ is also independent of $x$ because a different choice of lift has the form $hx$ for some $h \in G(K^s)$, and then we may replace $g_{\sigma}$ with $g'_{\sigma} = h g_{\sigma}^\sigma h^{-1}$, which relates $\sigma(hx)$ to $hx$. Now

(2.35) \[ t_{hx}^{-1}\left( g'_{\sigma}^\sigma g'_{\tau}(g'_{\sigma_{\tau}})^{-1} \right) = t_{hx}^{-1}\left( \left( h g_{\sigma}^\sigma h^{-1} \right)^{\sigma} \left( h g_{\tau}^\tau h^{-1} \right) \left( h g_{\sigma_{\tau}}^\sigma h^{-1} \right)^{-1} \right) \]

(2.36) \[ = t_{hx}^{-1}\left( \left( h g_{\sigma}^\sigma h^{-1} \right) \left( \sigma h_{\sigma}^\sigma g_{\tau} g_{\sigma_{\tau}}^{-1} h^{-1} \right) \left( \sigma h g_{\sigma_{\tau}}^\tau h^{-1} \right) \right) \]

(2.37) \[ = t_{hx}^{-1}\left( h g_{\sigma}^\sigma g_{\tau} g_{\sigma_{\tau}}^{-1} h^{-1} \right) \]

(2.38) \[ = t_{x}^{-1}\left( g_{\sigma}^\sigma g_{\tau} g_{\sigma_{\tau}}^{-1} \right). \]

Now if $X_y(K)$ is nonempty, then we may take $x \in X_y(K)$ and $g_{\sigma} = 1$, so that $d$ is trivial. This proves the first part of:

**Proposition 2.4.** Suppose $G_x$ is abelian for $x \in X_y(K^s)$. Define $G_y$ and $d$ as above. Then:

1. If $X_y(K)$ is nonempty, then $d$ is trivial.
2. If $X = V$, then $d$ is invariant under pure inner twists. In particular, if $V_y^c(K)$ is nonempty, then $d$ is trivial.
3. If $d$ is trivial and $H^1(K, G) = 0$, then $X_y(K)$ is nonempty.
4. If $X = V$ and $d$ is trivial, then $V_y^c(K)$ is nonempty for some $c \in H^1(K, G)$.

**Proof.** To prove (2), suppose $c \in H^1(K, G)$ is a given cocycle and fix $h \in GL(V)(K^s)$ for which $c_{\sigma} = h^{-1}\sigma(h)$. Also fix $v \in V_y(K^s)$ and $g_{\sigma}$ with $g_{\sigma}^\sigma v = v$. Then $hv \in
So a pure inner twist amounts to replacing \( g_{\sigma} \) with \( g_{\sigma}c_{\sigma}^{-1} \) as well as replacing \( (g_{\sigma}) \) with \( c_{\sigma}(g_{\sigma})c_{\sigma}^{-1} \). But

\[
(2.40) \quad \left( g_{\sigma}c_{\sigma}^{-1} \right) \left( c_{\sigma} \left( g_{\tau}c_{\tau}^{-1} \right) c_{\sigma}^{-1} \right) \left( g_{\tau\sigma}c_{\tau\sigma}^{-1} \right)^{-1} = g_{\sigma}g_{\tau}(c_{\tau})^{-1}c_{\tau\sigma}^{-1}c_{\sigma\tau}g_{\sigma\tau}^{-1} = g_{\sigma}g_{\tau}g_{\sigma\tau}^{-1}
\]

showing that \( d \) remains unchanged.

To prove (3) and (4), fix \( x \in X_{y}(K) \). Then it’s enough to show:

**Claim 2.5.** If \( d \) is trivial, then the \( g_{\sigma} \) may be chosen to form a cocycle.

The claim implies (3) since if \( H^{1}(K, G) \) is trivial, then \( g_{\sigma} = h^{-1}\sigma(h) \) for some \( h \in G(K^{s}) \), and then \( hx \in X(K) \). It implies (4) by the same reasoning, using an appropriate \( h \in GL(V)(K^{s}) \) so that \( hx \in V_{y}(K^{s}) \) for \( c_{\sigma} = g_{\sigma} \).

It remains to show the claim. If \( d \) is trivial, then it is a \( G_{y} \)-valued coboundary, so there exist \( b_{\sigma} \in G_{y}(K^{s}) \) for which

\[
(2.41) \quad \tau_{x}^{-1} \left( g_{\sigma}^{-1}g_{\tau}g_{\sigma\tau}^{-1} \right) = b_{\sigma}^{-1}b_{\tau}^{-1}b_{\sigma\tau}^{-1}.
\]

Now letting \( a_{\sigma} = b_{\sigma}^{-1} \) and using the commutativity of \( G_{y} \), we find

\[
(2.42) \quad \tau_{x} \left( a_{\sigma}^{-1}a_{\tau}a_{\sigma\tau}^{-1} \right) g_{\sigma}g_{\tau}g_{\sigma\tau}^{-1} = 1.
\]

But by the computations showing that \( d \) was well-defined, taking \( g'_{\sigma} = \tau_{x} \left( a_{\sigma} \right) g_{\sigma} \) shows that

\[
(2.43) \quad (g'_{\sigma})^{\sigma}(g'_{\tau})g'_{\sigma\tau}^{-1} = 1
\]

which verifies the claim. \( \square \)
As an example, we show that we may always lift $\mathbb{G}_m$-quotients:

Lemma 2.6. Suppose $G = \mathbb{G}_m$. Then $d$ is trivial and $X_y(K)$ is nonempty.

Proof. First, observe that $G$ is abelian. In this case, choose $x \in X_y(K^*)$. Then we have a map $j : G_y(K^*) \to G(K^*)$ by composing $t_x$ with inclusion of $G_x$ into $G(K^*)$. This map is seen to independent of $x$ and compatible with the Galois action, and therefore descends to a map $G_y \to G$ of group schemes. Now $t_x(d_{\sigma, \tau}) = g_{\sigma} g_{\tau} g_{\sigma \tau}^{-1}$, which is visibly a coboundary in $G$, so

$$d \in \ker \left( j : H^2(K, G_y) \to H^2(K, G) \right) = \text{im} \left( \delta : H^1(K, G/G_y) \to H^2(K, G_y) \right).$$

But for $G = \mathbb{G}_m$, $G/G_y$ is either trivial or isomorphic to $\mathbb{G}_m$. In each of these cases, $H^1(K, G/G_y)$ is trivial, so $d$ is trivial. Finally, since $H^1(K, \mathbb{G}_m)$ is trivial, $d$ being trivial implies $X_y(K)$ is nonempty. \qed

3. Moduli of Interest

3.1. The Moduli Space of Binary Forms. Fix a positive integer $n \geq 3$. If $W$ is the standard representation of $SL(2)$, then $V_n = \text{Sym}^n W$ is a vector space of dimension $n + 1$ with an action of $SL(2)$. If $n$ is even, this action descends to an action of $PGL(2)$, since $-I$ acts trivially. In this case $V_n = \text{Sym}^n W \otimes (\Lambda^2 W)^{\otimes -n/2}$ as a $GL(2)$-representation. Let $S_n$ denote the ring of invariants of the symmetric algebra of $V_n$, graded by degree, and consider the spaces

$$\mathfrak{A}_n = \text{Spec } S_n$$
$$\mathfrak{B}_n = \text{Proj } S_n$$

These spaces arise as categorical quotients as $\mathfrak{A}_n = V_n/\!/ SL(2)$ and $\mathfrak{B}_n = (\mathfrak{A}_n \setminus 0)//\! \mathbb{G}_m$.

$\mathfrak{B}_n$ is called the moduli space of semistable binary forms. It is a fact that a binary form is semistable if and only if every root has multiplicity at most $n/2$, and stable if
and only if every root has multiplicity strictly less than \( \frac{n}{2} \). In the case where \( n \) is even, the locus of strictly semistable binary forms is mapped down to a single point in \( \overline{B}_n \), called the semistable point.

Inside \( \overline{B}_n \), we may consider \( B_n \), the locus of stable binary forms, and \( B_{n}^{\text{sm}} \), the locus of smooth binary forms (those without repeated roots). Then \( B_{n}^{\text{sm}} \) is easily seen to be isomorphic to the moduli space \( \mathcal{M}_{0,n} \) of smooth genus 0 curves with \( n \) (unordered) marked points. Thus \( \overline{B}_n \) can be seen as an alternate compactification of \( \mathcal{M}_{0,n} \), differing from the moduli space \( \overline{\mathcal{M}}_{0,n} \) of stable genus 0 curves with \( n \) marked points. In fact, the natural isomorphism extends to a map \( \overline{\mathcal{M}}_{0,n} \to \overline{B}_n \), which contracts most components of the boundary divisor to smaller dimensional spaces.

If \( n = 2g + 2 \) is even, then we may consider the closure \( \overline{\mathfrak{H}}_g \) of \( \mathfrak{H}_g \) in \( \overline{\mathcal{M}}_g \), which may be identified with the Hurwitz space of admissible degree 2 covers of stable genus 0 curves branched at \( 2g + 2 \) points. The map to \( \overline{\mathcal{M}}_{0,2g+2} \) which remembers only the base curve with the branch divisor is an isomorphism. In this way, \( \overline{B}_{2g+2} \) is a compactification of \( \mathfrak{H}_g \).

### 3.2. The Relative Curve Over Moduli Space

Suppose now \( n = 2g + 2 \) is even. Writing \( V = V_{2g+2} = \text{Spec} \ K[a_0, \ldots, a_{2g+2}] \), we define a curve \( C \to V \) by taking \( C \) to be the subvariety of \( V \times \mathbb{P}(1, 1, g+1) \) defined by

\[
y^2 = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1}z + \cdots + a_0 z^{2g+2}.
\]  

(3.3)

In fact \( C \) is a double cover of \( V \times \mathbb{P}^1 \). The curve \( C \) is meant to capture all genus \( g \) curves with a two-to-one map onto \( \mathbb{P}^1 \). To capture the isomorphisms, we need a group action on \( C \). Define the group

\[
\tilde{G} = (GL(2) \times \mathbb{G}_m) / (aI, a^{g+1}).
\]

(3.4)
The action on $C$ is defined by letting $(M, u)$ map $(x, z, y)$ to $(Mx, Mz, uy)$. Observe that the element $(I, -1) \in \tilde{G}$ corresponds to the hyperelliptic involution. In particular, it is trivial on the quotient $V \times \mathbb{P}^1$. We embed $\mu_2 \hookrightarrow G$ by taking $-1$ to $(I, -1)$, and let $G = \tilde{G}/\mu_2$; then the action of $\tilde{G}$ on $C$ descends to an action of $G$ on $V \times \mathbb{P}^1$.

Here is the significance of $C$ and $\tilde{G}$: for any $v \in V$, let $C_v$ be the fiber of $v$ in $C$. Then for $v \in V^{\text{sm}}$, $C_v$ is a smooth hyperelliptic curve of genus $g$. On the other hand:

**Proposition 3.1.** Let $g \geq 2$.

1. If $C$ is a genus $g$ curve with a degree 2 map onto $\mathbb{P}^1$, then $C$ is isomorphic to $C_v$ for some $v \in V^{\text{sm}}$.

2. Given an isomorphism $\phi : C_v \rightarrow C_w$ with $v, w \in V^{\text{sm}}$, there exists a unique $\gamma \in \tilde{G}$ such that $w = \gamma v$ and $\phi$ is given by the action of $\gamma$ on $C$.

**Proof.** (1) Suppose $\pi : C \rightarrow \mathbb{P}^1$ has degree 2. Fix a point $p \in \mathbb{P}^1$ and let $D = \pi^{-1}(p)$ be a divisor on $C$. By Riemann-Roch, $H^0(\mathcal{O}_C(-D))$ is 2-dimensional; let $x$ and $z$ be two linearly independent global sections. Now $H^0(\mathcal{O}_C(-(g + 1)D))$ is $g + 3$-dimensional and contains $\text{Sym}^{g+1}H^0(\mathcal{O}_C(-D))$ as a subspace of dimension $g + 2$. Letting $\iota$ be the hyperelliptic involution on $C$, $\iota^*$ acting on $H^0(\mathcal{O}_C(-(g + 1)D))$ is an involution which fixes precisely $\text{Sym}^{g+1}H^0(\mathcal{O}_C(-D))$. Hence the $-1$-eigenspace of $\iota^*$ is 1-dimensional; let $y$ be a nonzero section in this subspace. The map

$$\varphi : C \xrightarrow{[x : z : y]} \mathbb{P}(1, 1, g + 1)$$

is an embedding, since by Riemann-Roch it remains an embedding after composing with the map $\mathbb{P}(1, 1, g + 1) \rightarrow \mathbb{P}^{g+2}$.

Now $y^2 \in H^0(\mathcal{O}_C(-(2g + 2)D))$ is fixed by $\iota_*$, so must be a homogeneous polynomial of degree $2g + 2$ in $x$ and $z$; that is, we must have

$$y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0z^{2g+2}$$
for some $a_i$. In other words, $\varphi(C) \subseteq C_v$ for some $v \in V$. Since $C \hookrightarrow C_v$ and $C$ is smooth of genus $g$, the embedding must be an isomorphism and $v \in V^{sm}$.

(2) Fix $p \in \mathbb{P}^1$ as before. Associated to $C_v$ and $C_w$ we obtain divisors $D$ and $D'$, triples of sections $(x, z, y)$ and $(x', z', y')$, which are unique up to scaling, and maps $\varphi : C_v \to \mathbb{P}(1, 1, g + 1)$ and $\varphi' : C_w \to \mathbb{P}(1, 1, g + 1)$.

From $\pi_v = \pi_w \circ \phi$ we necessarily have $D = \phi^*(D')$. Hence $(\phi^*x', \phi^*z')$ is a unique linear combination of $(x, z)$ and $\phi^*y'$ is a scalar multiple of $y$. Hence $\varphi$ and $\varphi' \circ \phi$ differ by some $(M, u) \in GL(2) \times \mathbb{G}_m$ depending only on $x, z, y, x', z', y'$. But $\varphi' \circ \phi$. This gives us what we want up to the choices of $(x, z, y)$ and $(x', z', y')$. Different choices of $(x, z, y)$ and $(x', z', y')$ differ by scalar multiples of each triple, which replaces $(M, u)$ by $(aM, a^{g+1}u)$ for some scalar $a$. This proves uniqueness.

We have a more explicit description of $\tilde{G}$ depending on the parity of $g$:

**Proposition 3.2.** $\tilde{G}$ is isomorphic to $GL(2)$ if $g$ is even, and $PGL(2) \times \mathbb{G}_m$ if $g$ is odd. In both cases, $G$ is isomorphic to $PGL(2) \times \mathbb{G}_m$.

**Proof.** First if $g$ is even we have a map $GL(2) \to \tilde{G}$ given by $M \mapsto (M, (\det M)^{g/2})$. We can define a map in the other direction by $(M, u) \mapsto \frac{(\det M)^{g/2}}{u} M$, which is well-defined. These maps are inverses by inspection.

Now if $g$ is odd, then the natural projection $\tilde{G} \to PGL(2)$ with kernel $\mathbb{G}_m$ admits a section $[M] \mapsto (M, (\det M)^{(g+1)/2})$. This shows $\tilde{G} \cong PGL(2) \times \mathbb{G}_m$ in this case. A similar argument shows $G$ is always isomorphic to $PGL(2) \times \mathbb{G}_m$. 

Under the isomorphism $G \cong PGL(2) \times \mathbb{G}_m$, the action on $V \times \mathbb{P}^1$ is the expected one. $PGL(2)$ acts on $V$ by the action on binary forms and on $\mathbb{P}^1$ by the standard action, while $\mathbb{G}_m$ acts on $V$ by scaling and acts trivially on $\mathbb{P}^1$. 
Using this characterization, we can see why $\mathfrak{B}_{2g+2}$ is a compactification of $\mathfrak{H}_g$. Indeed, on the semistable locus of $V$ we have a commutative diagram

\[
\begin{array}{ccc}
\mathcal{C} & \longrightarrow & V \times \mathbb{P}^1 \\
\downarrow & & \downarrow \\
\mathcal{C} // \tilde{G}_0 & \longrightarrow & (V \times \mathbb{P}^1) // G_0 \\
\downarrow & & \downarrow \\
\mathcal{C} // \tilde{G} & \longrightarrow & (V \times \mathbb{P}^1) // G \\
\end{array}
\]

(3.7)

where $G_0 = PGL(2)$ and $\tilde{G}_0$ is the preimage of $G_0$, isomorphic to $SL(2) \subseteq GL(2)$ if $g$ is even and $PGL(2) \times \mu_2 \subseteq PGL(2) \times \mathbb{G}_m$ if $g$ is odd.

The quotients $G/G_0$ and $\tilde{G}/\tilde{G}_0$ are isomorphic to $\mathbb{G}_m$, so we can always lift from the third row to the second row. Meanwhile, in the second row, $(V \times \mathbb{P}^1) // G_0$ is defined by the graded ring of covariants. We expect to have an identification

\[
(3.8) \quad V \times \mathbb{P}^1 \cong V \times \mathbb{A}_{2g+2} (V \times \mathbb{P}^1) // G_0
\]

over the locus of $V$ with trivial $G_0$-stabilizer. As long as this identification holds, the fibers of $(V \times \mathbb{P}^1) // G_0 \to \mathbb{A}_{2g+2}$ will be genus 0 curves with extra structure given by the binary form $V$.

### 4. Lifts From Moduli Space

#### 4.1. Lifting to Binary Forms

Suppose $[p]$ is a $K$-point of $\mathfrak{B}_n$. We wish to consider whether $[p]$ lifts to a binary form in $V_n(K)$. First, by the lemma on $\mathbb{G}_m$-quotients, we know that $[p]$ must lift to nonzero $K$-point $p$ in $\mathbb{A}_n$.

Next, suppose $f$ is a stable binary form defined over $K^*$ which maps down to a $K$-point $p$ of $\mathbb{A}_n$. Let $H = SL(2)$ if $n$ is odd, and $H = PGL(2)$ if $n$ is even, so that $\mathbb{A}_n = V_n // H$, and if $f$ is chosen generically, the stabilizer of $f$ under the action of $H$ is trivial.
When $n$ is odd, $H^1(K, SL(2))$ is trivial, and so in the case where the $H$-stabilizer is trivial, $p$ lifts to a binary form defined over $K$. On the other hand, when $n$ is even, $H^1(K, PGL(2))$ classifies quaternion algebras over $K$, and $p$ lifts to a unique $K$-orbit of twisted binary forms over a quaternion algebra.

We now give the definition of a twisted binary form of even degree $n = 2m$. If $B$ is a quaternion algebra over $K$, let $A$ denote the adjoint representation of $B$, given by elements of $B$ having trace zero, on which $PB^\times = B^\times/K^\times$ acts by conjugation. If $\Sigma$ denotes the graded algebra $\text{Sym}^\bullet A/I$, where $I$ is the homogeneous ideal generated by the norm form, then the degree $m$ part $\Sigma_m$ of $\Sigma$ is a representation of $PB^\times$ of dimension $2m + 1$. In the case where $B$ is a matrix algebra, then $\Sigma_m$ is simply the representation $V_{2m}$.

Now an element of $H^1(K, PGL(2))$ can be given the form $\phi^{-1} \circ \phi^\sigma$, where $\phi : \text{Mat}_2(K^\times) \to B(K^\times)$ is an isomorphism. Then $\phi$ maps the determinant to the norm and is functorial with representations, so transfers the representation $V_n$ to $\Sigma_m$.

We now define a twisted binary form of degree $n$ to be an element of $\Sigma_m$. Although $\Sigma_m$ is defined as a quotient of $\text{Sym}^m A$, we have a decomposition $\text{Sym}^m A \cong \Sigma_m \oplus \text{Sym}^{m-2} A$, and so $\Sigma_m$ can be identified as a canonical summand of $\text{Sym}^m A$. Specifically, $\Sigma_m$ consists of the ternary forms of degree $m$ which are harmonic with respect to the norm form restricted to traceless elements of $B$. A twisted binary form of degree $n$, up to scaling, can be thought of as a divisor of degree $n$ on the conic $C$ defined by the norm. In the case where the divisor is reduced, this gives a smooth genus 0 curve with a marked effective divisor of degree $n$.

Here is an explicit way to produce a twisted binary form from an element of $H^1(K, PGL(2))$, via an isomorphism $PGL(2) \cong SO(3)$. An element of $H^1(K, SO(3))$ arising from $f$ provides a projective Galois action on the space of binary forms over $K^\times$, which is a $K$-linear action on binary forms of even degree, fixing $f$. By mapping $H^1(K, SO(3)) \to H^1(K, SL(3)) = 0$, we find that there exists a basis $b_1, b_2, b_3$ of
binary quadratic forms fixed by this action, whose determinant is 1. From the $b_i$, we can produce a ternary quadratic form $q$ of discriminant 1 with coefficients in $K$ such that

\begin{equation}
q(b_1, b_2, b_3) = 0.
\end{equation}

Next, there exists a unique $q$-harmonic ternary form $F$ of degree $m$ such that

\begin{equation}
f(x, y) = F(b_1, b_2, b_3).
\end{equation}

The conditions defining $F$ are preserved by the Galois group, and so $F$ necessarily has coefficients in $K$. The pair $(q, F)$ defines a twisted binary form.

4.2. Lifting to Hyperelliptic Curves. Suppose now that $[X] \in \mathcal{H}_g(K)$. Then $X$ has a representative $C_v$ for some $v \in V(K^*)$, and we get a Galois action $g_\sigma$, well-defined up to stabilizer.

**Theorem 4.1.** (1) $X$ is $K^*$-isomorphic to $C_w$ for some $w \in V(K)$ if and only if $g_\sigma$ can be chosen to be a $\tilde{G}$-valued coboundary.

(2) $X$ is $K^*$-isomorphic to a curve defined over $K$ if and only if $g_\sigma$ can be chosen to be a $\tilde{G}$-valued cocycle.

**Proof.** (1) Suppose $\phi : C_v \to C_w$ is an isomorphism with $w \in V(K)$. Then $\phi$ is represented by a unique $h \in \tilde{G}$. Now $\sigma(h)$ and $h g_\sigma$ both map $C_{\sigma(v)}$ to $C_w$, so $g_\sigma = h^{-1} \sigma(h)$ up to stabilizer. Conversely, given such an $h$, then take $w = h v$, a vector in $V(K)$.

(2) If $\phi : C_v \to C$ with $C$ defined over $K$, then by the same argument as above, up to stabilizer, $g_\sigma = \phi^{-1} \circ \sigma \phi$, which is a cocycle by the usual argument. Conversely, if $g_\sigma$ is a cocycle, let $\Sigma$ be the set of Galois conjugates of $v$ (finite since we must have $v \in V(L)$ for some finite extension $L/K$). The cocycle
condition yields a curve $C_{\Sigma}$ defined over $K^s$ along with compatible isomorphisms $\iota_w : C_{\Sigma} \to C_w$ for $w \in \Sigma$. $C_{\Sigma}$ admits a natural Galois action, which allows $C_{\Sigma}$ to descend to $K$.

One might ask for an explicit form of the curve constructed in the “only if” implication of (2). Suppose the Galois action is given by a cocycle $c$. Then we have a twisted representation $V^c$, and so a reasonable approach would be to construct a curve $C^c \to V^c$ defined over $K$, isomorphic to $C \to V$ over $K^s$, such that $v$ is mapped to an element of $V^c(K)$ under this isomorphism. In this situation, $C_v$ would be mapped to a curve defined over $K$, constructing our desired curve.

Indeed, we construct $C^c$ directly, depending on the parity of $g$. If $g$ is even, then $\widetilde{G} \cong GL(2)$ implies $H^1(K, \widetilde{G}) = 0$. Hence $c$ is a coboundary, in which case there is nothing to produce. Now if $g$ is odd, then $\widetilde{G} \cong PGL(2) \times \mathbb{G}_m$. Now $c$ is determined by its pushforward under the map $\widetilde{G} \to PGL(2)$, and so $V^c$ is the vector space of $Q$-harmonic ternary forms $F$ of degree $g+1$, where $Q$ is some fixed ternary quadratic form. Then $C^c$ may be constructed as the subvariety of $V^c \times \mathbb{P}(1, 1, 1, \frac{g+1}{2})$ defined by the equations

\begin{align}
Q(x, y, z) &= 0 \\
F(x, y, z) &= w^2
\end{align}

which gives a covering of the conic $Q = 0$ of degree 2 branched at the common zero locus of $Q$ and $F$.

As an example of our work here, we may now prove Theorem 1.1

\textit{Proof for even $g$.} If $K$ is a $p$-adic field or number field, it is well known that there exists a ternary quadratic form $Q$ defined over $K$ such that the conic $Q = 0$ contains no $K$-points. By choosing $F$ a ternary form of $g + 1$ generically, we may arrange
that the divisor \( \{ Q = F = 0 \} \) is reduced and that the stabilizer of \((Q, F)\) under the action of \( SO(Q)(K^*) \) is trivial. Over some finite Galois extension \( L/K \), \( Q \) becomes rational, and so \( F \) corresponds to some binary form \( f \) defined over \( L \). Let \( C \) be the curve \( C_f \); that is, \( y^2 = f(x) \).

Now \( C \) has field of moduli contained in \( K \). Indeed, if \( \varphi : \mathbb{P}^1 \to \{ q = 0 \} \) has \( \varphi^*(F) = f \), then applying \( \sigma \in \text{Gal}(L/K) \) to \( f \) changes \( f \) by the automorphism \( \varphi^{-1} \circ \sigma \varphi \) of \( \mathbb{P}^1 \). On the other hand, \( C \) cannot admit \( K \) as a field of definition. Since \( g \) is even, \( H^1(K, \tilde{G}) = 0 \), and so this would only be possible if \( C \) were \( K^* \)-isomorphic to \( C_w \) for some \( w \in V(K) \). This means \( w = \gamma f \) for some \( \gamma \in \tilde{G}(K^*) \). But \( f \) has trivial stabilizer under the action of \( PGL(2)(K^*) \), so is \( K^* \)-isomorphic to at most one \( K \)-orbit of twisted binary forms. Hence \( w \) and \((q, F)\) differ by a \( K \)-isomorphism. In particular, \( \{ q = 0 \} \) must be isomorphic to \( \mathbb{P}^1 \), a contradiction. \( \square \)

**Proof for odd \( g \).** Fix \( v \in V(K^*) \) so that \( C_v \) is a representative of our curve. We wish to show \( g_\sigma \) can be chosen to be a \( \tilde{G} \)-valued cocycle. Equivalently, we wish to show \( d \) is trivial. Indeed, \( d \) is valued in \( 1 \times \mu_2 \subseteq PGL(2) \times \mathbb{G}_m \). Letting \( g_\sigma = (A_\sigma, b_\sigma) \), we find that \( A_\sigma \) is a cocycle while \( b_\sigma \) generates a \( \mathbb{G}_m \)-valued analogue of \( d \). By Lemma 2.6, this analogue of \( d \) is trivial. Hence we may modify the \( b \)'s to be a cocycle, which transforms \( g_\sigma \) into a cocycle. This shows what we want.

Alternatively, we know \( v \) has a twisted binary form \((q, F)\) via some cocycle \( c \in H^1(K, PGL(2)) \). Now using our construction of the curve \( C^c \), we know that \( C_v \) is \( K^* \)-isomorphic to \( C^c_{(q, F)} \), which is defined over \( K \). \( \square \)

5. **INTERPRETATION OF \( \mathcal{M}_{2g+2} \)**

The group \( \mathcal{G} \) acts by isomorphisms on hyperelliptic curves. The space \( \Omega^g \) of top forms is 1-dimensional, and we may pick out a distinguished element given a defining
equation for our hyperelliptic curve: to the equation $y^2 = f(x)$, associate the element

\[(5.1) \quad \omega = \frac{dx}{y} \wedge x \frac{dx}{y} \wedge \cdots \wedge x^{g-1} \frac{dx}{y}.\]

Then $(M, u) \in \mathcal{G}$ sends $\omega$ to $\frac{(\det M)^{\frac{g+1}{2}}}{u^g} \omega$. Hence $\omega$ is preserved if and only if $u^g = (\det M)^{\frac{g+1}{2}}$. This subgroup corresponds to $PGL(2) \times \mu_g$ if $g$ is odd, and the subgroup of matrices of $GL(2)$ such that $(\det M)^{\frac{g}{2}} = 1$ if $g$ is even. In particular, we see that the moduli space of hyperelliptic curves of genus $g$ with a fixed top form is a finite quotient of $\mathfrak{A}_{2g+2}$; if $g \leq 2$, we have equality.

Here is another interpretation of $\mathfrak{A}_{2g+2}$ that pins down the space exactly. A binary form of degree $2g + 2$ can be viewed as a global section of $\mathcal{O}_{\mathbb{P}^1}(-2g - 2) = \Omega_{\mathbb{P}^1}^{(g+1)}$. Hence $\mathfrak{A}_{2g+2}$ can be viewed as the moduli space of genus 0 curves $C$ with a global section of $\Omega_C^{(g+1)}$. This can equivalently be viewed as the moduli space of hyperelliptic curves $C$ of genus $g$ together with a global section $s$ of $\Omega_{C_0}^{(g+1)}$, where $C \to C_0$ is the curve defined by the canonical divisor, such that the vanishing locus of $s$ coincides with the branch locus of $C \to C_0$.

6. INVARIANTS OF SYSTEMS OF BINARY QUADRATIC FORMS

The invariant theory of systems of binary quadratic forms makes essential use of the fact that the discriminant is a quadratic form, so it will be more convenient to make use of the isomorphism $PGL(2) \cong SO(3)$.

Consider more generally the group $SO(n)$ acting on the representation $W^\oplus n$, where $W$ is the standard representation of $SO(n)$. If $\langle \ , \ \rangle$ denotes the bilinear form on $SO(n)$, then $A_{ij} = \langle w_i, w_j \rangle$ and $R = w_1 \wedge \cdots \wedge w_n$ are invariants of $W^\oplus n$ under the action of $SO(n)$, satisfying the relation $R^2 = (\star) \det(A_{ij})$. We claim that these generate the ring of invariants, and that generically the action of $SO(n)$ is simply transitive over $K^*$.
To see this, consider the case where the $w_i$ are linearly independent. Then the $SO(n)$-stabilizer is clearly trivial. To see transitivity, consider the quadratic form

\begin{align}
\tag{6.1} g(x_1, \ldots, x_n) &= q(x_1w_1 + \cdots + x_nw_n) \\
\tag{6.2} &= \sum_{i,j} A_{ij}x_ix_j.
\end{align}

Then the vector space $K^n$ with quadratic form $g$ is isometric to $W$ over $K^s$ (or some orthogonal space $W'$ with square discriminant over $K$). The set of isometries form a principal homogeneous space for $O(W')$, so the constraint that the $A_{ij}$ be fixed shows that any other set of $n$ vectors with the same invariants must differ by an element of $O(W')$. But also the determinant multiplies $R$, so the constraint that $R$ be fixed shows the element must lie in $SO(W')$.

We can also consider the situation where the quadratic form $g$ has rank $n - 1$. In this case, $\text{span}(w_1, \ldots, w_n)$ has dimension $n - 1$. WLOG $w_n \in \text{span}(w_1, \ldots, w_{n-1})$, writing

\begin{equation}
\tag{6.3} w_n = \lambda_1 w_1 + \cdots + \lambda_{n-1} w_{n-1}.
\end{equation}

Then $g(x_1, \ldots, x_{n-1}, 0)$ is nondegenerate. Then $\langle w_i, w_j \rangle$ for $i, j \leq n - 1$ uniquely determine an $SO(n)$-orbit of $w_1, \ldots, w_{n-1}$ (over $K^s$) with trivial stabilizer. To see that the action of $SO(n)$ is simply transitive on $w_1, \ldots, w_n$, it then remains to see that the $\lambda_i$ are then uniquely determined from the $\langle w_i, w_j \rangle$ for $i, j \leq n - 1$. In fact, we have the equations

\begin{equation}
\tag{6.4} \lambda_1 A_{i1} + \cdots + \lambda_{n-1} A_{i(n-1)} = A_{in}
\end{equation}

and $g$ having rank $n - 1$ shows that this linear system can be solved uniquely for $\lambda_i$.

To apply this to binary forms, take $W$ the standard space for $SO(3)$, $V_{2m}$ the space of binary forms of dimension $2m$, and suppose we have a covariant map $V_{2m} \rightarrow W^{\otimes 3}$,
that is, three covariant binary quadratic forms. Then the above invariants of $W^{\oplus 3}$ will yield invariants of $V_{2m}$.

However, given fixed invariants of a binary form, lifting the ones associated to $W^{\oplus 3}$ to three elements $w_1, w_2, w_3$ of $W$ can be used to lift from invariants to a binary form. Indeed, we may associate a wedge product on $W$ via the isomorphisms

$$(6.5) \quad \wedge^2 W \cong W^* \cong W$$

and define $w_1^* = w_2 \wedge w_3$, $w_2^* = w_3 \wedge w_1$, $w_3^* = w_1 \wedge w_2$. Then in the space $\Sigma_2$, we have

$$(6.6) \quad g(w_1^*, w_2^*, w_3^*) = 0.$$ 

If $w_1, w_2, w_3$ are linearly independent, so are $w_1^*, w_2^*, w_3^*$, and in fact any $u$ in $W$ is determined by

$$(6.7) \quad Ru = \langle u, w_1 \rangle w_1^* + \langle u, w_2 \rangle w_2^* + \langle u, w_3 \rangle w_3^*.$$ 

If $w_1, w_2, w_3$ are covariants of $f \in V_{2m}$, then viewing $f$ as an element of $\Sigma_m$, i.e. a polynomial of degree $m$ in $W$, we can express $R^m f$ as a polynomial in the $w_i^*$; this polynomial is unique if we also impose the condition of being $g$-harmonic. The coefficients of this polynomial are necessarily $SO(3)$-invariant.

In this way we can recover $f$ from the $w_i$ and the invariants associated to $f$. In other words, we have the diagram

$$(6.8)$$

![Diagram](attachment:diagram.png)

and away from the vanishing locus of $R$, we have an isomorphism

$$(6.9) \quad V_{2m} \cong A_{2m} \times_{W^{\oplus 3} \sslash SO(3)} W^{\oplus 3}.$$
7. The Genus 2 Case

7.1. Constructing the Twisted Representation. Much of this was done by work of Mestre. Here three covariant binary quadratic forms $x_1, x_2, x_3$ are constructed, whose determinant $R$ gives essentially the only invariant of odd degree. These forms can then be used to produce a twisted representation as long as $R \neq 0$. Since the invariants are generated by $R$ and invariants of even degree, having $R = 0$ is equivalent to the $\mathbb{G}_m$-stabilizer containing $\mu_2$. In particular, this case covers all binary forms with trivial stabilizer.

However, from $x_1, x_2, x_3$, we can obtain additional covariant quadratics $x_1^*, x_2^*, x_3^*$. If any of the sets $\{x_1, x_2, x_3\}$, $\{x_1^*, x_2, x_3\}$, $\{x_1, x_2^*, x_3\}$, or $\{x_1, x_2, x_3^*\}$ are linearly independent, then we may produce a twisted representation.

On the other hand, suppose we have dependence relations from all four sets. A dependence relation between $x_1, x_2, x_3^*$ implies $x_1$ and $x_2$ have a common root. The same goes for $x_1$ and $x_3$, and $x_2$ and $x_3$. But dependence between $x_1, x_2, x_3$ shows that one of the $x_i$ is spanned by the other two, so in fact $x_1, x_2, x_3$ all have a root in common. This root will also be shared by $x_1^*, x_2^*, x_3^*$. In this case the quadratic form generated by $x_1, x_2, x_3$ has rank at most 1.

We believe this exceptional case coincides with exactly the curves of nontrivial $PGL(2)$-stabilizer in genus 2. However, in sufficiently high genus, no three covariant quadratics will suffice, since the locus where a quadratic form has rank at most 1 is of codimension at most 3, whereas the locus of binary forms with nontrivial automorphisms is of much larger codimension for $g$ sufficiently large.

7.2. Genus 2 Curves With Stabilizer. There are two loci of genus 2 curves with a nontrivial $PGL(2)$-stabilizer: $ax^6 + bx^3 z^3 + cz^6$ and $ax^5 z + bx^3 z^3 + cx z^5$. We would like to know which forms have field of moduli $K$. To do this, note that applying Galois will give a form in the same locus, and we wish to know whether this action arises from a $PGL(2)$ transformation. The transformations preserving these loci,
except in very special cases, are extensions of $\mu_2$ by $\mathbb{G}_m$. The $x^3z^3$ term is unaffected by the $\mathbb{G}_m$ part, so descends to $\mu_2$. So $b^2 \in K$. If $b \in K^\times$, then the obstruction class $d$ arises from $\mathbb{G}_m$, and is therefore trivial.

If $c = 0$, then the form is not stable. So $c \neq 0$; after an appropriate transformation by an element in the torus, we can assume $c = 1$, and then $a \in K$.

As an example, consider $K = k_0(t,u)$, and the binary form

$$(7.1) \quad -tx^5z + \sqrt{u}x^3z^3 + xz^5.$$ 

The Galois group $\text{Gal}(K(\sqrt{u})/K)$ acts on this form by $g_\sigma$, where

$$(7.2) \quad g_\sigma = \begin{cases} 
1 & \sigma(\sqrt{u}) = \sqrt{u} \\
0 & \sigma(\sqrt{u}) = \sqrt{u}
\end{cases}$$

$$(7.3) \quad d_{\sigma,\tau} = g_\sigma g_\tau g_\sigma^{-1} = \begin{cases} 
-1 & \sigma(\sqrt{t}) = -\sqrt{t}, \tau(\sqrt{u}) = -\sqrt{u} \\
0 & \text{otherwise.}
\end{cases}$$

Identify the $\mu_2$ portion of the stabilizer with $\mu_2 \subseteq \mathbb{G}_m$, and consider $d_{\sigma,\tau}$ as having values in $\mathbb{G}_m$. Then defining

$$(7.4) \quad b(\sigma) = \begin{cases} 
1 & \sigma(\sqrt{t}) = \sqrt{t} \\
\sigma(\sqrt{u}) & \sigma(\sqrt{t}) = -\sqrt{t}
\end{cases}$$
and \( \tilde{d} = d \cdot \left( b(\sigma)b(\tau)b(\sigma\tau)^{-1} \right) \), then we have

\[
(7.5) \quad \tilde{d}_{\sigma,\tau} = \begin{cases} 
  u & \sigma(\sqrt{t}) = -\sqrt{t}, \tau(\sqrt{t}) = -\sqrt{t} \\
  1 & \text{otherwise.}
\end{cases}
\]

We see that the class \( \tilde{d} \) corresponds to the quaternion algebra \( i^2 = t, j^2 = u \) — that is, a universal quaternion algebra. Hence any possible obstruction in \( H^2(K, \mu_2) \) can occur. In particular no twisted representation exists in the generic case.

8. The Moduli Space as an \( SL(3) \)-Quotient

Let \( V \) be the space of binary forms and \( G = PGL(2) \cong SO(3) \). We will express the quotient \( V//G \) as a quotient \( \mathcal{E}//\mathcal{G} \), for \( \mathcal{G} = SL(3) \). In particular, \( K \)-points of \( \mathcal{E}//\mathcal{G} \) will correspond to \( K \)-orbits of \( \mathcal{E} \) by Hilbert 90. We take \( \mathcal{E} \) to be the set of \((q, F)\) for \( q \) a conic of discriminant 1 and \( F \) a ternary \((g + 1)\)-form which is \( q \)-harmonic. Letting \( \mathcal{G}_0 = SO(3) \) be the automorphism group of the split conic \( q_0 \) and \( \mathcal{E}_0 \) the fiber over \( q_0 \), then \( V//G \) can be identified with \( \mathcal{E}_0//\mathcal{G}_0 \).

Now \( \mathcal{E}_0//\mathcal{G}_0 \) is a graded ring of \( SO(3) \)-invariant \( q_0 \)-harmonic polynomials. By the First Fundamental Theorem for invariants of \( SO(3) \), invariants of multiple linear forms are generated by the bilinear forms and the determinant forms. Hence all covariants can be specified in terms of the bilinear form, the determinant form, and the identification of the standard representation with its dual. On the other hand, these functions all extend to regular functions on \( \mathcal{E} \) which are \( SL(3) \)-invariant. We conclude that the map

\[
(8.1) \quad \mathcal{E}_0//\mathcal{G}_0 \to \mathcal{E}//\mathcal{G}
\]

is an isomorphism.
Part 2. The 2-Selmer Group May be Arbitrarily Large

9. Introduction

Let $K$ be a field of characteristic not equal to 2, and $J$ be an abelian variety defined over $K$. An important problem in number theory is to describe the abelian group $J(K)$ of $K$-points of $J$. Examples of abelian varieties $J$ which one could be interested in include elliptic curves, or more generally, Jacobians of arbitrary curves.

If $K$ is a number field, then the Mordell-Weil theorem implies $J(K)$ is finitely generated. The torsion subgroup is well understood, so in order to determine the structure of $J(K)$, it’s enough to find its rank.

Often, in order to study $J(K)$ one looks at simpler objects — the so-called weak Mordell-Weil groups $J(K)/mJ(K)$ where $m > 1$ is an integer. These groups are finite, an in fact understanding $J(K)/mJ(K)$ for any $m > 1$ can be used to determine $J(K)$. This is true for two reasons. One is that, if the torsion part of $J(K)$ is known, then one can compute the rank of $J(K)$. If $p$ is any prime dividing $m$, then

\[(9.1) \quad \text{rank } J(K) = \dim_{\mathbb{F}_p} J(K)/pJ(K) - \dim_{\mathbb{F}_p} J(K)_{tor}/pJ(K)_{tor}.\]

Another is that, in the proof of the Mordell-Weil theorem, there is an algorithm that, given a finite generating set of $J(K)/mJ(K)$, produces a finite generating set of $J(K)$.

On the other hand, the finiteness of $J(K)/mJ(K)$, and one method to determine the group, follows from a descent argument. We will be interested in the case $m = 2$. Recall that the exact sequence

\[(9.2) \quad 0 \to J[2] \to J \xrightarrow{\delta} J \to 0\]

of étale group schemes gives rise to an exact sequence

\[(9.3) \quad 0 \to J(K)/2J(K) \xrightarrow{\delta} H^1(K, J[2]) \xrightarrow{j} H^1(K, J)[2] \to 0\]
where we have written $H^i(K, M)$ for the Galois cohomology group

$$H^i(K, M) = H^i(\text{Gal}(K^s/K), M(K^s)).$$

In the case that $K$ is a global field, for every place $v$ of $K$ we may write $\alpha \mapsto \alpha_v$ for the natural map $H^1(K, J[2]) \to H^1(K_v, J[2])$, and $\delta_v$ and $j_v$ for the corresponding maps in the sequence [9.3]. Then the 2-Selmer group is

$$S_2(K, J) = \{ \alpha \in H^1(K, J[2]) : j_v(\alpha_v) = 0 \forall v \}. \quad (9.5)$$

That is, a cohomology class $\alpha \in H^1(K, J[2])$ lies in $S_2(K, J)$ if and only if $\alpha_v$ comes from an element of $J(K_v)/2J(K_v)$ for every place $v$. In particular, $J(K)/2J(K)$ embeds into $S_2(K, J)$, and this embedding fits into an exact sequence

$$0 \to J(K)/2J(K) \to S_2(K, J) \to \Sha[2] \to 0 \quad (9.6)$$

where $\Sha$ denotes the Shafarevich-Tate group of $J$, and is defined as

$$\Sha = \{ \theta \in H^1(K, J) : \theta_v = 0 \forall v \}. \quad (9.7)$$

The importance of the 2-Selmer group comes from the following fact:

**Fact 9.1.** $S_2(K, J)$ is finite.

Knowing the size of $S_2(K, J)$ would allow us to bound $J(K)/2J(K)$, and therefore the rank of $J$.

We can in fact say more, which allows an effective bound on the size of $S_2(K, J)$. If $v$ is a finite place not dividing 2 for which $J$ has good reduction, then the local condition $j_v(\alpha_v) = 0$ is simple to describe, and the conditions for all such $v$ fit together in a coherent manner. As a special case, consider the situation where $J[2]$ consists entirely of $K$-points. Then the set $H^1(K, J[2])$, which naturally contains $S_2(K, J)$,
has the form

\[ H^1(K, J[2]) \cong H^1(K, (\mathbb{Z}/2\mathbb{Z})^{\oplus 2g}) \cong \prod_{2g} K^\times/(K^\times)^2 \]

where \( g \) is the dimension of \( J \). Now for the all but finitely many \( v \) described above, we have

\[ j_v(\alpha_v) = 0 \iff \alpha_v \in \prod_{2g} \mathcal{O}_v^\times/(\mathcal{O}_v^\times)^2. \]

If we take \( S \) to be the set of places dividing 2, the real places, and the primes where \( J \) has bad reduction, then if \( \alpha \in S_2(K, J) \), then in particular we must have \( j_v(\alpha_v) = 0 \) for \( \alpha \notin S \). This nearly implies \( \alpha \in \prod_{2g} \mathcal{O}_S^\times/(\mathcal{O}_S^\times)^2 \); it will be true if we enlarge \( S \) to contain all 2-torsion in the class group. But now, the structure of \( \mathcal{O}_S^\times \) shows that \( \alpha \) is contained in an explicitly finite set. This allows us to compute \( S_2(K, J) \), since it is a subset of this finite set described by the remaining local conditions \( j_v(\alpha_v) = 0 \) for \( v \in S \).

However, this argument also shows the difficulties in trying to produce a \( J \) with high rank, or even high 2-Selmer rank. Indeed, there is a uniform bound of the form

\[ |S_2(K, J)| \leq f(g, K, |S|) \]

and so if we were to fix \( g \) and \( K \), in order for \( S_2(K, J) \) to be large, we would necessarily have to make \( S \) large. But this is the set of \( v \) for which the local condition \( j_v(\alpha_v) = 0 \) is not solved by the above criterion. For these \( v \), we have something to check.

We provide another method of verifying local conditions in Section \[10\]. Checking that \( j_v(\alpha_v) = 0 \) is equivalent to showing \( \alpha \in \text{im}(\delta_v) \), and we may describe \( \text{im}(\delta_v) \) by applying \( \delta_v \) to specific elements of \( J(K_v)/2J(K_v) \). We examine specifically the case of 2-torsion points; this amounts to considering the embedding

\[ J(K_v)[2]/2J(K_v)[4] \hookrightarrow J(K_v)/2J(K_v). \]
On the other hand, this embedding is often surjective, in which case we can describe all of \( \text{im}(\delta_v) \). We have:

**Proposition 9.2.** Suppose \( v \) is a finite place not dividing 2. Then we have an isomorphism

\[
J(K_v)/2J(K_v) \cong J(K_v)[2].
\]

**Corollary 9.3.** For \( v \) a finite place not dividing 2, the embedding

\[
J(K_v)[2]/2J(K_v)[4] \hookrightarrow J(K_v)/2J(K_v)
\]

is an isomorphism if and only if \( J(K_v) \) contains no points of exact order 4.

*Proof of proposition.* If \( v \) divides an odd prime \( p \), then \( J(K_v) \) admits a normal pro-\( p \) subgroup of finite index. In particular, the pro-\( p \) part is 2-divisible, so if we let \( Q \) be the quotient, then the natural map \( J(K_v) \to Q \) induces isomorphisms \( J(K_v)[2] \cong Q[2] \) and \( J(K_v)/2J(K_v) \cong Q/2Q \). However, as \( Q \) is a finite abelian group, we have \( Q/2Q \cong Q[2] \), and so the result follows. \( \square \)

We are interested in the situation where \( J \) is the Jacobian of a hyperelliptic curve. Now fix a positive integer \( g \) and a polynomial \( f(x) \in K[x] \) which is monic of degree \( 2g + 1 \) and has distinct roots. Consider the curve \( C \) defined by the equation

\[
y^2 = f(x)
\]

a hyperelliptic curve of genus \( g \) having a rational Weierstrass point, which we denote by \( \infty \). We will now consider the case where \( J \) is the Jacobian of \( C \).
For any \( d \in K^\times/(K^\times)^2 \), we may consider the quadratic twist \( C^d \) defined by either of the following two equivalent equations:

\[
\begin{align*}
(9.15) & \quad dy^2 = f(x) \\
(9.16) & \quad y^2 = d^{2g+1}f\left(\frac{x}{d}\right)
\end{align*}
\]

Let \( J^d \) be the Jacobian of \( J \).

The aim of this part is to show that for any number field \( K \) and any \( f \), as \( d \) varies, the dimension of \( S_2(K, J^d) \) as an \( \mathbb{F}_2 \)-vector space is unbounded. Bölling, in [2], has shown this result in the case \( g = 1 \), and in fact shows that \( \text{III}^d[2] \) is unbounded where \( \text{III}^d \) denotes the Shafarevich-Tate group of \( J^d \); this part generalizes his methods to raise the Selmer rank. We will prove that the Selmer rank may be raised in the case of arbitrary \( g \).

Notice that \( S_2(K, J^d) \) being unbounded will imply either \( J^d(K)/2J^d(K) \) or \( \text{III}^d[2] \) is unbounded. Given the difficulties in producing elliptic curves of high rank and the results of Bölling’s paper, we expect that a refinement of our methods will show that \( \text{III}^d[2] \) is unbounded for hyperelliptic curves of arbitrary genus.

Here is more precise statement of what we will prove:

**Theorem 9.4.** Suppose \( K \) is a number field and \( f \) and \( J \) are as above. Then there exists \( d \in K^\times/(K^\times)^2 \) such that

\[
S_2(K, J) \subsetneq S_2(K, J^d).
\]

Repeatedly applying Theorem 9.4 shows that arbitrarily large ranks may occur. This is because we may find \( d_1, d_2, \ldots \) such that

\[
\begin{align*}
(9.18) & \quad S_2\left(K, J\right) \subsetneq S_2\left(K, J^{d_1}\right)
(9.19) & \quad S_2\left(K, J^{d_1}\right) \subsetneq S_2\left(K, (J^{d_1})^{d_2}\right)
\end{align*}
\]
and so on, and so we find an infinite ascending chain

\[ S_2(K, J) \subset S_2(K, J^{d_1}) \subset S_2(K, J^{d_1d_2}) \subset \cdots. \]

Aside from gaining some insight into the 2-Selmer groups, this specific result has a consequence in arithmetic invariant theory. Benedict Gross in [1] has examined the action of \( SO(2g + 1) \) on \( \text{Sym}^2(2g + 1) \), the symmetric square of the standard representation. This is equivalent to the conjugation action of \( SO(2g + 1) \) on self-adjoint \((2g+1)\times(2g+1)\) matrices. Over a separably closed field, the generic orbits are determined entirely by the characteristic polynomial of the matrix. More precisely, if \( f \) is a polynomial of degree \( 2g + 1 \) with distinct roots, then any two self-adjoint matrices with the same characteristic polynomial \( f \) are \( SO(2g + 1) \)-conjugate. On the other hand, our results on unboundedness of the 2-Selmer rank shows:

**Corollary 9.5.** Let \( K \) be a number field and \( f(x) \in K[x] \) be a polynomial of degree \( 2g + 1 \) with distinct roots. Then there exist infinitely many \( SO(2g + 1)(K) \)-conjugacy classes of \((2g+1)\times(2g+1)\) self-adjoint matrices defined over \( K \) having characteristic polynomial \( f \).

Indeed, for every \( d \) there is an embedding of \( S_2(K, J^d) \) into the set of conjugacy classes.

**10. Cohomology Classes Arising From 2-Torsion**

We now return to \( K \) being an arbitrary field of odd characteristic. With \( f \) as before, we let \( e_i \) be the roots of \( f \), so that over an algebraic closure of \( K \), we have

\[ f(x) = (x - e_1)(x - e_2)\cdots(x - e_{2g+1}). \]

The significance of the \( e_i \) is that the Weierstrass points of \( C \) other than \( \infty \) are the points \((e_i, 0)\). Let \( L \) be the étale \( K \)-algebra \( K[x]/f(x) \), and let \( \beta \) be the image of \( x \) in this quotient.
Proposition 10.1. We have an identification of Galois modules

\begin{equation}
J[2] \cong (\text{Res}_{L/K}\mu_2)_{N=1},
\end{equation}

which results in

\begin{equation}
H^1(K, J[2]) \cong (L^\times/(L^\times)^2)_{N=1}
\end{equation}

consisting of those elements of $L^\times/(L^\times)^2$ whose norm is a square.

Proof. Any 2-torsion point $P$ of $J$ may be expressed as a linear combination of Weierstrass points, whose degree is zero. So $P$ may be expressed as a linear combination of $(e_i, 0) - (\infty)$’s. On the other hand, we have the unique relation

\begin{equation}
(e_1, 0) + \cdots + (e_{2g+1}, 0) = (2g + 1) \cdot (\infty).
\end{equation}

(Existence is shown by considering the principal divisor $(y)$.) So $P$ may be expressible uniquely in the form

\begin{equation}
P = (e_{i_1}, 0) + \cdots + (e_{i_2r}, 0) - 2r(\infty), \quad 1 \leq i_1 < \cdots < i_{2r} \leq 2g + 1
\end{equation}

for some $r$. Using this characterization, we obtain a map $J[2](K^*) \to \mu_2 \otimes_K L = \text{Res}_{L/K}\mu_2$ by $P \mapsto \chi_P$, where $\chi_P$ is a function on the $e_i$ defined by

\begin{equation}
\chi_P(e_i) = \begin{cases}
-1 & i = i_1, \ldots, i_{2r} \\
1 & \text{otherwise}.
\end{cases}
\end{equation}

The map $P \mapsto \chi_P$ is compatible with the action of the Galois group, and is injective with image the elements of norm 1. This shows $J[2] \cong (\text{Res}_{L/K}\mu_2)_{N=1}$. 

Before determining $H^1$, we note that this submodule of $\text{Res}_{L/K}\mu_2$ actually splits as

\begin{equation}
\text{Res}_{L/K}\mu_2 = \left( \text{Res}_{L/K}\mu_2 \right)_{N=1} \oplus \mu_2
\end{equation}

where the $\mu_2$ summand consists of the constant functions $\{e_1, e_2, \ldots, e_{2g+1}\} \to \pm 1$. Indeed, the nontrivial element of $\mu_2$ has norm $(-1)^{2g+1} = -1$. Now from this splitting and the Kummer sequence, we obtain a splitting

\begin{equation}
L^\times/(L^\times)^2 \cong H^1(K, (\text{Res}_{L/K}\mu_2)_{N=1}) \oplus K^\times/(K^\times)^2
\end{equation}

where the map $L^\times/(L^\times)^2 \to K^\times/(K^\times)^2$ arises from the norm map $L^\times \to K^\times$. This proves

\begin{equation}
H^1(K, (\text{Res}_{L/K}\mu_2)_{N=1}) \cong (L^\times/(L^\times)^2)_{N=1}
\end{equation}

which gives us what we wanted. \hfill \Box

Under the identification given by (10.3), our map $\delta$ may be considered as a map $\delta : J(K)/2J(K) \to (L^\times/(L^\times)^2)_{N=1}$. We wish to describe the image of $\delta$ restricted to the domain $J(K)[2]/2J(K)[4]$. Note that if $J(K)$ contains no point of exact order 4, then this will determine $\delta$ entirely. Recall from the above proof that any 2-torsion point $P$ of $J$ may be expressible uniquely in the form

\begin{equation}
P = (e_{i_1}, 0) + \cdots + (e_{i_2r}, 0) - 2r(\infty), \quad 1 \leq i_1 < \cdots < i_{2r} \leq 2g + 1
\end{equation}
for some \( r \). The point \( P \) determines a factorization of \( f \) into polynomials of odd and even degree, namely

\[
(10.11) \quad f_0(x) = \prod_{j=1}^{2r} (x - e_i)
\]

\[
(10.12) \quad f_1(x) = \frac{f(x)}{f_0(x)}.
\]

From this factorization we obtain a decomposition of \( L \) as

\[
(10.13) \quad L \cong L/f_0(\beta) \oplus L/f_1(\beta).
\]

and can represent elements of \( L \) according to this identification. In other words, \( \gamma \in L \) has the form \( (\gamma_0, \gamma_1) \) if and only if \( \gamma \equiv \gamma_0 \pmod{f_0(\beta)} \) and \( \gamma \equiv \gamma_1 \pmod{f_1(\beta)} \).

In [3], it is shown that

\[
(10.14) \quad \delta(P) = f_0(\beta) - f_1(\beta)
\]

\[
(10.15) \quad = (-f_1(\beta), f_0(\beta)).
\]

Suppose now that \( d \in K^\times/(K^\times)^2 \) and we replace \( J \) by \( J^d \). Under the definition of \( C^d \) via (9.16), we see that \( e_i \) and \( \beta \) are replaced by \( de_i \) and \( d\beta \), respectively. Hence \( \delta(P) \) will be replaced by

\[
(10.16) \quad \delta^d(P) = (-df_1(\beta), f_0(\beta))
\]

\[
(10.17) \quad = f_0(\beta) - df_1(\beta).
\]

In particular, we see that the cohomology class \( f_0 - df_1(\beta) \) is contained in \( \text{im} \delta^d = \ker j^d \).
Now the map $j^d$ has been given a description in terms of homogeneous spaces as part of X. Wang’s thesis [4]. Let $T : L \to L$ be the linear map given by

\begin{align}
T(\mu) &= \beta^{2g} \text{ coefficient of } \mu \\
&= \operatorname{Tr} \left( \frac{\mu}{f'(\beta)} \right).
\end{align}

Then given $\alpha \in (L^\times/(L^\times)^2)_{N=1}$, we associate the pencil of quadrics in $\mathbb{P}(L \oplus K) \cong \mathbb{P}^{2g+1}$ defined by

\begin{align}
Q(\lambda, a) &= T(\alpha \lambda^2) \\
Q'(\lambda, a) &= T(\alpha \beta \lambda^2) + da^2.
\end{align}

**Fact 10.2.** $j^d(\alpha)$ is the Fano variety of the base locus of this pencil. That is to say,

\begin{align}
\ker j^d &= \left\{ \alpha \in (L^\times/(L^\times)^2)_{N=1} : \exists V \in \mathbb{C}(g - 1, 2g + 1)(K) \text{ with } Q|_V = Q'|_V = 0 \right\}.
\end{align}

For reference, we will explicitly describe a $(g - 1)$-plane that trivializes the homogeneous space $j^d(\delta^d(P))$ for $P$ a 2-torsion point of $J^d$. (Such a plane must exist since $j^d \circ \delta^d$ is the zero map on cohomology.) Indeed, for $\delta^d(P)$ as described by (10.16), let deg $f_0 = 2g_0$ and deg $f_1 = 2g_1 + 1$, with $g_0 + g_1 = g$.

**Proposition 10.3.** The linear subspace

\begin{align}
V &= \left\{ (\lambda, a) : \lambda = (R_0(\beta), R_1(\beta)) : \deg R_i \leq g_i - 1 (i = 1, 2), R_0(\beta) = a\beta^{g_0-1} + \cdots \right\}
\end{align}

of $\mathbb{P}(L \oplus K)$ of dimension $g - 1$ has the property that the quadrics $Q$ and $Q'$ vanish on all of $V$. 
Proof. Let $\alpha = \delta^d(P) = (-df_1(\beta), f_0(\beta))$. Observe that for $(\lambda, a) \in V$, we have

\begin{align}
\alpha \lambda^2 &= \left(-df_1(\beta)R_0(\beta)^2, f_0(\beta)R_1(\beta)^2\right) \\
&= f_0(\beta)R_1(\beta)^2 - df_1(\beta)R_0(\beta)^2.
\end{align}

But $f_0(\beta)R_1(\beta)^2$ has degree at most $2g_0 + 2(g_1 - 1) = 2g - 2$, while $df_1(\beta)R_0(\beta)^2$ has degree at most $(2g_1 + 1) + 2(g_0 - 1) = 2g - 1$. In particular, we see that $\alpha \lambda^2$ is expressible as a polynomial in $\beta$ of degree at most $2g - 1$, and with $\beta^{2g-1}$ term equal to $-da^2$. Hence we see that $T(\alpha \lambda^2) = 0$ and $T(\alpha \beta \lambda^2) = -da^2$, so that the quadrics $(10.20)$ and $(10.21)$ vanish. \hfill \Box

11. Proof of Theorem 9.4

Recall that we are given a polynomial $f(x) \in K[x]$ of degree $2g + 1$, and $J$ the Jacobian of the hyperelliptic curve $y^2 = f(x)$. We wish to find $d$ such that $S_2(K, J^d)$ strictly contains $S_2(K, J)$.

We may construct such $d$ using Cebotarev. Given any finite Galois extension $\tilde{K}$ of $K$, we may find a prime ideal $p$ of $O_K$ whose Frobenius element is given by any element of $\text{Gal}(\tilde{K}/K)$ we choose. In particular, we may find $p$ which splits in $\tilde{K}$. If $\tilde{K}$ contains the Hilbert class field of $K$, then $p$ is principal, of the form $(\pi)$ for some $\pi$. We may consider $d = \pi$ or $d$ equal to a product of multiple such $\pi$’s. In addition, the local field $K_\pi$ will contain $\tilde{K}$, so we may set $\tilde{K}$ up to simplify the local condition at $\pi$.

Recall that for all but finitely many places $v$ of $K$, the local condition at $v$ amounts to a simple criterion:

**Proposition 11.1.** Suppose $\theta \in (L^\times / (L^\times)^2)_{n=1}$ and $v$ is a finite place not dividing 2, such that $J$ has good reduction at $v$. Then the following are equivalent:

1. $j_v(\theta_v) = 0$.

2. The restriction of $\theta_v$ to $K_v^{ur}$ is zero.
(3) \( \text{val}_v(\theta(e_i)) \) is even for all \( i \).

(4) \( \theta_v \) has a representative in \( \left( \mathcal{O}^\times_{L_v}/(\mathcal{O}^\times_{L_v})^2 \right)_{N=1} \).

Proof. (1) \( \iff \) (2): This holds for arbitrary abelian varieties. Consider the diagram

\[
\begin{array}{cccccc}
H^1\left( \hat{\mathbb{Z}}, J(K_v^{\text{ur}})[2] \right) & \longrightarrow & H^1\left( \hat{\mathbb{Z}}, J(K_v^{\text{ur}}) \right)[2] \\
\downarrow & & \downarrow \\
0 & \longrightarrow & J(K_v)/2J(K_v) & \longrightarrow & H^1(K_v, J)[2] & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J(K_v^{\text{ur}})/2J(K_v^{\text{ur}}) & \longrightarrow & H^1(K_v^{\text{ur}}, J)[2] & \longrightarrow & 0
\end{array}
\]

(11.1)

where \( \hat{\mathbb{Z}} \) is identified with \( \text{Gal}(K_v^{\text{ur}}/K_v) \) by choosing the Frobenius as a topological generator. We want to show that \( j_v(\theta_v) = 0 \) if and only if \( \text{res}(\theta_v) = 0 \). The “if” implication follows from \( H^1\left( \hat{\mathbb{Z}}, J(K_v^{\text{ur}})[2] \right) = 0 \), while the “only if” implication follows from \( J(K_v^{\text{ur}})/2J(K_v^{\text{ur}}) = 0 \).

To see these, we use the reduction exact sequence

\[
0 \rightarrow J_1(K_v^{\text{ur}}) \rightarrow J(K_v^{\text{ur}}) \rightarrow \overline{J}(k_v) \rightarrow 0
\]

(11.2)

where \( k_v \) is the residue field of \( K_v \) and \( J_1 \) is the kernel of reduction. \( J_1 \) is pro-\( \ell \) where \( \ell \) is the residue characteristic of \( v \), so multiplication by 2 is invertible. Also \( \overline{J}(k_v) \) is divisible, so \( J(K_v^{\text{ur}}) \) is 2-divisible. This gives \( J(K_v^{\text{ur}})/2J(K_v^{\text{ur}}) = 0 \). For \( H^1 \), we consider the cohomology of the exact sequence, and note that \( J(K_v) \rightarrow \overline{J}(k_v) \) is still surjective, so we find

\[
0 \rightarrow H^1\left( \hat{\mathbb{Z}}, J_1(K_v^{\text{ur}}) \right) \rightarrow H^1\left( \hat{\mathbb{Z}}, J(K_v^{\text{ur}}) \right) \rightarrow H^1\left( \hat{\mathbb{Z}}, \overline{J}(k_v) \right)
\]

(11.3)

and the last term is zero by Lang’s theorem. So \( H^1\left( \hat{\mathbb{Z}}, J(K_v^{\text{ur}}) \right) \cong H^1\left( \hat{\mathbb{Z}}, J_1(K_v^{\text{ur}}) \right) \), on which multiplication by 2 is invertible. In particular, the 2-torsion subgroup is trivial, as claimed.
(2) \implies (3): We’re given that \( \theta_v \) is a square in \( L_v^{ur} \). In particular, each \( \theta_v(e_i) \) is a square in \( L_v^{ur} \), so must have even valuation.

(3) \implies (4): The integers \( n_i = \text{val}_v(\theta(e_i)) \) are even and preserved under the action of Galois. Letting \( \varpi \) be a uniformizer of \( K_v \), then there exists a unique \( \vartheta \in L_v^\times \) with \( \vartheta(e_i) = \varpi^{n_i/2} \). Now \( \vartheta/\varpi^2 \in \mathcal{O}_L^\times \).

(4) \implies (1): It’s enough to show that \( \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \) is trivial. Since \( J \) has good reduction at \( v \), all \( e_i \) lie in \( K_v^{ur} \). So \( \mathcal{O}_L^\times \) is isomorphic to a product of \( 2g \) copies of \( \mathcal{O}_K^\times \), and every element of \( \mathcal{O}_K^\times \) is a square. \( \square \)

Now in order to show that a given \( \theta \in H^1(K, J^d[2]) \) lies in \( S_2(K, J^d) \), we may apply the criterion in Proposition 11.1 for all places except those dividing \( 2d \Delta \infty \), where \( \Delta \) is the discriminant of \( f \). Now the places dividing \( 2\Delta \infty \) are fixed, and so we will choose the primes dividing \( d \) to behave “nicely” at these places. Then only the places dividing \( d \) remain to be checked.

11.1. The Reducible Case. Suppose \( f(x) \in K[x] \) is reducible, and fix a factorization \( f = f_0 f_1 \) with \( f_0 \) nonconstant, and as before \( f_0 \) having even degree and \( f_1 \) having odd degree. Let \( \tilde{K} \) be a finite Galois extension of \( K \) such that the following hold:

(1) \( \tilde{K} \) contains the ray class field \( K(8\Delta \infty) \) to modulus \( 8\Delta \infty \), for \( \Delta \) the discriminant of \( f \).

(2) \( \tilde{K} \) contains \( E \) and square roots of the \( f_0(e_i) \) and the \( -f_1(e_i) \).

(3) The restriction of \( S_2(K, J) \) to \( \tilde{K} \) is zero. This can be done since \( S_2(K, J) \) is a finite subgroup of \( H^1(K, J^d[2]) \) and every Galois cocycle becomes trivial when restricted to an appropriate finite extension. Explicitly, if \( \theta \in H^1(K, J^d[2]) \cong (L^\times/(L^\times)^2)_{\equiv 1} \) is given by a function \( \{e_1, \ldots, e_{2g+1}\} \rightarrow K^\times/(K^\times)^2 \) with norm a square, then \( \theta \) becomes trivial over a field containing square roots of all \( \theta(e_i) \).

There exists a prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \) which splits in \( \tilde{K} \). Such a \( \mathfrak{p} \) is principal, of the form \( (\pi) \) for some totally positive \( \pi \equiv 1 \pmod{8\Delta} \). We also see that \( \tilde{K} \) embeds into
the local field $K_p = K_\pi$. Now set $d = \pi$ and define $\alpha \in L^\times/(L^\times)^2$ by

$$\alpha \equiv \pi \pmod{f_0}, \quad \alpha \equiv 1 \pmod{f_1}$$

having norm $\pi^{\deg f_0}$, a square. That is, $\alpha = (\pi, 1)$ according to our notation. We will see that $\alpha \notin S_2(K, J)$ and that $S_2(K, J) \cup \{\alpha\} \subseteq S_2(K, J^\pi)$.

Proof that $S_2(K, J) \subseteq S_2(K, J^\pi)$. Suppose $\theta \in S_2(K, J)$. We wish to show that $\theta \in S_2(K, J^\pi)$ as well. For $v$ not dividing 2, $\pi$, $\Delta$, or $\infty$, we verify the Selmer condition at $v$ by applying Proposition 11.1. We want that $\theta_v$ restricts to zero in $K_v^\text{ur}$ for these $v$. But this must be true since $\theta$ was in $S_2(K, J)$ to begin with.

For $v$ dividing 2, $\Delta$, or $\infty$, $\pi \in (K_v^\times)^2$, so that $J$ and $J^\pi$ are isomorphic over $K_v$. Hence $\theta$ still satisfies the Selmer condition at $v$.

Finally, at $\pi$, $\theta_\pi$ is in fact the trivial class in $H^1(K_\pi, J^\pi[2])$ by design, as $K_\pi$ contains $\overline{K}$.

Proof that $\alpha \notin S_2(K, J)$. Since the image of $S_2(K, J)$ in $H^1(K_\pi, J^\pi[2])$ is trivial, it is enough to show that $\alpha_\pi$ is nontrivial. Indeed if $\alpha_\pi$ were trivial, then we would have $\alpha_\pi(e_i) \in (K_\pi^\times)^2$ for every $i$. But $\pi \notin ((K_\pi^\times)^2$, a contradiction.

Proof that $\alpha \in S_2(K, J^\pi)$. To see that $\alpha$ satisfies the Selmer condition for $v$ not dividing 2, $\pi$, $\Delta$, or $\infty$, we apply Proposition 11.1. For these $v$, we have $\pi \in \mathcal{O}_v^\times$, and therefore $\alpha_v \in \mathcal{O}_v^\times$.

For $v$ dividing 2, $\Delta$, or $\infty$, again we use the fact that $\pi \in (K_v^\times)^2$. Replacing $\pi$ with a square root in the expression (11.4) shows that $\alpha_v$ is trivial.

Finally, at $\pi$, the class $(-f_1(\beta), f_0(\beta))$ is trivial in $K_\pi$. Therefore we have $\alpha_\pi = (-\pi f_1(\beta), f_0(\beta))$ and so by (10.16), $\alpha_\pi = \delta^\pi(P)$ where $P \in J(K)[2]$ corresponds to the factorization $f = f_0 f_1$.

11.2. The Irreducible Case. Since $f$ is irreducible, the group $\Gamma$ embeds into $S_{2g+1}$ as a transitive subgroup. Fix a root $e_1$ of $f$, and let $E_1 = K(e_1)$. $e_1$ determines a
factorization \( f = f_0 f_1 \) in \( E_1[x] \), with \( f_1(x) = x - e_1 \). By the work of the previous section, we could certainly raise the Selmer rank if we were working over \( E \), or even \( E_1 \); our goal here is to show that enough of the argument in the previous section descends to \( K \), and then patch up the holes that remain.

To motivate the construction of our new elements of \( H^1(K, J[2]) \), over \( E \) and using the factorization of \( f \) above, we can produce elements such as

\[
\alpha = (1, \Pi, \Pi, \ldots, \Pi)
\]

for some appropriate \( \Pi \in \mathcal{O}_E \), which resemble the elements used in the reducible case. However, such an \( \alpha \) does not lie in \( L \) and so we need to multiply \( \alpha \) by its Galois conjugates, also keeping in mind the action of \( \text{Gal}(E/K) \) on roots of \( f \). This product results in an element of \( L^\times \) whose value at \( e_i \) is the product of all \( \sigma \Pi \) over \( \sigma \) such that \( \sigma(e_1) \neq e_i \). These elements are the ones we will consider.

We will choose primes according to the following:

\[ \text{Lemma 11.2. There exist elements } \Pi \text{ and } \Pi' \text{ of } E, \text{ generating distinct prime ideals, such that the following hold:} \]

1. \( \Pi \) and \( \Pi' \) are totally positive and congruent to 1 modulo \( 8\Delta \).
2. \( S_2(K, J) \) restricts to zero in \( K_\Pi \) and \( K_{\Pi'} \).
3. \( K_\Pi \) and \( K_{\Pi'} \) contain square roots of \( -f_1(e_i) \) and \( f_0(e_i) \).
4. \( \left( \frac{\Pi}{\Pi'} \right) = \left( \frac{\Pi'}{\Pi} \right) = 1 \). Here \((\cdot)\) denotes the quadratic character.
5. For every nontrivial \( \sigma \in \Gamma \), we have

\[
\left( \frac{\sigma \Pi'}{\Pi'} \right) = \left( \frac{\sigma \Pi}{\Pi'} \right) = \left( \frac{\sigma \Pi'}{\Pi} \right) = \left( \frac{\sigma \Pi}{\Pi} \right).
\]
Suppose now we set

\[(11.7) \quad \Pi = N_{E/E_1} \Pi \]
\[(11.8) \quad \pi = N_{E_1/K} \Pi \]

and for \(1 \leq i \leq 2g + 1\), we define \(\Pi_i = \sigma \Pi\) if \(\sigma e_1 = e_i\); this is well-defined. Define \(\gamma \in L^\times\) by

\[(11.9) \quad \gamma(e_i) = \pi \Pi_i^{-1} \cdot \]

In particular, the norm of \(\gamma\) is \(\pi^{2g}\), a square. \(\Pi', \pi', \Pi'_i, \) and \(\gamma'\) are defined analogously. Hence \(\gamma\) and \(\gamma'\) are elements of \(H^1(K, J[2])\).

(6) We can arrange that \(\gamma_v = \gamma'_v\) for every \(v\) which is either real or divides \(2\Delta\).

Proof. Fix a finite Galois extension \(F\) of \(E\) containing square roots of \(-f_1(e_i)\) and \(f_0(e_i)\), such that the restriction of \(S_2(K, J)\) to \(F\) is zero. Now for \(j \geq 1\), we inductively define \(\Pi^{(j)}\) as follows: let \(\tilde{E}\) be the Galois closure of

\[(11.10) \quad E \left(8\Delta \infty \prod_{k<j} \Pi^{(k)}\right) F\]

over \(E\).

Claim 11.3. All of the \(\sigma \Pi^{(k)}\) for \(k < j\) and nontrivial \(\sigma \in \Gamma\) are unramified in \(\tilde{E}\).

(To see the claim, the \(\sigma \Pi^{(k)}\) do not divide \(8\Delta \infty \prod_{k<j} \Pi^{(k)}\) so do not ramify over the ray class field. They do not ramify over \(F\) because the \(\Pi^{(k)}\) split over \(F\), which we will see by construction.)

As a result, \(\tilde{E}\) along with each of the \(E \left(\sqrt{\sigma \Pi^{(k)}}\right)\) — taken over nontrivial \(\sigma \in \Gamma\) and \(k < j\) — are linearly disjoint over \(E\). Hence for \(\tilde{E}\) a finite Galois extension of \(E\) containing \(\tilde{E}\) and the \(E \left(\sqrt{\sigma \Pi^{(k)}}\right)\), there exists \(\tau \in \text{Gal}(\tilde{E}/E)\) such that \(\tau\) restricted
to \( \bar{E} \) is trivial, while

\[
(11.11) \quad \frac{\tau \sqrt{\sigma \Pi^{(k)}}}{\sqrt{\sigma \Pi^{(k)}}} = \left( \frac{\sigma \Pi^{(k)}}{\Pi^{(k)}} \right)
\]

for every nontrivial \( \sigma \in \Gamma \) and \( k < j \). Now there exists a prime \( p \) of \( \mathcal{O}_K \) which splits over \( E \), such that for some \( \mathfrak{p} \) dividing \( p \) in \( E \), the Frobenius of \( \mathfrak{p} \) on \( \bar{E} \) is given by the conjugacy class of \( \tau \). Take \( \Pi^{(j)} \) to be an appropriate generator of \( \mathfrak{p} \). So \( \Pi^{(j)} \) has the following properties:

1. The \( \sigma \Pi^{(j)} \) are all distinct as \( \sigma \in \text{Gal}(E/K) \) varies.
2. \( \Pi^{(j)} \) is totally positive.
3. \( \Pi^{(j)} \equiv 1 \pmod{8\Delta} \).
4. \( \Pi^{(j)} \equiv 1 \pmod{\Pi^{(k)}} \) for every \( k < j \).
5. \( \mathfrak{p} = (\Pi) \) splits over \( F \).
6. \( \left( \frac{\sigma \Pi^{(k)}}{\Pi^{(j)}} \right) = \left( \frac{\sigma \Pi^{(k)}}{\Pi^{(j)}} \right) \) for every \( k < j \) and nontrivial \( \sigma \).

Now if we were to take \( \Pi = \Pi^{(k)} \) and \( \Pi' = \Pi^{(j)} \) for some \( k < j \), then all of the conditions of Lemma 11.2 will be satisfied except possibly

\[
(11.12) \quad \left( \frac{\sigma \Pi'}{\Pi'} \right) = \left( \frac{\sigma \Pi}{\Pi} \right)
\]

for all nontrivial \( \sigma \in \Gamma \), and assertion (6). To see this, assertions (1) through (3) are clear. \( \Pi' \equiv 1 \pmod{\Pi} \) implies in particular \( \left( \frac{\Pi'}{\Pi} \right) = 1 \), and then quadratic reciprocity implies \( \left( \frac{\Pi}{\Pi'} \right) = 1 \) as well. We also have \( \left( \frac{\sigma \Pi}{\Pi} \right) = \left( \frac{\sigma \Pi}{\Pi} \right) \) and

\[
(11.13) \quad \left( \frac{\sigma \Pi'}{\Pi} \right) = \left( \frac{\Pi}{\sigma \Pi'} \right) = \left( \frac{\sigma^{-1} \Pi'}{\Pi} \right) = \left( \frac{\sigma^{-1} \Pi'}{\Pi} \right) = \left( \frac{\Pi}{\sigma \Pi'} \right) = \left( \frac{\sigma \Pi}{\Pi} \right).
\]

We also “nearly” obtain assertion (6). For \( v \) dividing \( 2, \Delta, \) or \( \infty \), we find that \( \Pi, \Pi' \), and their images under \( \Gamma \) all lie in \( ((E^v)\setminus)^2 \). Hence \( \gamma_v \) and \( \gamma'_v \) both restrict to zero.
in $H^1(E^v, J[2])$, meaning they are both inflated from elements of $H^1(\Gamma^v, J(E^v)[2])$, a finite group.

Finally, by the Pigeonhole Principle, we can choose $k < j$ such that [11.12] and assertion (6) both hold as well. This is because the tuples

\[(11.14) \left( \left( \frac{\sigma \Pi(k)}{\Pi(k)} \right)_{\sigma \neq 1}, \left( \gamma_v(k) \right)_{v | 2 \Delta \infty} \right)\]

all lie in a finite set, and so some two must agree. For such a $k$ and $j$, $\Pi$ and $\Pi'$ satisfy all of the desired assertions. \hfill \square

Now we take $d = \pi \pi'$ and $\alpha = \gamma \gamma'$. For the primes dividing $d$, observe that $K_\pi \cong E_\Pi$ and $K_{\pi'} \cong E_{\Pi'}$.

Again we show that $\alpha \notin S_2(K, J)$ and that $S_2(K, J) \cup \{\alpha\} \subseteq S_2(K, J^d)$. The proofs that $S_2(K, J) \subseteq S_2(K, J^d)$ and $\alpha \notin S_2(K, J)$ are essentially the same as before.

**Proof that $\alpha \in S_2(K, J^d)$**. The criterion in Proposition [11.1] is clearly satisfied by both $\gamma$ and $\gamma'$, hence $\alpha$. For $v$ dividing 2, $\Delta$, or $\infty$, we have $\gamma_v = \gamma_v'$, and so $\alpha_v = \gamma_v^2 = 1$.

Finally, it remains to check the local conditions at $\pi$ and $\pi'$. By symmetry in the assertions in Lemma [11.2] we will simply check at $\pi$. In $K_\pi \cong E_\Pi$, observe that $\Pi' \in (O_\Pi^\times)^2$ and $(\sigma \Pi)(\sigma \Pi') \in (O_\Pi^\times)^2$ for nontrivial $\sigma \in \Gamma$. Hence modulo square factors, we have

\[(11.15) \quad d \equiv \Pi\]

\[(11.16) \quad \pi \pi'(\Pi_i \Pi_i)^{-1} \equiv \begin{cases} 1 & i = 1 \\ \Pi & \text{otherwise} \end{cases}\]

and so we can conclude that $\alpha_\Pi = (\Pi, 1) = (d, 1) = (-df_1(\beta), f_0(\beta))$ with our choice of $f_0$ and $f_1$. Again we are done by [10.16]. \hfill \square
REFERENCES


