Two-Descent on the Jacobians of Hyperelliptic Curves

Jaclyn Lang
Churchill College

I declare that this essay is work done as part of the Part III Examination. I have read and understood the Statement of Plagiarism for Part III and Graduate Courses issued by the Faculty of Mathematics, and have abided by it. This essay is the result of my own work and, except where explicitly stated otherwise, only includes material undertaken since the publication of the list of essay titles, and includes nothing which was performed in collaboration. No part of this essay has been submitted, or is concurrently being submitted, for any degree, diploma or similar qualification at any university or similar institution.

Signed:
Date:

Home address: 1905 Lochmore Drive, Longmont, CO 80504, USA

Two Descent on the Jacobians of Hyperelliptic Curves

Acknowledgements
I would like to thank Dr. Tom Fisher for setting this essay and for advising me in writing it. I would also like to thank Dr. Tim Dokchitser, Alex Bartel, James Bridgewater, and Jennifer Redmond for helpful conversations and advice regarding this essay.

1 Introduction

Throughout this paper, $\mathcal{C}$ will be a curve defined over a field K. The field K will often be the rational numbers or a number field, but we will also use curves defined over algebraically closed fields, extensions of the p-adics, and finite fields. When appropriate, $\mathcal{O}_K$ denotes the ring of integers of K. We will use $\overline{K}$ to denote a fixed algebraic closure of the field K. Whenever M is a $\mathrm{Gal}(\overline{K}/K)$-module, we will write $H^i(K, M)$ instead of $H^i(\mathrm{Gal}(\overline{K}/K), M)$ for the i-th cohomology group of M.

Recall that the curve $\mathcal{C}$ defined over $\overline{K}$ has the group $\mathrm{Pic}(\mathcal{C})$ associated to it, where $\mathrm{Pic}(\mathcal{C})$ is the divisors of $\mathcal{C}$ modulo linear equivalence. The subgroup of $\mathrm{Pic}(\mathcal{C})$ of divisors of degree zero is denoted $\mathrm{Pic}^0(\mathcal{C})$. There is a well defined action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{Pic}^0(\mathcal{C})$ that will be described in section 2. This leads to

Definition 1. *The Jacobian of a curve $\mathcal{C}$ is the group $\mathrm{Pic}^0(\mathcal{C})$. If $\mathcal{C}$ is defined over a field K, we will let $J(K)$ denote the $\mathrm{Gal}(\overline{K}/K)$-invariant elements of J. We call elements of $J(K)$ K-rational elements.*

The Jacobian of a curve is not only a group, but has the structure of a variety. However, we shall be concerned with the arithmetic of the Jacobian in this essay and hence we are primarily interested in the group structure of the Jacobian.

The Mordell-Weil theorem states that for any curve $\mathcal{C}$ defined over a number field K, the K-rational elements of the Jacobian, J(K), form a finitely generated abelian group. The proof of this fact is in two parts. First, one proves that $J(K)/2J(K)$ is a finite group, a fact known as the weak Mordell-Weil theorem. One then applies the theory of heights to the generators of $J(K)/2J(K)$, of which there are only a finite number, to conclude that $J(K)$ must be finitely generated.

If the generators of $J(K)/2J(K)$ are known, it is possible to recover generators for $J(K)$. As the torsion subgroup of $J(K)$, denoted $J(K)_{tors}$, is easy to compute it is then possible to determine the free rank of $J(K)$. Unfortunately, there is no known algorithm for finding generators for $J(K)/2J(K)$. The process of two descent is an algorithm for finding generators for a finite group called the 2-Selmer group of J over K, denoted $\mathrm{Sel}_2(J/K)$. As we will discuss in this essay, it is known that there is an injective homomorphism

$$J(K)/2J(K) \hookrightarrow \mathrm{Sel}_2(J/K),$$

and so two descent gives an upper bound on the size of $J(K)/2J(K)$ and thus also an upper bound for the rank of $J(K)$. Given a particular example, one hopes to be able to find the same number of

independent points in $J(K)/2J(K)$ as this upper bound and hence be able to calculate the rank of $J(K)$ exactly.

This essay will focus on the process of two descent. We will prove why the algorithm gives the claimed bound on the rank, calculate some explicit examples for elliptic curves and hyperelliptic curves of genus two, and discuss results about two descent on hyperelliptic curves of arbitrary genus.

Before proceeding to the results about two descent, we prove a theorem from Kummer theory that will be useful in what follows. Moreover, the structure of the proof of Theorem 1 is similar to that used to construct the injection $J(K)/2J(K) \hookrightarrow \mathrm{Sel}_2(J/K)$ that is central to two descent.

Theorem 1. *[9, p. 199] For any field K, let $K^\times$ denote the multiplicative group $K \setminus \{0\}$, let $K^{\times 2} = \{x^2 | x \in K^\times\}$ and let $\mu_2(\overline{K})$ be the second roots of unity in $\overline{K}$. Then*

$$K^\times / K^{\times 2} \cong H^1(K, \mu_2(\overline{K})).$$

Proof. Let $s : \overline{K}^\times \to \overline{K}^\times$ be the squaring map $s(x) = x^2$. As $\overline{K}$ is algebraically closed, s is surjective and we have the short exact sequence

$$1 \to \mu_2(\overline{K}) \to \overline{K}^\times \xrightarrow{s} \overline{K}^\times \to 1.$$

This yields the standard long exact sequence in Galois cohomology

$$1 \to H^0(K, \mu_2(\overline{K})) \to H^0(K, \overline{K}^\times) \xrightarrow{s} H^0(K, \overline{K}^\times) \xrightarrow{\delta} H^1(K, \mu_2(\overline{K})) \to H^1(K, \overline{K}^\times).$$

Recall that the zeroth homology is defined to be the $\mathrm{Gal}(\overline{K}/K)$-invariant elements of the module. In particular, $H^0(K, \overline{K}^\times) = K^\times$. Using exactness and the first isomorphism theorem we note that

$$\begin{aligned}
\ker\left(H^1(K, \mu_2(\overline{K})) \to H^1(K, \overline{K}^\times)\right) &= \mathrm{Im}\left(K^\times \xrightarrow{\delta} H^1(K, \mu_2(\overline{K}))\right) \\
&\cong K^\times / \ker\left(K^\times \xrightarrow{\delta} H^1(K, \mu_2(\overline{K}))\right) \\
&= K^\times / \mathrm{Im}(s|_{K^\times}) \\
&= K^\times / K^{\times 2}.
\end{aligned}$$

Hence, from the long exact sequence we extract the short exact sequence

$$1 \to K^\times / K^{\times 2} \xrightarrow{\delta} H^1(K, \mu_2(\overline{K})) \to H^1(K, \overline{K}^\times).$$

Now, Hilbert's Theorem 90 states that $H^1(K, \overline{K}^\times) = 0$ [9, p. 335]. Thus, $K^\times / K^{\times 2} \cong H^1(K, \mu_2(\overline{K}))$ as claimed. □

Note that the isomorphism found in the proof of Theorem 1 is the connecting homomorphism arising from the Snake Lemma in the construction of the long exact sequence. It is given by

$$\begin{aligned}
\delta : K^\times / K^{\times 2} &\to H^1(K, \mu_2(\overline{K})) \\
x &\mapsto \xi_x,
\end{aligned}$$

where $\xi_x(\sigma) = \frac{\sigma(\sqrt{x})}{\sqrt{x}}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We will map frequent use of this map and its inverse throughout the paper.

2 Theory of descent

The theory of descent on Jacobians of hyperelliptic curves can be done most generally via Galois cohomology. In this section we give the proof of descent via Galois cohomology in the greatest generality we will require in this paper. Further sections explore how these results can be interpreted and explicitly calculated depending on the genus of the curve and the degree of the defining polynomial.

Let K be a field of characteristic zero and $\mathcal{C}$ the non-singular model of the curve defined over K by

$$\mathcal{C} : y^2 = f(x) = \prod_{i=1}^{d}(x - \alpha_i),$$

where the $\alpha_i \in \overline{K}$ are distinct. Let $J[2]$ denote the 2-torsion subgroup of $J(\overline{K})$.

Recall that elements of $J(\overline{K})$ are linear equivalence classes of divisors on $\mathcal{C}$. There is an action of $\mathrm{Gal}(\overline{K}/K)$ on $J(\overline{K})$ defined as follows. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $D = \sum_{i=1}^{n}(P_i)$, where $P_i \in \mathcal{C}(\overline{K})$. Then

$$D^\sigma = \sum_{i=1}^{n}({P_i}^\sigma),$$

where σ acts coordinate-wise on points P_i of $\mathcal{C}$. This action is well-defined since if $D = D'$ in $J(\overline{K})$ there is a rational function $g \in \overline{K}(\mathcal{C})$ such that $D - D' = \mathrm{div}(g)$. As σ is a nonzero field homomorphism, it follows that $D^\sigma - D'^\sigma = \mathrm{div}(\sigma(g))$, where $\sigma(g)$ indicates σ applied to all coefficients of g. This is the action referred to in Definition 1. Note that it is not necessary for every point of a divisor to be defined over K in order for the divisor to be K-rational. It is simply necessary that for every point P appearing in the divisor, all Galois conjugates of P also appear in the divisor with the same multiplicity as that of P.

In order to find the desired injection $J(K)/2J(K) \hookrightarrow \mathrm{Sel}_2(J/K)$ we begin with the multiplication-by-two map $[2] : J(\overline{K}) \to J(\overline{K})$, where $[2](P) = P + P$ and $+$ is the group operation in $J(\overline{K}) = \mathrm{Pic}^0(\mathcal{C})$. The kernel of $[2]$ is $J[2]$ and $[2]$ is surjective since we are working over the algebraically closed field $\overline{K}$. Thus, we obtain an exact sequence

$$0 \to J[2] \to J(\overline{K}) \xrightarrow{[2]} J(\overline{K}) \to 0$$

which is analogous to that which began the proof of Theorem 1 (although these groups are additive rather than multiplicative). Proceeding as in the proof of Theorem 1, we take Galois cohomology to get the long exact sequence

$$0 \to H^0(K, J[2]) \to H^0(K, J(\overline{K})) \xrightarrow{[2]} H^0(K, J(\overline{K})) \xrightarrow{\kappa} H^1(K, J[2]) \to H^1(K, J(\overline{K})).$$

As before, we may extract the exact sequence

$$0 \to J(K)/2J(K) \xrightarrow{\kappa} H^1(K, J[2]) \to H^1(K, J(\overline{K})).$$

However unlike in the proof of Theorem 1, $H^1(K, J(\overline{K}))$ is not necessarily zero. The map $\kappa : J(K)/2J(K) \hookrightarrow H^1(K, J[2])$ is the connecting homomorphism given by

$$\begin{aligned} \kappa : J(K)/2J(K) &\to H^1(K, J[2]) \\ P &\mapsto \xi_P, \end{aligned}$$

where $\xi_P(\sigma) = Q^\sigma - Q$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, where $Q \in J(\overline{K})$ such that $2Q = P$.

Now let K be a number field and $\mathfrak{p}$ a (possibly infinite) prime of K. Let $K_\mathfrak{p}$ be the completion of K with respect to the standard normalized absolute value associated to $\mathfrak{p}$. The inclusion $K \hookrightarrow K_\mathfrak{p}$ induces natural maps $i_\mathfrak{p} : J(K)/2J(K) \to J(K_\mathfrak{p})/2J(K_\mathfrak{p})$ and $\beta_\mathfrak{p} : H^1(K, J[2]) \to H^1(K_\mathfrak{p}, J(\overline{K_\mathfrak{p}})[2])$. Applying the above process to each $K_\mathfrak{p}$ gives a homomorphism $\kappa_\mathfrak{p}$, and so we have the following commutative diagram.

$$\begin{array}{ccc} J(K)/2J(K) & \xrightarrow{\quad\kappa\quad} & H^1(K, J[2]) \\ \Big\downarrow{\scriptstyle \prod_\mathfrak{p} i_\mathfrak{p}} & & \Big\downarrow{\scriptstyle \prod_\mathfrak{p} \beta_\mathfrak{p}} \\ \prod_\mathfrak{p} J(K_\mathfrak{p})/2J(K_\mathfrak{p}) & \xrightarrow{\prod_\mathfrak{p} \kappa_\mathfrak{p}} & \prod_\mathfrak{p} H^1(K, J(\overline{K_\mathfrak{p}})[2]) \end{array} \tag{1}$$

Our goal is to understand the image of κ. By the commutativity of (1), it follows that $\mathrm{Im}\,\kappa$ is contained in the preimage under $\beta_\mathfrak{p}$ of $\mathrm{Im}\,\kappa_\mathfrak{p}$ for all $\mathfrak{p}$. Thus, we define

Definition 2. *The 2-Selmer group of $J(K)$ is*

$$\mathrm{Sel}_2(J/K) = \bigcap_\mathfrak{p} {\beta_\mathfrak{p}}^{-1}(\mathrm{Im}\,\kappa_p).$$

It is important to note that although $\mathrm{Im}\,\kappa \subseteq \mathrm{Sel}_2(J/K)$, there may not be equality. This is because the local-global principle, or Hasse principle, fails in general for curves of genus greater than zero. That is, analyzing the Jacobian $J(K_\mathfrak{p})$ over all completions $K_\mathfrak{p}$ of K does not necessarily give enough information to understand the rational points $J(K)$ completely. The failure of the Hasse principal for a particular Jacobian is measured in part by the size of the quotient $\mathrm{Sel}_2(J/K)/(\mathrm{Im}\,\kappa)$. This group is

Definition 3. *The 2-part of the Tate-Shafarevich group of J is denoted $Ш_2(J/K)$ and is defined such that the sequence*

$$0 \to J(K)/2J(K) \xrightarrow{\kappa} \mathrm{Sel}_2(J/K) \to Ш_2(J/K) \to 1$$

is exact.

When $Ш_2(J/K)$ is trivial, two descent gives an algorithm to find the rank of $J(K)$. The examples in this paper will all have trivial $Ш_2$. Unfortunately, relatively little is known about the group $Ш_2$ in general and it is often difficult to prove that a discrepancy between the number of known generators for $J(K)$ and the upper bound found through two descent is due to nontrivial elements of $Ш_2$.

3 Two descent for elliptic curves

We will now examine the case of two descent on an elliptic curve. We begin by analyzing the groups and maps in diagram (1) in more detail with the goal of being able to compute them for specific elliptic curves. In addition to being used in the examples, this analysis provides motivation for the more general analysis of diagram (1) over higher genus curves in section 4. After the analysis we then proceed to an example of two descent on an elliptic curve in which we successfully calculate the rank.

Let K be a field of characteristic zero and E the elliptic curve defined by

$$y^2 = f(x) = (x-\alpha)(x-\beta)(x-\gamma),$$

where $\alpha, \beta, \gamma \in K$ are distinct. The assumption that all of the roots of f lie in K can be relaxed. We deal with this in the general case in section 4. Denote by $\mathcal{O}$ the point at infinity; that is, the point $[0:1:0]$ on the projective curve $zy^2 = (x - z\alpha)(x - z\beta)(x - z\gamma)$. Let $E[2]$ denote the 2-torsion subgroup of E, so

$$E[2] = \{\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)\}.$$

Note that in the case of elliptic curves, the points of E represent the Jacobian so we shall use the notation $E(K)$ rather than $J(K)$.

Now, the map defined in the previous section $\kappa : E(K)/2E(K) \to H^1(K, E[2])$ gives an injection of $E(K)/2E(K)$ into an infinite group. We will now analyze the group $H^1(K, E[2])$ with the goal of understanding $\operatorname{Im}\kappa$. Recall that $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This isomorphism can be seen via the Weil pairing, e_2. Namely, let e be the map defined by

$$\begin{aligned} e : E[2] &\to \mu_2(\overline{K}) \times \mu_2(\overline{K}) \\ P &\mapsto (e_2(P, (\alpha, 0)), e_2(P, (\beta, 0))). \end{aligned}$$

The fact that e_2 is non-degenerate and bilinear ensures that e is an isomorphism. Thus we have

Lemma 2. *With notation as above, there is a monomorphism*

$$H^1(K, E[2]) \hookrightarrow K^\times/K^{\times 2} \times K^\times/K^{\times 2}.$$

Proof. The map e induces an isomorphism

$$\begin{aligned} \hat{e} : H^1(K, E[2]) &\to H^1(K, \mu_2(\overline{K}) \times \mu_2(\overline{K})) \\ \xi &\mapsto e \circ \xi. \end{aligned}$$

Further, we have an injection

$$\begin{aligned} f : H^1(K, \mu_2(\overline{K}) \times \mu_2(\overline{K})) &\hookrightarrow H^1(K, \mu_2(\overline{K})) \times H^1(K, \mu_2(\overline{K})) \\ (\sigma \mapsto (x, y)) &\mapsto (\sigma \mapsto x, \sigma \mapsto y). \end{aligned}$$

Composing these maps with the isomorphism δ found in Theorem 1, we obtain an injection

$$H^1(K, E[2]) \xrightarrow{\hat{e}} H^1(K, \mu_2(\overline{K}) \times \mu_2(\overline{K})) \xrightarrow{f} H^1(K, \mu_2(\overline{K})) \times H^1(K, \mu_2(\overline{K})) \xrightarrow{\delta^{-1}\times\delta^{-1}} K^\times/K^{\times 2} \times K^\times/K^{\times 2},$$

as desired. □

By composing κ with the isomorphism in Lemma 2 we have an injection $\lambda : E(K)/2E(K) \hookrightarrow K^\times/K^{\times 2} \times K^\times/K^{\times 2}$. It will be useful to have an explicit description of this map, so we have

Theorem 3. *There is an injective homomorphism*

$$\lambda : E(K)/2E(K) \hookrightarrow K^\times/K^{\times 2} \times K^\times/K^{\times 2}$$

$$P \mapsto \begin{cases} (x-\alpha, x-\beta) & P = (x,y), x \neq \alpha, x \neq \beta \\ ((\alpha-\beta)(\alpha-\gamma), \alpha-\beta) & P = (\alpha, 0) \\ (\beta-\alpha, (\beta-\alpha)(\beta-\gamma)) & P = (\beta, 0) \\ (1,1) & P = \mathcal{O}. \end{cases}$$

Proof. We wish to see that λ is the composition

$$E(K)/2E(K) \xrightarrow{\kappa} H^1(K, E[2]) \xrightarrow{\hat{e}} H^1(K, \mu_2(\overline{K}) \times \mu_2(\overline{K})) \xrightarrow{f} H^1(K, \mu_2(\overline{K})) \times H^1(K, \mu_2(\overline{K})) \xrightarrow{\delta^{-1}\times\delta^{-1}} K^\times/K^{\times 2} \times K^\times/K^{\times 2}.$$

Let $P \in E(K)/2E(K)$ and $Q \in E(\overline{K})$ such that $2Q = P$. The case $P = \mathcal{O}$ is clear, so let $P = (x_1, y_1)$. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. By definition of the above maps we have,

$$f \circ \hat{e} \circ \kappa(P)(\sigma) = \left(e_2(Q^\sigma - Q, (\alpha, 0)), e_2(Q^\sigma - Q, (\beta, 0))\right).$$

We will show that when $P \neq (\alpha, 0)$, $e_2(Q^\sigma - Q, (\alpha, 0)) = \frac{\sigma(\sqrt{x_1-\alpha})}{\sqrt{x_1-\alpha}} = \delta(x_1 - \alpha)(\sigma)$. It then follows for any P other than $(\alpha, 0), (\beta, 0), \mathcal{O}$ that we have

$$\begin{aligned}(\delta^{-1} \times \delta^{-1}) \circ f \circ \hat{e} \circ \kappa(P)(\sigma) &= (\delta^{-1} \times \delta^{-1}) \left(e_2(Q^\sigma - Q, (\alpha, 0)), e_2(Q^\sigma - Q, (\beta, 0))\right) \\ &= (\delta^{-1} \times \delta^{-1}) \left(\frac{\sigma(\sqrt{x_1-\alpha})}{\sqrt{x_1-\alpha}}, \frac{\sigma(\sqrt{x_1-\beta})}{\sqrt{x_1-\beta}}\right) \\ &= (x-\alpha, x-\beta) = \lambda(P),\end{aligned}$$

as desired.

Recall that for $S, T \in E[2]$, the Weil pairing is defined by

$$e_2(S,T) = \frac{f_T(S)}{f_S(T)},$$

where $f_T, f_S \in \overline{K}(E)$ have disjoint support and $\operatorname{div} f_T = 2T$ and $\operatorname{div} f_S = 2S$. In our case, let $S = (Q^\sigma) - (Q)$ and $T = ((\alpha, 0)) - (\mathcal{O})$. We may take $f_T = X - \alpha$ since $\operatorname{div}(X-\alpha) = 2((\alpha,0)) - 2(\mathcal{O}) = 2T$. Since $2Q = P$ in $E(K)$ there is a function $g \in \overline{K}(E)$ such that $\operatorname{div} g = 2(Q) - (P)$. Then for any $\sigma \in \operatorname{Gal}(\overline{K}/K)$ we have $\operatorname{div}(g^\sigma) = 2(Q^\sigma) - (P^\sigma) = 2(Q^\sigma) - (P)$ since $P \in E(K)$. Therefore we may take $f_S = g^\sigma/g$ since $\operatorname{div}(g^\sigma/g) = 2(Q^\sigma) - (P) - 2(Q) + (P) = 2(Q^\sigma) - 2(Q)$. As $P \neq \mathcal{O}$ it follows that Q and Q^σ are not $\mathcal{O}$ or $(\alpha, 0)$. Thus,

$$\begin{aligned} e_2(Q^\sigma - Q, (\alpha,0)) &= \frac{f_T(S)}{f_S(T)} = \frac{(X-\alpha)(Q^\sigma - Q)}{(g^\sigma/g)((\alpha,0) - \mathcal{O})} \\ &= \left(\frac{(X-\alpha)(Q^\sigma)}{g^\sigma((\alpha,0)-\mathcal{O})}\right)\left(\frac{(X-\alpha)(Q)}{g((\alpha,0)-\mathcal{O})}\right)^{-1} \\ &= \left(\frac{(X-\alpha)(Q)}{g((\alpha,0)-\mathcal{O})}\right)^{\sigma}\left(\frac{(X-\alpha)(Q)}{g((\alpha,0)-\mathcal{O})}\right)^{-1}. \end{aligned}$$

We shall show that $(X-\alpha)(Q)/g((\alpha,0)-\mathcal{O})$ is a square root of $x_1 - \alpha = (X-\alpha)(P)$. Using Weil reciprocity we have

$$\begin{aligned} \left(\frac{(X-\alpha)(Q)}{g((\alpha,0)-\mathcal{O})}\right)^2 &= \frac{(X-\alpha)(2Q)}{g(2(\alpha,0)-2\mathcal{O})} = \frac{(X-\alpha)(2Q)}{g(\operatorname{div}(X-\alpha))} = \frac{(X-\alpha)(2Q)}{(X-\alpha)(\operatorname{div}(g))} \\ &= \frac{(X-\alpha)(2Q)}{(X-\alpha)(2Q-P)} = (X-\alpha)(P), \end{aligned}$$

as desired.

It remains to check the point $(\alpha, 0)$. Since $(\alpha,0) = (\beta,0) + (\gamma,0)$ we have

$$\begin{aligned} f \circ \hat{e} \circ \kappa((\alpha,0))(\sigma) &= f \circ \hat{e} \circ \kappa((\beta,0))(\sigma) f \circ \hat{e} \circ \kappa((\gamma,0))(\sigma) \\ &= \left(\frac{\sigma(\sqrt{\beta-\alpha})}{\sqrt{\beta-\alpha}}\frac{\sigma(\sqrt{\gamma-\alpha})}{\sqrt{\gamma-\alpha}}, \frac{\sigma(\sqrt{\alpha-\beta})}{\sqrt{\alpha-\beta}}\right) \\ &= \left(\frac{\sigma(\sqrt{(\alpha-\beta)(\alpha-\gamma)})}{\sqrt{(\alpha-\beta)(\alpha-\gamma)}}, \frac{\sigma(\sqrt{\alpha-\beta})}{\sqrt{\alpha-\beta}}\right). \end{aligned}$$

This completes the proof. □

Now let K be a number field. For each prime $\mathfrak{p}$ of K, the inclusion $K \hookrightarrow K_\mathfrak{p}$ induces a natural map $j_\mathfrak{p} : K^\times/K^{\times 2} \to {K_\mathfrak{p}}^\times/{K_\mathfrak{p}}^{\times 2}$. Applying Theorem 3 to each $K_\mathfrak{p}$ gives a homomorphism $\lambda_\mathfrak{p}$. Let λ be the map of Theorem 3 applied to K. We have the following commutative diagram.

$$\begin{array}{ccc} E(K)/2E(K) & \xrightarrow{\quad\lambda\quad} & K^\times/K^{\times 2} \times K^\times/K^{\times 2} \\ \downarrow{\scriptstyle \prod_\mathfrak{p} i_\mathfrak{p}} & & \downarrow{\scriptstyle \prod_\mathfrak{p} j_\mathfrak{p}} \\ \prod_\mathfrak{p} E(K_\mathfrak{p})/2E(K_\mathfrak{p}) & \xrightarrow{\prod_\mathfrak{p} \lambda_\mathfrak{p}} & \prod_\mathfrak{p} {K_\mathfrak{p}}^\times/{K_\mathfrak{p}}^{\times 2} \times {K_\mathfrak{p}}^\times/{K_\mathfrak{p}}^{\times 2} \end{array} \tag{2}$$

This is just the diagram (1) with the first cohomology groups on the right replaced with the multiplicative group of the field modulo squares and the morphisms adjusted accordingly using Lemma 2. These groups are more concrete than the cohomology groups and will facilitate our analysis of $\mathrm{Im}\ \lambda$. In this setting we have

$$\mathrm{Sel}_2(E/K) = \bigcap_{\mathfrak{p}} {j_{\mathfrak{p}}}^{-1}(\mathrm{Im}\ \lambda_p).$$

This is an isomorphic copy of the group given in Definition 2, but we will use the same notation. This will not cause confusion as we will not need to work with the cohomological definition for the remainder of this section.

The idea of two descent is to find $\mathrm{Im}\ \lambda_{\mathfrak{p}}$ for all $\mathfrak{p}$ and pull these sets back to $K^\times/K^{\times 2} \times K^\times/K^{\times 2}$ via the maps $j_{\mathfrak{p}}$. The intersection of these pullbacks is $\mathrm{Sel}_2(E/K)$. In order to make this procedure practicable with a given elliptic curve, it is necessary to reduce the number of primes $\mathfrak{p}$ that must be considered to a finite set. To this effect, we have

Proposition 4. *Let S be the set of all primes where E has bad reduction together with primes lying above 2 and the infinite primes of K. If $\mathfrak{p} \notin S$ then ${j_{\mathfrak{p}}}^{-1}(\mathrm{Im}\ \lambda_{\mathfrak{p}}) = \ker j_{\mathfrak{p}}$. In particular,*

$$\mathrm{Sel}_2(E/K) \subseteq \bigcap_{\mathfrak{p} \in S} {j_{\mathfrak{p}}}^{-1}(\mathrm{Im}\ \lambda_{\mathfrak{p}}).$$

Proof. Let $\mathfrak{p}$ be a prime of K, and let k be the residue field of $K_{\mathfrak{p}}$ of size q. We begin by defining the maximal unramified extension of the completion $K_{\mathfrak{p}}$ and establishing some of its basic properties. Recall that for every positive integer n there is a unique unramified extension of $K_{\mathfrak{p}}$ of degree n given by $K_{\mathfrak{p}}(\zeta_{q^n-1})$, where ζ_{q^n-1} is a primitive (q^n-1)-th root of unity in $\overline{K_{\mathfrak{p}}}$. The residue field of this degree n extension is the unique degree n extension of k. Let ${K_{\mathfrak{p}}}^{nr}$ be the compositium in $\overline{K_{\mathfrak{p}}}$ of all such extensions of $K_{\mathfrak{p}}$. That is,

$${K_{\mathfrak{p}}}^{nr} = \left\langle \bigcup_{n \in \mathbb{Z}^+} K_{\mathfrak{p}}(\zeta_{q^n-1}) \right\rangle.$$

Next we define the unique valuation v on ${K_{\mathfrak{p}}}^{nr}$ extending the valuation $v_{\mathfrak{p}}$ on $K_{\mathfrak{p}}$. Note that any $x \in {K_{\mathfrak{p}}}^{nr}$ is an element of some finite compositum

$$L_x = K_{\mathfrak{p}}(\zeta_{q^{n_1}-1}) \cdots K_{\mathfrak{p}}(\zeta_{q^{n_r}-1}),$$

which is unramified since each individual field is unramified. There is a unique extension v_{L_x} of $v_{\mathfrak{p}}$ to L_x and we define $v(x) = v_{L_x}(x)$. This is well defined by the uniqueness of extensions of valuations. Recall that if $L/K_{\mathfrak{p}}$ is unramified then the unique extension of the valuation $v_{\mathfrak{p}}$ to L is equal to $v_{\mathfrak{p}}$ on elements of $K_{\mathfrak{p}}$. Thus, for all elements $x \in K_{\mathfrak{p}}$ it follows that $v(x) = v_{\mathfrak{p}}(x)$.

Finally, we note that the residue field of ${K_{\mathfrak{p}}}^{nr}$ is $\overline{k}$. This follows from the fact that the residue field of ${K_{\mathfrak{p}}}^{nr}$ must contain the residue field of each subfield of ${K_{\mathfrak{p}}}^{nr}$. As $K_{\mathfrak{p}}(\zeta_{q^n-1}) \subseteq {K_{\mathfrak{p}}}^{nr}$ for all n and has residue field $\mathbb{F}_{q^n}$, we must have $\overline{k}$ as the residue field of ${K_{\mathfrak{p}}}^{nr}$.

We will use the following standard notation in the remainder of the proof. For a field $L/K_\mathfrak{p}$ with residue field ℓ, let $\tilde{E}(\ell)$ be the points on the elliptic curve E with coordinates in ℓ, where the defining coefficients for E are viewed in ℓ via the natural map $L \to \ell$. Let $E_{ns}(\ell)$ be all of the non-singular points of $\tilde{E}(\ell)$. Let $E_0(L)$ be the points of $E(L)$ that map to non-singular points under the reduction map $E(L) \to \tilde{E}(\ell)$, and let $E_1(L)$ be the kernel of the reduction map.

Now let $\mathfrak{p}$ be a prime of K not in S. Letting ${K_\mathfrak{p}}^{nr}$ be L of the last paragraph and recalling that $\mathfrak{p} \notin S$ means that E has good reduction modulo $\mathfrak{p}$, we see that $E_{ns}(\overline{k}) = \tilde{E}(\overline{k})$ and $E_0({K_\mathfrak{p}}^{nr}) = E({K_\mathfrak{p}}^{nr})$. Therefore, the reduction map induces the exact sequence in the rows of the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1({K_\mathfrak{p}}^{nr}) & \longrightarrow & E({K_\mathfrak{p}}^{nr}) & \longrightarrow & \tilde{E}(\overline{k}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \\ 0 & \longrightarrow & E_1({K_\mathfrak{p}}^{nr}) & \longrightarrow & E({K_\mathfrak{p}}^{nr}) & \longrightarrow & \tilde{E}(\overline{k}) & \longrightarrow & 0 \end{array}$$

By applying the Snake Lemma to the above diagram we may extract the exact sequence

$$E_1({K_\mathfrak{p}}^{nr})/2E_1({K_\mathfrak{p}}^{nr}) \to E({K_\mathfrak{p}}^{nr})/2E({K_\mathfrak{p}}^{nr}) \to \tilde{E}(\overline{k})/2\tilde{E}(\overline{k}).$$

As $\overline{k}$ is an algebraically closed field, the nonzero morphism $[2] : \tilde{E}(\overline{k}) \to \tilde{E}(\overline{k})$ is surjective and hence $\tilde{E}(\overline{k})/2\tilde{E}(\overline{k}) = 0$. Also, recall that $E_1({K_\mathfrak{p}}^{nr})$ is a formal group and as $\mathfrak{p} \notin S$ and hence $2 \in {\mathcal{O}_{K_\mathfrak{p}}}^{\times}$, it follows that $[2]$ is an isomorphism on $E_1({K_\mathfrak{p}}^{nr})$. Thus, $E_1({K_\mathfrak{p}}^{nr})/2E_1({K_\mathfrak{p}}^{nr}) = 0$ and by exactness we must have $E({K_\mathfrak{p}}^{nr})/2E({K_\mathfrak{p}}^{nr}) = 0$.

Therefore $\operatorname{Im} \lambda_\mathfrak{p} = 0$ and ${j_\mathfrak{p}}^{-1}(\operatorname{Im} \lambda_\mathfrak{p}) = \ker j_\mathfrak{p} = K^\times/K^{\times 2} \cap {K_\mathfrak{p}}^{\times 2}$, as claimed. □

Proposition 4 allows us to consider only a finite set of primes when trying to understand $\operatorname{Im} \lambda$ inside $K^\times/K^{\times 2} \times K^\times/K^{\times 2}$. The proof shows that we will not obtain any new information about $\operatorname{Im} \lambda$ by considering primes outside of S. This will be useful in the example in section 3.2.

3.1 Local Analysis

In this section we briefly discuss the size of $J(K_\mathfrak{p})/2J(K_\mathfrak{p})$, where K is a number field, $\mathfrak{p}$ is a prime of K and J is the Jacobian of a hyperelliptic curve of genus one or two. This information is crucial in the examples of two descent that follow as it allows us to compute $\operatorname{Im} \lambda_\mathfrak{p}$. One we have these groups we can take preimages under the maps $j_\mathfrak{p}$ to compute the 2-Selmer group.

Recall from the theory of elliptic curves that $J(K_\mathfrak{p})$ contains a subgroup $\mathcal{H}$ such that $\mathcal{H} \cong (\mathfrak{p}, +)$ and the index $[J(K_\mathfrak{p}) : \mathcal{H}]$ is finite. There is an analogous result for Jacobians of hyperelliptic curves of genus two. In this case, there is a subgroup $\mathcal{H}$ of $J(K_\mathfrak{p})$ of finite index such that $\mathcal{H} \cong (\mathfrak{p} \times \mathfrak{p}, +)$ [3, p. 71]. The proof is analogous to that for elliptic curves and relies on the theory of formal groups. Using this fact we have

Proposition 5. *[3, p. 72] Let K be a number field, $\mathfrak{p}$ a prime of K, and J the Jacobian of a hyperelliptic curve defined over K of genus one or two. Then*

$$\#J(K_\mathfrak{p})/2J(K_\mathfrak{p}) = (\#J(K_\mathfrak{p})[2])(\#\mathfrak{p}/2\mathfrak{p})^g.$$

Proof. Let $\mathcal{H}$ be the subgroup of $J(K_\mathfrak{p})$ of finite index described prior to the statement of the proposition. Applying the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{H} & \longrightarrow & J(K_\mathfrak{p}) & \longrightarrow & J(K_\mathfrak{p})/\mathcal{H} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \\ 0 & \longrightarrow & \mathcal{H} & \longrightarrow & J(K_\mathfrak{p}) & \longrightarrow & J(K_\mathfrak{p})/\mathcal{H} & \longrightarrow & 0 \end{array}$$

yields the long exact sequence

$$\begin{aligned} 0 \to \mathcal{H}[2] \to J(K_\mathfrak{p})[2] \to (J(K_\mathfrak{p})/\mathcal{H})[2] \to \mathcal{H}/2\mathcal{H} \\ \to J(K_\mathfrak{p})/2J(K_\mathfrak{p}) \to (J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H}) \to 0. \end{aligned}$$

As $\mathcal{H}$ is isomorphic to either $(\mathfrak{p}, +)$ or $(\mathfrak{p} \times \mathfrak{p}, +)$, there are no elements of order two in $\mathcal{H}$, so $\mathcal{H}[2] = 0$. Note that if $\pi : J(K_\mathfrak{p}) \to J(K_\mathfrak{p})/\mathcal{H}$ is the natural projection map, then $(J(K_\mathfrak{p})/\mathcal{H})[2] = \pi(J(K_\mathfrak{p})[2])$. If $P \in J(K_\mathfrak{p})[2]$ and $\pi(P) = 0$ then $P = 0$ since P is a torsion element and $\mathcal{H}$ is torsion free. Therefore $\pi(J(K_\mathfrak{p})[2]) \cong J(K_\mathfrak{p})[2]$. Hence we may extract the exact sequence

$$0 \to \mathcal{H}/2\mathcal{H} \to J(K_\mathfrak{p})/2J(K_\mathfrak{p}) \to (J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H}) \to 0.$$

As all of these groups are finite we have

$$\#J(K_\mathfrak{p})/2J(K_\mathfrak{p}) = (\#\mathcal{H}/2\mathcal{H})(\#(J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H})). \tag{3}$$

We also have the exact sequence

$$0 \to (J(K_\mathfrak{p})/\mathcal{H})[2] \to J(K_\mathfrak{p})/\mathcal{H} \xrightarrow{[2]} J(K_\mathfrak{p})/\mathcal{H} \to (J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H}) \to 0$$

from which we conclude that

$$(\#(J(K_\mathfrak{p})/\mathcal{H})[2])(\#J(K_\mathfrak{p})/\mathcal{H}) = (\#J(K_\mathfrak{p})/\mathcal{H})(\#(J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H})).$$

Since $[J(K_\mathfrak{p}) : \mathcal{H}]$ is finite and $(J(K_\mathfrak{p})/\mathcal{H})[2] \cong J(K_\mathfrak{p})[2]$ we have

$$\#(J(K_\mathfrak{p})/\mathcal{H})/2(J(K_\mathfrak{p})/\mathcal{H}) = \#J(K_\mathfrak{p})[2].$$

Therefore (3) becomes

$$\#J(K_\mathfrak{p})/2J(K_\mathfrak{p}) = (\#\mathcal{H}/2\mathcal{H})(\#J(K_\mathfrak{p})[2]).$$

If $g = 1$ then $\mathcal{H} \cong \mathfrak{p}$ and $\#\mathcal{H}/2\mathcal{H} = \#\mathfrak{p}/2\mathfrak{p}$. If $g = 2$ then $\mathcal{H} \cong \mathfrak{p} \times \mathfrak{p}$ and $\#\mathcal{H}/2\mathcal{H} = \#(\mathfrak{p} \times \mathfrak{p})/2(\mathfrak{p} \times \mathfrak{p}) = \#(\mathfrak{p}/2\mathfrak{p})^2$. In either case we have proved the claim. □

We now address the case $K_{\mathfrak{p}} = \mathbb{R}$. Recall that for curves of genus one and two, $\#J(\mathbb{R})/2J(\mathbb{R})$ counts the number of connected components on the graph of $\mathcal{C}$. For example, an elliptic curve with three zeros has two connected components over $\mathbb{R}$ and in this case $\#E(\mathbb{R})/2E(\mathbb{R}) = 2$. On the other hand, an elliptic curve with one real root has one connected component over $\mathbb{R}$ and in this case $\#E(\mathbb{R})/2E(\mathbb{R}) = 1$. This generalizes to hyperelliptic curves of genus two. In fact, we may express this in terms of $J(\mathbb{R})[2]$ since the number of real zeros of $f(x)$ determines both the number of components and $J(\mathbb{R})[2]$. More precisely we have

$$\#J(\mathbb{R})/2J(\mathbb{R}) = \#J(\mathbb{R})[2]/(2^g), \tag{4}$$

where $g = 1$ or $g = 2$ is the genus of $\mathcal{C}$ [3, p. 74].

3.2 Example of Two Descent

It is convenient to use SAGE to perform various computations in this example. All of the programs referred to in the essay can be found in the appendix together with a brief description of their input and output and how they work. SAGE programs are in bold print.

We start with a straightforward example where all of the roots of the cubic equation are in $\mathbb{Q}$, followed by some comments about how the algorithm generalizes to number fields.

Example 1.

Let E be the elliptic curve defined by

$$E : y^2 = f(x) = (x-2)(x-8)(x-1).$$

The discriminant of E is $\Delta_E = 28224 = 2^6 \cdot 3^2 \cdot 7^2$. We will show that E has rank 1.

First we find the torsion subgroup $E(\mathbb{Q})_{tors}$. Note that $E[2] \subseteq E(\mathbb{Q})_{tors}$ as all of the roots of f are in $\mathbb{Q}$. To see that $E[2] = E(\mathbb{Q})_{tors}$, recall that $E(\mathbb{Q})_{tors} \hookrightarrow E(\mathbb{F}_p)$ for any $p \nmid \Delta_E$. Using the SAGE function **points_in** we see that $\#E(\mathbb{F}_5) = 8$ and $\#E(\mathbb{F}_{13}) = 20$. As $\#E(\mathbb{Q})_{tors}$ divides both 8 and 20, it follows that $\#E(\mathbb{Q})_{tors} \leq 4$. Thus, $E[2] = E(\mathbb{Q})_{tors}$, as claimed. We may take generators of $E(\mathbb{Q})_{tors}$ to be $T_1 = (2, 0)$ and $T_2 = (8, 0)$.

A search for rational points on E yields $P = (10, 12)$ which must be of infinite order since $P \notin E[2]$. Thus P, T_1, T_2 are represent independent elements in $E(\mathbb{Q})/2E(\mathbb{Q})$. Now, the map $\lambda : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ of Theorem 3 is given by

$$Q \mapsto \begin{cases} (x-2, x-8) & Q = (x, y), x \neq 2, 8 \\ ((2-8)(2-1), 2-8) = (-6, -6) & Q = (2, 0) \\ (8-2, (8-2)(8-1)) = (6, 42) & Q = (8, 0) \\ (1, 1) & Q = \mathcal{O}. \end{cases}$$

Thus λ acts on the independent points P, T_1, T_2 as follows:

$$\begin{aligned} P &\mapsto (8,2) = (2,2) \\ T_1 &\mapsto (-6,-6) \\ T_2 &\mapsto (6,42). \end{aligned}$$

Let H be the subgroup generated by $(2,2), (-6,-6), (6,42)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We shall show that $\mathrm{Sel}_2(E/\mathbb{Q}) = H$. By Proposition 4, it follows that $\mathrm{Sel}_2(E/\mathbb{Q}) \subseteq \mathbb{Q}(S) \times \mathbb{Q}(S)$, where $\mathbb{Q}(S)$ is the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by -1 and the primes dividing Δ_E. In this case,

$$\mathbb{Q}(S) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

For notational convenience we will write $\mathbb{Q}(S)^2$ for $\mathbb{Q}(S) \times \mathbb{Q}(S)$.

First consider the prime $\mathfrak{p} = \infty$, so $\mathbb{Q}_\mathfrak{p} = \mathbb{R}$. Now, $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$. By formula (4) in section 3.1 we know that $\#E(\mathbb{R})/2E(\mathbb{R}) = \#E(\mathbb{R})[2]/2 = 4/2 = 2$. As $\lambda_\infty(T_1) = (-1,-1)$ it follows that $\mathrm{Im}(\lambda_\infty) = \langle T_1 \rangle$. Therefore,

$$j_\infty{}^{-1}(\mathrm{Im}(\lambda_\infty)) = \langle \ker j_\infty, \lambda(T_1) \rangle.$$

As we know that $\mathrm{Sel}_2(E/\mathbb{Q}) \subseteq \mathbb{Q}(S)^2$ we may consider only those elements of $\ker j_\infty$ also in $\mathbb{Q}(S)^2$. Therefore,

$$j_\infty{}^{-1}(\mathrm{Im}(\lambda_\infty)) = \langle (2,1), (1,2), (1,3), (3,1), (1,7), (7,1), (-6,-6) \rangle.$$

Note that this restriction on $\mathrm{Sel}_2(E/\mathbb{Q})$ has eliminated half of the elements of $\mathbb{Q}(S)^2$, namely all those where the coordinates have different signs.

Next we consider the prime $\mathfrak{p} = 3$. Recall that for all $p \neq 2$, the group ${\mathbb{Q}_p}^\times/{\mathbb{Q}_p}^{\times 2}$ has four elements. We claim that ${\mathbb{Q}_3}^\times/{\mathbb{Q}_3}^{\times 2} = \{\pm 1, \pm 3\}$. This can be seen by noting that $x^2 + 1$ is irreducible modulo 3 and $x^2 \pm 3$ are both irreducible modulo 9. Therefore $-1, \pm 3 \notin {\mathbb{Q}_3}^{\times 2}$. As $-1 \cdot 3 = -3 \neq 1$ it follows that $-1, 3, -3$ are independent modulo squares in ${\mathbb{Q}_3}^\times$.

We will need to know the representative of ${\mathbb{Q}_3}^\times/{\mathbb{Q}_3}^{\times 2}$ corresponding to each element of $\mathbb{Q}(S)$. We use Hensel's Lemma to show that $-2, 7 \in {\mathbb{Q}_3}^{\times 2}$. Note that $x^2 + 2$ has the root $x \equiv 1 \pmod 3$ and $2 \cdot 1 \not\equiv 0 \pmod 3$, so by Hensel's Lemma $-2 \in {\mathbb{Q}_3}^{\times 2}$. As $x^2 - 7 \equiv x^2 + 2 \pmod 3$ it follows from the argument in the previous sentence that $7 \in {\mathbb{Q}_3}^{\times 2}$. Using these facts we have

$$\begin{aligned} 1 &\equiv -2, 7, -14 && (\mathrm{mod}\ {\mathbb{Q}_3}^{\times 2}) \\ -1 &\equiv 2, -7, 14 && (\mathrm{mod}\ {\mathbb{Q}_3}^{\times 2}) \\ 3 &\equiv -6, 21, -42 && (\mathrm{mod}\ {\mathbb{Q}_3}^{\times 2}) \\ -3 &\equiv 6, -21, 42 && (\mathrm{mod}\ {\mathbb{Q}_3}^{\times 2}). \end{aligned}$$

By Theorem 5 we know that $\#E(\mathbb{Q}_3)/2E(\mathbb{Q}_3) = \#E(\mathbb{Q}_3)[2] = 4$. As $\lambda_3(P) = (-1,-1)$ and $\lambda_3(T_1) = (3,3)$ it follows that $E(\mathbb{Q}_3)/2E(\mathbb{Q}_3) = \langle P, T_1 \rangle$. Therefore,

$$j_3{}^{-1}(\mathrm{Im}(\lambda_3)) = \langle (-2,1), (1,-2), (7,1), (1,7), (-1,-1), (3,3) \rangle,$$

where $(-2,1),(1,-2),(7,1),(1,7)$ generate the part of $\ker j_3$ that is contained in $\mathbb{Q}(S)^2$.

Finally, we consider the prime $\mathfrak{p}=7$. (As we will see, it is sufficient in this example to consider only the primes $\infty, 3, 7$ and not 2.) Again, we know ${\mathbb{Q}_7}^\times/{\mathbb{Q}_7}^{\times 2}$ has four elements. We claim that ${\mathbb{Q}_7}^\times/{\mathbb{Q}_7}^{\times 2}=\{\pm 1,\pm 7\}$. We proceed as above. The polynomials x^2+1 and $x^2\pm 7$ are irreducible modulo 7 and 49, respectively, so $-1,\pm 7\notin {\mathbb{Q}_7}^{\times 2}$. As $-1\cdot 7=-7$, it follows that $-1,7,-7$ are independent modulo squares in ${\mathbb{Q}_7}^\times$.

Note that x^2-2 has the root $x\equiv 3 \pmod 7$ and $2\cdot 3\not\equiv 0 \pmod 7$, so by Hensel's Lemma $2\in {\mathbb{Q}_7}^{\times 2}$. Similarly, x^2+3 has the root $x\equiv 2 \pmod 7$ and $2\cdot 2\not\equiv 0 \pmod 7$, so $-3\in {\mathbb{Q}_7}^{\times 2}$. Using these facts we find the following representatives in ${\mathbb{Q}_7}^\times/{\mathbb{Q}_7}^{\times 2}$ for elements of $\mathbb{Q}(S)$:

$$\begin{aligned} 1 &\equiv 2,-3,-6 && \pmod{{\mathbb{Q}_7}^{\times 2}}\\ -1 &\equiv -2,3,6 && \pmod{{\mathbb{Q}_7}^{\times 2}}\\ 7 &\equiv 14,-21,-42 && \pmod{{\mathbb{Q}_7}^{\times 2}}\\ -7 &\equiv -14,21,42 && \pmod{{\mathbb{Q}_7}^{\times 2}}. \end{aligned}$$

By Theorem 5 we know that $\#E(\mathbb{Q}_7)/2E(\mathbb{Q}_7)=\#E(\mathbb{Q}_7)[2]=4$. As $\lambda_7(P)=(1,1)=\lambda_7(T_1)$ and $\lambda_7(T_2)=(-1,-7)$ we need to find another generator for $\mathrm{Im}(\lambda_7)$. Note that $2^2-f(4)\equiv 0 \pmod 7$ and $2\cdot 2\not\equiv 0 \pmod 7$. By Hensel's Lemma there is a $\gamma\in\mathbb{Q}_7$ such that $(4,\gamma)\in E(\mathbb{Q}_7)$. Now $\lambda_7((4,\gamma))=(1,-1)$ is independent from $\lambda_7(T_2)$. Therefore $\mathrm{Im}(\lambda_7)=\langle(1,-1),(-1,-7)\rangle$. Taking the preimage under j_7 yields

$${j_7}^{-1}(\mathrm{Im}(\lambda_7))=\langle(1,2),(2,1),(1,-3),(-3,1),(1,-1),(-1,-7)\rangle,$$

where $(1,2),(2,1),(1,-3),(-3,1)$ generate the part of $\ker j_7$ contained in $\mathbb{Q}(S)^2$.

Now the group $\mathrm{Sel}_2(E/\mathbb{Q})$ is contained in

$$\begin{aligned} \bigcap_{\mathfrak{p}\in\{3,7,\infty\}} {j_\mathfrak{p}}^{-1}(\mathrm{Im}(\lambda_\mathfrak{p})) =&\langle(2,1),(1,2),(1,3),(3,1),(1,7),(7,1),(-6,-6)\rangle\\ &\cap\langle(-2,1),(1,-2),(7,1),(1,7),(-6,-6),(2,2)\rangle\\ &\cap\langle(1,2),(2,1),(1,-3),(-3,1),(1,-1),(6,42)\rangle. \end{aligned}$$

Using the SAGE functions **cp_span**, **multi_intersect**, and **same_set** we see that this intersection is in fact equal to H. It follows that $E(\mathbb{Q})/2E(\mathbb{Q})=\langle P,T_1,T_2\rangle$. As the T_i are torsion points, we have shown that the elliptic curve E has rank 1.

Notice that an important part of the two descent process was computing the finite group $\mathbb{Q}(S)\subseteq \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We will now discuss how this set $K(S)$ can be found for any number field K. Note that if K is the field of fractions of a principal ideal domain R, then $K^\times/K^{\times 2}\cong R^\times/R^{\times 2}\oplus\oplus_\mathfrak{p}\mathbb{Z}/2\mathbb{Z}$, where $\mathfrak{p}$ ranges over prime ideals in R and $R^\times$ denotes the units in R. This is because every element $\alpha\in K$ can be written as $\alpha=u\cdot {p_1}^{e_1}\cdots {p_r}^{e_r}$ where $u\in R^\times, e_i\in\mathbb{Z}$, and p_i are primes in R. Then viewing α in $K^\times/K^{\times 2}$ we see that $u\in R^\times/R^{\times 2}$ and $e_i=0$ or 1, giving the desired isomorphism.

Returning to the case where K is a number field, if $\mathcal{O}_K$ is a principal ideal domain then we may take R to be $\mathcal{O}_K$ and $K(S)$ is the subgroup corresponding to ${\mathcal{O}_K}^\times/{\mathcal{O}_K}^{\times 2} \oplus \oplus_{\mathfrak{p}\in S}\mathbb{Z}/2\mathbb{Z}$ under the above isomorphism. The case where $\mathcal{O}_K$ is not a principal ideal domain, that is when K has non-trivial class group, is more complicated. For this case we have

Proposition 6. *[6, p. 127] Let K be a number field. Then there is a principal ideal domain R such that $\mathcal{O}_K \subseteq R \subseteq K$ and $R^\times$ is finitely generated.*

Proof. Let h be the class number of K and $I_1, \ldots, I_h$ ideals in $\mathcal{O}_K$ that represent the elements of the class group of K. Let I_1 represent the class of principal ideals. For each j, fix a nonzero $u_j \in I_j$ and define $u = u_1 \cdots u_h$. Note that $u \in I_j$ for all j. Let $T = \{u^n : n \in \mathbb{Z}, n \geq 0\}$. As $0 \notin T, 1 \in T$ and T is multiplicatively closed, the localization $T^{-1}\mathcal{O}_K$ is a ring and $\mathcal{O}_K \subseteq T^{-1}\mathcal{O}_K \subseteq K$. Let $R = T^{-1}\mathcal{O}_K$.

To see that R is a principal ideal domain, let J be an ideal in R. Then $J = T^{-1}I$ for some ideal I of $\mathcal{O}_K$. Let I_j be the representative of the ideal class of I in the class group of K. We may write $I = \alpha^{-1}\beta I_j$ for some non-zero $\alpha, \beta \in \mathcal{O}_K$. Since $u \in I_j$, we have $\alpha^{-1}\beta u \in I$ and hence $(\alpha^{-1}\beta u)/u \in T^{-1}I$. To see that $(\alpha^{-1}\beta u)/u$ generates $T^{-1}I$, let $a/u^m \in T^{-1}I$ with $a \in I$ and $m \geq 0$. Then $a = \alpha^{-1}\beta b$ for some $b \in I_j$ since $I = \alpha^{-1}\beta I_j$. Thus, $a/u^m = (b/u^m)((\alpha^{-1}\beta u)/u) \in \langle(\alpha^{-1}1\beta u)/u\rangle$. Therefore J is principal generated by $(\alpha^{-1}\beta u)/u$. As J was an arbitrary ideal of R, we have shown that R is a principal ideal domain.

It remains to show that $R^\times$ is finitely generated. As $\mathcal{O}_K$ is a Dedekind domain we can uniquely factor $\langle u\rangle = {\mathfrak{p}_1}^{k_1} \cdots {\mathfrak{p}_n}^{k_n}$, where the $\mathfrak{p}_i$ are distinct prime ideals in $\mathcal{O}_K$ and $k_i \in \mathbb{Z}^+$. As h is the class number of K, we know that ${\mathfrak{p}_i}^h$ is principal. For each $1 \leq i \leq n$ fix $\gamma_i \in \mathcal{O}_K$ such that ${\mathfrak{p}_i}^h = \langle\gamma_i\rangle$. For each $1 \leq j \leq n$, fix some $0 \leq r_j \leq h-1$ and consider the ideal ${\mathfrak{p}_1}^{r_1} \cdots {\mathfrak{p}_n}^{r_n}$. If this ideal is principal, let $\delta_{r_1,\ldots,r_n} \in \mathcal{O}_K$ be a generator. Otherwise, set $\delta_{r_1,\ldots,r_n} = 1$. Finally, recall that by Dirichlet's unit theorem ${\mathcal{O}_K}^\times$ is finitely generated. Let $g_1, \ldots, g_m$ be generators for ${\mathcal{O}_K}^\times$. Let $G = \{g_1, \ldots, g_m, \gamma_i, \delta_{r_1,\ldots,r_n} : 1 \leq i \leq n, 0 \leq r_j \leq h-1\}$ and note that G is a finite set. We claim that $R^\times$ is generated by G.

To prove the claim, let $a/u^s \in R^\times$ with $a \in \mathcal{O}_K$ and $s \geq 0$. Write $(a/u^s)^{-1} = b/u^t$ for some $b \in \mathcal{O}_K$ and $t \geq 0$. Since $1 = (a/u^s)(b/u^t)$ and there are no zero divisors in R, we have $ab = u^{s+t}$. Let $r = s + t \geq 0$. Factoring the ideal $\langle ab\rangle$ yields

$$\langle ab\rangle = \langle u\rangle^r = {\mathfrak{p}_1}^{k_1 r} \cdots {\mathfrak{p}_n}^{k_n r}.$$

By unique factorization of ideals in $\mathcal{O}_K$ it follows that $\langle a\rangle = {\mathfrak{p}_1}^{\ell_1} \cdots {\mathfrak{p}_n}^{\ell_n}$, where $0 \leq \ell_i \leq k_i r$ for each $1 \leq i \leq n$. Using the division algorithm for each i, write $\ell_i = q_i h + r_i$ with $0 \leq r_i \leq h-1$. Then we have

$$\langle a\rangle = \prod_{i=1}^{n} {\mathfrak{p}_i}^{\ell_i} = \prod_{i=1}^{n} {\mathfrak{p}_i}^{q_i h + r_i} = \prod_{i=1}^{n} \langle\gamma_i\rangle^{q_i} {\mathfrak{p}_i}^{r_i} = \langle {\gamma_1}^{q_1} \cdots {\gamma_n}^{q_n}\rangle {\mathfrak{p}_1}^{r_1} \cdots {\mathfrak{p}_n}^{r_n}. \tag{5}$$

As the left hand side of (5) is principal, it follows that ${\mathfrak{p}_1}^{r_1} \cdots {\mathfrak{p}_n}^{r_n}$ is principal. Therefore we may write $a = \varepsilon\delta_{r_1,\ldots,r_n}{\gamma_1}^{q_1} \cdots {\gamma_n}^{q_n}$ for some $\varepsilon \in {\mathcal{O}_K}^\times$. Hence, $a \in \langle G\rangle$. By a similar argument u can

be written in terms of elements of G. As $(a/u^s) \in R^\times$ was arbitrary, it follows that $R^\times = \langle G \rangle$, as claimed. □

As the proof of Proposition 6 is constructive, we can use it to construct the set $K(S)$ that is needed for two descent. However, as this computation requires knowledge of the unit group and class group of the number field K, it quickly becomes unwieldy. We demonstrate how to find $K(S)$ with an example of a real quadratic field.

Example 2.

Let $K = \mathbb{Q}(\sqrt{10})$ and suppose the set S consists of primes lying above 2 and 7. Using SAGE, we find that K has class number two. Let $\mathfrak{p} = \langle 2, \sqrt{10} \rangle$ and note that $\mathfrak{p}^2 = \langle 2 \rangle$. This can be verified using the Kummer-Dedekind theorem, which also implies that $\mathfrak{p}$ is a prime ideal. Using SAGE we can check that $\mathfrak{p}$ is not principal. Hence, in the notation of the proof of Proposition 6 we have $I_1 = \mathcal{O}_K$ and $I_2 = \mathfrak{p}$. Furthermore, we may take $u_1 = 1$ and $u_2 = 2$ so that $u = u_1 u_2 = 2$. Then $\gamma_1 = 2$ and there are only two δ_{r_1} both of which are 1. Using SAGE we find that a fundamental unit in K is $3 + \sqrt{10}$ and so the set G of generators for $R^\times$ is $\{-1, 3 + \sqrt{10}, 2\}$.

Using the Kummer-Dedekind theorem, we see that 7 is inert in $\mathcal{O}_K$, so 7 generates a prime ideal in R. As 2 is a unit in R, we do not have to consider any other primes in R. Hence, in this case the group $K(S)$ is

$$\begin{aligned} K(S) = \{&1, -1, 3 + \sqrt{10}, -3 - \sqrt{10}, 2, -2, 6 + 2\sqrt{10}, -6 - 2\sqrt{10}, 7, -7, \\ &21 + 7\sqrt{10}, -21 - 7\sqrt{10}, 14, -14, 42 + 14\sqrt{10}, -42 - 14\sqrt{10}\}. \end{aligned}$$

4 Two descent on the Jacobians of higher genus hyperelliptic curves

In this section we focus on results proved by E.F. Schaefer about two descent on the Jacobians of hyperelliptic curves [8]. We follow his proof closely. First we establish some notation. Let J be the Jacobian of the curve

$$\mathcal{C} : y^2 = f(x) = \prod_{i=1}^{d} (x - \alpha_i),$$

where the α_i are distinct and f is defined over a field K of characteristic zero. The roots α_i need not be in K. Assume that the degree d of f is odd. Define the K-algebra

$$L = K[T]/\langle f(T) \rangle$$

and let

$$\overline{L} = \overline{K}[T]/\langle f(T) \rangle.$$

Note that $\overline{L} \cong \oplus_{i=1}^{d} \overline{K}$ via the map $T \mapsto (\alpha_1, \ldots, \alpha_d)$. We shall often make use of this identification by writing elements of $\overline{L}$ as ordered d-tuples of elements of $\overline{K}$. Let $\mu_2(\overline{L})$ be all elements of $L^\times$ of order dividing two. That is, $\mu_2(\overline{L})$ consists of d-tuples where all coordinates are 1 or -1. For a prime $\mathfrak{p}$ of K, define $L_\mathfrak{p} = K_\mathfrak{p}[T]/f(T)$.

There is an action of $\mathrm{Gal}(\overline{K}/K)$ on $\overline{L}$ given by $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \sigma(a_i) x^i$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $a_i \in \overline{K}$. This is well defined since f is defined over K. Under the isomorphism $\overline{L} \cong \oplus_{i=1}^{d} \overline{K}$ this action becomes

$$\sigma\left(x_1, \ldots, x_d\right) = \left(\sigma\left(x_{\sigma^{-1}(1)}\right), \ldots, \sigma\left(x_{\sigma^{-1}(d)}\right)\right),$$

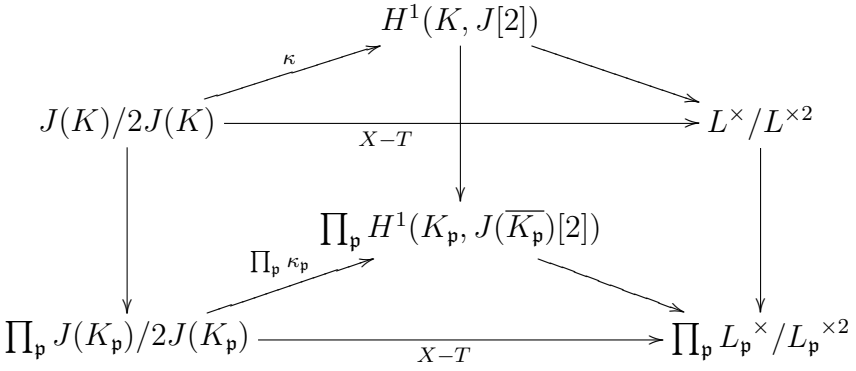
where $\sigma^{-1}(i) = j$ when $\sigma^{-1}(\alpha_i) = \alpha_j$. Thus, elements of $\mathrm{Gal}(\overline{K}/K)$ act on L in two ways; they act in the natural way on the coordinates $x_i \in \overline{K}$ and they also permute the coordinates.

It will be useful to identify L with the $\mathrm{Gal}(\overline{K}/K)$-invariants of $\overline{L}$. To see why this is possible, note that as f is defined over K there is a well defined injection $\iota : L \hookrightarrow \overline{L}$. Clearly any element in $\mathrm{Im}\,\iota$ is $\mathrm{Gal}(\overline{K}/K)$-invariant. Now let $g(x) \in \overline{L}$ be $\mathrm{Gal}(\overline{K}/K)$-invariant. Without loss of generality we may assume $\deg g < d$. Then for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have

$$g(x) - \sigma g(x) = k_\sigma(x) f(x)$$

for some $k_\sigma(x) \in \overline{K}[x]$. But $\deg(g(x) - \sigma g(x)) < \deg g < d$, so $k_\sigma(x) = 0$ and $g(x) = \sigma g(x)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Thus $g(x) \in \mathrm{Im}\,\iota$, as desired. Hence we may identify L with the $\mathrm{Gal}(\overline{K}/K)$-invariants of $\overline{L}$.

The idea of this section is to obtain a commutative diagram similar to (1) that retains all of the information needed for two descent, but that contains groups that are easier to calculate than $H^1(K, J[2])$. In particular, we will find maps that make the following diagram commute.



(6)

All of the downward arrows are induced by the inclusion map $K \hookrightarrow K_\mathfrak{p}$. Notice that the back left face of the diagram is precisely diagram (1) and the front face is analogous to diagram (2) for elliptic curves. As was demonstrated in the example in section 3.2, it is relatively easy to do computations with $L^\times/L^{\times 2}$ and ${L_\mathfrak{p}}^\times/{L_\mathfrak{p}}^{\times 2}$ compared with the first Galois cohomology groups.

We now define the maps that are used to fill in the above diagram. There is an isomorphism $\delta : L^\times/L^{\times 2} \to H^1(K, \mu_2(\overline{L}))$ given by $\delta(x)(\sigma) = \sigma(\sqrt{x})/\sqrt{x}$ [8]. This comes from the connecting

homomorphism that arises when taking the Galois cohomology of the short exact sequence arising from the squaring map on $\overline{L}^\times$:

$$1 \to \mu_2(\overline{L}) \to \overline{L}^\times \to \overline{L}^\times \to 1.$$

Let $k : L^\times/L^{\times 2} \to H^1(K, \mu_2(\overline{L}))$ be the inverse of δ. It is k that we will make frequent use of, although it is easier to dirictly compute δ.

Note that the construction of the Weil pairing for elliptic curves is defined on $\mathrm{Pic}^0(\mathcal{C})$ and does not require any special properties of elliptic curves. Hence, we have an analogous pairing on $J[2]$ for any hyperelliptic curve, which we will denote e_2, with all of the desired properties. That is, e_2 is bilinear, alternating, non-degenerate, adjoint and $\mathrm{Gal}(\overline{K}/K)$-equivariant. Using this pairing we define the homomorphism

$$\begin{aligned} \hat{w} : J[2] &\to \mu_2(\overline{L}) \\ Q &\mapsto (e_2(Q, (\alpha_1, 0)), \ldots, e_2(Q, (\alpha_d, 0))). \end{aligned}$$

This induces a map on cohomology groups

$$\begin{aligned} w : H^1(K, J(\overline{K})[2]) &\to H^1(K, \mu_2(\overline{L})) \\ (\xi : \sigma \mapsto Q) &\mapsto (\xi : \sigma \mapsto \hat{w}(Q)). \end{aligned}$$

Finally, recall that we have the map $\kappa : J(K)/2J(K) \to H^1(K, J[2])$ given in section 2 defined by $\kappa(P)(\sigma) = Q^\sigma - Q$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, where $Q \in J(\overline{K})$ such that $P = 2Q$. Having defined the necessary maps, we will now return to diagram (6).

Before we show that diagram (6) commutes, it is necessary to make sure that the map $X - T : J(K) \to L^\times/L^{\times 2}$ is well defined. As $X - T$ is only naturally defined on non-Weierstrass points, we will show that every element of $J(K)$ can be represented as a divisor without any Weierstrass points and then check that $X - T$ agrees on any two linearly equivalent divisors that have do not contain Weierstrass points. In order to prove that every element of $J(K)$ can be represented as a divisor without Weierstrass points, we need the following simplifying lemma.

Lemma 7. *Let D be a divisor of degree zero defined over K; that is, D is $\mathrm{Gal}(\overline{K}/K)$-invariant. Then D can be written as a sum and difference of divisors of the form*

$$\sum_{i=1}^{r} (Q^{\sigma_i}) - r(\infty),$$

where the set $\{Q^{\sigma_i} : 1 \le i \le r\}$ is a complete set of the $\mathrm{Gal}(\overline{K}/K)$-conjugates of Q.

Proof. Let D be a divisor of degree zero defined over K. Then we may write

$$D = \sum_{i=1}^{n} (P_i) - \sum_{i=0}^{n} (Q_i)$$

for some $n \geq 0$. We proceed by induction on n. The base case $n = 0$ is trivial and when $n = 1$ it follows that P_1 and Q_1 must be defined over K giving

$$D = ((P_1) - (\infty)) - ((Q_1) - (\infty)).$$

Assume the claim holds for all $k < n$. Note that it suffices to show that any sum of the form $\sum_{i=0}^{n}(P_i) - n(\infty)$ can be written in the desired form, for then applying this to $\sum_{i=0}^{n}(P_i) - n(\infty)$ and $\sum_{i=0}^{n}(Q_i) - n(\infty)$ yields the result.

Consider the $\mathrm{Gal}(\overline{K}/K)$-orbit of P_1 which is $\{{P_1}^{\sigma} : \sigma \in \mathrm{Gal}(\overline{K}/K)\}$. As D is defined over K, this orbit must consist of a subset of $\{P_i : 1 \leq i \leq n\}$. Without loss of generality, assume the orbit is $\{P_i : 1 \leq i \leq r\}$ for some $r \leq n$. Thus we have

$$\sum_{i=1}^{n}(P_i) - n(\infty) = \sum_{i=1}^{r}({P_1}^{\sigma_i}) - r(\infty) + \sum_{i=r+1}^{n}(P_i) - (n-r)(\infty),$$

where the $\sigma_i \in \mathrm{Gal}(\overline{K}/K)$ such that ${P_1}^{\sigma_i} = P_i$ for $1 \leq i \leq r$. If $r = d$, we have written the sum in the desired form. If $r < d$, then the sum $\sum_{i=r+1}^{d}(P_i) - (n-r)(\infty)$ can be written in the desired form by induction. Thus, in either case the claim is proved. □

With this way of writing elements of $J(K)$ we can now prove

Proposition 8. *[8] Every element of $J(K)$ can be represented by a divisor of degree zero that is disjoint from the Weierstrass points.*

Proof. By Lemma 7 it suffices to show that any divisor of the form $D = \sum_{i=1}^{r}(Q^{\sigma_i}) - r(\infty)$ is linearly equivalent to a divisor of without any Weierstrass points, where the $\sigma_i \in \mathrm{Gal}(\overline{K}/K)$ such that $Q^{\sigma_1}, \ldots, Q^{\sigma_r}$ is a complete list of the $\mathrm{Gal}(\overline{K}/K)$-conjugates of Q.

First consider the case where Q is not a Weierstrass point, so $Q = (x_1, y_1)$ with $y_1 \neq 0$. Let $x_1, \ldots, x_d$ be the zeros of ${y_1}^2 = f(x)$, and let $Q_j = (x_j, y_1)$. Also, let $R_1 = (x_1, -y_1)$. As d is odd, we may write $d = 2g + 1$ for some non-negative integer g. (In fact, g is the genus of $\mathcal{C}$, but we will not need this fact.) Then we have

$$\begin{aligned}
\mathrm{div}\left(\prod_{i=1}^{r}\frac{(X-\sigma_i(x_1))^g}{Y-\sigma_i(y_1)}\right) &= \sum_{i=1}^{r} g\,\mathrm{div}(X-\sigma_i(x_1)) - \mathrm{div}(Y-\sigma_i(y_1)) \\
&= \sum_{i=1}^{r} g((\sigma_i(Q)) + (\sigma_i(R_1)) - 2(\infty)) - \left(\sum_{j=1}^{d}(\sigma_i(Q)) - d(\infty)\right) \\
&= r(\infty) + g\sum_{i=1}^{r}(\sigma_i(R_1)) + g\sum_{i=1}^{r}(\sigma_i(Q_1)) - \sum_{j=1}^{d}\sum_{i=1}^{r}(\sigma_i(Q_j)).
\end{aligned}$$

Adding D to the above yields that D is linearly equivalent to

$$D + \mathrm{div}\left(\prod_{i=1}^{r}\frac{(X-\sigma_i(x_1))^g}{Y-\sigma_i(y_1)}\right) = g\sum_{i=1}^{r}(\sigma_i(R_1)) + g\sum_{i=1}^{r}(\sigma_i(Q_1)) - \sum_{j=2}^{d}\sum_{i=1}^{r}(\sigma_i(Q_j)). \quad (7)$$

Now suppose that Q is a Weierstrass point and without loss of generality say $Q = (\alpha_1, 0)$. Then the conjugates of Q are other Weierstrass points. If all of the other Weierstrass points are conjugates of Q then letting $\sigma_i \in \mathrm{Gal}(\overline{K}/K)$ such that $Q^{\sigma_i} = (\alpha_i, 0) = Q_i$ we have

$$D = \sum_{i=1}^{d}(Q_i) - d(\infty) = \sum_{i=1}^{d}(Q^{\sigma_i}) - d(\infty) = \mathrm{div}(Y).$$

Thus, D is linearly equivalent to the divisor of any K-rational function. In particular, we may take the zero divisor to represent the linear equivalence class of D, which is certainly disjoint from the Weierstrass points. Thus we will assume that $Q_1, \ldots, Q_r$ are the conjugates of Q, with $Q_i = (\alpha_i, 0)$ and $r < d$.

Furthermore, we may assume that $r < d/2$ as follows. Let $g(X, Y) = \frac{\prod_{i=r+1}^{d}(X-\alpha_i)}{Y}$, so

$$\begin{aligned}\mathrm{div}(g) = \sum_{i=r+1}^{d}\mathrm{div}(X-\alpha_i) - \mathrm{div}(Y) &= \sum_{i=r+1}^{d}(2((\alpha_i,0)) - 2(\infty)) - \sum_{i=1}^{d}((\alpha_i,0)) + d(\infty) \\ &= -\sum_{i=1}^{r}((\alpha_i,0)) + \sum_{i=r+1}^{d}((\alpha_i,0)) + (d-2r)(\infty).\end{aligned}$$

Adding $\mathrm{div}(g)$ to D, we see that D is linearly equivalent to

$$\begin{aligned}\mathrm{div}(g) + D &= -\sum_{i=1}^{r}((\alpha_i,0)) + \sum_{i=r+1}^{d}((\alpha_i,0)) + (d-2r)(\infty) + \sum_{i=1}^{r}((\alpha_i,0)) - r(\infty) \\ &= \sum_{i=r+1}^{d}((\alpha_i,0)) - (d-r)(\infty).\end{aligned}$$

Thus, by possibly replacing D with $D + \mathrm{div}(g)$ we may assume that $r < d/2$.

Let $f(X, Y) = Y - \prod_{i=1}^{r}(X - \alpha_i)$. Notice that if $f(x, y) = 0$ then $y = \prod_{i=1}^{r}(x - \alpha_i)$. Thus, $\prod_{i=1}^{d}(x - \alpha_i) = y^2 = \prod_{i=1}^{r}(x - \alpha_i)^2$ and so

$$0 = \prod_{i=1}^{d}(x-\alpha_i) - \prod_{i=1}^{r}(x-\alpha_i)^2 = \prod_{i=1}^{r}(x-\alpha_i)\left[\prod_{i=r+1}^{d}(x-\alpha_i) - \prod_{i=1}^{r}(x-\alpha_i)\right].$$

For $r + 1 \leq i \leq d$, let $P_i = (x_i, y_i)$ be the points on $\mathcal{C}$ such that x_j is a zero of $\prod_{i=r+1}^{d}(x - \alpha_i) - \prod_{i=1}^{r}(x - \alpha_i)$ and $y_j = \prod_{i=1}^{r}(x_j - \alpha_i) \neq 0$. Then

$$\mathrm{div}(f) = \sum_{i=1}^{r}(Q_i) + \sum_{i=r+1}^{d}(P_i) - d(\infty).$$

Now let $h = \prod_{i=r+1}^{d}(X - x_i)$. Then

$$\operatorname{div}(h) = \sum_{i=r+1}^{d}((P_i) + (R_i)) - 2(d-r)(\infty),$$

where $R_i = (x_1, -y_i)$. We have that D is linearly equivalent to

$$\begin{aligned} &D + \operatorname{div}(h) - \operatorname{div}(f) \\ &= \sum_{i=1}^{r}(Q_i) - r(\infty) + \sum_{i=r+1}^{d}((P_i) + (R_i)) - 2(d-r)(\infty) - \sum_{i=1}^{r}(Q_i) - \sum_{i=r+1}^{d}(P_i) + d(\infty) \\ &= \sum_{i=r+1}^{d}(R_i) - (d-r)(\infty). \end{aligned}$$

As $y_i \neq 0$ for $r+1 \leq i \leq d$, it follows that the R_i are not Weierstrass points. Therefore, D is linearly equivalent to $D + \operatorname{div}(g) - \operatorname{div}(f)$ which does not contain any Weierstrass points, as desired. □

Having established that every linear equivalence class of $J(K)$ contains a divisor of degree zero that does not contain any Weierstrass points, we need only show that the function $X - T : J(K) \to L^{\times}/L^{\times 2}$ respects linear equivalence on such divisors.

Proposition 9. *[8] If $D_1 = D_2$ in $J(K)$ and D_1, D_2 do not contain any Weierstrass points, then $(X-T)(D_1) \equiv (X-T)(D_2) \pmod{L^{\times 2}}$.*

Proof. Let D_1, D_2 be linearly equivalent divisors of degree zero defined over K, neither containing any Weierstrass points. Then there is a function h defined over K such that $\operatorname{div}(h) = D_1 - D_2$. Recall that $\operatorname{div}(X-T) = \sum_{i=1}^{d} 2((\alpha_i, 0)) - 2d(\infty)$ since $T \mapsto (\alpha_1, \ldots, \alpha_d)$ under the isomorphism $\overline{L} \cong \oplus_{i=1}^{d}\overline{K}$. As $\operatorname{div}(h)$ does not contain any Weierstrass points by assumption and $\operatorname{div}(X-T)$ is made up entirely of Weierstrass points, we may apply Weil reciprocity to calculate

$$\begin{aligned} (X-T)(D_1 - D_2) = (X-T)(\operatorname{div}(h)) &= h(\operatorname{div}(X-T)) \\ &= h\left(\sum_{i=1}^{d} 2((\alpha_i, 0)) - 2d(\infty)\right) = \left(h\left(\sum_{i=1}^{d}((\alpha_i, 0)) - d(\infty)\right)\right)^2. \end{aligned}$$

As h is defined over K and $\sum_{i=1}^{d}((\alpha_i, 0)) - d(\infty)$ is $\operatorname{Gal}(\overline{K}/K)$-invariant, it follows that

$$h\left(\sum_{i=1}^{d}((\alpha_i, 0)) - d(\infty)\right) \in L^{\times}.$$

Thus, $(X-T)(D_1) \equiv (X-T)(D_2) \pmod{L^{\times 2}}$, as desired. □

We are now ready to prove the commutativity of diagram (6). In particular, we have

Theorem 10. *[8] The functions $X-T : J(K)/2J(K) \to L^\times/L^{\times 2}$ and $k\circ w\circ\kappa : J(K)/2J(K) \to L^\times/L^{\times 2}$ are equal.*

Proof. Let $P \in J(K)$. By Proposition 8 we may take a degree zero divisor representing P that does not contain any Weierstrass points. Let $Q \in J(\overline{K})$ such that $2Q = P$. As Proposition 8 applies to any field of characteristic zero, we may similarly take Q not containing any Weierstrass points.

By definition of κ,

$$\kappa(P) = (\xi : \sigma \mapsto Q^\sigma - Q).$$

By definition of w we have

$$w\circ\kappa(P) = (\xi : \sigma \mapsto \hat{w}(Q^\sigma - Q)) = (\xi : \sigma \mapsto (e_2(Q^\sigma - Q, (\alpha_1, 0) - \infty), \ldots, e_2(Q^\sigma - Q, (\alpha_d, 0) - \infty))),$$

so we need to compute $e_2(Q^\sigma - Q, (\alpha_i, 0) - \infty)$. This part of the proof is similar to the proof of Theorem 3. We need functions with divisors $2(Q^\sigma) - 2(Q)$ and $2((\alpha_i, 0)) - 2(\infty)$. As $2Q = P$ there is a function g such that $\mathrm{div}(g) = 2(Q) - (P)$. Applying any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we find that $\mathrm{div}(g^\sigma) = 2(Q^\sigma) - (P^\sigma) = 2(Q^\sigma) - (P)$ since P is defined over K. Therefore,

$$\mathrm{div}(g^\sigma/g) = 2(Q^\sigma) - (P) - 2(Q) + (P) = 2(Q^\sigma) - 2(Q).$$

Also, $\mathrm{div}(X - \alpha_i) = 2((\alpha_i, 0)) - 2(\infty)$. Thus we have

$$\begin{aligned} e_2(Q^\sigma - Q, (\alpha_i, 0) - \infty) &= \frac{(X-\alpha_i)(Q^\sigma - Q)}{\frac{g^\sigma}{g}((\alpha_i, 0) - \infty)} \\ &= \left(\frac{(X-\alpha_i)(Q^\sigma)}{(X-\alpha_i)(Q)}\right)\left(\frac{g((\alpha_i, 0) - \infty)}{g^\sigma((\alpha_i, 0) - \infty)}\right) \\ &= \left(\frac{(X-\alpha_i)(Q)}{g((\alpha_i, 0) - \infty)}\right)^\sigma \left(\frac{(X-\alpha_i)(Q)}{g((\alpha_i, 0) - \infty)}\right)^{-1}. \end{aligned}$$

Letting $\beta_i = (X-\alpha_i)(Q)/g((\alpha_i, 0)-\infty)$ and $\beta = (\beta_1, \ldots, \beta_d)$ we use Weil reciprocity to calculate that

$$\begin{aligned} \beta^2 = ({\beta_1}^2, \ldots, {\beta_d}^2) &= \left(\left(\frac{(X-\alpha_1)(Q)}{g((\alpha_1, 0) - \infty)}\right)^2, \ldots, \left(\frac{(X-\alpha_d)(Q)}{g((\alpha_d, 0) - \infty)}\right)^2\right) \\ &= \left(\frac{(X-\alpha_1)(2Q)}{g(2(\alpha_1, 0) - 2\infty)}, \ldots, \frac{(X-\alpha_d)(2Q)}{g(2(\alpha_d, 0) - 2\infty)}\right) \\ &= \frac{(X-T)(2Q)}{(X-T)(\mathrm{div}(g))} \\ &= \frac{(X-T)(2Q)}{(X-T)(2Q-P)} \\ &= \delta((X-T)(P)). \end{aligned}$$

Applying $\delta^{-1} = k$ to both sides and evaluating at any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we find that

$$(X - T)(P)(\sigma) = k^{-1}(\beta^2)(\sigma) = \sigma(\beta)/\beta = w \circ \kappa(P).$$

Therefore $k \circ w \circ \kappa = X - T$, as claimed. □

In order to use this theory in explicit examples, we need to know how to compute the map $X - T$. We will make use of this in the example of two descent on the Jacobian of a hyperelliptic curve of genus two in section 5.2.

Proposition 11. *Let $D = \sum_{i=1}^{r}(\sigma_i(Q)) - r(\infty)$, where $\sigma_1(Q), \ldots, \sigma_r(Q)$ are all of the $\mathrm{Gal}(\overline{K}/K)$-conjugates of Q. If Q is not a Weierstrass point then*

$$(X - T)(D) = \prod_{i=1}^{r}(X(\sigma_i(Q)) - T).$$

If Q is a Weierstrass point, say $Q = (\alpha_1, 0)$ and $\sigma_i(Q) = (\alpha_i, 0)$. Then

$$(X - T)(D) = \prod_{i=1}^{r}(\alpha_i - T) + \prod_{i=r+1}^{d}(\alpha_i - T).$$

Proof. Throughout this proof we will use the same notation as in Proposition 8. By Proposition 9 it follows that we may compute $(X - T)(D)$ by applying $X - T$ to the right hand side of (7). Recalling that $X(Q) = X(R_1)$ and $Y(Q)^2 = (X(Q_1) - \alpha_1) \cdots (X(Q_d) - \alpha_d)$ and that the image of $X - T$ is only defined up to squares we have

$$\begin{aligned}
(X - T)(D) &= (X - T)\left(g\sum_{i=1}^{r}(\sigma_i(Q)) - \sum_{j=2}^{d}\sum_{i=1}^{r}(\sigma_i(Q_j)) + g\sum_{i=1}^{r}(\sigma_i(R_1))\right) \\
&= \prod_{i=1}^{r}\frac{(X(\sigma_i(Q)) - T)^g(X(\sigma_i(R_1)) - T)^g}{\prod_{j=2}^{d}(X(\sigma_i(Q_j)) - T)} \\
&= \prod_{i=1}^{r}\frac{(X(\sigma_i(Q)) - T)^{2g+1}}{\prod_{j=1}^{d}(X(\sigma_i(Q_j)) - \alpha_j - (T - \alpha_j))} \\
&= \prod_{i=1}^{r}\frac{(X(\sigma_i(Q)) - T)^{2g+1}}{\prod_{j=1}^{d}(X(\sigma_i(Q_j)) - \alpha_j) - \prod_{j=1}^{d}(T - \alpha_j)} \\
&= \prod_{i=1}^{r}\frac{(X(\sigma_i(Q)) - T)^{2g+1}}{Y(\sigma_i(Q))^2 - f(T)} \\
&= \prod_{i=1}^{r}(X(\sigma_i(Q)) - T)\left(\frac{(X(\sigma_i(Q_j)) - T)^g}{Y(\sigma_i(Q))}\right)^2 \\
&= \prod_{i=1}^{r}X(\sigma_i(Q)) - T,
\end{aligned}$$

as claimed.

For the case when Q is a Weierstrass point, recall that in the proof of Proposition 8 we showed that D is linearly equivalent to

$$\sum_{i=r+1}^{d} (R_i) - (d-r)(\infty),$$

were $R_i = (x_i, y_i)$ such that the x_i are the roots of the polynomial

$$\prod_{i=r+1}^{d} (X - \alpha_i) - \prod_{i=1}^{r} (X - \alpha_i)$$

and $y_j = \prod_{i=1}^{r} x_j - \alpha_i$. Since $X - T$ respects linear equivalence we have may compute $(X-T)(D)$ by computing $(X-T)\left(\sum_{i=r+1}^{d}(R_i) - (d-r)(\infty)\right)$. Note that

$$\prod_{i=r+1}^{d} (T - x_i) = \prod_{i=r+1}^{d} (T - \alpha_i) - \prod_{i=1}^{r} (T - \alpha_i)$$

since both are monic degree $(d-r)$ polynomials with roots $x_{r+1}, \ldots, x_d$. Using this together with the fact that d is odd and the result when Q is not a Weierstrass point we have

$$\begin{aligned}
(X-T)(D) &= (X-T)\left(\sum_{i=r+1}^{d} (R_i) - (d-r)(\infty)\right) = \prod_{i=r+1}^{d} (X(R_i) - T) \\
&= (-1)^{d-r} \prod_{i=r+1}^{d} (T - X(R_i)) = (-1)^{d-r}\left(\prod_{i=r+1}^{d} (T - \alpha_i) - \prod_{i=1}^{r} (T - \alpha_i)\right) \\
&= (-1)^{d-r}\left((-1)^{d-r} \prod_{i=r+1}^{d} (\alpha_i - T) + (-1)^{r+1} \prod_{i=1}^{r} (\alpha_i - T)\right) \\
&= \prod_{i=r+1}^{d} (\alpha_i - T) + \prod_{i=1}^{r} (\alpha_i - T),
\end{aligned}$$

as claimed. □

Having shown that diagram (6) commutes, we would like to analyze the image of $X - T$ instead of the image of κ. As $k \circ w$ is an injection, we will not lose any information by making this translation. In order to analyze the image of $X - T$, it will be useful to have a description of $\mathrm{Im}(k \circ w)$ in $L^\times / L^{\times 2}$. In particular, we have

Proposition 12. *Let $N : L \to K$ be the norm map given by $N(x_1, \ldots, x_d) = x_1 \cdots x_d$. Although it is an abuse of notation, we will also use N to denote any maps induced by N. This should not cause confusion. Then*

$$\mathrm{Im}(k \circ w) = \ker(N : L^\times / L^{\times 2} \to K^\times / K^{\times 2}).$$

Proof. We begin by showing that

$$0 \to J[2] \xrightarrow{w} \mu_2(\overline{L}) \xrightarrow{N} \mu_2(\overline{K}) \to 1$$

is a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules. To see that w and N commute with the $\mathrm{Gal}(\overline{K}/K)$-action on each of the modules, let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then for any $Q \in J[2]$, using the definition of the $\mathrm{Gal}(\overline{K}/K)$-action on $\mu_2(\overline{L})$ and the fact that e_2 maps into ± 1 which are fixed by all elements of $\mathrm{Gal}(\overline{K}/K)$, we have

$$\begin{aligned}
\sigma(w(Q)) &= \sigma\left(e_2(Q,(\alpha_1,0)-\infty),\ldots,e_2(Q,(\alpha_d,0)-\infty)\right)\\
&= \left(e_2(Q,(\sigma^{-1}(\alpha_1),0)-\infty),\ldots,e_2(Q,(\sigma^{-1}(\alpha_d),0)-\infty)\right)\\
&= \left(e_2(Q^\sigma,(\alpha_1,0)-\infty)^{\sigma^{-1}},\ldots,e_2(Q^\sigma,(\alpha_2,0)-\infty)^{\sigma^{-1}}\right)\\
&= \left(e_2(Q^\sigma,(\alpha_1,0)-\infty),\ldots,e_2(Q^\sigma,(\alpha_2,0)-\infty)\right)\\
&= w(Q^\sigma).
\end{aligned}$$

Also, for any $(x_1,\ldots,x_d) \in \mu_2(\overline{L})$ with $x_i \in \{\pm 1\}$ we have

$$\begin{aligned}
\sigma(N(x_1,\ldots,x_d)) &= \sigma(x_1\cdots x_d) = x_1\cdots x_d = x_{\sigma^{-1}(1)}\cdots x_{\sigma^{-1}(d)}\\
&= N(x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(d)}) = N(\sigma(x_1,\ldots,x_d)),
\end{aligned}$$

where $\sigma^{-1}(j) = i$ when $\sigma^{-1}(\alpha_j) = \alpha_i$. Thus, w and N are maps of $\mathrm{Gal}(\overline{K}/K)$-modules.

We now show that the sequence is exact. For exactness at $J[2]$, suppose $Q \in J[2]$ such that $w(Q) = (1,\ldots,1)$. Then

$$(1,\ldots,1) = w(Q) = (e_2(Q,(\alpha_1,0)-\infty),\ldots,e_2(Q,(\alpha_d,0)-\infty)),$$

so $e_2(Q,(\alpha_i,0)-\infty) = 1$ for all $1 \le i \le d$. As $\{(\alpha_i,0)-\infty : 1 \le i \le d-1\}$ is a basis for $J[2]$ and e_2 is bilinear, it follows that $e_2(Q,P) = 1$ for all $P \in J[2]$. By the non-degeneracy of e_2, it follows that $Q = \mathcal{O}$ and so w is injective. Thus, the sequence is exact at $J[2]$.

Note that $N(-1,\ldots,-1) = (-1)^d = -1$ since d is odd. Therefore $N : \mu_2(\overline{L}) \to \mu_2(\overline{K}) = \{\pm 1\}$ is surjective and the sequence is exact at $\mu_2(\overline{K})$.

Next we show that $\mathrm{Im}\, w \subseteq \ker N$. Let $Q \in J[2]$. Then using the fact that $(\alpha_d,0)-\infty = \sum_{i=1}^{d-1}(\alpha_i,0)-(d-1)\infty$ in $J(\overline{K})$ and the bilinearity of e_2 we have

$$\begin{aligned}
N(w(Q)) &= N\left(e_2(Q,(\alpha_1,0)-\infty),\ldots,e_2(Q,(\alpha_d,0)-\infty)\right)\\
&= N\left(e_2(Q,(\alpha_1,0)-\infty),\ldots,e_2(Q,(\alpha_{d-1},0)-\infty),e_2\left(Q,\sum_{i=1}^{d-1}(\alpha_i,0)-(d-1)\infty\right)\right)\\
&= N\left(e_2(Q,(\alpha_1,0)-\infty),\ldots,e_2(Q,(\alpha_{d-1},0)-\infty),\prod_{i=1}^{d-1}e_2(Q,(\alpha_i,0)-(d-1)\infty)\right)\\
&= \prod_{i=1}^{d-1}e_2(Q,(\alpha_i,0)-\infty)^2 = \prod_{i=1}^{d-1}e_2(Q,2(\alpha_i,0)-2\infty) = \prod_{i=1}^{d-1}e_2(Q,\mathcal{O}) = 1.
\end{aligned}$$

Hence, $\operatorname{Im} w \subseteq \ker N$.

To prove exactness at $\mu_2(\overline{L})$, we use the fact that all of the groups are $\mathbb{F}_2$-vector spaces. Using the first isomorphism theorem and the fact that $N : \mu_2(\overline{L}) \to \mu_2(\overline{K})$ is surjective we have $\mu_2(\overline{K}) \cong \mu_2(\overline{L})/\ker N$. Taking $\mathbb{F}_2$-dimensions, it follows that

$$\dim_{\mathbb{F}_2} \ker N = \dim_{\mathbb{F}_2} \mu_2(\overline{L}) - \dim_{\mathbb{F}_2} \mu_2(\overline{K}) = d - 1.$$

As $\operatorname{Im} w \subseteq \ker N$ and $\dim_{\mathbb{F}_2} \operatorname{Im} w = \dim_{\mathbb{F}_2} J[2] = d - 1 = \dim_{\mathbb{F}_2} \ker N$, it follows that $\operatorname{Im} w = \ker N$, as desired. Thus, we have the required short exact sequence of $\operatorname{Gal}(\overline{K}/K)$-modules.

Now we obtain the standard long exact sequence in cohomology. Namely,

$$\begin{aligned} 0 \to H^0(K, J[2]) &\xrightarrow{w} H^0(K, \mu_2(\overline{L})) \xrightarrow{N} H^0(K, \mu_2(\overline{K})) \\ &\xrightarrow{\delta} H^1(K, J[2]) \xrightarrow{w} H^1(K, \mu_2(\overline{L})) \xrightarrow{N} H^1(K, \mu_2(\overline{K})). \end{aligned}$$

Note that $(-1, \ldots, -1) \in H^0(K, \mu_2(\overline{L}))$ and $N(-1, \ldots, -1) = (-1)^d = -1$ since d is odd. Therefore N is surjective. By exactness at $H^0(K, \mu_2(\overline{K}))$ we have $\ker \delta = \operatorname{Im} N = H^0(K, \mu_2(\overline{K}))$ and so δ is the zero map. Hence we map extract the exact sequence

$$0 \to H^1(K, J[2]) \xrightarrow{w} H^1(K, \mu_2(\overline{L})) \xrightarrow{N} H^1(K, \mu_2(\overline{K})). \tag{8}$$

Now, we have the isomorphisms from Kummer theory given by

$$\begin{aligned} \delta_K : K^\times/K^{\times 2} &\to H^1(K, \mu_2(\overline{K})) \\ x &\mapsto (\xi : \sigma \mapsto \sigma(\sqrt{x})/\sqrt{x}) \end{aligned}$$

and

$$\begin{aligned} &\delta_L : L^\times/L^{\times 2} \to H^1(K, \mu_2(\overline{L})) \\ &(x_1, \ldots, x_d) \mapsto \left(\xi : \sigma \mapsto \left(\frac{\sigma(\sqrt{x_1})}{\sqrt{x_1}}, \ldots, \frac{\sigma(\sqrt{x_d})}{\sqrt{x_d}}\right)\right). \end{aligned}$$

It is easy to check that the diagram

$$\begin{array}{ccc} L^\times/L^{\times 2} & \xrightarrow{\delta_L} & H^1(K, \mu_2(\overline{L})) \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\ K^\times/K^{\times 2} & \xrightarrow{\delta_K} & H^1(K, \mu_2(\overline{K})) \end{array} \tag{9}$$

commutes. Namely, let $(x_1, \ldots, x_d) \in L^\times/L^{\times 2}$. Then for any $\sigma \in \operatorname{Gal}(\overline{K}/K)$ we have

$$N \circ \delta_L(x_1, \ldots, x_d)(\sigma) = \frac{\sigma(\sqrt{x_1})}{\sqrt{x_1}} \cdots \frac{\sigma(\sqrt{x_d})}{\sqrt{x_d}} = \frac{\sigma(\sqrt{x_1 \cdots x_d})}{\sqrt{x_1 \cdots x_d}} = \delta_K \circ N(x_1, \ldots, x_d)(\sigma).$$

Let $k_K = {\delta_K}^{-1}$ and note that ${\delta_L}^{-1} = k$. Putting the above commutative square (9) together with the exact sequence (8) we obtain the following commutative diagram with exact top row.

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(K, J(\overline{K})[2]) & \xrightarrow{w} & H^1(K, \mu_2(\overline{L})) & \xrightarrow{N} & H^1(K, \mu_2(\overline{K})) \\ & & & & \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle k_K} \\ & & & & L^\times/L^{\times 2} & \xrightarrow{N} & K^\times/K^{\times 2} \end{array}$$

This allows us to calculate

$$\operatorname{Im} k \circ w = k(\ker N : H^1(K, \mu_2(\overline{L})) \to H^1(K, \mu_2(\overline{K}))) = \ker(N : L^\times/L^{\times 2} \to K^\times/K^{\times 2}),$$

which proves the proposition. □

We will now describe the algorithm of two descent which we follow closely in all of the examples in this essay. Let $\mathcal{C}, J, K, L$ be as above. We can write $L \cong \oplus_{i=1}^{c} L_i$, where c is the number of irreducible factors of f over K and each L_i is the corresponding field obtained by taking the quotient of $K[T]$ by the i-th irreducible factor of f. We will often make use of this identification and talk about coordinates in the image of the $X - T$ map. Let λ denote the map $X - T : J(K)/2J(K) \to L^\times/L^{\times 2}$. For a prime $\mathfrak{p}$ of L_i, let $j_{i\mathfrak{p}} : {L_i}^\times/{L_i}^{\times 2} \to {L_{i\mathfrak{p}}}^\times/{L_{i\mathfrak{p}}}^{\times 2}$ be the map induced by the inclusion $L_i \hookrightarrow L_{i\mathfrak{p}}$. Let $j_\mathfrak{p} : L^\times/L^{\times 2} \to {L_\mathfrak{p}}^\times/{L_\mathfrak{p}}^{\times 2}$ be the map induced by $L \hookrightarrow L_\mathfrak{p}$, which is the Cartesian product of the $j_{i\mathfrak{p}}$ maps.

The first step is to understand $J(K)_{tors}$. The 2-torsion is easy to find as it comes from the Weierstrass points on $\mathcal{C}$. Other torsion elements may be found through a search. To confirm that all torsion points have been found we find $J(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$ for a prime $\mathfrak{p}$ of K, where $\mathcal{C}$ has good reduction at $\mathfrak{p}$. As $\#J(K)_{tors} \mid \#J(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$ for all such $\mathfrak{p}$, a few such calculations usually confirm the size of $J(K)_{tors}$.

Next we look for other K-rational points on $\mathcal{C}$. This can be done by a short computer search. Let H be the subgroup generated by the known points of $J(K)$, both those found by the search and $J(K)_{tors}$. Let G be a generating set for H. As $J(K)$ is known to be finitely generated and $H \leq J(K)$, it follows that G may be taken to be finite. For ease of calculation, G should be taken to be as small as possible.

Recall that we want to understand $\operatorname{Im} \lambda$, so we calculate $\lambda(H) \leq \operatorname{Im} \lambda$. To do this, let S be the set of primes of K where $\mathcal{C}$ has bad reduction together with the primes over 2 and the infinite primes. For each $1 \leq i \leq c$ we wish to construct a finite subgroup $L_i(S) \subseteq {L_i}^\times/{L_i}^{\times 2}$ such that the i-th coordinate of all elements of $\operatorname{Im} \lambda$ will be in $L_i(S)$. This is the procedure discussed at the end of section 3.2, where we consider all primes of L_i lying over those in S. Recall that this makes use of Proposition 6 and uses information about the class group and unit group of L_i.

We can now calculate $\lambda(H)$ by taking $\lambda(P) = (X - T)(P)$ for each $P \in G$. Note that in the special case where the roots α_i of f are all in K, $\lambda(P) = (x - \alpha_1, \ldots x - \alpha_d)$ for $P = (x, y)$ not a Weierstrass point. This is because $L \cong \oplus_{i=1}^{d} K$ via $T \mapsto (\alpha_1, \ldots, \alpha_d)$. In this situation we may

drop the last coordinate as it is determined by the first $d-1$ since all coordinates must multiply to a square in K. Each $x - \alpha_i \in K(S)$ and $\lambda(H) = \langle \lambda(P) : P \in G \rangle$.

We now move on to the local analysis. Fix a prime $\mathfrak{p} \in S$. For each $1 \leq i \leq c$ we must determine a set of representatives for ${L_i}_{\mathfrak{p}}{}^{\times}/{L_i}_{\mathfrak{p}}{}^{\times 2}$, which is always finite. We then determine where $L_i(S)$ maps under ${L_i}^{\times}/{L_i}^{\times 2} \to {L_i}_{\mathfrak{p}}{}^{\times}/{L_i}_{\mathfrak{p}}{}^{\times 2}$. This can be done via sign considerations if ${L_i}_{\mathfrak{p}} = \mathbb{R}$ or using Hensel's Lemma for finite primes. With this information we can calculate $L_i(S) \cap \ker j_{i\mathfrak{p}}$ as well as $\left(\prod_{i=1}^{c} j_{i\mathfrak{p}}\right) \circ \lambda(P) = \lambda_{\mathfrak{p}}(P)$ for all $P \in G$.

Recall that we have an injection $\lambda_{\mathfrak{p}} : J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}}) \hookrightarrow \oplus_{i=1}^{c} {L_i}_{\mathfrak{p}}{}^{\times}/{L_i}_{\mathfrak{p}}{}^{\times 2}$, so $\#J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}}) = \#\operatorname{Im}\lambda_{\mathfrak{p}}$. Using Theorem 5 and formula (4) in section 3.1 we know $\#J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}})$, and we calculated $\langle \lambda(P) : P \in G \rangle$ in the previous paragraph. If $\#\langle \lambda_{\mathfrak{p}}(P) : P \in G \rangle = \#J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}})$, then

$$j_{\mathfrak{p}}{}^{-1}(\operatorname{Im}\lambda_{\mathfrak{p}}) = \langle K(S) \cap \ker j_{\mathfrak{p}}, \lambda(P) : P \in G \rangle.$$

Otherwise we must find more elements of $\operatorname{Im}\lambda_{\mathfrak{p}}$. This can be done by searching for points on $\mathcal{C}(K_{\mathfrak{p}})$, using Hensel's Lemma for example, and then constructing elements of $J(K_{\mathfrak{p}})$ that are independent from those in G. The SAGE function **find_new_gens** performs this search for the examples in this essay. Let $Q_1, \ldots, Q_\ell \in J(K_{\mathfrak{p}})$ such that $\operatorname{Im}\lambda_{\mathfrak{p}} = \langle \lambda_{\mathfrak{p}}(Q_1), \ldots, \lambda_{\mathfrak{p}}(Q_\ell), \lambda_{\mathfrak{p}}(P) : P \in G \rangle$. In this case we have

$$j_{\mathfrak{p}}(\operatorname{Im}\lambda_{\mathfrak{p}}) = \langle K(S) \cap \ker j_{\mathfrak{p}}, j_{\mathfrak{p}}{}^{-1}(\lambda_{\mathfrak{p}}(Q_1)), \ldots, j_{\mathfrak{p}}{}^{-1}(\lambda_{\mathfrak{p}}(Q_\ell)), \lambda(P) : P \in G \rangle.$$

We repeat the above analysis for all primes in S and then calculate

$$\bigcap_{\mathfrak{p} \in S} j_{\mathfrak{p}}{}^{-1}(\operatorname{Im}\lambda_{\mathfrak{p}}).$$

The hope is that this set will be equal to $\langle \lambda(P) : P \in G \rangle = \lambda(H)$. If so, then $J(K)/2J(K) = \langle G \rangle$ and the rank of $J(K)$ is equal to the number of independent non-torsion elements of G. If $\cap_{\mathfrak{p} \in S} j_{\mathfrak{p}}{}^{-1}(\operatorname{Im}\lambda_{\mathfrak{p}})$ strictly contains $\lambda(H)$, then we cannot compute the rank of $J(K)$ exactly using two descent.

5 Jacobians of hyperelliptic curves of genus two

In this section we investigate the case of Jacobians of hyperelliptic curves of genus two in detail. First we describe a canonical way of representing elements of the Jacobian that is analogous to the representation we have for elliptic curves. After establishing some facts about the two torsion and the structure of K-rational elements of the Jacobian, we give an example of two descent on the Jacobian of a hyperelliptic curve of genus two. This will make use of the general theorems that were proved in section 4.

5.1 Elements of the Jacobian of a hyperelliptic curve of genus two

Much of the theory of elliptic curves is made easier by the fact that we can represent the Jacobian of a curve as points on the curve with the group law being given by the secant-tangent construction. This concrete description of the group is much easier than working with the abstract group $\mathrm{Pic}^0(E)$ of degree zero divisors modulo linear equivalence. Unfortunately, for higher genus curves such a concrete description of the Jacobian becomes more difficult. This section is devoted to describing jacobians of hyperelliptic curves of genus two in an analogous way to that of elliptic curves. This will be useful for calculating the torsion subgroup of Jacobians of hyperelliptic curves of genus two in the next section.

In general, the non-singular model of a hyperelliptic curve $\mathcal{C}$ of genus two is the solution set in $\mathbb{P}^4$ of [3]

$$\mathcal{C}: \begin{cases} Y^2 = f_0{X_0}^2 + f_1X_0X_1 + f_2{X_1}^2 + f_3X_1X_2 + f_4{X_2}^2 + f_5X_2X_3 + f_6{X_3}^2 \\ 0 = X_1X_3 - {X_2}^2 \\ 0 = X_0X_2 - {X_1}^2 \\ 0 = X_0X_3 - X_1X_2. \end{cases} \tag{10}$$

Notice that by projecting to the $X_0 = 1$ chart, this simplifies to

$$y^2 = \sum_{i=0}^{6} f_i x^i,$$

where x is X_1. It is often convenient to work in this chart where the point (x, y) corresponds to the projective point $[1 : x : x^2 : x^3 : y]$. Of course, there are points that are not in this chart, namely those where $X_0 = 0$. Note that when $X_0 = 0$ we also have $X_1 = X_2 = 0$ and (10) reduces to $Y^2 = f_6{X_3}^2$. We must have $X_3 \neq 0$ (otherwise all of the projective coordinates would be zero), so by scaling we may take $X_3 = 1$. Thus, $Y^2 = f_6$ and the only points not in the $X_0 = 1$ chart are

$$\infty^+ = [0 : 0 : 0 : 1 : \sqrt{f_6}] \qquad\qquad \infty^- = [0 : 0 : 0 : 1 : -\sqrt{f_6}].$$

If $f_6 = 0$ there is only one point missing from the $X_0 = 1$ chart, namely $\infty = [0 : 0 : 0 : 1 : 0]$. For notational convenience, we shall sometimes write $\infty^0 = \infty$ when there is only one point at infinity. If $\mathcal{C}$ is defined over a field K, the points at infinity should only be considered K-rational if f_6 is a square in K.

Recall that in the case of elliptic curves, the Riemann-Roch Theorem allows us to write each element of $\mathrm{Pic}^0(E)$ uniquely as $(P) - (\infty)$. Similarly, in the case of hyperelliptic curves of genus two the Riemann-Roch Theorem allows us to write any nontrivial divisor $D \in \mathrm{Pic}^0(\mathcal{C})$ uniquely as

$$D = (P_1) + (P_2) - (\infty^\varepsilon) - (\infty^{-\varepsilon}),$$

where $\varepsilon = 1$ if $f_6 \neq 0$ and $\varepsilon = 0$ if $f_6 = 0$ and P_1, P_2 are points on $\mathcal{C}$ such that D is not the divisor of a function. In the case where D is the trivial divisor, it can be represented as the divisor of any

function. In particular, $D = \mathrm{div}(X - x_1)$ for any point $P = (x_1, y_1) \in \mathcal{C}$. Thus we may write we may write

$$D = \mathrm{div}(X - x_1) = (P) + (\overline{P}) - (\infty^{\varepsilon}) - (\infty^{-\varepsilon}),$$

where $\overline{P} = (x_1, -y_1)$ and ε is as above. We will use the shorthand notation $\{P, Q\}$ to denote the divisor class in $\mathrm{Pic}^0(\mathcal{C})$ of $(P) + (Q) - (\infty^{\varepsilon}) - (\infty^{-\varepsilon})$. Thus, there is a bijective correspondence between non-identity elements of the Jacobian J and the set of unordered pairs of points

$$\{\{P, Q\} : P, Q \in \mathcal{C}, P \neq \overline{Q}\}.$$

All pairs of points $\{P, \overline{P}\}$ represent the identity element of the Jacobian which will henceforth be denoted by $\mathcal{O}$.

Having established this correspondence, it is easy to see that for any points $P, Q \in \mathcal{C}$,

$$\{P, Q\} + \{\overline{P}, \overline{Q}\} = \{P, \overline{P}\} + \{Q, \overline{Q}\} = \mathcal{O} + \mathcal{O} = \mathcal{O},$$

so the inverse of $\{P, Q\}$ is $\{\overline{P}, \overline{Q}\}$. Hence, the 2-torsion elements of the Jacobian are those where $\{P, Q\} = \{\overline{P}, \overline{Q}\}$. Therefore,

$$J[2] = \{\{P, Q\} : P = (\alpha, 0), Q = (\beta, 0), \alpha \neq \beta\} \cup \{\mathcal{O}\}.$$

Now that we have a way to represent elements of $J(\overline{K})$, we make a few remarks about the K-rational elements $J(K)$. This is used primarily in the SAGE program **J(L,F)** which calculates $J(\mathbb{F}_p)$ for some prime p. Recall from Definition 1 that the K-rational points are elements that are invariant under the $\mathrm{Gal}(\overline{K}/K)$-action. In the case of a curve of genus two, a K-rational element is a pair $\{P, Q\} \in J(\overline{K})$ with the property that $\{P, Q\} = \{P^{\sigma}, Q^{\sigma}\}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Hence, either P, Q are both defined over K, in which case $P^{\sigma} = P$ and $Q^{\sigma} = Q$, or P and Q are conjugates. That is, there is some quadratic extension $K(\sqrt{\alpha})/K$ such that $P = (a + b\sqrt{\alpha}, c + d\sqrt{\alpha})$ and $Q = (a - b\sqrt{\alpha}, c - d\sqrt{\alpha})$. Then every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ restricts to an element of $\mathrm{Gal}(K(\sqrt{\alpha})/K)$ and so sends $\sqrt{\alpha}$ to $\pm\sqrt{\alpha}$. Thus, in this case there are elements $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that $P^{\sigma} = Q$ and $Q^{\sigma} = P$.

5.2 Example of two descent

We have now established everything that is needed to perform two descent on the Jacobians of hyperelliptic curves of genus two. In this section we carry out such a calculation and find the rank of the Jacobian of a genus two hyperelliptic curve. The method is similar to that used in Example 1 but makes use of the more general theorems proved in section 4.

Example 3.

Let $\mathcal{C}$ be the curve given by

$$\mathcal{C} : y^2 = f(x) = x(x - 3)(x - 4)(x - 6)(x - 7),$$

and let J be the Jacobian of $\mathcal{C}$. We will show that $J(\mathbb{Q})$ has rank zero. The discriminant of $\mathcal{C}$ is $\Delta_{\mathcal{C}} = 1316818944 = 2^{12} \cdot 3^8 \cdot 7^2$. The rank of $J(\mathbb{Q})$ was originally found using homogeneous spaces, but we exploit Theorem 5 to obtain the result [5], [3]. The advantage of avoiding homogeneous spaces is that they become quite complicated for higher genus curves.

As all of the roots of f are in $\mathbb{Q}$, it follows that all of the 2-torsion of J is rational. As $\#J[2] = 16$, we have $16|\#J(\mathbb{Q})_{tors}$. As with elliptic curves, we have $J(\mathbb{Q})_{tors} \hookrightarrow J(\mathbb{F}_p)$ for all primes p not dividing $\Delta_{\mathcal{C}}$. Using the SAGE function **len(J(L,F))**, we see that $\#J(\mathbb{F}_5) = 16$, so we must have $J(\mathbb{Q})_{tors} = J[2]$. Thus,

$$J(\mathbb{Q})_{tors} = \langle \{(0,0), \infty\}, \{(3,0), \infty\}, \{(4,0), \infty\}, \{(6,0), \infty\} \rangle.$$

For notational convenience we will write $T_1 = \{(0,0), \infty\}, T_2 = \{(3,0), \infty\}, T_3 = \{(4,0), \infty\}, T_4 = \{(6,0), \infty\}$.

Since f splits over $\mathbb{Q}$, the algebra $\mathbb{Q}[T]/f(T) \cong \oplus_{i=1}^{5} \mathbb{Q}$. As mentioned in section 4, the image of the map $\lambda : J(\mathbb{Q})/2J(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^5$ is determined by the first four coordinates since all five coordinates must multiply to a square in $\mathbb{Q}^\times$. Therefore, we will only use the first four coordinates in the remainder of the example. Using Proposition 11 we find that the images of the T_i under λ are

$$\begin{aligned}
T_1 &\mapsto ((-3)(-4)(-6)(-7), -3, -4, -6) = (14, -3, -1, -6) \\
T_2 &\mapsto (3, (3)(-1)(-3)(-4), -1, -3) = (3, -1, -1, -3) \\
T_3 &\mapsto (4, 1, (4)(1)(-2)(-3), -2) = (1, 1, 6, -2) \\
T_4 &\mapsto (6, 3, 2, (6)(3)(2)(-1)) = (6, 3, 2, -1).
\end{aligned}$$

Let $H = \operatorname{Im}\lambda = \langle (14, -3, -1, -6), (3, -1, -1, -3), (1, 1, 6, -2), (6, 3, 2, -1) \rangle$. We will show that $H = \mathrm{Sel}_2(J/\mathbb{Q})$. We have that $\mathrm{Sel}_2(J/\mathbb{Q}) \subseteq \mathbb{Q}(S)^4$, where $\mathbb{Q}(S)$ is the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by -1 and the prime divisors of $\Delta_{\mathcal{C}}$. That is,

$$\mathbb{Q}(S) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

First consider the prime $\mathfrak{p} = \infty$, so $\mathbb{Q}_\mathfrak{p} = \mathbb{R}$. Recall that $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$. By Theorem 5 we know that $\#J(\mathbb{R})/2J(\mathbb{R}) = \#J(\mathbb{R})[2]/2^2 = 16/4 = 4$. As $\lambda_\infty(T_1) = \lambda_\infty(T_2) = (1, -1, -1, -1)$ and $\lambda_\infty(T_3) = \lambda_\infty(T_4) = (1, 1, 1, -1)$, it follows that

$$J(\mathbb{R})/2J(\mathbb{R}) = \langle T_1, T_3 \rangle$$

and

$$\operatorname{Im}(\lambda_\infty) = \langle (1, -1, -1, -1), (1, 1, 1, -1) \rangle.$$

Therefore,

$$\begin{aligned}
{j_\infty}^{-1}(\operatorname{Im}(\lambda_\infty)) = \langle &(2,1,1,1), (1,2,1,1), (1,1,2,1), (1,1,1,2), (3,1,1,1), (1,3,1,1), \\
&(1,1,3,1), (1,1,1,3), (7,1,1,1), (1,7,1,1), (1,1,7,1), (1,1,1,7), \\
&(14,-3,-1,-6), (1,1,6,-2) \rangle.
\end{aligned}$$

Next consider the prime $\mathfrak{p} = 2$. We know that $\mathbb{Q}_2^{\times}/\mathbb{Q}_2^{\times 2}$ has eight elements, and we claim that

$$\mathbb{Q}_2{}^{\times}/\mathbb{Q}_2{}^{\times 2} = \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

As $x^2 + 1, x^2 \pm 2, x^2 - 3, x^2 \pm 6$ are irreducible modulo 4 and $x^2 + 3$ is irreducible modulo 8, it follows that $-1, \pm 2, \pm 3, \pm 6 \notin \mathbb{Q}_2{}^{\times 2}$. As $\{\pm 1, \pm 2, \pm 3, \pm 6\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it follows that this set is a complete set of representatives for $\mathbb{Q}_2{}^{\times}/\mathbb{Q}_2{}^{\times 2}$.

We will let $|\cdot|_p$ be the normalized absolute value corresponding to p. That is, for any $x \in \mathbb{Q}^{\times}$, $|x|_p = (1/p)^{v_p(x)}$, where $v_p(x)$ is the p-adic valuation of x. Now, $|1^2 + 7|_2 = 1/8 < 1/4 = |2 \cdot 1|_2{}^2$ so $-7 \in \mathbb{Q}_2{}^{\times 2}$ by Hensel's Lemma. Using this information we find that

$$\begin{aligned}
1 &\equiv -7 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
-1 &\equiv 7 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
2 &\equiv -14 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
-2 &\equiv 14 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
3 &\equiv -21 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
-3 &\equiv 21 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
6 &\equiv -42 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2})\\
-6 &\equiv 42 && (\mathrm{mod}\ \mathbb{Q}_2{}^{\times 2}).
\end{aligned}$$

Therefore it follows that $\lambda_2(T_1) = (-2, -3, -1, -6), \lambda_2(T_2) = (3, -1, -1, -3), \lambda_2(T_3) = (1, 1, 6, -2), \lambda_2(T_4) = (6, 3, 2, -1)$. As these four images generate a group of order 16 they are independent. By Theorem 5 we know that $\#J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = \#J(\mathbb{Q}_2)[2] \cdot 2^2 = 16 \cdot 4 = 64$, so we must find two additional generators for $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

Note that $|4^2 - f(18)|_2 = 1/2^8 < 1/2^6 = |2 \cdot 4|_2{}^2$, so by Hensel's Lemma there is an element $\gamma \in \mathbb{Q}_2$ such that $(18, \gamma) \in \mathcal{C}(\mathbb{Q}_2)$. Thus, $P = \{(18, \gamma), \infty\} \in J(\mathbb{Q}_2)$. Furthermore, using the SAGE function **cp_span** we find that $\lambda_2(P) = (2, -1, -2, 3)$ is not in the span of $\lambda_2(T_1), \lambda_2(T_2), \lambda_2(T_3), \lambda_2(T_4)$. Similarly, $|8^2 - f(23)|_2 = 1/2^9 < 1/2^8 = |2 \cdot 8|_2{}^2$, so by Hensel's Lemma there is an element $\delta \in \mathbb{Q}_2$ such that $(23, \delta) \in \mathcal{C}(\mathbb{Q}_2)$. Thus, $Q = \{(23, \delta), \infty\} \in J(\mathbb{Q}_2)$. Furthermore, **cp_span** can be used to check that $\lambda_2(Q) = (-1, -3, 3, 1)$ is not in the span of the elements found thus far. Therefore we have that

$$J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = \langle T_1, T_2, T_3, T_4, P, Q\rangle$$

and

$$\mathrm{Im}(\lambda_2) = \langle (-2, -3, -1, -6), (3, -1, -1, -3), (1, 1, 6, -2), (6, 3, 2, -1), (2, -1, -2, 3), (-1, -3, 3, 1)\rangle.$$

Therefore,

$$\begin{aligned}
j_2{}^{-1}(\mathrm{Im}(\lambda_2)) = \langle &(-7, 1, 1, 1), (1, -7, 1, 1), (1, 1, -7, 1), (1, 1, 1, -7), (14, -3, -1, -6),\\
&(3, -1, -1, -3), (1, 1, 6, -2), (6, 3, 2, -1), (2, -1, -2, 3), (-1, -3, 3, 1)\rangle.
\end{aligned}$$

Finally we consider $\mathfrak{p} = 7$. Recall that in Example 1 we found that $\mathbb{Q}_7/{\mathbb{Q}_7}^{\times 2} = \{\pm 1, \pm 7\}$. We also found the representative modulo ${\mathbb{Q}_7}^{\times 2}$ for all elements of $\mathbb{Q}(S)$. Using this information, it follows that under λ_7

$$\begin{aligned} T_1 &\mapsto (7, 1, -1, 1) \\ T_2 &\mapsto (-1, -1, -1, 1) \\ T_3 &\mapsto (1, 1, -1, -1) \\ T_4 &\mapsto (-1, -1, 1, -1). \end{aligned}$$

Now, $\lambda_7(T_4) = \lambda_7(T_2)\lambda_7(T_3)$, but $\lambda_7(T_1), \lambda_7(T_2), \lambda_7(T_3)$ are independent. By Theorem 5 we know that $\#J(\mathbb{Q}_7)/2J(\mathbb{Q}_7) = \#J(\mathbb{Q}_7)[2] = 16$, so we need to find another generator for $J(\mathbb{Q}_7)/2J(\mathbb{Q}_7)$.

Note that $|21^2 - f(35)|_7 = 1/7^3 < 1/7^2 = {|2 \cdot 21|_7}^2$ so by Hensel's Lemma there is an element $\eta \in \mathbb{Q}_7$ such that $(35, \eta) \in \mathcal{C}(\mathbb{Q}_7)$. Therefore, $R = \{(35, \eta), \infty\} \in J(\mathbb{Q}_7)$. Furthermore, $\lambda_7(R) = (-7, 1, -1, 1)$ which is not in the span of $\lambda_7(T_1), \lambda_7(T_2), \lambda_7(T_3)$. It follows that

$$J(\mathbb{Q}_7)/2J(\mathbb{Q}_7) = \langle T_1, T_2, T_3, R \rangle$$

and

$$\operatorname{Im} \lambda_7 = \langle (7, 1, -1, 1), (-1, -1, -1, 1), (1, 1, -1, -1), (-7, 1, -1, 1) \rangle.$$

Therefore,

$$\begin{aligned} {j_7}^{-1}(\operatorname{Im} \lambda_7) = &\langle (2, 1, 1, 1), (1, 2, 1, 1), (1, 1, 2, 1), (1, 1, 1, 2), (-3, 1, 1, 1), (1, -3, 1, 1), \\ &(1, 1, -3, 1), (1, 1, 1, -3), (14, -3, -1, -6), (3, -1, -1, -3), (1, 1, 6, -2), (-7, 1, -1, 1) \rangle. \end{aligned}$$

Using the SAGE functions **cp_span**, **multi_intersect**, and **same_set** we find that $H \subseteq \mathrm{Sel}_2(J/\mathbb{Q}) \subseteq \bigcap_{\mathfrak{p}=2,7,\infty} {j_\mathfrak{p}}^{-1}(\operatorname{Im} \lambda_\mathfrak{p}) = H$, so $H = \mathrm{Sel}_2(J/\mathbb{Q})$. Therefore T_1, T_2, T_3, T_4 generate $J(\mathbb{Q})/2J(\mathbb{Q})$ and $J(\mathbb{Q})$ has rank zero, as claimed.

6 Appendix: SAGE programs

This section contains the SAGE programs used to do many of the calculations for the examples contained in this paper together with a brief description of how they work. They are listed in alphabetical order by the name of the program. All functions are in bold text for easy reference.

conj

This function takes as input the quadratic extension K of $\mathbb{F}_p$ for some prime p and an element $x \in K$. If we choose a basis $\{1, \alpha\}$ for $K/\mathbb{F}_p$ and $x = a + b \cdot \alpha$, then this function returns the conjugate of x, namely $a - b \cdot \alpha$.

```
def conj(x,K):
    p=K.characteristic()
    for i in GF(p):
        if x-i*(K.gen()) in GF(p):
            b=-i
            a=x-i*(K.gen())
    return a+b*(K.gen())
```

cp_multiplication

This function gives the group operation on the Cartesian product of some finite number of copies of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, say n copies. It takes as input two n-tuples a, b (in the form of lists) of non-zero rational numbers and returns the n-tuple $a \cdot b$, where each entry is taken modulo $\mathbb{Q}^{\times 2}$. It calls the function **square_free_part**.

```
def cp_multiplication(a,b):
    P=[]
    for j in range(len(a)):
        P.append(square_free_part(a[j]*b[j]))
    return P
```

cp_product

This function allows one to multiply any (finite) number of elements of the Cartesian product of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with itself n times. It takes as input a list of the n-tuples that are to be multiplied and returns their product as an n-tuple with entries taken modulo $\mathbb{Q}^{\times 2}$. It calls the function **cp_multiplication**.

```
def cp_product(list):
    p=[]
        for i in list[0]:
        p.append(1)
    for i in range(len(list)):
        p=cp_multiplication(p,list[i])
    return p
```

cp_span

This function takes as input a list of elements of the n copies of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and returns the subgroup they generate in the Cartesian product of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with itself n times. It calls the built in SAGE function **combinations()** as well as **cp_product**. As all elements of the group n copies of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ have order two, the group generated by some list of elements is obtained by multiplying all possible combinations of the generators *without* multiplicity. This function is used to calculate the full group ${j_p}^{-1}(\mathrm{Im}(\lambda_p))$ from the generators in the examples.

```
def cp_span(gens):
    L=[]
    for i in range(len(gens)+1):
        M=combinations(gens,i)
        if M==[[]]:
            for j in gens[0]:
                M[0].append(1)
            M=[M]
        for j in M:
            if cp_product(j) not in L:
                L.append(cp_product(j))
    return L
```

find_new_gens

This function takes as input a polynomial F, four roots of F called $a1, a2, a3, a4$, a prime p, positive integers i and n, a list reps, and a list gen_knows. It is used to find further generators of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ when the known rational elements are not sufficient. The list gen_knowns consists of a list of the images of the known rational elements of $J(\mathbb{Q})$ under the map $\kappa_{\mathfrak{p}}$. The list reps consists of a complete list of representative elements of ${\mathbb{Q}_p}^{\times}/{\mathbb{Q}_p}^{\times 2}$. The function calculates the subgroup generated by the images under $\kappa_{\mathfrak{p}}$ of the known rational points. It then calls **find_possibilities** and calculates the images of the points in that list under $\kappa_{\mathfrak{p}}$. If this image is not in the subgroup generated by the known rational points, it adds the new possible generator to the list. It returns a list of elements of $\operatorname{Im}\kappa_{\mathfrak{p}}$ that are not in the span of the image of the known rational points. Besides **find_possibilities** it also calls **cp_span** and **Q_p_mod_squares**.

```
def find_new_gens(F,a1,a2,a3,a4,p,i,reps,n,gen_knowns):
    known_elements=cp_span(gen_knowns)
    new_gens=[]
    for x in find_possibilities(F,p,i):
        x=ZZ(x)
        ex_bar=[Q_p_mod_squares(x-a1, p, reps, n),
                Q_p_mod_squares(x-a2, p, reps, n),
                Q_p_mod_squares(x-a3, p, reps, n),
                Q_p_mod_squares(x-a4, p, reps, n)]
        if not ex_bar in known_elements and not x in new_gens:
            if 0 not in ex_bar:
                new_gens.append(x)
    return new_gens
```

find_possibilities

This function takes as input a polynomial F, a prime p, and a positive integer i. It returns a

list of x values such that there is a point (x, y) on the curve $y^2 = F(x)$ with $x, y \in \mathbb{Q}_p$. It tests all of the integers in $\mathbb{Z}/p^i\mathbb{Z}$. It calls **squares_mod_with_roots**, **squares_mod**, and **val** as well as the built in SAGE function **Integers(x)**.

```
def find_possibilities(F,p,i):
    possibilities=[]
    for x in Integers(p^i):
        if (F(x)%(p^i)) in squares_mod(p^i):
            x=ZZ(x)
            for y in squares_mod_with_roots(p^i):
                if y[0]==(F(x)%(p^i)):
                    if y[1]^2-F(x)==0 and not x in possibilities:
                     if not y[1]==0:
                         possibilities.append(x)
                    if not y[1]^2-F(x)==0 and x not in possibilities:
                     if not y[1]==0:
                         if val(y[1]^2-F(x),p)>2*val(2*y[1],p):
                             possibilities.append(x)
    return possibilities
```

intersect

This function takes as input two lists X, Y (representing mathematical sets) and returns their set-wise intersection $X \cap Y$ as a list. Of course, it does not matter which order the lists X and Y are given to the function.

```
def intersect(X,Y):
    intersection=[]
    for x in X:
        if x in Y:
            intersection.append(x)
    return intersection
```

J(L,F)

This function takes as input the unique quadratic extension field L of F_p for some prime p and a quintic polynomial F defining a hyperelliptic curve. It returns all of the elements on $J(\mathbb{F}_p)$, represented as pairs of unordered points on the curve $y^2 = F(x)$. The identity element is represented by the string 'O' and the point at infinity on the curve is represented by the string 'infty'. There are three main 'for' loops in the program. The first finds all elements of $J(\mathbb{F}_p)$ of the form $\{(x, y), \infty\}$ with $x, y \in \mathbb{F}_p$. The second loop finds all elements of the form $\{(x_1, y_1), (x_2, y_2)\}$, where $x_i, y_i \in \mathbb{F}_p$. The third loop finds all elements that come from the quadratic extension L that have not already been counted. That is, if $L = \mathbb{F}_p(\alpha)$, it finds

all points of the form $\{(a+b\cdot\alpha, c+d\cdot\alpha), (a-b\cdot\alpha, c-d\cdot\alpha)\}$ with $b \neq 0$. This function calls **conj**, **points_not_in_ground_field**, and **points_in**. By taking **len(J(L,F))**, we get the number of elements of $J(\mathbb{F}_p)$.

```
def J(L,F):
    p=L.characteristic()
    elements=['O']
    for x in points_in(GF(p),F):
        elements.append([x,'infty'])
    for x in points_in(GF(p),F):
        for y in points_in(GF(p),F):
            if not x[0]==y[0] and [y,x] not in elements:
                elements.append([x,y])
            if x[0]==y[0] and not x[1]==-y[1]:
                if not [y,x] in elements:
                    elements.append([x,y])
    for x in points_not_in_ground_field(L,F):
        for y in points_not_in_ground_field(L,F):
            if not x[0]==conj(x[0],L):
                if conj(x[0],L)==y[0] and conj(x[1],L)==y[1]:
                    if [y,x] not in elements:
                        elements.append([x,y])
    return elements
```

multi_intersect

This function takes as input a list of lists, where each element in the big list represents a mathematical set. It returns the set-wise intersection of all of the sets in the list as a list. It calls **intersect**. Again, it does not matter the order the sets are put into the big list. This is used for determining $\cap_p {j_p}^{-1}(\operatorname{Im}\lambda_p)$ in the examples after each individual ${j_p}^{-1}(\operatorname{Im}\lambda_p)$ has been computed using **cp_span**.

```
def multi_intersect(list):
    set=list[0]
    for j in range(len(list)):
        set=intersect(set,list[j])
    return set
```

points_in

This function takes as input a field K and a polynomial F. In our cases, the polynomial is the equation defining the elliptic or hyperelliptic curve that we are studying. It returns a list of points on the curve $y^2 = F(x)$ with $x, y \in K$. It does not include any points at infinity.

For each element of $i \in K$, it tests if $F(i)$ is a square by calling **squares**. It then calculates the y values and adds the points $(x, y), (x, -y)$ to the list, unless $y = 0$ in which case it only adds (x, y) to the list. We can use this function to figure out the number of points a curve has over a finite field by taking **len(points_in(K,F))** and adding any points at infinity.

```
def points_in(K,F):
    points=[]
    for i in K:
        if K(F(i)) in squares(K) and [i, sqrt(F(i))] not in points:
            points.append([i, sqrt(F(i))])
            if not sqrt(F(i))==0:
                points.append([i, -sqrt(F(i))])
    return points
```

points_not_in_ground_field

This function takes as input a field K of positive characteristic and a polynomial F, as in **points_in**. It returns all of the points on the curve $y^2 = f(x)$ with $(x, y) \in K$ but not both in the prime subfield. This calls the built in SAGE function **characteristic()** to determine the characteristic of K and also calls **points_in**.

```
def points_not_in_ground_field(K,F):
    p=K.characteristic()
    v=[]
    for x in points_in(K,F):
        if x[0] not in GF(p) or x[1] not in GF(p):
            v.append(x)
    return v
```

prime_divisors

This function takes as input a nonzero rational number x and returns the list of primes where x has nonzero valuation. It calls the built in SAGE function **factor()**.

```
def prime_divisors(x):
    primes=[]
    F=factor(x)
    for i in F:
        primes.append(i[0])
    return primes
```

Q_p_mod_squares

This function has four input values: a rational number x, a prime number p, a list of representatives of the group ${\mathbb{Q}_p}^{\times}/{\mathbb{Q}_p}^{\times 2}$, and a positive integer n. It uses Hensel's Lemma to try to

find the representative from the given list of the coset containing x in ${\mathbb{Q}_p}^\times/{\mathbb{Q}_p}^{\times 2}$. The positive integers n tells the program at which power of p to stop looking. By taking n sufficiently large, this will always return the desired representative. If $x = 0$, the function returns 0. The function calls **squares_mod_with_roots** and **val**. The idea is that x lies in exactly one coset of ${\mathbb{Q}_p}^\times/{\mathbb{Q}_p}^{\times 2}$. As every coset has order two the product $x \cdot j$, for a representative j from reps, will be a square in $\mathbb{Q}_p$ if and only if x and j are in the same coset. This function runs through all possible products $x \cdot j$ and uses the criterion of Hensel's Lemma to determine when the correct representative has been found. This function is used for calculating the images of points under the $\lambda_\mathfrak{p}$ maps.

```
def Q_p_mod_squares(x, p, reps, n):
    for i in range(1,n+1):
        for j in reps:
            if ((x*j)%(p^i)) in squares_mod(p^i):
                for y in squares_mod_with_roots(p^i):
                    if y[0]==((x*j)%(p^i)) and not y[1]==0:
                        if y[1]^2-x*j==0:
                            return j
                            break
                        if val(y[1]^2-x*j, p) > 2*val(2*y[1],p):
                            return j
                            break
    return 0
```

same_set

This function takes as input two lists X, Y representing mathematical sets and returns 'True' if $X = Y$ as sets and 'False' otherwise. This function is used in the examples to determine if the intersection found using **multi_intersect** is equal to the known elements in $\mathrm{Im}\,\lambda$.

```
def same_set(X,Y):
    for x in X:
        if not x in Y:
            return False
            break
    for y in Y:
        if not y in X:
            return False
            break
    return True
```

square_free_part

This function takes as input a rational number x and returns the square free representative of

x in the group $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. It calls the built in SAGE function **factor()** which returns a list of tuples of the form (p, e), where p is a prime and $e \in \mathbb{Z}$ is the p-adic valuation of x. It also stores the sign of x as **factor(x).unit()**.

```
def square_free_part(x):
        F=factor(x)
        u=F.unit()
        for i in F:
            if i[1]%2==1:
                u=u*i[0]
        return u
```

squares

This function takes as input a field K and returns a list of the elements that are squares. It tests if each element in K is a square by calling a built in SAGE function **is_square.()**.

```
def squares(K):
    squares=[]
    for a in K:
        if a.is_square():
            squares.append(a)
    return squares
```

squares_mod

This function takes as input a positive integer n and returns the squares modulo n. It is similar to **squares** but does not require working over a field.

```
def squares_mod(n):
    v=[]
    for i in range(n):
        if i^2%n not in v:
            v.append(i^2%n)
    return v
```

squares_mod_with_roots

This function takes as input a positive integer n and returns a list of pairs, where the first coordinate of each pair is a square modulo n and the second number is a square root of the first modulo n. Every possible such pair appears in the list exactly once.

```
def squares_mod_with_roots(n):
    v=[]
```

```
    for i in range(n):
        v.append([i^2%n, i])
    return v
```

val

This function takes as input a nonzero rational number x and a prime number p. It returns the p-adic valuation of x. It calls the function **prime_divisors**.

```
def val(x, p):
    v=0
    while p in prime_divisors(x):
        v=v+1
        x=ZZ(x/p)
    return v
```

References

[1] A. Brumer and K. Kramer, "The rank of elliptic curves", *Duke Math. J.* **44** (1977), No. 4, 715–743.

[2] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts 24, CUP, 1991.

[3] J.W.S Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, LMS Lecture Note Series, CUP, 1996.

[4] E.V. Flynn, B. Poonen, E.F. Schaefer, "Cycles of quadratic polynomials and rational points on a genus 2 curve", *Duke Math. J.* **90** (1997), No. 3, 435–463.

[5] D.M. Gordon and D. Grant, "Computing the Mordell-Weil rank of jacobians of curves of genus 2", *Trans. Amer. Math. Soc.* **337**, 807–824.

[6] A.W. Knapp, *Elliptic Curves*, Mathematical Notes 40, Princeton University Press, 1992.

[7] [Sage] William A. Stein et al., Sage Mathematics Software (Version 4.1). The Sage Development Team, 2009, http://www.sagemath.org.

[8] E.F. Schaefer, "2-descent on the Jacobians of hyperelliptic curves", *J. Number Theory* **51** (1995), No. 2, 219–232.

[9] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer, 1986.

[10] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98** (2001), No. 3, 245–277.