2-Descent on the Jacobians of Hyperelliptic Curves

November 9, 2010

Contents

Introduction

The Mordell-Weil Theorem, in its full generality, states that for any abelian variety A, defined over a field k which is finitely generated over its prime subfield, the group $A(k)$ of k-rational points on A is finitely generated. Thus, by the structure theorem, we have

$$A(k) \cong A(k)_{\text{tors}} \oplus \mathbb{Z}^r \tag{0.1}$$

where $A(k)_{\text{tors}}$, the torsion subgroup of $A(k)$, is finite, and $r \geq 0$ is called the (algebraic) rank of $A(k)$.

In this essay we will describe the method of 2-descent, which is used to calculate an upper bound for the rank r in certain special cases. The special cases we will be considering are when k is a number field and A is the Jacobian of a hyperelliptic curve define over k. In these cases, the aim of a 2-descent calculation is to give an upper bound on the size of the group $A(k)/2A(k)$, which will in turn give an upper bound for the rank of $A(k)$. To this end, we will give various proofs of the so called "Weak Mordell-Weil Theorem", which states that $A(k)/2A(k)$ is finite. We will then use the methods of these proofs to give explicit examples of descent calculations.

For the majority of the essay, we will be concentrating on concrete methods of descent, since these are best suited for practical computations. In the last section we will discuss a more abstract interpretation, which will provide more straightforward proofs of results that we require in order to successfully perform 2-descent calculations.

The simplest possible case is when A is an elliptic curve defined over the rationals, and that is the case we will be considering first.

Note. All number field calculations in this essay are done using a combination of **MAGMA** (version 2.16) [19] and *Mathematica* (version 7.0) [20].

1 2-Descent on Elliptic Curves

The first section of this essay will describe the technique of 2-descent for elliptic curves over number fields. We will prove the Weak Mordell-Weil Theorem in this special case, and give examples of rank computations to illustrate the methods involved.

1.1 The Weak Mordell-Weil Theorem over $\mathbb{Q}$

In this section we will develop methods which will be used to prove the Weak Mordell-Weil Theorem in general, and then use them to prove it in the special case of an elliptic curve defined over $\mathbb{Q}$.

Theorem 1.1.1. *(Weak Mordell-Weil) For all $m \geq 2$ the group $E(K)/mE(K)$ is finite.*

Our goal will be to prove this Theorem in the case $m = 2$. Our proof will give an upper bound of the size of $E(K)/2E(K)$, and thus an upper bound on the rank r. Indeed, if we write

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r \tag{1.1}$$

then

$$E(K)/2E(K) \cong G \times (\mathbb{Z}/2\mathbb{Z})^r \tag{1.2}$$

where G is some contribution from the 2-power torsion of $E(K)$. This torsion contribution is easy to calculate, thus knowing the size of $E(K)/2E(K)$ will tell us the rank of $E(K)$.

Our first objective will be to give the proof when $K = \mathbb{Q}$, following Cassels [3], Chapter 15. Since we will need most of the methods later in a more general context, we will develop them over an arbitrary field k of characteristic zero, and will specialise to the case $k = \mathbb{Q}$ at the end of this section. So let E/k be an elliptic curve over a field k of characteristic 0, and pick a Weiertsrass model for E

$$E : y^2 = f(x) \tag{1.3}$$

with $f \in k[T]$ of degree 3. We define the k-algebra

$$A_k := \frac{k[T]}{(f(T))} \tag{1.4}$$

which is a direct sum of fields, one for each irreducible factor of $f(T)$ over k. For $\alpha \in A_k$, we will refer to its components to mean the images of α in the summands of A_k.

Define the norm map $\mathrm{N}_{A_k/k} : A_k \to k$ by $\mathrm{N}_{A_k/k}(\alpha) = \det(A_k \overset{\times\alpha}{\to} A_k)$, the determinant of the multiplication by α map on A_k. It is multiplicative on the summands on A_k. Write Θ for the image of T in A_k, thus $A_k = k[\Theta]$.

Fact.

1. If $a \in k$, $\mathrm{N}_{A_k/k}(a - \Theta) = f(a)$
2. $\alpha \in A_k^* \Leftrightarrow \mathrm{N}_{A_k/k}(\alpha) \in k^*$

We wish to define a map

$$\begin{aligned} \lambda_k : E(k) &\to A_k^* \\ P &\mapsto x(P) - \Theta \end{aligned} \tag{1.5}$$

If $y(P) \neq 0$ then this makes sense, for then $\mathrm{N}_{A_k/k}(x(P) - \Theta) = F(x(P)) = y(P)^2 \neq 0$ and $x(P) - \Theta$ is a unit in A_k. This does not work if $y(P) = 0$. But then $P = (a, 0) \in E(k)[2]$ and $(T - a) \mid f(T)$. Write $f(T) = g(T)(T - a)$ with $g(T) \in k[T]$, then

$$A_k \cong k \oplus \frac{k[T]}{(g(T))} \tag{1.6}$$

Send $P = (a, 0)$ to $(g(a), a - \Phi) \in A_k^*$ (here Φ is the image of T in $k[T]/(g(T))$). This does make sense, since E/k non-singular $\Rightarrow$ $(T - a)$ is a simple root of $f(T)$. If $P = O$ we set $\lambda_k(P) = 1$. Let $\bar{\lambda}_k : E(k) \to A_k^*/(A_k^*)^2$ be the composition of λ_k with the projection map. Our first observation about $\bar{\lambda}_k$ is trivial.

Lemma 1.1.2. $\bar{\lambda}_k(P) \subset \mathcal{M} := \ker\left(\mathrm{N}_{A_k/k} : A_k^*/(A_k^*)^2 \to k^*/(k^*)^2\right)$

Proof. If $P \in E(k)[2]$, write $P = (a, 0)$, $f(T) = (T - a)g(T)$ and $A_k = k \oplus A'_k$, where $A'_k = k[T]/(g(T))$. Then

$$\mathrm{N}_{A_k/k}(g(a), a - \Phi) = g(a)\mathrm{N}_{A'_k/k}(a - \Phi) = g(a)^2 \in (k^*)^2 \tag{1.7}$$

If $P \notin E(k)[2]$ then

$$\mathrm{N}_{A_k/k}(\lambda_k(P)) = \mathrm{N}_{A_k/k}(x(P) - \Theta) = f(x(P)) = y(P)^2 \in (k^*)^2 \tag{1.8}$$

□

Our next observation is less trivial.

Lemma 1.1.3. *The map* $\bar{\lambda}_k : E(k) \to A_k^*/(A_k^*)^2$ *is a group homomorphism.*

Proof. Since $\lambda_k(P)\lambda_k(-P) = \lambda_k(P)^2$, it suffices to show that if $P, Q, R \in E(k)$ are colinear then $\lambda_k(P)\lambda_k(Q)\lambda_k(R) \in (A_k^*)^2$. Suppose that one of $P, Q, R = O$, say $P = O$. Then either $Q = R$ or $Q, R \notin E(k)[2]$ and $x(Q) = x(R)$. In both cases $\lambda_k(P)\lambda_k(Q)\lambda_k(R)$ is a square, so we may assume that none of P, Q, R are O. We divide into cases.

1. Suppose that $P, Q, R \notin E(k)[2]$. P, Q, R lie on a line $y = rx + s$, with $r, s \in k$. Then

$$(rT + s)^2 - f(T) = (x(P) - T)(x(Q) - T)(x(R) - T) \tag{1.9}$$

in $k[T]$, and passing to the quotient $k[\Theta] = k[T]/(f(T))$ gives $(x(P) - \Theta)(x(Q) - \Theta)(x(R) - \Theta) = (r\Theta + s)^2$.

2. Suppose $P \in E(k)[2]$ and $Q, R \notin E(k)[2]$ lie on the line $y = rx + s$. Write $P = (a, 0)$, then

$$(rT + s)^2 - (T - a)g(T) = (a - T)(x(Q) - T)(x(R) - T) \tag{1.10}$$

and $A_k \cong k \oplus k[T]/(g(T))$. Let Φ be the image of T in $k[T]/(g(T)))$. Then

$$\begin{aligned} \lambda_k(P) &= (g(a), a - \Phi) \\ \lambda_k(Q) &= (x(Q) - a, x(Q) - \Phi) \\ \lambda_k(R) &= (x(R) - a, x(R) - \Phi) \end{aligned} \tag{1.11}$$

Thus

$$\lambda_k(P)\lambda_k(Q)\lambda_k(R) = (g(a)(x(Q) - a)(x(R) - a), (a - \Phi)(x(Q) - \Phi)(x(R) - \Phi)) \tag{1.12}$$

Since $g(\Phi) = 0$ by definition of Φ, (1.10) shows us that $(a-\Phi)(x(Q)-\Phi)(x(R)-\Phi)$ is a square in $(k[T]/(g(T)))^*$. Letting $T = a$ in (1.10), we see that $ra + s = 0$, and thus dividing out by $T - a$ gives

$$g(T) - r^2(T-a) = (x(Q) - T)(x(R) - T) \tag{1.13}$$

Letting $T = a$ again gives $g(a) = (x(Q)-a)(x(R)-a)$ an it follows that $g(a)(x(Q)-a)(x(R)-a)$ is a square in k^*.

3. If $P, Q, R \in E(k)[2]$ are all $\neq O$ then $f(T) = (T-a)(T-b)(T-c)$ with $a, b, c \in k$, and $P = (a, 0), Q = (b, 0), R = (c, 0)$. Then

$$A_k \cong k \oplus k \oplus k \tag{1.14}$$

and

$$\begin{aligned} \lambda_k(P) &= ((a-b)(a-c), a-b, a-c) \\ \lambda_k(Q) &= (b-a, (b-a)(b-c), b-c) \\ \lambda_k(R) &= (c-a, c-b, (c-a)(c-b)) \end{aligned} \tag{1.15}$$

Thus $\lambda_k(P)\lambda_k(Q)\lambda_k(R)$ is visibly a square in A_k^*.

□

It is clear that $2E(k) \subset \ker \bar{\lambda}_k$, since $\lambda_k(2P) = \lambda_k(P)^2$. Thus $\bar{\lambda}_k$ descends to a homomorphism $\tilde{\lambda}_k : E(k)/2E(k) \to A_k^*/(A_k^*)^2$.

Lemma 1.1.4. *$\tilde{\lambda}_k : E(k)/2E(k) \to A_k^*/(A_k^*)^2$ is injective.*

Proof. We must show that $\ker \bar{\lambda}_k \subset 2E(k)$. So suppose $\lambda_k(P)$ is a square in A_k^*. If $y(P) \neq 0$ then

$$x(P) - \Theta = (\alpha\Theta^2 + \beta\Theta + \gamma)^2 \tag{1.16}$$

with $\alpha, \beta, \gamma \in k$. Note that $\alpha \neq 0$ since Θ cannot satisfy a non-trivial polynomial of degree < 3. We wish to solve the equation

$$(b - \Theta)(\alpha\Theta^2 + \beta\Theta + \gamma) = (r\Theta + s) \tag{1.17}$$

for $b, r, s \in k$ If f is given by $f(T) = T^3 + a_2T^2 + a_1T + a_0$ then multiplying out (1.17) gives

$$(\alpha(b + a_2) - \beta)\Theta^2 + (\alpha a_1 + \beta b - \gamma)\Theta + b\gamma + \alpha a_0 = r\Theta + s \tag{1.18}$$

Thus ($\alpha \neq 0$) we take $b = \frac{\beta}{\alpha} - a_2$, $r = \alpha a_1 + \beta b - \gamma$ and $s = \alpha a_0 + b\gamma$. Multiplying (1.16) by $(b - \Theta)^2$ gives

$$(b - \Theta)^2(x(P) - \Theta) - (r\Theta + s)^2 = 0 \tag{1.19}$$

for some $b, r, s \in k$. Thus $(b-T)^2(x(P)-T) - (rT+s)^2$ lies in $f(T)k[T]$, and by comparing coefficients we see that

$$(b - T)^2(x(P) - T) = (rT + s)^2 - f(T) \tag{1.20}$$

But this precisely says that the line $y = rx + s$ meets $E(k)$ at $\pm P$ with multiplicity 1, and at another point Q with multiplicity 2. It follows that $\pm P \in 2E(k)$ and so $P \in 2E(k)$.

Finally suppose that $y(P) = 0$. In the decomposition $A_k \cong k \oplus \frac{k[T]}{g(T)}$ we have $\lambda_k = (g(x(P)), x(P) - \Phi)$, and hence $\bar{\lambda}_k(P) = 1 \Rightarrow x(P) - \Phi$ is a square in $k[T]/(g(T))$. Thus $x(P) - \Theta = (0, x(P) - \Phi)$ is a square in A_k and we can proceed exactly as above. □

Thus to prove Theorem 1.1.1, it suffices to prove that for a number field K the image $\bar{\lambda}_K(E(K)) \subset \mathcal{M}$ is finite. We now specialise to the case $k = \mathbb{Q}$.

Theorem 1.1.5. *$\bar{\lambda}_{\mathbb{Q}}(E(\mathbb{Q})) \subset \mathcal{M}$ is finite.*

Proof. The image of 2 torsion is finite, so we only need consider the image of $E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, on which the map $\lambda_{\mathbb{Q}}$ is defined by $P \mapsto x(P) - \Theta$. Let $\epsilon_1, \epsilon_2, \epsilon_3$ be the roots of f in some fixed extension K of $\mathbb{Q}$. By rescaling x and y we may assume that the leading coefficient of f is 1, thus the ϵ_i are algebraic integers. Define $K_i := \mathbb{Q}(\epsilon_i)$.

Given $(x, y) \in E(\mathbb{Q})$ write $x = \frac{r}{t^2}, y = \frac{s}{t^3}$ for $r, s, t \in \mathbb{Z}$ with $\mathrm{hcf}(r, t) = \mathrm{hcf}(s, t) = 1$. Then

$$s^2 = (r - \epsilon_1 t^2)(r - \epsilon_2 t^2)(r - \epsilon_3 t^2) \tag{1.21}$$

Consider the ideal $[r - \epsilon_1 t^2, r - \epsilon_2 t^2] \subset \mathcal{O}_K$. Then $r(\epsilon_1 - \epsilon_2), t^2(\epsilon_1 - \epsilon_2) \in [r - \epsilon_1 t^2, r - \epsilon_2 t^2]$ and hence $r, t \in \mathbb{Z}$ coprime $\Rightarrow (\epsilon_1 - \epsilon_2) \in [r - \epsilon_1 t^2, r - \epsilon_2 t^2]$. Similarly $\epsilon_2 - \epsilon_3 \in [r - \epsilon_2 t^2, r - \epsilon_3 t^2]$ and $\epsilon_3 - \epsilon_1 \in [r - \epsilon_3 t^2, r - \epsilon_1 t^2]$.

Write $[r - \epsilon_i t] = \mathfrak{d}_i \mathfrak{u}_i^2$ with $\mathfrak{d}_i$ square-free ideals in $\mathcal{O}_K$. Then any prime ideal $\mathfrak{p}$ dividing $\mathfrak{d}_1$ must divide $[s^2]$, and hence divide $[r - \epsilon_1 t^2][t - \epsilon_2 t^2][r - \epsilon_3 t^2]$ an even number of times. Hence $\mathfrak{p}$ must divide either $[r - \epsilon_2 t^2]$ or $[r - \epsilon_3 t^2]$, say $\mathfrak{p} \mid [r - \epsilon_2 t^2]$. Thus $\mathfrak{p} \mid [r - \epsilon_1 t^2, r - \epsilon_2 t^2]$ and hence $\mathfrak{p} \mid (\epsilon_1 - \epsilon_2)$. Applying this for all prime factors of each $\mathfrak{d}_i$ shows us that

$$\mathfrak{d}_i \mid (\epsilon_1 - \epsilon_2)(\epsilon_2 - \epsilon_3)(\epsilon_3 - \epsilon_1) \tag{1.22}$$

Also, since $[r - \epsilon_1 t^2][r - \epsilon_2 t^2][r - \epsilon_3 t^2] = [s^2]$ it follows that $\mathfrak{d}_1 \mathfrak{d}_2 \mathfrak{d}_3$ is an ideal square. Hence the set of all possible $\mathfrak{d}_i$ is finite. Let $\mathcal{I}(\mathcal{O}_K)$ denote the group of fractional ideals of $\mathcal{O}_K$, and $\mathrm{Cl}(K)$ the class group of K. We have proved that the set

$$\mathcal{N} := \left\{ r - \epsilon_i t^2 \mid \left(\frac{r}{t^2}, \frac{s}{t^3} \right) \in E(\mathbb{Q}), 1 \leq i \leq 3 \right\} \subset K^* \tag{1.23}$$

has finite image under the map $K^* \to \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$.

Define $\Gamma := \ker(K^*/(K^*)^2 \to \mathrm{Cl}(K)/\mathrm{Cl}(K)^2)$. We have a homomorphism $\psi : \Gamma \to \mathrm{Cl}(K)$ defined by $\alpha(K^*)^2 \mapsto I_\alpha$ where $\alpha \mathcal{O}_K = I_\alpha^2$. Changing α by a square changes I_α by a principal ideal, so ψ is well defined. Suppose that $\alpha(K^*)^2 \in \ker \psi$. Then $\alpha \mathcal{O}_K = \beta^2 \mathcal{O}_K$ for some $\beta \in K$, and $\alpha = u\beta^2$ for some $u \in \mathcal{O}_K^*$. We thus have a well defined injection $\ker \psi \hookrightarrow \mathcal{O}_K^*/(\mathcal{O}_K^*)^2$. Hence $\ker \psi$ is finite (as $\mathcal{O}_K^*$ is finitely generated), and thus the exact sequence

$$1 \to \ker \psi \to \Gamma \to \mathrm{Cl}(K) \to 1 \tag{1.24}$$

together with finiteness of $\mathrm{Cl}(K)$, shows that Γ is finite. Hence the image of $\mathcal{N}$ in $K^*/(K^*)^2$ is finite. $[K : K_i] \leq 2$ for each i, say $K = K_i(\sqrt{\alpha_i})$, $\alpha_i \in K_i^*$. $\ker : \left(K_i^*/(K_i^*)^2 \to K^*/(K^*)^2\right)$ is the subgroup generated by α_i, which is finite (indeed, of order $[K : K_i]$). Thus $\mathcal{N}_i := \{r - \epsilon_i t^2 \mid (\frac{r}{t^2}, \frac{s}{t^3}) \in E(\mathbb{Q})\} \subset \mathbb{Q}(\epsilon_i)$ has finite image in $K_i^*/(K_i^*)^2$. But this is just the image of $E(\mathbb{Q})$ in the direct summand of $A_{\mathbb{Q}}^*/(A_{\mathbb{Q}}^*)^2$ corresponding to ϵ_i, so $\bar{\lambda}_{\mathbb{Q}}(E(\mathbb{Q})) \subset \mathcal{M}$ is finite, as required.

□

This is not the finiteness proof that we will be generalising to Jacobians, and so we only give one short example of its implementation in a 2-descent calculation.

Example. We calculate the rank of the curve

$$E/\mathbb{Q} : y^2 = x^3 - x \tag{1.25}$$

over $\mathbb{Q}$. $A_{\mathbb{Q}} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$, and let the three components correspond to the roots $-1, 0, 1$ of f in that order. The image of $\lambda_{\mathbb{Q}}$ on consists of triples (d_1, d_2, d_3), with $d_i \in \mathbb{Z}$ square-free, $d_1 d_2 d_3$ a square and $d_i \mid 2$. Thus $d_i \in \{\pm 1, \pm 2\}$. This is true by the previous theorem for points $P \notin E(\mathbb{Q})[2]$, and by direct calculation for 2 torsion points.

Suppose that $(\frac{r}{t^2}, \frac{s}{t^3}) \in E(\mathbb{Q})$ is not a 2 torsion point, with image (d_1, d_2, d_3) in $A_{\mathbb{Q}}^*/(A_{\mathbb{Q}}^*)^2$. Then $\mathrm{hcf}(d_1, d_2)$ and $\mathrm{hcf}(d_2, d_3)$ divide 1, and $\mathrm{hcf}(d_1, d_3)$ divides 2. Moreover $r + t^2 > r > r - t^2 \Rightarrow$

$d_1 > \alpha d_2 > \beta d_3$ for $\alpha, \beta > 0$. Hence the only possible sign combinations are $(+,+,+)$ and $(+,-,-)$. Thus for $P \notin E(\mathbb{Q})[2]$, $\lambda_{\mathbb{Q}}(P)$ lies in the set

$$\{(1,1,1),(2,1,2),(1,-1,-1),(2,-1,-2)\} \tag{1.26}$$

By direct calculation, $\lambda_{\mathbb{Q}}(E(\mathbb{Q})[2])$ also lies in this set, hence $E(\mathbb{Q})/2E(\mathbb{Q})$ has size ≤ 4. $E(\mathbb{Q})[2]$ realises a subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ of order 4, hence $E(\mathbb{Q})$ has rank zero, and $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}}$.

Remark. It can be easily seen using the results of Section 1.4 that in fact $E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})[2]$ and hence $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Note. We will generally not distinguish between $\lambda_k, \bar{\lambda}_k$ and $\tilde{\lambda}_k$ for the remainder of this essay. No confusion should be caused by this.

1.2 The Selmer Group

The proof that the image of λ_K is finite does not work over general number fields. Greatest common divisors only exist for ideals in the ring of integers $\mathcal{O}_K$ of K, not for the elements themselves. Instead, we will gain information about $E(K)/2E(K)$ by looking at the groups $E(K_v)/2E(K_v)$ for all places v of K. We have a commutative diagram.

$$\begin{tikzcd}
0 \arrow[r] & E(K)/2E(K) \arrow[r, "\lambda_K"] \arrow[d, "\text{res}"] & A_K^*/(A_K^*)^2 \arrow[d, "\text{res}"] \\
0 \arrow[r] & \prod_v E(K_v)/2E(K_v) \arrow[r, "\prod_v \lambda_{K_v}"] & \prod_v A_{K_v}^*/(A_{K_v}^*)^2
\end{tikzcd} \tag{1.27}$$

Define the 2-Selmer group

$$S^2(E,K) = \{\alpha \in \ker(\mathrm{N}_{A_K/K} : A_K^*/(A_K^*)^2 \to K^*/(K^*)^2) \mid \operatorname{res}(\alpha) \in \operatorname{im}(\prod_v \lambda_{K_v})\} \tag{1.28}$$

(This is not the usual definition of the Selmer group in terms of tgroup cohomology, however, we will prove their equivalence later on in the essay). It is clear from (1.27) that $\lambda_K(E(K)/2E(K)) \subset S^2(E,K)$, and we will use $S^2(E,K)$ to estimate the size of $E(K)/2E(K)$. To do this we will need to analyse the maps $\lambda_{K_v} : E(K_v)/2E(E_v) \to A_{K_v}^*/(A_{K_v}^*)^2$ more closely.

1.3 Local Considerations

In this section we gather information about the image of $\lambda_{K_v} : E(K_v)/2E(K_v) \to A_{K_v}^*/(A_{K_v}^*)^2$. In general we follow Brumer and Kramer [2]. K_v will denote a completion of a number field at a finite place v with ring of integers $\mathcal{O}_v$, maximal ideal $\mathfrak{m}_v$, uniformiser π_v and residue field k_v. Our first result tells is the size of the group we are interested in.

Proposition 1.3.1. *$\#E(K_v)/2E(K_v) = [\mathcal{O}_v : 2\mathcal{O}_v]\#E(K_v)[2]$*

Proof. $E(K_v)$ has a subgroup of finite index $\cong \mathcal{O}_v$, and we have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_v \arrow[r] \arrow[d, "{[2]}"] & E(K_v) \arrow[r] \arrow[d, "{[2]}"] & A \arrow[r] \arrow[d, "{[2]}"] & 0 \\
0 \arrow[r] & \mathcal{O}_v \arrow[r] & E(K_v) \arrow[r] & A \arrow[r] & 0
\end{tikzcd} \tag{1.29}$$

with A finite. The snake lemma gives the exact sequence

$$0 \to E(K_v)[2] \to A[2] \to \mathcal{O}_v/2\mathcal{O}_v \to E(K_v)/2E(K_v) \to A/2A \to 0 \tag{1.30}$$

Since A is finite, the exact sequence $0 \to A[2] \to A \to A \to A/2A \to 0$ tells us that $\#A/2A = \#A[2]$, so $\#E(K_v)/2E(K_v) = [\mathcal{O}_v : 2\mathcal{O}_v]\#E(K_v)[2]$ as required. □

It is relatively easy to calculate $\lambda_k(E(K_v)/2E(K_v))$ for places v of good reduction.

Proposition 1.3.2. *Suppose that E has good reduction over K_v, and that $\mathrm{char}(k_v) \neq 2$. Let K_v^{nr} be the maximal unramified extension of K_v. Then $E(K_v^{\mathrm{nr}})/2E(K_v^{\mathrm{nr}}) = 0$.*

Proof. Since E has good reduction over K_v, it has good reduction over K_v^{nr}. We have the commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & E_1(K_v^{\mathrm{nr}}) \arrow[r] \arrow[d, "{[2]}"] & E(K_v^{\mathrm{nr}}) \arrow[r] \arrow[d, "{[2]}"] & \tilde{E}(\bar{k}_v) \arrow[r] \arrow[d, "{[2]}"] & 0 \\ 0 \arrow[r] & E_1(K_v^{\mathrm{nr}}) \arrow[r] & E(K_v^{\mathrm{nr}}) \arrow[r] & \tilde{E}(\bar{k}_v) \arrow[r] & 0 \end{tikzcd} \tag{1.31}$$

The snake lemma gives the exact sequence

$$E_1(K_v^{\mathrm{nr}})/2E_1(K_v^{\mathrm{nr}}) \to E(K_v^{\mathrm{nr}})/2E(K_v^{\mathrm{nr}}) \to \tilde{E}(\bar{k}_v)/2\tilde{E}(\bar{k}_v) \to 0 \tag{1.32}$$

$\bar{k}$ is algebraically closed, so $\tilde{E}(\bar{k}_v)/2\tilde{E}(\bar{k}_v) = 0$.

Thus $E_1(K_v^{\mathrm{nr}})/2E_1(K_v^{\mathrm{nr}})$ surjects onto $E(K_v^{\mathrm{nr}})/2E(K_v^{\mathrm{nr}})$. Since $\mathrm{char}(k_v) \neq 2$, $E_1(K_v^{\mathrm{nr}})$ is divisible by 2, so $E_1(K_v^{\mathrm{nr}})/2E_1(K_v^{\mathrm{nr}}) = 0$. Hence so is $E(K_v^{\mathrm{nr}})/2E(K_v^{\mathrm{nr}})$. □

Proposition 1.3.3. *Suppose that E has good reduction over K_v, and that $\mathrm{char}(k_v) \neq 2$. Then every element in $\mathrm{im}(\lambda_{K_v})$ has a representative $\alpha \in A_{K_v}^*$ with each component a unit.*

Proof. Suppose that $A_{K_v} \cong \bigoplus_{i=1}^n L_i$ with each L_i a finite extension of K_v, $n \in \{1,2,3\}$. Any element in $\lambda_{K_v}(E(K_v)/2E(K_v))$ is of the form $(d_1, \ldots, d_n)(A_{K_v}^*)^2$, with $d_i \in L_i$. We may assume that $v_i(d_i) \in \{0,1\}$ where v_i is the unique valuation on L_i extending v. We have a commutative diagram

$$\begin{tikzcd} E(K_v)/2E(K_v) \arrow[r] \arrow[d] & A_{K_v}^*/(A_{K_v}^*)^2 \arrow[d] \\ E(K_v^{\mathrm{nr}})/2E(K_v^{\mathrm{nr}}) \arrow[r] & A_{K_v^{\mathrm{nr}}}^*/(A_{K_v^{\mathrm{nr}}}^*)^2 \end{tikzcd} \tag{1.33}$$

and hence $(d_1, \ldots, d_n)$ must become a square in $A_{K_v^{\mathrm{nr}}}^*/(A_{K_v^{\mathrm{nr}}}^*)^2$. Thus each component d_i becomes a square in an unramified extension of L_i, i.e. $v_i(d_i)$ is even for all i. We are assuming $v_i(d_i) \in \{0,1\}$ whence $v_i(d_i) = 0$ as required. □

In fact, a simple counting argument shows us that we now know the group $\lambda_{K_v}(E(K_v)/2E(K_v)$ completely.

Corollary 1.3.4. *Let v be a finite place of good reduction, with $\mathrm{char}(k_v) \neq 2$. Then $\lambda_k(E(K_v)/2E(K_v))$ consists of those elements of $A_{K_v}^*/(A_{K_v}^*)^2$ with each component a unit, and whose norm is a square in K_v^**

Proof. K_v is a finite extension of $\mathbb{Q}_p$ with $p > 2$. Thus so is each component L_i of A_{K_v}, $i = 1, \ldots, n$, $n \in \{1,2,3\}$. Write $\mathcal{O}_i$ for the ring of integers of L_i. Then $\mathcal{O}_i^*/(\mathcal{O}_i^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$ and the size of the subgroup of $A_{K_v}^*/(A_{K_v}^*)^2$ with each component a unit is 2^n. Thus the size of the subgroup of $A_{K_v}^*/(A_{K_v}^*)^2$ with each component a unit and the norm a square is 2^{n-1}, which is the size of $E(K_v)/2E(K_v)$ by 1.3.1. □

This is enough to prove the Weak Mordell-Weil Theorem over number fields.

Theorem 1.3.5. *Let K be a number field. Then $S^2(E,K)$ is finite.*

Proof. It suffices to prove that for a number field K, and a finite set of places $S = \{v_1, \ldots, v_n\}$ including all infinite places, the set $H = \{\alpha \in K^*/(K^*)^2 \mid v(\alpha) \equiv 0 \bmod 2 \ \forall v \notin S\}$ is finite. H has finite image under the map $K^*/(K^*)^2 \to \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$, and thus, as in Theorem 1.1.5, H is finite. □

Corollary 1.3.6. *Let K be a number field. Then $E(K)/2E(K)$ is finite.*

By following the proof, it is relatively straightforward to obtain an upper bound for the rank of an elliptic curve defined over K, provided it is computationally feasible to work with the number fields L_i which appear in the decomposition of A_K. In general this bound will be fairly weak, since it only uses information from finite places of good reduction. By calculating the group $E(K_v)/2E(K_v)$ for places of bad reduction and infinite places we will get stronger bounds on $S^2(E, K)$.

The first thing to note is that Corollary 1.3.4 holds more generally, indeed, it will hold if $\text{char}(k_v) \neq 2$ and $[E(K_v) : E_0(K_v)]$ is odd. The above arguments show that for $\text{char}(k_v) \neq 2$, $E_0(K_v)/2E_0(K_v)$ always satisfies the conclusions of 1.3.4, and $[E(K_v) : E_0(K_v)]$ odd $\Rightarrow E(K_v)/2E(K_v) = E_0(K_v)/2E_0(K_v)$. The following theorem is needed if we are to use this information.

Theorem 1.3.7. *Let v be a finite place of a number field K, and E/K an elliptic curve. Choose a minimal model for E at v, and let $n = v(\Delta)$ be the valuation of its discriminant.*

- *If E/K_v has split multiplicative reduction then $E(K_v)/E_0(K_v) \cong \mathbb{Z}/n\mathbb{Z}$.*
- *If E/K_v has non-split multiplicative reduction, then $E(K_v)/E_0(K_v)$ is 0 if n is odd, and $\cong \mathbb{Z}/2\mathbb{Z}$ if n is even.*

Proof. See Chapter 4 of Silverman [17]. □

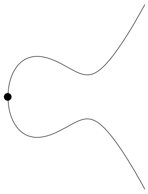
The following proposition tells us all we need to know about infinite places.

Proposition 1.3.8. *1. $\bar{\lambda}_{\mathbb{C}}(E(\mathbb{C}))$ is trivial.*

2.
- *If $\Delta(f) < 0$ then $A_{\mathbb{R}} \cong \mathbb{R} \oplus \mathbb{C}$ and $\bar{\lambda}_{\mathbb{R}}(E(\mathbb{R}))$ is trivial.*
- *If $\Delta(f) > 0$ then $A_{\mathbb{R}} \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. Let the first component of $A_{\mathbb{R}}$ correspond the smallest real root of f. Then $\bar{\lambda}_{\mathbb{R}}(E(\mathbb{R}))$ is of order 2, generated by $(1, -1, -1)(A_{\mathbb{R}}^*)^2$*

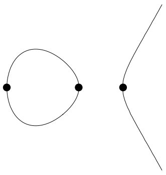
Proof. The first statement is clear, since $\mathbb{C}$ is algebraically closed.

Suppose $\Delta(f) < 0$. Then $f(T) = (T - a)g(T)$ where $g(T)$ is irreducible over $\mathbb{R}$. In this case $A_{\mathbb{R}} \cong \mathbb{R} \oplus \mathbb{C}$. Since all elements of $\mathbb{C}$ are squares, $\bar{\lambda}_{\mathbb{R}}(E(\mathbb{R}))$ is trivial in the second component. Let a be the real root of f. A sketch of the real locus of E



shows that $x(P) - a > 0$ for all $P \in E(\mathbb{R})$ not equal to $(a, 0)$. By definition of $\lambda_{\mathbb{R}}(a, 0)$, the first component must be positive. Since all positive elements of $\mathbb{R}$ are squares, $\bar{\lambda}_{\mathbb{R}}(E(\mathbb{R})) = (1, 1)$.

Now suppose that $\Delta(f) > 0$. Then $f(T) = (T - a)(T - b)(T - c)$ with $a < b < c \in \mathbb{R}$ and $A_{\mathbb{R}} \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. A sketch of the real locus of E



shows that every element of the right-hand segment is trivial in $2E(\mathbb{R})$. For any $P \notin \{(a, 0), (b, 0)\}$ lying in the left-hand segment, $x(P) - a > 0$, $x(P) - b < 0$ and $x(P) - c < 0$, and so $\bar{\lambda}_{\mathbb{R}}(P) = (1, -1, -1)$. From the definition, $\bar{\lambda}_{\mathbb{R}}(a, 0)$ and $\bar{\lambda}_{\mathbb{R}}(b, 0)$ have the form $(+, -, -)$ as required.

□

The analysis of $E(K_v)/2E(K_v)$ could be taken further, and the primes over 2 and those of bad reduction dealt with. We will not go into this detail, since it will add little to the general discussion of 2 descent. The case of multiplicative reduction and of reduction over 2 is dealt with in detail in Brumer and Kramer [2]. In our examples, knowing the size of $\lambda_{K_v}(E(K_v)/2E(K_v))$ will be enough to determine the group for places of bad reduction.

Remark. It may seem that λ_k is non-canonical, as it depends on the choice of Weierstrass model for E. In Section 4 we will prove the equivalence of λ_k with a map defined intrinsically on E, thus showing independence of our results from any particular model for E.

1.4 Torsion Contribution

If we are to make the weak Mordell-Weil Theorem effective, we must also be able to calculate the contribution to $E(K)/2E(K)$ from the torsion subgroup. Since $E(K)$ is finitely generated, the torsion subgroup is finite, and the exact sequence

$$0 \to E(K)[2] \to E(K)_{\text{tors}} \to E(K)_{\text{tors}} \to E(K)_{\text{tors}}/2E(K)_{\text{tors}} \to 0 \tag{1.34}$$

$\Rightarrow \#E(K)_{\text{tors}}/2E(K)_{\text{tors}} = \#E(K)[2]$. Thus to know the contribution of torsion to $E(K)/2E(K)$, it suffices to know the size of the 2-torsion subgroup, which is easy to calculate.

Although we only need to understand the 2-torsion to use $E(K)/2E(K)$ to give an upper bound for r, we will be interested in computing the torsion subgroup in full, as in many examples this will enable us to give the structure of $E(K)$ as an abstract group. There is only one result we need.

Proposition 1.4.1. *Let v be a finite place of a number field K, and suppose that E/K has good reduction at v. Let $m \in \mathbb{N}$ with $v(m) = 0$. Then $E(K)[m]$ injects into $\tilde{E}(k_v)$*

Proof. Since $E(K) \hookrightarrow E(K_v)$ it suffices to prove the result for K_v, the completion of K at v. The kernel of reduction is the formal group $\hat{E}(\mathfrak{m}_v)$, which has no non-trivial m-torsion if $v(m) = 0$. □

1.5 Rank Computations

In this section we use our results proved so far to illustrate the method of computing ranks of elliptic curves.

Example. We compute the Mordell-Weil group of the curve

$$E/\mathbb{Q} : y^2 = x(x+5)(x-5) = x^3 - 25x \tag{1.35}$$

This has good reduction away from $2, 5$, and $A_{\mathbb{Q}} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$. For all primes $p \neq 2, 5$, each component in the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ is divisible by 2 and 5 only.

$\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^2 = \langle 2, 5 \rangle$, and $\#E(\mathbb{Q}_5)/2E(\mathbb{Q}_5) = 4$. It follows that the image of $E(\mathbb{Q}_5)/2E(\mathbb{Q}_5)$ in $A^*_{\mathbb{Q}_5}/(A^*_{\mathbb{Q}_5})^2$ consists precisely of the elements $(1,1,1)$, $(5,1,5)$, $(2,5,10)$, $(10,5,2)$ given by the four 2-torsion points. Thus all elements of the Selmer group are of the form $(\pm1,\pm1,\pm1)$, $(\pm5,\pm1,\pm5)$, $(\pm2,\pm5,\pm10)$, $(\pm10,\pm5,\pm2)$. The group $\lambda_{\mathbb{R}}(E(\mathbb{R})/2E(\mathbb{R}))$ is of order two, and consists of the elements $(1,1,1)$ and $(1,-1,-1)$. Thus the Selmer group is of order at most 8, and consists at most of the elements $(1,1,1)$, $(5,1,5)$, $(2,5,10)$, $(10,5,2)$, $(1,-1,-1)$, $(5,-1,-5)$, $(2,-5,-10)$, $(10,5,2)$.

The 2-torsion of E is all defined over $\mathbb{Q}$, so $E[2]$ generates a subgroup of $S^2(E,\mathbb{Q})$ of order 4. Thus the rank of E is ≤ 1. The point $P = (-\frac{5}{9}, \frac{100}{27})$ cannot be a torsion point, since it's image under $\lambda_{\mathbb{Q}}$ is independent of the image of $E(\mathbb{Q})[2]$. Thus the rank of $E(\mathbb{Q})$ is 1.

To fully determine the structure of $E(\mathbb{Q})$, it remains to calculate the torsion subgroup. The curve has good reduction at 3, and $\#\tilde{E}(\mathbb{F}_3) = 4$. Hence there can be no exact p-torsion for $p \neq 2, 3$. $E(\mathbb{Q})[3] \hookrightarrow \tilde{E}(\mathbb{F}_7)$, which has order 8, hence there can be no 3-torsion. Thus there is only 2-power torsion, which injects into a group of order 4. Thus $E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})[2] = (O, (0,0), (5,0), (-5,0))$. Hence $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Example. We compute the Mordell-Weil group of the curve

$$E/\mathbb{Q} : y^2 = x^3 + x = x(x+i)(x-i) \tag{1.36}$$

This has good reduction away from 2, and $A_{\mathbb{Q}} \cong \mathbb{Q} \oplus \mathbb{Q}(i)$. Elements of $S^2(E, \mathbb{Q})$ have $\{1, 2\}$ in the first component, and $\{1, i, 1+i, 1-i\}$ in the second. The norm condition reduces to the possibilities $(1,1), (1,i), (2, 1+i), (2, 1-i)$. The group $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ has order 4, generated by the images of $(0,0)$ and $(\frac{1}{8}, \epsilon)$. The group $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ has order 8 and is generated by $2, 3, 5$. The group $\mathbb{Q}_2(1+i)^*/(\mathbb{Q}_2(1+i)^*)^2$ has order 16.

The image of $E(\mathbb{Q}_2)/2E(\mathbb{Q})_2$ in $A_{\mathbb{Q}_2}$ consists of the four points $(1,1), (1,i), (2, 8+i), (2, 1-8i)$. It thus remains to check whether $9-7i, 7+9i$ are squares in $\mathbb{Z}_2[i]$. They cannot be since $7, 9$ are both coprime to 2. Hence only $(1,1), (1,i)$ can lie in the image locally at 2. The image of $\lambda_{\mathbb{R}}$ is trivial in this case, and the Selmer group is precisely $\{(1,1), (1,i)\}$. We have the 2-torsion point $(0,0)$ defined over $\mathbb{Q}$, and thus the rank of $E(\mathbb{Q})$ is 0. To determine the torsion, note $\#\tilde{E}(\mathbb{F}_3) = 2$ and $\#\tilde{E}(\mathbb{F}_5) = 4$, hence there can be at most 2-power torsion, which injects into a group of order 2. Thus $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$.

Example. We calculate the Mordell-Weil group of the curve

$$E/\mathbb{Q} : y^2 = x^3 - 2 \tag{1.37}$$

In this case $A_{\mathbb{Q}} \cong \mathbb{Q}(\sqrt[3]{2})$ is a field, with class number 1. E has good reduction away from $2, 3$. The only prime lying above 2 in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$ and the only prime lying above 3 is $\sqrt[3]{2}+1$. The group of units in $\mathbb{Q}(\sqrt[3]{2})$ is $\{1, -1\} \times \mathbb{Z}$, and a fundamental unit is $\sqrt[3]{2}-1$. Thus the Selmer group is generated by -1, $\sqrt[3]{2}-1$, $\sqrt[3]{2}+1$, $\sqrt[3]{2}$. The norm condition excludes all but $\sqrt[3]{2}-1$. Thus the Selmer group has size ≤ 2.

The curve has good reduction at $5, 7$, and $\#\tilde{E}(\mathbb{F}_5) = 6$, $\tilde{E}(\mathbb{F}_7) = 7$. Thus $E(\mathbb{Q})_{\text{tors}}$ is trivial. The point $P = (3, 5)$ in $E(\mathbb{Q})$, so the rank of $E(\mathbb{Q})$ is exactly 1 and $E(\mathbb{Q}) \cong \mathbb{Z}$.

In all these examples we took advantage of the fact that all number fields considered had class number 1, which simplifies the calculations. In general it can be harder to perform a successful 2-descent.

2 Hyperelliptic Curves and their Jacobians

In this section we introduce our objects of study for the remainder of this essay, namely hyperelliptic curves and their Jacobians. Elliptic curves (over fields of characteristic $\neq 2$) are given by equations of the form $y^2 = f(x)$ where f is a cubic polynomial with distinct roots. Hyperelliptic curves arise when we let f be an polynomial of arbitrary degree. As in the elliptic case, f having distinct roots is equivalent to the affine curve $y^2 = f(x)$ being non-singular. In the hyperelliptic case there is an extra complication in the fact that points at infinity are singular if $\deg f \geq 4$.

Hyperelliptic curves (of genus > 1) no longer posses a group structure, and instead we consider the Picard group $\mathrm{Pic}^0(C)$ of degree zero divisors modulo linear equivalence. This is a generalisation of the group structure of an elliptic curve E, since in this case we have an isomorphism of $\mathrm{Gal}(\bar{k}/k)$-modules $E \cong \mathrm{Pic}^0(E)$. The Jacobain of the curve C is a way of assigning a group variety structure to $\mathrm{Pic}^0(C)$. Since we will eventually be interested in the method of 2-descent, we will concentrate only on hyperelliptic curves defined over fields of characteristic zero, the main motivation being algebraic extensions of $\mathbb{Q}$ and $\mathbb{Q}_p$, and their residue fields. k will denote a field of characteristic zero, and $G_k = \mathrm{Gal}(\bar{k}/k)$ its absolute Galois group.

Denote the group of degree zero divisors of C by $\mathrm{Div}^0(C)$, and its G_k invariants by $\mathrm{Div}^0_k(C)$. We will denote by $\mathrm{Pic}^0_k(C)$ the group $\mathrm{Div}^0_k(C)$ modulo linear equivalence, note than in general this is only a subgroup of the G_k-invariants of $\mathrm{Pic}^0(C)$. We will return to this point later.

2.1 Hyperelliptic Curves

Definition. A hyperelliptic curve C/k is a projective plane curve of the form $y^2 = f(x)$, for some $f \in k[x]$ with distinct roots in $\bar{k}$.

The more highbrow definition of a hyperelliptic curve is a (smooth, projective) curve C together with a separable degree 2 morphism $C \to \mathbb{P}^1$. It is easily seen (in characteristic zero) that any such curve is birational to a plane curve of the form $y^2 = f(x)$. f having distinct roots is equivalent to the affine curve $y^2 = f(x)$ being non-singular, however, if $\deg f \geq 4$ then the unique point at infinity $[0 : 1 : 0]$ on the projective completion is singular. Suppose that C has the form

$$y^2 = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1} + \ldots + a_0 \tag{2.1}$$

where $a_{2g+1}a_{2g+2} \neq 0$ but either a_{2g+2} or a_{2g+1} may be zero. Thus C has genus g. Consider the curve $C^\# \subset \mathbb{P}^{g+1}$ defined by

$$\begin{aligned} Y^2 &= a_{2g+2}X_{g+1}^2 + a_{2g+1}X_{g+1}X_g + \ldots + a_1X_1X_0 + a_0X_0^2 \\ X_0X_2 &= X_1^2\ ,\ X_2^2 = X_1X_3\ ,\ \ldots\ ,\ X_1X_g = X_{g+1}X_0 \end{aligned} \tag{2.2}$$

It is readily checked that this curve is non-singular. There are rational maps $\phi : C^\# \to C$ and $\psi : C \to C^\#$ defined by

$$\begin{aligned} \phi([X_0 : \ldots : X_{g+1} : Y]) &= [X_1 : Y : X_0] \\ \psi([X : Y : Z]) &= [Z^{g+1} : XZ^g : \ldots : X^{g+1} : YZ^g] \end{aligned} \tag{2.3}$$

These are easily seen to be rational inverses, and induce isomorphisms

$$C^{\#} \setminus \phi^{-1}([0:1:0]) \leftrightarrow C \setminus [0:1:0] \tag{2.4}$$

A quick calculation shows that $\phi^{-1}([0:1:0])$ consists of the point(s) $[0:\ldots:1:\pm\sqrt{a_{2g+2}}]$. Thus if $\deg f$ is odd there exists exactly one point of $C^{\#}$ lying above $[0:1:0]$, and this point is k-rational, if $\deg f$ is even there are two points of $C^{\#}$ lying above $[0:1:0]$, defined over the field $k(\sqrt{a_{2g+2}})$, and conjugate over k.

2.2 Jacobian Varieties

For an elliptic curve E/k with specified point $O \in E(k)$, we have a G_k-module isomorphism $E \to \mathrm{Pic}^0(E)$, $P \mapsto [(P)-(O)]$. Thus $\mathrm{Pic}^0(E)$ has the structure of an abelian variety defined over k. This is true for any (smooth, projective) curve C/k of genus g. There exists an projective abelian variety J/k of dimension g, defined over k together with a G_k-module isomorphism $J \to \mathrm{Pic}^0(C)$. This variety is called the Jacobian of C. For any $P_0 \in C$ there exists an injective morphism $C \hookrightarrow J$ induced by $C \hookrightarrow \mathrm{Pic}^0(C), P \mapsto [(P)-(P_0)]$. This is defined over $k \Leftrightarrow P_0 \in C(k)$.

In the elliptic curve case, every k-rational divisor class in $\mathrm{Pic}^0(C)$ contains a k-rational divisor, i.e. $\mathrm{Pic}^0_k(C)$ is the full group of G_k invariants of $\mathrm{Pic}^0(C)$, but this is not true in general. If we make the additional assumption that $C(k) \neq \emptyset$, then in fact $(\mathrm{Pic}^0(C))^{G_k} = \mathrm{Pic}^0_k(C)$, and hence we can identify $J(L)$ with $\mathrm{Pic}^0_L(C)$ for any algebraic extension L of k. For more details, and for a description of how to construct J, see Milne [10], Chapter 3.

We will not prove the existence of such an variety J, instead we will simply identify it with $\mathrm{Pic}^0(C)$, and use it as another notation for this group. In this section and the next we gather together results about Jacobian varieties generalising those used in Section 1 for elliptic curves. Unless otherwise stated, C will be a hyperelliptic curve of genus g defined over a field k of characteristic zero and J its Jacobian. Since we wish to identify $J(k)$ and $\mathrm{Pic}^0_k(C)$, we will make the additional assumption that $C(k) \neq \emptyset$. This is automatically satisfies if C is of the form $y^2 = f(x)$ with $\deg f$ odd, as the point at infinity $[0:1:0]$ is always k-rational. If $\deg f$ is even, however, then $C(k)$ could be empty. Our first result shows that we have a Weil pairing defined for Jacobians. We will require this in Section 4.

Theorem 2.2.1. *(Weil Pairing). There exists an alternating, bilinear, non-degenerate, G_k-invariant pairing*

$$e_m : J[m] \times J[m] \to \mu_m(\bar{k}) \tag{2.5}$$

Proof. (Sketch) Let $S, T \in J[m]$ be represented by divisors D_S, D_T. Pick functions $f_S, f_T \in \bar{k}(C)$ with $mD_S = \mathrm{div} f_S$, $mD_T = \mathrm{div} f_T$, and $\mathrm{div} f_S \cap D_T = \mathrm{div} f_T \cap D_S = \emptyset$. Define $e_m(S,T) = (f_S(D_T))/(f_T(D_S))$. Using Weil reciprocity it can be checked that this is well-defined (i.e. independent of the choices of D_S, D_T, f_S, f_T) and satisfies all the properties claimed. □

The following representation of points in $J(k)$ will also be useful.

Lemma 2.2.2. *Let $D \in \mathrm{Div}^0_k(C)$.*

1. *Suppose $\deg f$ is odd, i.e. there exists a unique point ∞ at infinity. Then D is linearly equivalent to a k-rational divisor of the form $(P_1)+\ldots+(P_g) - g(\infty)$ with $P_i \in C$.*
2. *Suppose that $\deg f$ is even, i.e. there exists two distinct points $\infty^{\pm}$ at infinity. Then D is linearly equivalent to a k-rational divisor of the form $(P_1)+\ldots+(P_{2r}) - r((\infty^+)+(\infty^-))$.*

Proof. 1. By Riemann-Roch, $\ell(D+g(\infty)) \geq \deg(D+g(\infty))+1-g \geq 1$ and there exists $h \in k(C)$ such that $\mathrm{div} h + D + n(\infty) \geq 0$. ($h$ is k-rational since $D+g(\infty)$ is). Thus $\mathrm{div} h + D + g(\infty)$ is an effective divisor of degree g, thus of the form $(P_1)+\ldots+(P_g)$ for $P_i \in C$. $(P_1)+\ldots+(P_g)-g(\infty)$ is k-rational as D and h are.

2. Similar, considering the divisor $D + r((\infty^+) + (\infty^-))$ for $2r \geq g$.

□

Our most useful tool in the study of elliptic curves over number fields was the exact sequence

$$0 \to E_1(K_v) \to E_0(K_v) \to \tilde{E}_{\mathrm{ns}}(k_v) \to 0 \tag{2.6}$$

for finite places v of k, together with the isomorphism $E_1(K_v) \cong \hat{E}(\mathfrak{m}_v)$ of $E_1(K_v)$ with a formal group. We also used the corresponding results with K_v replaced by its maximal unramified extension, to calculate the group $E(K_v)/2E(K_v)$ for primes (not lying above 2) of good reduction. This reduced the computation of $S^2(E, K)$ to consideration of a finite number of primes. The theory for Jacobians is far more involved, and we give here the briefest sketch of the results that we require.

2.3 Neron Models

Let K be a number field and C/K a hyperelliptic curve defined over K, with Jacobian J. For any finite place v of K we consider J as an abelian variety over K_v.

Theorem 2.3.1. *There exists a unique smooth, commutative group scheme $\mathcal{J}$ over $\mathrm{Spec}(\mathcal{O}_v)$, the Neron model of J/K_v, satisfying the following conditions.*

1. *The generic fibre $\mathcal{J}_{(0)} = \mathcal{J} \times_{\mathcal{O}_v} K_v$ is isomorphic to J.*
2. *For any smooth morphism $S \to \mathrm{Spec}(\mathcal{O}_v)$ the natural map $\mathrm{Hom}_{\mathcal{O}_v}(S, \mathcal{J}) \to \mathrm{Hom}_K(S \times_{\mathcal{O}_v} K_v, J)$ is bijective.*

Proof. This holds more generally for any abelian variety, for proof see Bosch, Lütkebohmert and Raynaud [1]. □

To explain this last condition, if $S \to \mathcal{J}$ is an $\mathcal{O}_v$-morphism, then composing this with the projection map $S \times_{\mathcal{O}_v} K_v \to S$ we get an $\mathcal{O}_v$-morphism $S \times_{\mathcal{O}_v} K_v \to \mathcal{J}$. We also have the projection morphism $S \times_{\mathcal{O}_v} K_v \to \mathrm{Spec}(K_v)$, and hence by the defining property of $\mathcal{J} \times_{\mathcal{O}_v} K_v$ we get an $\mathcal{O}_v$-morphism $S \times_{\mathcal{O}_v} K_v \to \mathcal{J} \times_{\mathcal{O}_v} K_v \cong J$. Condition 2. states that for any smooth $\mathcal{O}_v$-scheme S we have a bijection $\mathcal{J}(S) \leftrightarrow J(S \times_{\mathcal{O}_v} K_v)$ between the set of S valued points of $\mathcal{J}$ and the set of $S \times_{\mathcal{O}_v} K_v$ valued points of J. Taking $S = \mathrm{Spec}(\mathcal{O}_v)$ gives a bijection $\mathcal{J}(\mathcal{O}_v) \leftrightarrow J(K_v)$.

The special fibre $\mathcal{J}_v = \mathcal{J} \times_{\mathcal{O}_v} k_v$ is a group scheme over k_v. As before we have a natural map $\mathcal{J}(S) \to \mathcal{J}_v(S \times_{\mathcal{O}_v} k_v)$ for any smooth $\mathcal{O}_v$-scheme S, and taking $S = \mathrm{Spec}(\mathcal{O}_v)$ gives $\mathcal{J}(\mathcal{O}_v) \to \mathcal{J}_v(k_v)$. Thus by composing with the bijection $\mathcal{J}(\mathcal{O}_v) \leftrightarrow J(K_v)$ we get the reduction map $J(K_v) \to \mathcal{J}_v(k_v)$ which is the analogue of the usual reduction map $E(K_v) \to \tilde{E}(k_v)$ in the case of elliptic curves. We denote the connected component of $\mathcal{J}_v$ containing the identity by $\mathcal{J}_v^0$, and the component group $\mathcal{J}_v/\mathcal{J}_v^0$ by Φ_v. Let $J_0(K_v)$ denote the subgroup of $J(K_v)$ whose reduction lies in $\mathcal{J}_v^0(k_v)$, and $J_1(K_v)$ the kernel of reduction.

Theorem 2.3.2. *The following sequences are exact*

$$\begin{aligned} 0 \to J_0(K_v) \to J(K_v) \to \Phi_v(k_v) \to 0 \\ 0 \to J_1(K_v) \to J_0(K_v) \to \mathcal{J}_v^0(k_v) \to 0 \end{aligned} \tag{2.7}$$

There are two more results we require, one giving an isomorphism of $J_1(K_v)$ with a formal group and another giving a condition for 'good reduction' of $\mathcal{J}$ in terms of reduction of the curve C.

Theorem 2.3.3. 1. *There exists a g-parameter formal group $\mathcal{F} \in \mathcal{O}_v[[T_1, S_1, \ldots, T_g, S_g]]$ and an isomorphism $\mathcal{F}(\mathfrak{m}_v) \xrightarrow{\sim} J_1(K_v)$.*

2. *Let v be a finite place of the number field K, not dividing $2\Delta_f$. Then $\mathcal{J}_v^0 = \mathcal{J}_v$.*

3 Mordell-Weil and 2-Descent for Jacobians

In this Section we describe how the methods and results of Section 1 generalise to Jacobians of hyperelliptic curves of the form $y^2 = f(x)$. There are two distinct cases to consider, depending on whether $\deg f$ is even or odd. Although the basic ideas are the same in both cases, the extra points at infinity in the even degree case complicate matters. The odd degree case is simpler, and a more direct generalisation, and this is the case we deal with first.

3.1 The Odd Degree Case - Generalities

In this section, we will construct an analogous map to λ_k defined in the case of elliptic curves. Let k be an arbitrary field of characteristic zero, and G_k its absolute Galois group. C will denote the hyperelliptic curve $y^2 = f(x)$ defined over k, and J its Jacobian. Assume that $d = \deg f$ is odd, thus C has genus $g = \frac{1}{2}(d-1)$ and there is a single point ∞ at infinity, which lies in $C(k)$. By a change of co-ordinates, we may assume that the leading coefficient of f is 1. In general we follow Schaefer [12].

As before, define the k-algebra $A_k = k[T]/(f(T))$, a direct sum of fields, one for each irreducible factor of $f(T)$ over k. Denote by Θ the image of T in A_k. We have the norm map $\mathrm{N}_{A_k/k} : A_k \to k$, which is multiplicative, $\mathrm{N}_{A_k/k}(a - \Theta) = f(a)$ for $a \in k$, and $\alpha \in A_k^* \Leftrightarrow \mathrm{N}_{A_k/k}(\alpha) \in k^*$. Denote by $\mathrm{Div}_0^k(C)^\dagger$ the subgroup of $\mathrm{Div}_0^k(C)$ consisting of divisors whose support is disjoint from the Weierstrass points of C, i.e. those with y co-ordinate 0 or ∞. Define

$$\begin{aligned} \lambda_k : \mathrm{Div}_k^0(C)^\dagger &\to A_k \\ \sum_i n_i(P_i) &\mapsto \prod_i (x(P_i) - \Theta)^{n_i} \end{aligned} \tag{3.1}$$

We must check this is well defined, since *a priori* this is only a map to $A_{\bar{k}} = \bar{k}[T]/(f(T)) \cong \bar{k}^d$. $A_{\bar{k}}$ becomes a G_k-module via the action of G_k on $\bar{k}[T]$. The action of G_k is simply to permute the direct summands of $A_{\bar{k}}$ and the set of invariants is $A_k \subset A_{\bar{k}}$. If $D = \sum_i n_i(P_i) \in \mathrm{Div}_k^0(C)^\dagger$ is a k-rational divisor, then for any $\sigma \in G_k$

$$\begin{aligned} {}^\sigma\lambda_k(D) &= {}^\sigma \prod_i (x(P_i) - \Theta)^{n_i} = \prod_i {}^\sigma(x(P_i) - \Theta)^{n_i} \\ &= \prod_i ({}^\sigma x(P_i) - \Theta)^{n_i} = \prod_i (x({}^\sigma P_i) - \Theta)^{n_i} \\ &= \lambda_k({}^\sigma D) = \lambda_k(D) \end{aligned} \tag{3.2}$$

hence $\lambda_k(D)$ is G_k-invariant, and thus in A_k.

Lemma 3.1.1. *The image of λ_k lies in the subgroup $\{\alpha \in A_k \mid \mathrm{N}_{A_k/k}(\alpha) \in (k^*)^2\} \subset A_k$.*

Proof. Let $D = \sum_i n_i(P_i) \in \mathrm{Div}_k^0(C)^\dagger$, with $y(P_i) \in \bar{k}^*$ for all i. We calculate

$$\mathrm{N}_{A_k/k}(\lambda_k(D)) = \mathrm{N}_{A_k/k}\left(\prod_i (x(P_i)-\Theta)^{n_i}\right) = \prod_i \left(\mathrm{N}_{A_k/k}(x(P_i)-\Theta)\right)^{n_i} \tag{3.3}$$
$$= \prod_i f(x(P_i))^{n_i} = \prod_i y(P_i)^{2n_i} = \left(\prod_i y(P_i)^{n_i}\right)^2$$

As D is G_k-invariant, $\prod_i y(P_i)^{n_i} \in k^*$ and hence $\lambda_k(D) \in (k^*)^2$. □

Proposition 3.1.2. *The map λ_k induces a homomorphism $\lambda_k : J(k)/2J(k) \to A_k^*/(A_k^*)^2$*

Proof. $\lambda_k : \mathrm{Div}_k^0(C)^\dagger \to A_k^*/(A_k^*)^2$ is clearly a homomorphism, we claim that for every divisor class in $\mathrm{Pic}_k^0(C)$ we can pick a representative lying in $\mathrm{Div}_k^0(C)^\dagger$. Since there are only finitely many Weierstrass point, this follows from [8], p. 166.

It remains to show that any principal divisor div$f$ in $\mathrm{Div}_k^0(C)^\dagger$ has $\lambda_k(\mathrm{div}f) \in (A_k^*)^2$. It suffices to prove this on each direct summand of A_k. Let $A_k = \bigoplus_{i=1}^n L_i$, $L_i = k(\alpha_i)$. By Weil reciprocity, the ith component of $\lambda_k(\mathrm{div}f)$ satisfies $(\lambda_k(\mathrm{div}f))_i = (x-\alpha_i)(\mathrm{div}f) = f(\mathrm{div}(x-\alpha_i)) = f(2(\alpha_i,0)-2(\infty)) = f((\alpha_i,0)-(\infty))^2 \in (L_i^*)^2$. □

We will not prove here that the map $J(k)/2J(k)$ is injective, it will follow immediately from the cohomological interpretation we will describe in Section 4.

It may appear initially that our map is not strictly a generalisation of that defined in Section 1. If weview points of our elliptic curves as classes of divisors, via $P \mapsto [(P)-(O)]$, then our new definition does not make sense for divisors of this kind, since O is a Weierstrass point of the curve. We have thus defined *a priori* two different maps $E(k)/2E(k) \to A_k^*/(A_k^*)^2$ for elliptic curves, one via $x-\Theta$ on the point P, and another via $x-\Theta$ on a divisor linearly equivalent to $(P)-(O)$. The following Proposition tells us that the two maps are actually the same.

Proposition 3.1.3. *Let $D = (Q_1)+\cdots+(Q_N) - N(\infty)$ be a k-rational divisor, with no Q_i a Weierstrass point. Then*

$$\lambda_k(D) \equiv \prod_{i=1}^N (x(Q_i)-\Theta) \bmod (A_k^*)^2 \tag{3.4}$$

Proof. By dividing into orbits under the action of $\mathrm{Gal}(\bar{k}/k)$ we may assume that D takes the form $D = ({}^{\sigma_1}Q)+\cdots+({}^{\sigma_n}Q) - n(\infty)$, where the σ_i run over all embeddings $k(Q) \hookrightarrow \bar{k}$. Suppose that $Q=(a,b)$ and let $R=(a,-b)$. Let $Q=Q_1,Q_2,\ldots,Q_d$ be the d points of $C(\bar{k})$ (with multiplicities) satisfying $y(Q_j)=b$, and for each j define $\bar{Q}_j$ to be the divisor $\sum_{i=1}^n({}^{\sigma_i}Q_j)$. Also define $\bar{R} = \sum_{i=1}^n({}^{\sigma_i}R)$. Note that $D = \bar{Q}_1 - n(\infty)$. Consider the functions

$$h_1 = \prod_{i=1}^n \frac{1}{y-\sigma_i(b)} \; h_2 = \prod_{i=1}^n (x-\sigma_i(a))^g \tag{3.5}$$

Both are visibly Galois invariant and hence defined over k. They have divisors

$$\mathrm{div}h_1 = dn(\infty) - \sum_{j=1}^d (\bar{Q}_j) \tag{3.6}$$
$$\mathrm{div}h_2 = g\bar{Q}_1 + g\bar{R} - 2gn(\infty)$$

Thus adding the principal divisor $\mathrm{div}(h_1h_2)$ to $D = \bar{Q}_1 - n(\infty)$ shows that

$$D \sim g\bar{Q}_1 - \bar{Q}_2 - \ldots - \bar{Q}_d + g\bar{R} \tag{3.7}$$

(Note that $2g+1=d$). Since $y(Q_j)=b\neq 0,\infty$ and $y(R)=-b\neq 0,\infty$, each $\bar{Q}_j$ and $\bar{R}$ has support disjoint from Weierstrass points. Hence $g\bar{Q}_1-\bar{Q}_2-\ldots-\bar{Q}_d+g\bar{R}$ has support disjoint from Weierstrass points, and we can evaluate λ_k on it. Thus

$$\begin{aligned}\lambda_k(D)=\lambda_k(g\bar{Q}_1-\bar{Q}_2-\ldots-\bar{Q}_d+g\bar{R}) &= \frac{(\lambda_k(\bar{Q}_1)\lambda_k(\bar{R}))^g}{\lambda_k(\bar{Q}_2)\ldots\lambda_k(\bar{Q}_d)} \qquad (3.8)\\ =\prod_{i=1}^{n}\frac{(x({}^{\sigma_i}Q)-\Theta)^g(x({}^{\sigma_i}R)-\Theta)^g}{(x({}^{\sigma_i}Q_2)-\Theta)\ldots(x({}^{\sigma_i}Q_d)-\Theta)} &= \prod_{i=1}^{n}\frac{(x({}^{\sigma_i}Q)-\Theta)^{2g}}{(x({}^{\sigma_i}Q_2)-\Theta)\ldots(x({}^{\sigma_i}Q_d)-\Theta)}\\ =\prod_{i=1}^{n}\frac{(x({}^{\sigma_i}Q)-\Theta)^{2g+1}}{(x({}^{\sigma_i}Q_1)-\Theta)\ldots(x({}^{\sigma_i}Q_d)-\Theta)} &= \prod_{i=1}^{n}\frac{(x({}^{\sigma_i}Q)-\Theta)^{2g+1}}{y({}^{\sigma_i}Q)^2}\\ \equiv\prod_{i=1}^{n}(x({}^{\sigma_i}Q)-\Theta) \bmod (A_k^*)^2 &\end{aligned}$$

□

One can go further, and show that the new map agrees with the 'patched' definition of Section 1 on 2-torsion points. Let $\alpha_1,\ldots\alpha_d$ be the roots of f over $\bar{k}$.

Proposition 3.1.4. *Let $\pi\in S_d$ be a permutation, and $D=(\alpha_{\pi(1)},0)+\cdots+(\alpha_{\pi(r)},0)-r(\infty)$ a k-rational divisor. Then*

$$\lambda_k(D)\equiv\prod_{i=1}^{r}(\alpha_{\pi(i)}-\Theta)+\prod_{i=r+1}^{d}(\alpha_{\pi(i)}-\Theta) \bmod (A_k^*)^2 \qquad (3.9)$$

Proof. See Schaefer [12], Lemma 2.2. □

The final general result we require is a description of the 2-torsion subgroup of J, which tells us the size of the torsion contribution to $J(k)/2J(k)$.

Proposition 3.1.5. *The classes of $(\alpha_1,0)-(\infty),\ldots,(\alpha_{d-1},0)-(\infty)$ are an $\mathbb{F}_2$ basis for $J[2]$. $(\alpha_d,0)-(\infty)$ is linearly equivalent to $\sum_{i=1}^{d-1}(\alpha_i,0)-(\infty)$.*

Proof. $J[2]\cong(\mathbb{Z}/2\mathbb{Z})^{2g}$ (see Milne [10], Chapter 1), and we have $2(\alpha_i,0)-2(\infty)=\mathrm{div}(x-\alpha_i)$. Also, $\sum_{i=1}^{d}((\alpha_i,0)-(\infty))=\mathrm{div}f\Rightarrow\sum_{i=1}^{d-1}((\alpha_i,0)-(\infty))-((\alpha_d,0)-(\infty))=\mathrm{div}\left(\frac{f}{x-\alpha_d}\right)$

It thus suffices to show that the classes of $\{(\alpha_i,0)-(\infty)\mid 1\leq i\leq d\}$ span $J[2]$, for proof see Shaefer [13], Proposition 3.2. □

Corollary 3.1.6. *Suppose that f factors as $f_1\ldots f_m$ over k, with each f_i irreducible. Then $J(k)[2]$ has as an $\mathbb{F}_2$ basis the classes of the divisors $\{D_j:=\sum_{f_j(\alpha)=0}((\alpha,0)-(\infty))\mid 1\leq j\leq m-1\}$. The divisor $D_m:=\sum_{f_m(\alpha)=0}((\alpha,0)-(\infty))$ is linearly equivalent to $\sum_{j=1}^{m-1}D_j$.*

Proof. A divisor $\sum_i((\alpha_{n_i},0)-(\infty))$ is k-rational $\Leftrightarrow$ the α_{n_i} form a G_k sub-orbit of all the α_i $\Leftrightarrow$ $\prod_i(T-\alpha_{n_i})\in k[T]$. The result then follows from the previous Proposition and standard Galois theory. □

3.2 The Odd Degree Case - Number Fields

Now let K be a number field. Just as in the elliptic case, we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & J(K)/2J(K) \arrow[r, "\lambda_K"] \arrow[d, "\mathrm{res}"] & A_K^*/(A_K^*)^2 \arrow[d, "\mathrm{res}"] \\
0 \arrow[r] & \prod_v J(K_v)/2J(K_v) \arrow[r, "\prod_v \lambda_{K_v}"] & \prod_v A_{K_v}^*/(A_{K_v}^*)^2
\end{tikzcd} \tag{3.10}$$

where the product ranges over all places of K. As before, define the Selmer group

$$S^2(J,K) = \{\alpha \in A_K^*/(A_K^*)^2 \mid \mathrm{res}(\alpha) \in \mathrm{im}(\prod_v \lambda_{K_v})\} \tag{3.11}$$

Again (once we have proved injectivity of λ_K) we have $J(K)/2J(K) \hookrightarrow S^2(J,K)$, and we will estimate the rank of $J(K)$ by calculating the size of $S^2(J,K)$.

The generalisations to Jacobians of the classical exact sequences

$$\begin{aligned} 0 \to E_1(K_v) \to & E_0(K_v) \to \tilde{E}_{\mathrm{ns}}(k_v) \to 0 \\ 0 \to E_0(K_v) \to & E(K_v) \to E(K_v)/E_0(K_v) \to 0 \end{aligned} \tag{3.12}$$

and the formal group structure on $E_1(K_v)$, discussed in Section 2.3, show that all the results of Section 1.3 concerning the image of $E(K_v)/2E(K_v)$ for primes of good reduction carry over verbatim for Jacobians, with the same proofs.

In particular, let $\alpha \in S^2(J,K)$. Let $A_K = \bigoplus_{i=1}^n L_i$ be the decomposition of A_K as a direct sum of fields, and write $\alpha = (d_1, \ldots, d_n)$ in this decomposition. Then for all finite places v of L_i not dividing $2\Delta_f$, $v(d_i) \equiv 0 \bmod 2$. This suffices to prove finiteness of $S^2(J,K)$, in exactly the same way as for elliptic curves. Finally, we give an analogue of Proposition 1.3.8 describing the group $J(K_v)/2J(K_v)$ for infinite places v.

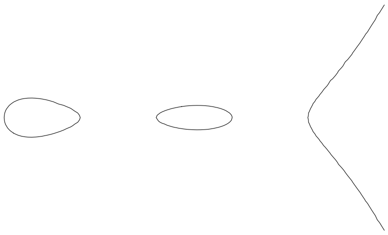
Proposition 3.2.1. *1. $A_\mathbb{C} \cong \mathbb{C}^d$ and $\lambda_\mathbb{C}(J(\mathbb{C})/2J(\mathbb{C}))$ is trivial.*

2. Suppose that f has $r = 2k+1$ roots over $\mathbb{R}$. Then $A_\mathbb{R} \cong \mathbb{R}^r \oplus \mathbb{C}^{g-k}$. Order the components of $A_\mathbb{R}$ isomorphic to $\mathbb{R}$ by increasing size of the corresponding roots of f. Then $\lambda_\mathbb{R}(J(\mathbb{R})/2J(\mathbb{R}))$ has order 2^k, with basis elements of the form

$$\begin{gathered} (1, \ldots, 1, -1, -1, 1 \ldots, 1) \\ (1, \ldots, 1, -1, -1, -1, -1, 1, \ldots, 1) \\ \vdots \\ (1, -1, \ldots, -1, -1, 1 \ldots, 1) \end{gathered} \tag{3.13}$$

Proof. 1. Clear since $\mathbb{C}$ is algebraically closed.

2. Lemma 3.2.2 below shows we only need to consider the image of divisors of the form $(P) - (\infty)$ for $P \in C(\mathbb{R})$, and Propositions 3.1.3 and 3.1.4 tell us the image of these divisors. The result follows from sketching the real locus of C.



Note that the number of connected components of $C(\mathbb{R})$ is $k+1$, and that the image of $\lambda_{\mathbb{R}}$ is trivial in all components of $A_{\mathbb{R}}$ isomorphic to $\mathbb{C}$. See the proof of Proposition 1.3.8 for comparison.

□

Lemma 3.2.2. *The image of $\lambda_{\mathbb{R}}$ is generated by the images of divisors of the form $(P)-(\infty)$, $P \in C(\mathbb{R})$.*

Proof. Let $D \in \mathrm{Div}^0_{\mathbb{R}}(C)$. By Lemma 2.2.2, we may assume that $D = (P_1) + \ldots + (P_n) - n(\infty)$. Divide D into $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ orbits, writing it as a sum of divisors of the form

- $(P)-(\infty)$ for $P \in C(\mathbb{R})$.
- $(P)+(\sigma P)-2(\infty)$ for $P \in C(\mathbb{C}) \setminus C(\mathbb{R})$ and $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, $\sigma \neq 1$.

We show that divisors of the second kind have trivial image in $A^*_{\mathbb{R}}/(A^*_{\mathbb{R}})^2$. If $y(P) \neq 0$ then Proposition 3.1.3 $\Rightarrow \lambda_{\mathbb{R}}((P)+(\sigma P)-2(\infty)) = (a-\Theta)(\bar{a}-\Theta)$ where $a = x(P)$. Clearly the image is a square in each component of $A_{\mathbb{R}}$ isomorphic to $\mathbb{C}$, so suppose that α is a real root of f. Then $(a-\alpha)(\bar{a}-\alpha)$ is positive, and hence trivial in $\mathbb{R}^*/(\mathbb{R}^*)^2$.

Suppose that $y(P)=0$, thus $P=(\beta,0)$ for some $\beta \in \mathbb{C}\setminus\mathbb{R}$. As before, the image is a square in each component of $A_{\mathbb{R}}$ isomorphic to $\mathbb{C}$, so let α be a real root of f. Then by Proposition 3.1.4, the image of $(P)+(\sigma P)-2(\infty)$ in the component of $A_{\mathbb{R}}$ corresponding to α is $(\beta-\alpha)(\bar{\beta}-\alpha)$ which again is positive and hence trivial in $\mathbb{R}^*/(\mathbb{R}^*)^2$. □

We finally remark that the contribution to $J(K)/2J(K)$ from torsion has size $\#J(K)[2]$, the proof is the same as in Section 1.4. We now use the ideas of this Section to calculate the Selmer group and rank of two Jacobians over $\mathbb{Q}$.

Example. We calculate the rank of $J(\mathbb{Q})$, where J is the Jacobian of the genus 2 curve

$$C/\mathbb{Q} : y^2 = x(x-2)(x-3)(x-6)(x-9) \tag{3.14}$$

The 2-torsion is all defined over $\mathbb{Q}$, and generates a subgroup of $J(\mathbb{Q})/2J(\mathbb{Q})$ of size 2^4. $A_{\mathbb{Q}} \cong \mathbb{Q}^5$ and $J/\mathbb{Q}$ has good reduction away from $2,3$. Thus $S^2(J,\mathbb{Q})$ is generated by $-1,2,3$ in each component. $\lambda_{\mathbb{R}}(J(\mathbb{R})/2J(\mathbb{R}))$ is generated by $(1,1,1,-1,-1)$ and $(1,-1,-1,-1,-1)$, and hence any element of $S^2(J,\mathbb{Q})$ has the form $(+,+,+,+,+)$, $(+,+,+,-,-)$, $(+,-,-,+,+)$ or $(+,-,-,-,-)$. $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ has order 2^6 and $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ has order 2^4. (To see this, modify the proof of Proposition 1.3.1 by taking a subgroup of finite index $\cong \mathcal{O}_v^g$). $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is generated by $-1,2,3$, and $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ is generated by $-1,3$.

The divisors $(0,0)-(\infty),(2,0)-(\infty)$ and $(6,0)-(\infty)$ generate a subgroup of order 2^3 inside $\lambda_{\mathbb{Q}_3}(J(\mathbb{Q}_3)/2J(\mathbb{Q}_3))$. By Hensel's Lemma one can check that there exists a point $P \in C(\mathbb{Q}_3)$ of the form $P = (-\frac{5}{2},\epsilon)$. Hence we have the following table giving generators of $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ and their images in $A^*_{\mathbb{Q}_3}/(A^*_{\mathbb{Q}_3})^2$. (It can be easily seen from the table that the images are linearly independent).

$\mathbb{Q}_3$	$x-0$	$x-2$	$x-3$	$x-6$	$x-9$
$(0,0)-(\infty)$	1	1	-3	3	-1
$(2,0)-(\infty)$	-1	1	-1	-1	-1
$(6,0)-(\infty)$	-3	1	3	3	-3
$(-9,\epsilon)-(\infty)$	-1	1	-3	3	1

(3.15)

The divisors $(0,0)-(\infty),(3,0)-(\infty)$ and $(6,0)-(\infty)$ generate a subgroup of order 2^3 inside $\lambda_{\mathbb{Q}_2}(J(\mathbb{Q}_2)/2J(\mathbb{Q}_2))$. By Hensel's Lemma, there exist points $P=(-5,\epsilon)$, $P'=(-6,\epsilon')$ and $P''=(-12,\epsilon'')$ in $C(\mathbb{Q}_2)$. Hence we have the following table giving generators of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ and their images in $A^*_{\mathbb{Q}_2}/(A^*_{\mathbb{Q}_2})^2$. (It can be seen from the table that the images are linearly independent).

$\mathbb{Q}_2$	$x-0$	$x-2$	$x-3$	$x-6$	$x-9$
$(0,0)-(\infty)$	1	-2	-3	-6	-1
$(3,0)-(\infty)$	3	1	6	-3	-6
$(6,0)-(\infty)$	6	1	3	-6	-3
$(-5,\epsilon)-(\infty)$	3	1	-2	-3	2
$(-6,\epsilon')-(\infty)$	-6	-2	-1	-3	1
$(-12,\epsilon'')-(\infty)$	-3	2	1	-2	3

(3.16)

We are now in a position to fully calculate the Selmer group $S^2(J,\mathbb{Q})$. For any $\alpha \in S^2(J,\mathbb{Q})$, each component lies in $\{\pm1,\pm2,\pm3,\pm6\}$, and hence the map $S^2(J,\mathbb{Q}) \to \lambda_{\mathbb{Q}_2}(J(\mathbb{Q}_2)/2J(\mathbb{Q}_2))$ tells us that $S^2(J,\mathbb{Q})$ lies in the subgroup of $A^*_{\mathbb{Q}}/(A^*_{\mathbb{Q}})^2$ generated by the 6 elements in Table 3.16. Writing out these 64 elements, we can see that only 16 of them have the allowed sign combinations, hence $\#(S^2(J,\mathbb{Q})) \leq 16$. Thus $J(\mathbb{Q})$ has rank zero, and $J(\mathbb{Q}) = J(\mathbb{Q})_{\text{tors}}$ is finite. Note that in particular, due to the injection $C \hookrightarrow J$, this implies that $C(\mathbb{Q})$ is finite, in accordance with Faltings' Theorem.

Example. We calculate the rank of $J(\mathbb{Q})$, where J is the Jacobian of the genus 2 curve

$$C/\mathbb{Q} : y^2 = (x^2-5)(x^3+10) \tag{3.17}$$

The algebra $A_{\mathbb{Q}}$ is isomorphic to $\mathbb{Q}(\sqrt{5}) \oplus \mathbb{Q}(\sqrt[3]{10})$. The discriminant of $f = (x^2-5)(x^3+10)$ is $\Delta_f = -2^4 3^3 5^7$, thus the primes of bad reduction are $2,3,5$. Both the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt[3]{10})$ have class number 1, and unit groups $\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$. A fundamental unit for $\mathbb{Q}(\sqrt{5})$ is $\eta := \frac{1}{2}(1+\sqrt{5})$, and one for $\mathbb{Q}(\sqrt[3]{10})$ is $\omega := \frac{1}{3}(23 + 11\sqrt[3]{10} + 5\sqrt[3]{10}^2)$. The primes $2,3,5$ factor in each field as follows.

	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt[3]{10})$
2	2	$p_1^3\omega^{-1}$
3	3	$p_2p_3^2$
5	$\sqrt{5}^2$	$p_4^3\omega$

(3.18)

where $p_1 = \frac{1}{3}(4 + \sqrt[3]{10} + \sqrt[3]{10}^2)$, $p_2 = \frac{1}{3}(1 - 2\sqrt[3]{10} + \sqrt[3]{10}^2)$, $p_3 = \frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{10}^2)$ and $p_4 = \frac{1}{3}(-5 + \sqrt[3]{10} + \sqrt[3]{10}^2)$. $J(\mathbb{Q})[2]$ has order 2, generated by $T = (\sqrt{5},0) + (-\sqrt{5},0) - 2(\infty)$. A quick computer search reveals the point $P = (i\sqrt{5}, -5i\sqrt{5}-5) + (-i\sqrt{5}, 5i\sqrt{5}-5) - 2(\infty) \in J(\mathbb{Q})$. f has 3 real roots and 2 complex roots, hence $A_{\mathbb{R}} \cong \mathbb{R}^3 \oplus \mathbb{C}$. Thus $A^*_{\mathbb{R}}/(A^*_{\mathbb{R}})^2$ has order 2, consisting of $(1,1,1,1)$ and $(1,-1,-1,1)$.

x^2-5 and x^3+10 are both irreducible over $\mathbb{Q}_5$, $A_{\mathbb{Q}_5} \cong \mathbb{Q}_5(\sqrt{5}) \oplus \mathbb{Q}_5(\sqrt[3]{10})$. Both fields are totally ramified over $\mathbb{Q}_5$. $\mathbb{Q}_5(\sqrt{5})^*/(\mathbb{Q}_5(\sqrt{5})^*)^2$ is generated by $\sqrt{5}, 2$ and $\mathbb{Q}_5(\sqrt[3]{10})^*/(\mathbb{Q}_5(\sqrt[3]{10})^*)^2$ is generated by $\sqrt[3]{10}, 2$. The following tables give the images of $-1, \eta, 2, 3, \sqrt{5}$, in $\mathbb{Q}_5(\sqrt{5})^*/(\mathbb{Q}_5(\sqrt{5})^*)^2$ and the images of $-1, \omega, p_1, p_2, p_3, p_4$ in $\mathbb{Q}_5(\sqrt[3]{10})^*/(\mathbb{Q}_5(\sqrt[3]{10})^*)^2$.

-1	1
η	2
2	2
3	2
$\sqrt{5}$	$\sqrt{5}$

-1	1
ω	1
p_1	2
p_2	2
p_3	2
p_4	$2\sqrt[3]{10}$

(3.19)

$J(\mathbb{Q}_5)/2J(\mathbb{Q}_5))$ has order 2, and the image of P in $A^*_{\mathbb{Q}_2}/(A^*_{\mathbb{Q}_2})^2$ is $(2,1)$. Hence applying the local restrictions at $5,\infty$ and primes of good reduction shows that $S^2(J,\mathbb{Q})$ is contained in the group generated by $\{-\eta, 2, 3\}$ in the first component, and $\{-1, \omega, p_1p_2, p_2p_3\}$ in the second. Moreover, the second component is negative if and only if the first component contains $-\eta$.

x^2-5 is irreducible over $\mathbb{Q}_3$. $\mathbb{Q}_3(\sqrt{5})$ is an unramified extension of $\mathbb{Q}_3$ with residue field $\mathbb{F}_3(\sqrt{2}) = \mathbb{F}_9$. The element $1+\sqrt{5}$ maps to $1+\sqrt{2}$ in the residue field, which is not a square, hence $\mathbb{Q}_3(\sqrt{5})^*/(\mathbb{Q}_3(\sqrt{5})^*)^2$ is generated by $3, 1+\sqrt{5}$. x^3-10 has a single root over $\mathbb{Q}_3$, say α, and $A_{\mathbb{Q}_3} \cong \mathbb{Q}_3(\sqrt{5}) \oplus \mathbb{Q}_3 \oplus \mathbb{Q}_3(\zeta_3)$. $\mathbb{Q}_3^*/(\mathbb{Q}_3)^2$ is generated by $3, -1$. $\mathbb{Q}_3(\zeta_3)$ is totally ramified over $\mathbb{Q}_3$, with uniformiser $1-\zeta_3$. $\mathbb{Q}_3(\zeta_3)^*/(\mathbb{Q}_3(\zeta_3)^*)^2$ is generated by $1-\zeta_3, -1$. The following tables give the images of $\{-\eta, 2, 3\}$ in $\mathbb{Q}_3(\sqrt{5})^*/(\mathbb{Q}_3(\sqrt{5})^*)^2$, and the images of $\{-1, \omega, p_1p_2, p_2p_3\}$ in $\mathbb{Q}_3^*/(\mathbb{Q}_3)^2$ and $\mathbb{Q}_3(\zeta_3)^*/(\mathbb{Q}_3(\zeta_3)^*)^2$.

$-\eta$	$1+\sqrt{2}$
2	1
3	3

-1	-1
ω	1
p_1p_2	-3
p_2p_3	3

-1	-1
ω	1
p_1p_2	1
p_2p_3	-1

(3.20)

The group $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ has order 2^2, the following table gives the images of $O, T, P, T+P$ in $A^*_{\mathbb{Q}_3}/(A^*_{\mathbb{Q}_3})^2$.

	$x-\sqrt{5}$	$x+\alpha$	$x+\zeta_3\alpha$
O	1	1	1
T	$1+\sqrt{2}$	-1	-1
P	1	3	-1
$P+T$	$1+\sqrt{2}$	-3	1

(3.21)

In particular, this shows that P is not a torsion point, and hence the rank of $J(\mathbb{Q})$ is at least 1. The local considerations at 3 show that the first component is generated by $-\eta, 2$. Enumerating the 32 possibilities left for elements of $S^2(J,\mathbb{Q})$ (recalling that the second component is negative $\Leftrightarrow$ the first contains $-\eta$) and comparing with the tables above gives us 16 possibilities for elements of $S^2(J,\mathbb{Q})$, namely $\{1,2\} \times \{1, \omega, p_2p_3, \omega p_2p_3\} \cup \{-\eta, -2\eta\} \times \{-1, -\omega, -p_2p_3, -\omega p_2p_3\}$.

x^2-5 is irreducible over $\mathbb{Q}_2$. By Hensel's Lemma, $\exists! \beta \in \mathbb{Z}_2$ such that $\beta \equiv 1 \bmod 4$ and $\beta^2 = -15$. Hence $\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}_2(\zeta_3)$. Thus is an unramified extension of $\mathbb{Q}_2$, with residue field $\mathbb{F}_2(\zeta_3) = \mathbb{F}_4$. Let $\mathcal{O}_{2,\zeta_3}$ be the ring of integers of $\mathbb{Q}_2(\zeta_3)$. Then Hensel's Lemma $\Rightarrow$ we can lift square roots from $(\mathcal{O}_{2,\zeta_3}/8\mathcal{O}_{2,\zeta_3})^*$ to $\mathcal{O}^*_{2,\zeta_3}$. Hence $\mathbb{Q}_2(\zeta_3)^*/(\mathbb{Q}_2(\zeta_3)^*)^2$ is generated by $2, 1-\zeta_3, 3, 1+3\zeta_3$. A quick calculation shows that $\beta \equiv 9 \bmod 16$, and hence the image of $\sqrt{5}$ in $\mathcal{O}_{2,\zeta_3}/8\mathcal{O}_{2,\zeta_3}$ is $2\zeta_3+5$.

x^3-10 is irreducible over $\mathbb{Q}_2$, $\mathbb{Q}_2(\sqrt[3]{10})$ is a totally ramified extension of $\mathbb{Q}_2$ with uniformiser $\sqrt[3]{10}$. By Hensel's Lemma we can lift square roots modulo $\sqrt[3]{10}^7$. The following tables give the images of $\{2, -\eta\}$ in $\mathbb{Q}_2(\zeta_3)^*/(\mathbb{Q}_2(\zeta_3)^*)^2$, and the images of $\{-1, \omega, p_2p_3\}$ in $\mathbb{Q}_2(\sqrt[3]{10})^*/(\mathbb{Q}_2(\sqrt[3]{10})^*)^2$.

2	2
$-\eta$	$1+3\zeta_3$

-1	1
ω	$1+\sqrt[3]{10}+\sqrt[3]{10}^2$
p_2p_3	$1+\sqrt[3]{10}$

(3.22)

The group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ has order 8, P and T generate an index 2 subgroup, as can be seen from the table below, and by Hensel's Lemma there exists $\epsilon \in \mathbb{Q}_2$ such that $(-5,\epsilon) \in C(\mathbb{Q}_2)$. The table below shows the images of $T, P, Q := (-5,\epsilon) - (\infty)$ in $A^*_{\mathbb{Q}_2}/(A^*_{\mathbb{Q}_2})^2$, which also proves that Q, T, P generate $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

	$x-\sqrt{5}$	$x+\sqrt[3]{10}$
T	$1+3\zeta_3$	1
P	2	$1+\sqrt[3]{10}^3+\sqrt[3]{10}^4+\sqrt[3]{10}^5$
Q	$(1-\zeta_3)(1+3\zeta_3)$	$1+\sqrt[3]{10}$

(3.23)

Hence the group $S^2(J,\mathbb{Q})$ consists of the 4 elements $\{(1,1), (2, \omega p_2p_3), (-\eta, -1), (-2\eta, -\omega p_2p_3)\}$, which are realised by the elements $O, T, P, T+P \in J(\mathbb{Q})$. Hence the rank of $J(\mathbb{Q})$ is exactly 1.

3.3 The Even Degree Case

In this section we consider hyperelliptic curves of the form $C : y^2 = f(x)$, $f \in k[T]$ with $d = \deg f$ even, in general following Flynn *et al* [5]. Unlike the odd degree case, it is not automatic that $C(k) \neq \emptyset$, and we will make this assumption, enabling us to identify $J(k)$ with $\mathrm{Pic}^0_k(C)$. There are two points lying at infinity, they are defined over $k(\sqrt{a_d})$, where a_d is the leading coefficient of f, and are conjugate over k. We will denote them by ∞^+ and ∞^-.

As before, denote by $\mathrm{Div}^0_k(C)^\dagger$ the set of divisors whose support does not meet the Weierstrass points of C. Let A_k be the k-algebra $k[T]/(f(T))$, and Θ the image of T in A_k. Define

$$\begin{aligned} \lambda_k : \mathrm{Div}^0_k(C)^\dagger &\to A_k^* \\ \sum_i n_i(P_i) &\mapsto \prod_i (x(P_i) - \Theta)^{n_i} \end{aligned} \tag{3.24}$$

As before, if $D \in \mathrm{Div}^0_k(C)^\dagger$ is G_k invariant, then $\lambda_k(D)$ does lie in $A_k^* \subset A_{\bar{k}}^*$. We wish to use λ_k to define a map on $J(k)$, however, the presence of two points at infinity complicates the matter.

Lemma 3.3.1. *λ_k induces a homomorphism $J(k) \to A_k^*/k^*(A_k^*)^2$.*

Proof. λ_k is clearly a homomorphism on $\mathrm{Div}^0_k(C)^\dagger$. As in the odd degree case, given any $D \in \mathrm{Div}^0_k(C)$ we can always pick a linearly equivalent divisor lying in $\mathrm{Div}^0_k(C)^\dagger$. Write $A_k = \bigoplus_{i=1}^n k(\alpha_i)$ as a direct sum of fields. If $h \in k(C)$ satisfies $\mathrm{div}h \in \mathrm{Div}^0_k(C)^\dagger$ then the ith component of $\lambda_k(\mathrm{div}h)$ satisfies

$$\begin{aligned} (\lambda_k(\mathrm{div}h))_i &= (x - \alpha_i)(\mathrm{div}h) \\ &= h(\mathrm{div}(x - \alpha_i)) \\ &= h\left(2(\alpha_i, 0) - (\infty^+) - (\infty^-)\right) \\ &= \frac{h(\alpha_i, 0)^2}{h(\infty^+)h(\infty^-)} \end{aligned} \tag{3.25}$$

Hence

$$\lambda_k(\mathrm{div}f) = \frac{1}{h(\infty^+)h(\infty^-)}(h(\alpha_1, 0), \ldots, h(\alpha_n, 0))^2 \in k^*(A_k^*)^2 \tag{3.26}$$

□

Lemma 3.3.2. *The image of λ_k lies in the kernel of the norm map $\mathrm{N}_{A_k/k} : A_k^*/k^*(A_k^*)^2 \to k^*/(k^*)^2$*

Remark. The norm map is well defined since $\alpha \in k^* \Rightarrow \mathrm{N}_{A_k/k}(\alpha) = \alpha^d \in (k^*)^2$ since d is even.

Proof. The proof is similar to that of Lemma 3.1.1.

□

It is clear that $2J(k) \subset \ker \lambda_k$, and we get a homomorphism $\lambda_k : J(k)/2J(k) \to A_k^*/k^*(A_k^*)^2$. Unlike the odd degree case, however, this map is not necessarily injective.

Theorem 3.3.3. *Let $P \in C(k)$. Then the kernel of λ_k is generated by $[2P - (\infty^+) - (\infty^-)]$.*

Proof. This is a consequence of the cohomological interpretation we will describe in Section 4. □

Thus $\ker \lambda_k$ has order ≤ 2, and is trivial $\Leftrightarrow$ $[2P - (\infty^+) - (\infty^-)]$ lies in $2J(k)$. We can also give the following necessary and sufficient condition for λ_k to be injective.

Proposition 3.3.4. *$\lambda_k : J(k)/2J(k)$ is injective $\Leftrightarrow$ one of the following two conditions holds.*

1. *f has a factor of odd degree in $k[x]$.*

2. *C has even genus, and f factors as $h \cdot {}^{\sigma}h$ over some quadratic extension L/k, $1 \neq \sigma \in \mathrm{Gal}(L/k)$.*

Proof. We will prove this is Section 4, Proposition 4.4.3. □

We will need know the size of $J(k)[2]$ in order to determine the torsion contribution to $J(k)/2J(k)$.

Proposition 3.3.5. *Let $\alpha_1, \dots, \alpha_d$ be the roots of f in $\bar{k}$. Then an $\mathbb{F}_2$ basis for $J[2]$ is given by the classes of the divisors $\{(\alpha_i, 0) + (\alpha_1, 0) - (\infty^+) - (\infty^-) \mid 2 \leq i \leq d-1\}$. The divisor $(\alpha_d, 0) + (\alpha_1) - (\infty^+) - (\infty^-)$ is linearly equivalent to $\sum_{i=2}^{d-1} ((\alpha_i, 0) + (\alpha_1, 0) - (\infty^+) - (\infty^-))$*

Proof. $2((\alpha_i, 0) + (\alpha_j, 0) - (\infty^+) - (\infty^-)) = \mathrm{div}((x-\alpha_i)(x-\alpha_j))$, hence every divisor of this type lies in $J[2]$, moreover $(\alpha_i, 0) + (\alpha_j) - (\infty^+) - (\infty^-)$ is linearly equivalent to $(\alpha_i, 0) - (\alpha_j, 0)$ and

$$\begin{aligned}(\alpha_d, 0) - (\alpha_1, 0) + \sum_{i=2}^{d-1} ((\alpha_i, 0) - (\alpha_1, 0)) &= \sum_{i=1}^{d} (\alpha_i, 0) - d(\alpha_1, 0) \\ &= \mathrm{div} f - (g+1)\mathrm{div}(x - \alpha_1)\end{aligned} \tag{3.27}$$

As in the odd degree case, $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$, hence it suffice to show that the classes of the divisors $\{(\alpha_i, 0) - (\alpha_1, 0) \mid 2 \leq i \leq d-1\}$ generate $J[2]$. The subgroup of $J[2]$ generated by these divisors contains the divisor classes of all divisors of the form $(\alpha_i, 0) - (\alpha_j, 0)$, and hence all degree zero divisors of the form $\sum_i n_i(\alpha_i, 0)$. By Proposition 6.2 of Poonen and Schaefer [11], this suffices to generate the whole of the group $J[2]$. □

Corollary 3.3.6. *Suppose that f factors over k as $f = f_1 \dots f_r$ with each f_j irreducible of degree d_j. Number the f_j so that $d_1, \dots, d_s$ are even and $d_{s+1}, \dots, d_r$ are odd. Define*

$$\begin{aligned} D_j &:= \left(\sum_{f_j(\alpha)} (\alpha, 0) \right) - \frac{d_j}{2}((\infty^+) + (\infty^-)), \quad 1 \leq j \leq s \\ E_j &:= \left(\sum_{f_j f_{j+1}(\alpha) = 0} (\alpha, 0) \right) - \frac{d_j + d_{j+1}}{2}((\infty^+) + (\infty^-)), \quad s+1 \leq j \leq r-1 \end{aligned} \tag{3.28}$$

Then $\{D_j \mid 1 \leq j \leq s-1\} \cup \{E_j \mid s+1 \leq j \leq r-1\}$ is an $\mathbb{F}_2$ basis for $J(k)[2]$. D_s is linearly equivalent to $\sum_{j=1}^{s-1} D_j + \sum_{j=s+1}^{r-s} E_j$.

Proof. The action of G_k on the divisors $(\alpha_i, 0) + (\alpha_j, 0) - (\infty^+) - (\infty^-)$ is the same as its action on unordered pairs of roots $\{\alpha_i, \alpha_j\}$, and the result follows from standard Galois theory. □

We have the following analogue of Propositions 3.1.3 and 3.1.4, enabling us to calculate the map λ_k more easily.

Proposition 3.3.7. 1. *Suppose that $\infty^{\pm} \in C(k)$, i.e. $a_d \in (k^*)^2$. If P is not a Weierstrass point of C then*

$$\lambda_k((P) - (\infty^{\pm})) \equiv x(P) - \Theta \bmod k^*(A_k^*)^2 \tag{3.29}$$

2. *Retaining the notation of the previous corollary,*

$$\begin{aligned} \lambda_k(D_j) &\equiv f_j(\Theta) - \prod_{i \neq j} f_i(\Theta) \bmod k^*(A_k^*)^2 \\ \lambda_k(E_j) &\equiv f_j(\Theta) f_{j+1}(\Theta) - \prod_{i \neq j, j+1} f_i(\Theta) \bmod k^*(A_k^*)^2 \end{aligned} \tag{3.30}$$

Proof. See Poonen and Schaefer [11]. □

We now turn to the case when K is a number field. If we assume that K has odd class number, then we have the following more direct proof that the image of λ_K is trivial at primes of good reduction.

Proposition 3.3.8. *Suppose that the class number h of K is odd, and let S be the set of places of K dividing $2, \infty, \Delta_f$. Write $A_K \cong \bigoplus_{i=1}^n L_i$ with $L_i = K(\alpha_i)$. Then for any $D = \sum_P n_P(P) \in \mathrm{Div}_K^0(C)^\dagger$ there exists $a \in K^*$ such that for any place $v \notin S$ and any place w_i of L_i dividing v, $w_i(a(\lambda_K(D))_i)$ is even.*

Proof. By symmetry we may assume that $i = 1$, we write $L = L_1$ and w for a normalised place of L dividing v (i.e. $w(L) = \mathbb{Z}$). Since v does not divide Δ_f, v is unramified in L and hence $w\mid_K = v$. Fix an extension to $\bar{K}$ of v, with corresponding embedding $\bar{K} \hookrightarrow \bar{K}_v$, such that $v\mid_L$ is equivalent to w. Since v is unramified in L, we have in fact that $v = w$ on L. Let D_v be the decomposition group (of our choice of extension) at v, i.e. the subgroup of G_K preserving the embedding $\bar{K} \hookrightarrow \bar{K}_v$, and let I_v be the subgroup of D_v that maps to the inertia group under the isomorphism $D_v \to G_{K_v}$. For each $v \notin S$, fix $\pi_v \in K$ such that $\pi_v \mathcal{O}_K = \mathfrak{p}_v^h$, (here $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}_K$ corresponding to v). Note that $v \notin S \Rightarrow v(\alpha_i) \geq 0$ for all i. We have

$$\begin{aligned} w((\lambda_K(D))_1) &= v((\lambda_K(D))_1) \\ &= v\left(\prod_P (x(P) - \alpha_1)^{n_P}\right) \\ &= \sum_{v(x(P)-\alpha_1)>0} v((x(P) - \alpha_1)^{n_P}) + \sum_{v(x(P)-\alpha_1)<0} v((x(P) - \alpha_1)^{n_P}) \end{aligned} \tag{3.31}$$

Suppose that $v(x(P) - \alpha_1) > 0$, then $v(\alpha_1) \geq 0 \Rightarrow v(x(P)) \geq 0$. Let $M \subset \bar{K}$ be a splitting field for f over $K(x(P))$ and let v' be the normalised place of M corresponding to our fixed extension of v to M. Denote the residue field of v' by $k_{v'}$. Then $v'(x(P)) \geq 0$, $v'(x(P) - \alpha_1) > 0$ and $v'(\alpha_i) \geq 0$ for all i, moreover the $\tilde{\alpha}_i$ are distinct in $k_{v'}$ since v' does not divide Δ_f. Then $v'(x(P) - \alpha_1) > 0 \Rightarrow \widetilde{x(P)} = \tilde{\alpha}_1$ in $k_{v'}$, hence $\widetilde{x(P)} \neq \tilde{\alpha}_i$ for $i \neq 1$, since the $\tilde{\alpha}_i$ are distinct. Hence $v'(x(P) - \alpha_i) = 0$ and $v(x(P) - \alpha_i) = 0$ for $i \neq 1$. Thus

$$\begin{aligned} v\left((x(P) - \alpha_1)^{n_P}\right) &= n_P v\left(\prod_{i=1}^{d} (x(P) - \alpha_i)\right) \\ &= n_P v\left(\frac{y(P)^2}{a_d}\right) \\ &= 2v(y(P)^{n_P}) \end{aligned} \tag{3.32}$$

since v does not divide a_d, as it does not divide Δ_f. Now, $\prod_{v(x(P)-\alpha_1)>0} y(P)^{n_P}$ is fixed by the inertial subgroup $I_v \subset G_{K_v}$, and hence lies in some unramified extension of K_v. Hence

$$v\left(\prod_{v(x(P)-\alpha_1)>0} y(P)^{n_P}\right) \tag{3.33}$$

is an integer, and

$$\sum_{v(x(P)-\alpha_1)>0} v((x(P) - \alpha_1)^{n_P}) \tag{3.34}$$

is an even integer. If $v(x(P)-\alpha_1)<0$, then $v(x(P)-\alpha_1)=v(x(P))$, since $v(\alpha_1)\geq 0$, and hence

$$\sum_{v(x(P)-\alpha_1)<0} v((x(P)-\alpha_1)^{n_P}) = v\left(\prod_{v(x(P)-\alpha_1)<0} x(P)^{n_P}\right) \tag{3.35}$$

Again, $\prod_{v(x(P)-\alpha_1)<0} x(P)^{n_P}$ is fixed by I_v, hence $n_v := v\left(\prod_{v(x(P)-\alpha_1)<0} x(P)^{n_P}\right)$ is an integer. Define

$$a = \prod_{v\notin S} \pi_v^{n_v} \tag{3.36}$$

where the product is finite, since only finitely many v divide $\prod_P x(P)^{n_P}$. Then $v(a) = hn_v = hv\left(\prod_{v(x(P)-\alpha_1)<0} x(P)^{n_P}\right)$ for all $v \notin S$ and, since we are assuming that h is odd, $w(a(\lambda_K(D))_1)$ is even, as required. □

We have a commutative diagram

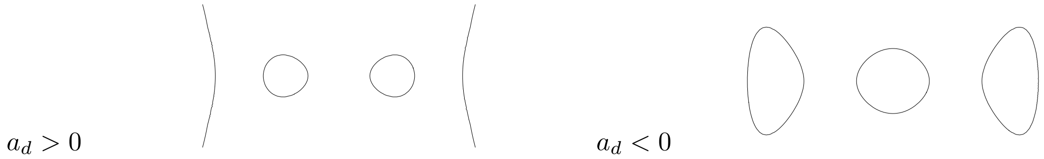
$$\begin{tikzcd} 0 \arrow[r] & J(K)/\left(\ker\lambda_K\right) \arrow[r, "\lambda_K"] \arrow[d, "\text{res}"] & A_K^*/K^*(A_K^*)^2 \arrow[d, "\text{res}"] \\ 0 \arrow[r] & \prod_v J(K_v)/\left(\ker\lambda_{K_v}\right) \arrow[r, "\prod_v \lambda_{K_v}"] & \prod_v A_{K_v}^*/K_v^*(A_{K_v}^*)^2 \end{tikzcd} \tag{3.37}$$

and we define the fake 2-Selmer group $\tilde{S}^2(J,K) = \{\alpha \in A_K^*/K^*(A_K^*)^2 \mid \text{res}(\alpha) \in \text{im}(\lambda_{K_v})\ \forall v\}$. The reason for the terminology is that it is not the exact analogue of the 2-Selmer group as defined in the odd degree case, as will be seen in Section 4. It is clear that $J(K)/\left(\ker\lambda_K\right) \hookrightarrow \tilde{S}^2(J,K)$ and we will estimate the rank of $J(K)$ by bounding $\#\tilde{S}^2(J,K)$ and calculating $[\ker\lambda_K : 2J(K)]$. The following Proposition gives a complete description of the image of $J(\mathbb{R})/2J(\mathbb{R})$ in $A_{\mathbb{R}}^*/\mathbb{R}^*(A_{\mathbb{R}}^*)^2$.

Proposition 3.3.9. *Suppose that f has $r=2k$ roots over $\mathbb{R}$. Then $A_{\mathbb{R}} \cong \mathbb{R}^r \oplus \mathbb{C}^{g+1-k}$. Order the components of $A_{\mathbb{R}}$ isomorphic to $\mathbb{R}$ by increasing size of the corresponding roots of f. Then $\lambda_{\mathbb{R}}(J(\mathbb{R})/2J(\mathbb{R}))$ has order 2^{k-1}, generated by*

1. $(-1,-1,1,\ldots,1),(1,1,-,1-,1,1\ldots,1),\ldots,(1,\ldots,1,-1,-1,1,\ldots,1)$ *if* $a_d>0$.
2. $(1,-1,-1,1,\ldots,1),(1,1,1,-1,-1,1,\ldots,1),\ldots,(1,\ldots,1,-1,-1,1,\ldots,1)$ *if* $a_d<0$.

Proof. $J(\mathbb{R})$ is generated by the images of divisors of the form $(P)+(Q)-((\infty^+)+(\infty^-))$ with $P,Q\in C(\mathbb{R})$ and those of the form $(P)+({}^\sigma P)-((\infty^+)+(\infty^-))$ where $P\in C(\mathbb{C})\setminus C(\mathbb{R})$ and $1\neq\sigma\in \text{Gal}(\mathbb{C}/\mathbb{R})$. A similar argument to Lemma 3.2.2 shows that divisors of the second kind have trivial image in $A_{\mathbb{R}}^*/(A_{\mathbb{R}}^*)^2$. The results then follows from sketching the real locus of f, noting the two distinct cases



See the proof of Propositions 3.2.1 and 1.3.8 for comparison. □

Example. To illustrate these ideas, we calculate the rank of $J(\mathbb{Q})$ where J is the Jacobian of the genus 2 curve

$$C/\mathbb{Q} : y^2 = x^6 + 3x^2 - 1 \tag{3.38}$$

Note that the leading coefficient is 1, hence $\infty^{\pm} \in C(\mathbb{Q})$. $f = x^6 + 3x^2 - 1$ is irreducible over $\mathbb{Q}$, let α be the positive real root of f in $\mathbb{C}$, and $K = \mathbb{Q}(\alpha)$. Then $A_{\mathbb{Q}} \cong K$, a field with class number 1. Denote the ring of integers of K by $\mathcal{O}_K$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\mathcal{O}_K^* \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^3$, the torsion free part being generated by $\alpha, \omega_1 := 1 + 2\alpha + \alpha^2 + \alpha^5$ and $\omega_2 := 37 + 65\alpha + 4\alpha^2 + 7\alpha^3 + 12\alpha^4 + 21\alpha^5$. $2, 3, 5$ factorise in K as follows.

p	Factorisation
2	$\omega_2^{-1} p_1^2$
3	$\alpha^{-1} p_2^3 p_3^3$
5	$\alpha^2 p_4 p_5 p_6^2$

(3.39)

where $p_1, \ldots, p_6$ are defined as follows, with norms as given.

x		$\mathrm{N}_{K/\mathbb{Q}}(x)$
α	α	-1
ω_1	$1 + 2\alpha + \alpha^2 + \alpha^5$	1
ω_2	$37 + 65\alpha + 4\alpha^2 + 7\alpha^3 + 12\alpha^4 + 21\alpha^5$	1
p_1	$6 + 10\alpha + \alpha^2 + \alpha^3 + 2\alpha^4 + 3\alpha^5$	8
p_2	$1 + \alpha$	3
p_3	$-1 + 3\alpha + \alpha^5$	-3
p_4	$1 + 2\alpha + \alpha^5$	-5
p_5	$-3 + 6\alpha + \alpha^3 - \alpha^4 + 2\alpha^5$	-5
p_6	$3 + \alpha^2 + \alpha^4$	25

(3.40)

f has exactly 2 real roots, $\pm\alpha$, hence $A_{\mathbb{R}} \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{C} \oplus \mathbb{C}$ and $\lambda_{\mathbb{R}}(J(\mathbb{R})/2J(\mathbb{R}))$ has order 1. The following table gives the images of $\alpha, \omega_1, \omega_2, p_1, p_2, p_3, p_4, p_5, p_6$ in $A_{\mathbb{R}}^*/\mathbb{R}^*(A_{\mathbb{R}}^*)^2$.

α	$(-1,1,1,1)$	p_3	$(-1,1,1,1)$
ω_1	$(-1,1,1,1)$	p_4	$(-1,1,1,1)$
ω_2	$(1,1,1,1)$	p_5	$(-1,1,1,1)$
p_1	$(1,1,1,1)$	p_6	$(1,1,1,1)$
p_2	$(1,1,1,1)$		

(3.41)

Thus applying the local restrictions at ∞ and primes of good reduction show that $\tilde{S}^2(J, \mathbb{Q})$ is contained in the subgroup of $K^*/\mathbb{Q}^*(K^*)^2$ generated by $\omega_2, p_1, p_2, p_6, \alpha\omega_1, \omega_1 p_3, p_3 p_4, p_4 p_5$ (since -1 is trivial in $K^*/\mathbb{Q}^*(K^*)^2$). Applying the norm condition shows that $\tilde{S}^2(J, \mathbb{Q})$ is generated by $\omega_2, p_4 p_5, p_6, \alpha p_2 p_3$, and has 2-rank at most 4.

f has two roots over $\mathbb{Q}_5$, say b_1, b_2, with $b_1 \equiv 2 \bmod 5$ and $b_2 \equiv 3 \bmod 5$. f factors has $f = (x - b_1)(x - b_2)g$ over $\mathbb{Q}_5$, where g is irreducible. The extension $\mathbb{Q}_5(\beta)$, where β is a root of g, is a degree 4 extension of $\mathbb{Q}_5$ with ramification degree and residue degree 2. A uniformiser is given by the image of p_6 in $\mathbb{Q}_5(\beta)$. The residue field is $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{3})$ and the image of β in the residue field is just $\sqrt{3}$. The group $\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^2$ is generated by $2, 5$ and the group $\mathbb{Q}_5(\beta)^*/(\mathbb{Q}_5(\beta)^*)^2$ is generated by $\beta, 3 + \beta^2 + \beta^4$. $J(\mathbb{Q}_5)/2J(\mathbb{Q}_5)$ has order $\#(J(\mathbb{Q}_5)[2]) = 2$, and $\ker \lambda_{\mathbb{Q}_5}/2J(\mathbb{Q}_5)$ is generated by $[(\infty^+) - (\infty^-)] = 2[(b_1, 0) - (\infty^-)] \in 2J(\mathbb{Q}_5)$. Hence the image of $J(\mathbb{Q}_5)$ in $A_{\mathbb{Q}_5}^*/\mathbb{Q}_5^*(A_{\mathbb{Q}_5}^*)^2$ has order 2. Hensel's Lemma $\Rightarrow \exists \epsilon \in \mathbb{Q}_5$ such that $(5, \epsilon) \in C(\mathbb{Q}_5)$. The image of the divisor $(5, \epsilon) - (\infty^-)$ in $A_{\mathbb{Q}_5}^*/\mathbb{Q}_5^*(A_{\mathbb{Q}_5}^*)^2$ is $(1, 1, \beta)$. The following table gives the images of $\omega_2, p_4 p_5, p_6, \alpha p_2 p_3$ in $A_{\mathbb{Q}_5}^*/\mathbb{Q}_5^*(A_{\mathbb{Q}_5}^*)^2$.

ω_2	$(1,1,1)$
$p_4 p_5$	$(1,1,1)$
p_6	$(1,1,3+\beta^2+\beta^4)$
$\alpha p_2 p_3$	$(1,1,1)$

(3.42)

Hence $\tilde{S}^2(J, \mathbb{Q})$ is generated by $\omega_2, p_4 p_5$ and $\alpha p_2 p_3$.

f factors as the product of two cubics over $\mathbb{Q}_3$, say $f = g_1 g_2$. Let β_1 and β_2 be roots of g_1 and g_2 respectively, then the fields $\mathbb{Q}_3(\beta_i)$ are both totally ramified extensions of $\mathbb{Q}_3$ with uniformisers $1+\beta_1$ and $-1+3\beta_2+\beta_2^5$ respectively. The groups $\mathbb{Q}_3(\beta_i)^*/(\mathbb{Q}_3(\beta_i)^*)^2$ are generated by -1 and the respective uniformisers. $\beta_1 \equiv 2 \bmod 3$ and $\beta_2 \equiv 1 \bmod 3$. The following table gives the images of $\omega_2, p_4p_5, \alpha p_2p_3$ in $A^*_{\mathbb{Q}_3}/\mathbb{Q}_3^*(A^*_{\mathbb{Q}_3})^2$

ω_2	$(1,1)$
p_4p_5	$(1,1)$
αp_2p_3	$(1+\beta_1,\epsilon')$

(3.43)

Where ϵ' is some element of $\mathbb{Q}_3(\beta_2)$. $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ is trivial, as $J(\mathbb{Q}_3)[2]$ is, and hence $\tilde{S}^2(J,\mathbb{Q})$ is generated by ω_2, p_4p_5.

f is irreducible over $\mathbb{Q}_2$, let γ be some root of f in $\bar{\mathbb{Q}}_2$. Then $A_{\mathbb{Q}_2} \cong \mathbb{Q}_2(\gamma)$ is a field extension of $\mathbb{Q}_2$ of degree 6, with ramification degree 2 and residue degree 3. Denote the ring of integers of $\mathbb{Q}_2(\gamma)$ by $\mathcal{O}$. A uniformiser is given by the image of p_1 in $\mathbb{Q}_2(\gamma)$, namely $\pi := 6+10\gamma+\gamma^2+\gamma^3+2\gamma^4+3\gamma^5$. By Hensel's Lemma, we can lift square roots from $\left(\mathcal{O}/\pi^5\mathcal{O}\right)^*$, and we use this to deal with the group $\mathbb{Q}_2(\gamma)^*/(\mathbb{Q}_2(\gamma)^*)^2$. Since f is irreducible over $\mathbb{Q}_2$, $J(\mathbb{Q}_2)[2]$ is trivial, and hence $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ has order 2.

By using the condition on injectivity of λ_k given by Proposition 3.3.4, it is easy to show that $\lambda_{\mathbb{Q}}$ (resp. $\lambda_{\mathbb{Q}_2}$) is injective if and only if there is a $\mathbb{Q}$-rational (resp. $\mathbb{Q}_2$-rational) point on the curve D defined by

$$12+4Y^2Z+3Z^2X^4=0\ ,\ 4X^2Y^2Z^2-Z^3X^6+1=0 \tag{3.44}$$

with Z integral and square-free. Over $\mathbb{Q}$, one can easily show there are no solutions by simple sign considerations. Hence $\ker\lambda_{\mathbb{Q}}$ has order 2. Over $\mathbb{Q}_2$, we note that there are no solutions on the reduced curve over $\mathbb{F}_2$, hence if there exists solutions, one of X, Y must have negative valuation. Since Z is integral and square-free, we may assume that $Z \in \{2,3,5,6,10,15,30\}$. By using the fact that any solutions must have at least one of $v_2(X), v_2(Y)$ negative, we can discount $Z \in \{2,6,10,30\}$. (Consider valuations of the first equation defining D). The last three possibilities for Z lead to the equations

$$108X^6+36X^2=1\ ,\ 500X^6+60X^2=1\ ,\ 13500X^6+180X^2=1 \tag{3.45}$$

all of which can have no solutions in $\mathbb{Q}_2$ by valuative considerations. Thus the image of $\lambda_{\mathbb{Q}_2}$ is trivial. The images of both ω_2 and p_4p_5 in $\mathbb{Q}_2(\gamma)$ do not lie in $\mathbb{Q}_2^*(\mathbb{Q}_2(\gamma)^*)^2$, (by looking at their images in $\mathcal{O}/\pi^7\mathcal{O}$) and hence the image of $\lambda_{\mathbb{Q}}$ is trivial. Hence the order of $J(\mathbb{Q})/2J(\mathbb{Q})$ is at most 2, and $J(\mathbb{Q})$ has rank at most 1.

Since f is irreducible over $\mathbb{Q}$, it follows that $J(\mathbb{Q})[2]$ is trivial, and hence the torsion contribution to $J(\mathbb{Q})/2J(\mathbb{Q})$ is zero. We claim that the torsion subgroup is in fact trivial. Indeed, if p is a prime of good reduction, then $J(\mathbb{Q})[q] \hookrightarrow \mathcal{J}_p(\mathbb{F}_p)$ is injective for any prime $q \neq p$ (see the Appendix to Katz [7]). To calculate $\#\mathcal{J}_p(\mathbb{F}_p)$ we use the formula

$$\#\mathcal{J}_p(\mathbb{F}_p)=\frac{1}{2}\#\tilde{C}(\mathbb{F}_{p^2})+\frac{1}{2}\#\tilde{C}(\mathbb{F}_p)-p \tag{3.46}$$

(see Flynn *et al* [4] and the references given there). We find that $\#\mathcal{J}_9(\mathbb{F}_9)=23$ and $\#\mathcal{J}_{11}(\mathbb{F}_{11}))=51=3.17$, and so $J(\mathbb{Q})_{\mathrm{tors}}=0$. In particular, this means that the point $[(\infty^+)-(\infty^-)]$ (which is not zero in $J(\mathbb{Q})$ by a standard Riemann-Roch argument) has infinite order, and $J(\mathbb{Q}) \cong \mathbb{Z}$.

4 Failure of 2-Descent and the Shafarevich-Tate Group

In all of the above examples, we have managed to calculate the exact size of $J(K)/2J(K)$, using our knowledge of $S^2(J,K)$ (or $\tilde{S}^2(J,K)$ in the even degree case). In general, however, this method will not work. Indeed, the 2-Selmer group $S^2(J,K)$ only records information about the groups $J(K_v)/2J(K_v)$ for all places v of K. The failure of the Hasse principle tells us that this is not sufficient for complete knowledge of $J(K)/2J(K)$. To fully understand the difference between $J(K)/2J(K)$ and $S^2(J,K)$ we re-interpret our results in terms of Galois cohomology.

4.1 Group Cohomology

We first recall the basic facts we need about low degree group cohomology. Let G be a profinite group. A G-module M is said to be continuous if the map $G \times M \to M,\ (g,m) \mapsto {}^g m$ is continuous when M is given the discrete and G the profinite topology. This is equivalent to requiring that for all $m \in M$, the stabiliser $\{g \in G \mid {}^g m = m\}$ is of finite index.

Example. Our motivating example is the action of G_k on J for a field k of characteristic zero.

Let G be a profinite group, and M a continuous G-module. Define the G-invariants of M, $M^G = \{m \in M \mid {}^g m = m\ \forall g \in G\}$. The functor $(-)^G : G\text{-}\mathfrak{Mod} \to \mathfrak{Ab}$ from continuous G-modules to abelian groups is left exact but not right exact. We thus have the sequence of right derived functors $R^i(-)^G : G\text{-}\mathfrak{Mod} \to \mathfrak{Ab}$, and we define the cohomology groups of the G-module M by $H^i(G,M) = R^i(-)^G(M)$. Thus given a short exact sequence of continuous G-modules $0 \to L \to M \to N \to 0$ we have a corresponding long exact sequence of cohomology groups

$$0 \to L^G \to M^G \to N^G \xrightarrow{\delta} H^1(G,L) \to H^1(G,M) \to H^1(G,N) \to \dots \tag{4.1}$$

The groups $H^1(G,-)$ and the connecting homomorphism δ have concrete descriptions. Let $Z^1(G,M)$ be the set of all continuous functions $\xi : G \to M$ such that $\xi(gh) = \xi(g) + {}^g\xi(h)$, and let $B^1(G,M)$ be the set of all functions $\xi : G \to M$ of the form $\xi(g) = {}^g m - m$, for some $m \in M$. By definition of the pro-finite topology, $\xi : G \to M$ is continuous if and only if it factors through a finite quotient of G. $Z^1(G,M)$ and $B^1(G,M)$ become abelian groups by addition in M, all elements of $B^1(G,M)$ are automatically continuous, (since all stabilisers are of finite index in G) and $B^1(G,M)$ is a subgroup of $Z^1(G,M)$.

Theorem 4.1.1. *Let G be a profinite group and L, M, N be continuous G-modules.*

1. *$H^1(G,M) \cong Z^1(G,M)/B^1(G,M)$.*

2. *If $0 \to L \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0$ is exact, then the connecting homomorphism $\delta : N^G \to H^1(G,L)$ is given by $\delta(n)(g) = \phi^{-1}({}^g m - m)$ for some (any) $m \in M$ with $\psi(m) = n$.*

Proof. See Cassels and Fröhlich [6], Chapter 4. □

We will henceforth use the terms G-module and continuous G-module interchangeably. Elements of $Z^1(G,M)$ are called cocylces and elements of $B^1(G,M)$ coboundaries.

4.2 Odd Degree Galois Cohomology and the Kummer Sequence

Let C/k be a hyperelliptic curve defined over an arbitrary field of characteristic zero, and J its Jacobian. We assume that C has a model of the form $y^2 = f(x)$ where $d = \deg f$ is odd. Let $G_k = \mathrm{Gal}(\bar{k}/k)$. We have a short exact sequence of G_k-modules

$$0 \to J[2] \to J \xrightarrow{[2]} J \to 0 \tag{4.2}$$

and taking G_k-invariants leads to the long exact sequence in cohomology

$$0 \to J(k)[2] \to J(k) \xrightarrow{[2]} J(k) \to H^1(G_k, J[2]) \to H^1(G_k, J) \xrightarrow{[2]} H^1(G_k, J) \tag{4.3}$$

from which we extract the Kummer sequence

$$0 \to J(k)/2J(k) \to H^1(G_k, J[2]) \to H^1(G_k, J)[2] \to 0 \tag{4.4}$$

Thus if K is a number field we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & J(K)/2J(K) \arrow[r, "\delta"] \arrow[d] & H^1(G_K, J[2]) \arrow[r] \arrow[d] & H^1(G_K, J)[2] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v J(K_v)/2J(K_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H^1(G_{K_v}, J(\bar{K}_v)[2]) \arrow[r] & \prod_v H^1(G_{K_v}, J(\bar{K}_v))[2] \arrow[r] & 0
\end{tikzcd} \tag{4.5}$$

where the product is over all places of K. We will show that this is essentially the same diagram as (1.27), following Schaefer [12]. Since we will need both the local and global case, we will take k to be any field of characteristic zero. The goal of this section is the following Theorem.

Theorem 4.2.1. *There is an isomorphism $w : H^1(G_k, J[2]) \to \ker(\mathrm{N}_{A_k/k} : A_k^*/(A_k^*)^2 \to k^*/(k^*)^2)$ such that $\lambda_k = e \circ \delta$.*

We will prove this Theorem in various stages. The first stage is to construct an isomorphism $H^1(G_k, \mu_2(A_{\bar{k}})) \cong A_k^*/(A_k^*)^2$, where here $\mu_2(A_{\bar{k}})$ is the group second roots of unity in $A_{\bar{k}}$, isomorphic as an abstract group to $(\mathbb{Z}/2\mathbb{Z})^d$. This is an easy consequence of Hilbert's Theorem 90.

Theorem 4.2.2. *(Hilbert's Theorem 90) Let k be a field of characteristic zero and A a finitely generated, unital k-algebra. Then $H^1(G_k, (A \otimes_k \bar{k})^*) = 0$.*

Proof. By Chapter 5 of Cassels and Frölich [6] it suffices to prove that $H^1(\mathrm{Gal}(K/k), (A \otimes_k K)^*) = 0$ for any finite Galois extension K/k. Since k has characteristic zero, it is infinite. The argument in this case is outlined in Chapter 10 of Serre [14]. □

Corollary 4.2.3. $H^1(G_k, \mu_2(A_{\bar{k}})) \cong A_k^*/(A_k^*)^2$

Proof. Consider the exact sequence of G_k-modules

$$0 \to \mu_2(A_{\bar{k}}) \to A_{\bar{k}}^* \xrightarrow{x^2} A_{\bar{k}}^* \to 0 \tag{4.6}$$

This induces a long exact sequence of homology groups

$$0 \to \mu_2(A_k) \to A_k^* \xrightarrow{x^2} A_k^* \to H^1(G_k, \mu_2(A_{\bar{k}})) \to H^1(G_k, A_{\bar{k}}) \tag{4.7}$$

By Hilbert's Theorem 90, $H^1(G_k, A_{\bar{k}}) = 0$ and hence we have a short exact sequence $0 \to A_k^*/(A_k^*)^2 \to H^1(G_k, \mu_2(A_{\bar{k}})) \to 0$ which is the isomorphism we require.

□

Since it will be important to keep track of the maps involved, we note here that the isomorphism $A_{\bar{k}}^*/(A_{\bar{k}}^*)^2 \to H^1(G_k, \mu_2(A_{\bar{k}}))$ is given by $\ell \mapsto [(\sigma \mapsto {}^{\sigma}\sqrt{\ell}/\sqrt{\ell})]$. By the same argument, $k^*/(k^*)^2 \cong H^1(G_k, \mu_2(\bar{k}))$, and we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_k, \mu_2(A_{\bar{k}})) \arrow[r] \arrow[d] & A_{\bar{k}}^*/(A_{\bar{k}}^*)^2 \arrow[r] \arrow[d] & 1 \\
0 \arrow[r] & H^1(G_k, \mu_2(\bar{k})) \arrow[r] & k^*/(k^*)^2 \arrow[r] & 1
\end{tikzcd} \tag{4.8}$$

where the vertical maps are those induced by the norm $\mathrm{N}_{A_{\bar{k}}/\bar{k}} : A_k \to k$. We now use the Weil pairing to construct a homomorphism $J[2] \to \mu_2(A_{\bar{k}})$. (For details on the Weil pairing, see Section 2). We can thus define $e : J[2] \to \mu_2(A_{\bar{k}})$ by

$$e(P) = (e_2(P, [(\alpha_1, 0) - (\infty)], \ldots, e_2(P, [(\alpha_d, 0) - (\infty)]) \tag{4.9}$$

where $d = \deg f$ and $\alpha_1, \ldots, \alpha_d$ are the roots of f in $\bar{k}$. The effect of Galois on $A_{\bar{k}}$ is to permute the summands corresponding to the α_i. Let $\sigma \in G_k$ and write π for the permutation of $\{1, \ldots, d\}$ induced by the action of σ on the α_i. Then the ith component of ${}^{\sigma}e(P)$ is given by

$$\begin{aligned}({}^{\sigma}e(P))_i &= {}^{\sigma}(e_2(P, [(\alpha_{\pi^{-1}(i)}) - (\infty)])) \\ &= e_2({}^{\sigma}P, [(\alpha_i, 0) - (\infty)]) = e({}^{\sigma}P)_i\end{aligned} \tag{4.10}$$

Hence ${}^{\sigma}e(P) = e({}^{\sigma}P)$ and e is G_k-module homomorphism.

Lemma 4.2.4.

$$0 \to J[2] \xrightarrow{e} \mu_2(A_{\bar{k}}) \xrightarrow{\mathrm{N}} \mu_2(\bar{k}) \to 1 \tag{4.11}$$

is an exact sequence of G_k-modules, where N *is the norm map, i.e. the product of the components.*

Proof. A basis for $J[2]$ is given by $\{[(\alpha_i) - (\infty)] \mid 1 \leq i \leq d-1\}$. Thus by non-degeneracy, $e(P) = 1 \Rightarrow e_2(P, [(\alpha_i, 0) - (\infty)]) = 1$ for all $i \Rightarrow e_2(P, Q) = 1$ for all $Q \in J[2]$ and $P = O$. Hence $e : J[2] \to \mu_2(A_{\bar{k}})$ is injective. The norm map is clearly surjective, $J[2]$ has size 2^{d-1}, $\mu_2(A_{\bar{k}})$ has size 2^d and $\mu_2(\bar{k})$ has size 2. It thus suffices to show that $\mathrm{N} \circ e = 1$. By Proposition 3.1.5,

$$[(\alpha_d, 0) - (\infty)] = \sum_{i=1}^{d-1} [(\alpha_i, 0) - (\infty)] \tag{4.12}$$

thus by bilinearity,

$$e_2(P, [(\alpha_d, 0) - (\infty)]) = \prod_{i=1}^{d-1} e_2(P, [(\alpha_i, 0) - (\infty)]) \tag{4.13}$$

Hence

$$\begin{aligned}\mathrm{N}(e(P)) &= \left(\prod_{i=1}^{d-1} e_2(P, [(\alpha_i, 0) - (\infty)])\right)^2 \\ &= \prod_{i=1}^{d-1} (e_2(P, [(\alpha_i, 0) - (\infty)]))^2 = 1\end{aligned} \tag{4.14}$$

since each $e_2(P, [(\alpha_i, 0) - (\infty)]) \in \mu_2(\bar{k}) = \{\pm 1\}$. □

We thus get a long exact sequence

$$0 \to J(k)[2] \to \mu_2(A_k) \to \mu_2(k) \to H^1(G_k, J[2]) \to H^1(G_k, \mu_2(A_{\bar{k}})) \to \dots \tag{4.15}$$

Since d is odd, the element $(-1, \dots, -1) \in A_{\bar{k}}$ is Galois invariant, and has norm -1, thus the map $\mu_2(A_k) \to \mu_2(k)$ is surjective, and we extract the exact sequence

$$0 \to H^1(G_k, J[2]) \to H^1(G_k, \mu_2(A_{\bar{k}})) \to H^1(G_k, \mu_2(\bar{k})) \tag{4.16}$$

Comparing this with diagram (4.8), and noting that the maps $H^1(G_k, \mu_2(A_{\bar{k}})) \to H^1(G_k, \mu_2(\bar{k}))$ are in both cases induced by the norm, and are thus equal, gives us the commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & & \\
 & H^1(G_k, J[2]) \arrow[d] & & \\
0 \arrow[r] & H^1(G_k, \mu_2(A_{\bar{k}})) \arrow[r] \arrow[d] & A_{\bar{k}}^*/(A_{\bar{k}}^*)^2 \arrow[r] \arrow[d] & 1 \\
0 \arrow[r] & H^1(G_k, \mu_2(\bar{k})) \arrow[r] & k^*/(k^*)^2 \arrow[r] & 1
\end{tikzcd} \tag{4.17}$$

Thus

$$\begin{aligned} H^1(G_k, J[2]) &\cong \ker\left(\mathrm{N} : H^1(G_k, \mu_2(A_{\bar{k}})) \to H^1(G_k, \mu_2(\bar{k}))\right) \\ &\cong \ker\left(\mathrm{N}_{A_k/k} : A_{\bar{k}}^*/(A_{\bar{k}}^*)^2 \to k^*/(k^*)^2\right) \end{aligned} \tag{4.18}$$

via an isomorphism we are calling w. We must show that $w \circ \delta = \lambda_k$. δ is just the connecting homomorphism $\delta : J(k)/2J(k) \hookrightarrow H^1(G_k, J[2])$ and is given by $P \mapsto {}^\sigma Q - Q$ for any $Q \in J$ with $2Q = P$. The map $H^1(G_k, J[2]) \to H^1(G_k, A_{\bar{k}}[2])$ is induced by the Weil pairing, hence the map $J(k)/2J(k) \to H^1(G_k, A_{\bar{k}}[2])$ is given by

$$P \mapsto (e_2({}^\sigma Q - Q, [(\alpha_1, 0) - (\infty)]), \dots, e_2({}^\sigma Q - Q, [(\alpha_d, 0) - (\infty)])) \tag{4.19}$$

Finally, the map $H^1(G_k, A_{\bar{k}}[2]) \to A_{\bar{k}}^*/(A_{\bar{k}}^*)^2$ is the inverse of the connecting homomorphism, which is given by $\ell \mapsto [\sigma \mapsto {}^\sigma\sqrt{\ell}/\sqrt{\ell}]$. Let $P \in J(k)$ and pick $Q \in J$ with $2Q = P$. Let P, Q be represented by divisors D_1, D_2 respectively, both of degree zero, with support disjoint from the Weierstrass points of C. Pick $g \in \bar{k}(C)$ with $\mathrm{div} g = 2D_2 - D_1$. Thus for any $\sigma \in G_k$ we have ${}^\sigma\mathrm{div} g = {}^\sigma 2D_2 - D_1$ and hence $\mathrm{div}({}^\sigma g/g) = {}^\sigma 2D_2 - 2D_2$. We also have $\mathrm{div}(x - \alpha_i) = 2(\alpha_i, 0) - 2(\infty)$.

Recalling the definition of the Weil pairing (2.2.1),

$$\begin{aligned} e_2({}^\sigma D_2 - D_2, [(\alpha_i, 0) - (\infty)]) &= \frac{({}^\sigma g/g)((\alpha_i, 0) - (\infty))}{(x - \alpha_i)({}^\sigma D_2 - D_2)} \\ &= \frac{{}^\sigma g(\alpha_i, 0) g(\infty)(x - \alpha_i)(D_2)}{{}^\sigma g(\infty) g(\alpha_i, 0)(x - \alpha_i)({}^\sigma D_2)} \end{aligned} \tag{4.20}$$

Given $\sigma \in G_k$, let π be the permutation of $\{1, \dots, d\}$ induced by the action of σ on $\alpha_1, \dots, \alpha_d$. Let $\beta \in A_{\bar{k}}$ be the element with $g(\alpha_i, 0)g(\infty)^{-1}(x - \alpha_i)(D_2)^{-1}$ in the component corresponding to α_i. Then ${}^\sigma\beta$ has ${}^\sigma g(\alpha_{\pi(i)}, 0){}^\sigma g(\infty)^{-1}(x - \alpha_{\pi(i)})({}^\sigma D_2)^{-1}$ in the component corresponding to $\alpha_{\pi(i)}$. Thus the image of P in $H^1(G_k, A_{\bar{k}}[2])$ is ${}^\sigma\beta/\beta$. The ith component of β^2 in $A_{\bar{k}}^*$ is given by

$$\begin{aligned} (\beta^2)_i &= \frac{g(\mathrm{div}(x - \alpha_i))}{(x - \alpha_i)(2D_2)} \\ &= \frac{(x - \alpha_i)(2D_2 - D_1)}{(x - \alpha_i)(2D_2)} \\ &= (x - \alpha_i)(D_1)^{-1} \end{aligned} \tag{4.21}$$

Thus $\beta^2 = \lambda_k(D_1)^{-1}$ is G_k-invariant, and lies in A_k^*. Hence $w \circ \delta(P) = \beta^2 = \lambda_k(P)^{-1} \equiv \lambda_k(P) \bmod (A_k^*)^2$. We have proved Theorem 4.2.1. As an immediate Corollary, this shows that λ_k is injective.

Corollary 4.2.5. *Let K be a number field. Then λ_K is an injective homomorphism $J(K)/2J(K) \hookrightarrow S^2(J,K)$.*

4.3 The Shafarevich-Tate and Weil-Châtelet Groups

The advantage of the cohomological interpretation, is that we now have a measure of the difference between $J(K)/2J(K)$ and $S^2(J,K)$.

Definition. The Shafarevich-Tate group of J/K

$$Ш(J,K) = \ker : H^1(G_K, J) \to \prod_v H^1(G_{K_v}, J(\bar{K}_v)) \tag{4.22}$$

The following is clear from the definition of $S^2(J,K)$ and $Ш(J,K)$, and the diagram (4.5).

Lemma 4.3.1. *There is an exact sequence*

$$0 \to J(K)/2J(K) \to S^2(J,K) \to Ш(J,K)[2] \to 0 \tag{4.23}$$

Thus the 2-torsion in $Ш(J,K)$ measures the difference between $J(K)/2J(K)$ and $S^2(J,K)$, and knowing $\#Ш(J,K)[2]$ will enable us to determine $\#J(K)/2J(K)$ exactly. The Shafarevich-Tate group, however, is entirely mysterious, and very little is known about it at all.

In the final section of this essay, we will give a more concrete interpretation of $Ш(J,K)$ in terms of principle homogeneous spaces, and the failure of the Hasse Principle for these spaces. Again, we assume that $d = \deg f$ is odd, and since we will need both the local and global case, k will be any field of characteristic zero.

Definition. A principal homogeneous space for J is a variety V/k defined over k, together with a simply transitive J action $\mu : J \times V \to V$ on V, satisfying the following equivalent conditions:

1. The addition map $\mu : J \times V \to V$ is a morphism.
2. The subtraction map $\nu : V \times V \to J$ defined (by simple transitivity) by $\mu(\nu(p,q),q) = p$ is a morphism.

We say that two principal homogeneous spaces $(V,\mu),(V',\mu')$ are equivalent if there is a k-isomorphism $\theta : V \to V'$ such that $\theta(\mu(P,p)) = \mu'(P,\theta(p))$ for all $P \in J$, $p \in V$.

The equivalence of the two conditions is not immediate, and we will not prove it here.

Example. J becomes a principal homogeneous space for itself via the usual addition map on points $J \times J \to J$.

Definition. The Weil-Châtelet group of J/k, $WC(J,k)$, is the set of principal homogeneous spaces for J modulo equivalence.

The goal of this section is the following characterisation of $H^1(G_k,J)$ and $Ш(J,K)$, which also justifies calling $WC(J,k)$ a group.

Theorem 4.3.2. *1. There is a bijection*

$$WC(J,k) \leftrightarrow H^1(G_k,J) \tag{4.24}$$

2. *If K is a number field then this induces a bijection between $\text{Ш}(J, K)$ and the set of (equivalence classes of) principal homogeneous spaces for J which have a point defined over K_v for every place v of K.*

We will usually denote $\mu(P, p)$ by $P + p$, and use upper case letters for points of J and lower case letter for those of V. Thus there should be no confusion with the group law on J. We also write $p - q$ for $\nu(p, q)$. The following Lemma tells is that this notation does not lead our intuition astray.

Lemma 4.3.3. *Let V be a principal homogeneous space for J/k, and let $P, Q \in J$ and $p, q \in V$. Denote by O the identity element of J.*

1. *$O + p = p$ and $p - p = O$*
2. *$(p - q) + q = p$ and $(P + q) - q = P$*
3. *$(P + p) - (Q + q) = (P - Q) + (p - q)$*
4. *Let $\theta : V \to V'$ be an equivalence of homogeneous spaces. Then $\theta(p) - \theta(q) = p - q$.*

Proof. Straighforward. □

Our first task is to define the map $WC(J, k) \to H^1(G_k, J)$. Given an element of $WC(J, k)$, represented by a principal homogeneous space V, pick $p_0 \in V$. Define $\xi_V : G_k \to J$ by $\xi_V(\sigma) = {}^\sigma p_0 - p_0$.

Proposition 4.3.4. *The function $V \mapsto \xi_V$ induces a well-defined injection $WC(J, k) \hookrightarrow H^1(G_k, J)$.*

Proof. We first show that ξ_V is a cocycle. Indeed, $\xi_V(\sigma\tau) = {}^{\sigma\tau}p_0 - p_0 = ({}^{\sigma\tau}p_0 - {}^\sigma p_0) + ({}^\sigma p_0 - p_0) = {}^\sigma\xi_V(\tau) + \xi_V(\sigma)$, by Lemma 4.3.3. It is continuous, since it factors through $\mathrm{Gal}(K/k)$ where K is the Galois closure of $k(p_0)/k$. Let p_0, p_1 be two points in V, and let $P = p_1 - p_0 \in J$. Then for $\sigma \in G_k$

$$ {}^\sigma p_1 - p_1 = {}^\sigma(P + p_0) - (P + p_0) = ({}^\sigma P + {}^\sigma p_0) - (P + p_0) = ({}^\sigma p_0 - p_0) + ({}^\sigma P - P) \tag{4.25}$$

The second equality comes from the fact that addition $\mu : J \times V \to V$ is defined over k, and the third from Lemma 4.3.3. Hence the two cocycles $\sigma \mapsto {}^\sigma p_0 - p_0$ and $\sigma \mapsto {}^\sigma p_1 - p_1$ differ by the co-boundary $\sigma \mapsto {}^\sigma P - P$ and thus represent the same element of $H^1(G_k, J)$. Hence $\xi_V \in H^1(G_k, J)$ is independent of the choice of p_0.

Now suppose that $\theta : V \to V'$ is an isomorphism defined over k, satisfying $\theta(P + p) = P + \theta(p)$ for all $P \in J$, $p \in V$. Suppose $p_0 \in V$ and let $p'_0 = \theta(p_0)$. By the preceding paragraph, we mas assume that ξ_V is given by $\sigma \mapsto {}^\sigma p_0 - p_0$ and ξ'_V by $\sigma \mapsto {}^\sigma p'_0 - p'_0$. Then by Lemma 4.3.3

$$ {}^\sigma p'_0 - p'_0 = {}^\sigma\theta(p_0) - \theta(p_0) = \theta({}^\sigma p_0) - \theta(p_0) = {}^\sigma p_0 - p_0 \tag{4.26}$$

Hence $\xi_V = \xi'_V$. Thus $V \mapsto \xi_V$ is a well defined function $WC(J, k) \to H^1(G_k, J)$. It remains to show that this function is injective. Let V, V' be principal homogeneous spaces for J, with $p_0 \in V$, $p'_0 \in V'$, and suppose that the co-cycles $\sigma \mapsto {}^\sigma p_0 - p_0$ and $\sigma \mapsto {}^\sigma p'_0 - p'_0$ differ by the co-boundary $\sigma \mapsto {}^\sigma P_0 - P_0$ for $P \in J$. Define $\theta : V \to V'$ by $\theta(p) = (P_0 + (p - p_0)) + p'_0$. This is a morphism since the addition maps $J \times J \to J$, $\mu : J \times V \to V$ and the subtraction map $\nu : V \times V \to J$ are. It has inverse $\theta^{-1}(q) = ((q - p'_0) - P_0) + p_0$ which is a morphism for the same reasons. It is defined over k since

$$\begin{aligned} \theta(p)^\sigma &= {}^\sigma P_0 + ({}^\sigma p - {}^\sigma p_0) + {}^\sigma p'_0 \\ &= P_0 + ({}^\sigma p - p_0) + p'_0 + [({}^\sigma P_0 - P_0) + ({}^\sigma p'_0 - p'_0) - ({}^\sigma p_0 - p_0)] \\ &= P_0 + ({}^\sigma p - p_0) + p'_0 = \theta({}^\sigma p) \end{aligned} \tag{4.27}$$

by various applications of Lemma 4.3.3. Finally, if $P \in J$ then

$$\theta(P+p) = P_0 + (P + p - p_0) + p_0' = P + [P_0 + (p - p_0) + p_0'] = P + \theta(p) \tag{4.28}$$

□

Corollary 4.3.5. *Let V be a principal homogeneous space for J. Then ξ_V lies in the trivial class in $H^1(G_k, J)$ if and only if $V(k) \neq \emptyset$.*

Proof. If $V(k) \neq \emptyset$ then let $p_0 \in V(k) \subset V$. Then $\xi_V(\sigma) = {}^\sigma p_0 - p_0 = 0$. Conversely, suppose that ξ_V is trivial in $H^1(G_k, J)$. Then for any $p_0 \in V$ there exists $P_0 \in J$ such that ${}^\sigma p_0 - p_0 = {}^\sigma(-P_0) - (-P_0)$ for all $\sigma \in G_k$. Thus ${}^\sigma P_0 + {}^\sigma p_0 = P_0 + p_0$ (by Lemma 4.3.3) and hence $P_0 + p_0$ lies in $V(k)$. □

Once we have proved surjectivity of $WC(J,k) \to H^1(G_k, J)$, this Corollary gives us the second part of Theorem 4.3.2. Indeed, if K is a number field, then $Ш(J,K) = \ker(WC(J,K) \to \prod_v WC(J, K_v))$ where the product is over all places of K. The previous Corollary says that $V \in WC(J,K)$ becomes trivial at all completions of K if and only if it has a point defined over all completions of K. Thus the only part of Theorem 4.3.2 that it remains to prove is the surjectivity of the map $WC(J,k) \to H^1(G_k, J)$.

Theorem 4.3.6. *Let $\xi : G_k \to J$ be a (continuous) co-cycle. Then there exists a principal homogeneous space V for J/k and a point $p_0 \in V$ with $\xi(\sigma) = {}^\sigma p_0 - p_0$ for all $\sigma \in G_k$.*

Proof. We give the argument described in Lang and Tate [9].

Let K/k be the field of definition of $\xi : G_k \to J$, i.e. the fixed field of the normal closure of $\xi^{-1}(0)$ in G_k. Then ξ continuous for the pro-finite topology $\Rightarrow [K : k] < \infty$. Let $G = \mathrm{Gal}(K/k)$. For every $\tau, \sigma \in G$ we define an isomorphism $f_{\tau,\sigma} : J \to J$, $f_{\tau,\sigma}(P) = P - \xi(\tau) + \xi(\sigma)$. If $\sigma, \tau, \rho \in G$ then $f_{\tau,\sigma} \circ f_{\sigma,\rho} = f_{\tau,\rho}$, and by the cocycle condition, if $\omega \in G_k$ then $f_{\omega\tau,\omega\sigma} = {}^\omega f_{\tau,\sigma}$. Jacobian varieties are projective, and the maps $f_{\tau,\sigma}$ are isomorphisms, hence we can apply Theorems 1 and 3 of Weil [18]. Thus there exists a variety V/k defined over k and a K isomorphism $F : J \to V$ such that $f_{\tau,\sigma} = {}^\tau F^{-1} \circ {}^\sigma F$ for all $\sigma, \tau \in G$.

Define $f_\sigma = P + \xi(\sigma)$ for any $\sigma \in G_k$, so $f_\sigma = F^{-1} \circ {}^\sigma F$. Define $\mu : J \times V \to V$ by $\mu(P,p) = F(P + F^{-1}(p))$. Then μ is a morphism, as a composition of the morphisms F, F^{-1} and $+ : J \times J \to J$, and is defined over k, since for $\sigma \in G_k$

$$\begin{aligned} {}^\sigma\mu(P,p) &= {}^\sigma(F(P + F^{-1}(p))) = F \circ f_\sigma({}^\sigma P + {}^\sigma F^{-1}({}^\sigma p)) \\ &= F({}^\sigma P + f_\sigma^{-1} \circ F^{-1}({}^\sigma p) + \xi(\sigma)) = F({}^\sigma P + F^{-1}({}^\sigma p)) = \mu({}^\sigma P, {}^\sigma p) \end{aligned}$$

Moreover, $\mu(O,p) = F(O + F^{-1}(p)) = F(F^{-1}(p)) = p$, and for any $p \in V$ for $P, Q \in J$, $p \in V$

$$\mu(P+Q, p) = F(P + Q + F^{-1}(p)) = F(P + F^{-1}(F(Q + F^{-1}(p)))) = \mu(P, \mu(Q,p)) \tag{4.29}$$

Hence $\mu : J \times V \to V$ does define an action, and V is a principal homogenous space for J over k. We finally show that ξ is the co-cycle coming from the pair $(V, F(O))$. Let $p_0 = F(O)$, then $\mu(\xi(\sigma), p_0) = F(\xi(\sigma) + F^{-1}(p_0)) = F \circ f_\sigma(O) = {}^\sigma F(O) = {}^\sigma p_0$. Hence $\xi(\sigma)$ satisfies the defining property for $\nu({}^\sigma p_0, p_0)$, and $\xi(\sigma) = {}^\sigma p_0 - p_0$ as required. □

4.4 Even Degree Cohomology

There is an analogous cohomological interpretation of the map $\lambda_k : J(k)/2J(k) \to A_k^*/k^*(A_k^*)^2$ in the case when C is defined by $y^2 = f(x)$ with $d = \deg f$ even. As this map is not necessarily injective, it cannot equal the coboundary map $\delta : J(k)/2J(k) \hookrightarrow H^1(G_k, J[2])$, and the description of λ_k is more involved than in the odd degree case. We only sketch the ideas here, and do not go into details of proofs. For these details, see Poonen and Schaefer [11]. So let k be a field of characteristic zero, C a hyperelliptic curve over k, defined by $y^2 = f(x)$, $f \in k[x]$ of even degree. Moreover assume that $C(k) \neq \emptyset$.

We use the Weil pairing on $J[2] \times J[2]$ to construct an isomorphism

$$\epsilon : J[2] \to \ker \left(\mathrm{N}_{A_{\bar{k}}/\bar{k}} : \frac{\mu_2(A_{\bar{k}})}{\mu_2(\bar{k})} \to \mu_2(\bar{k}) \right) \tag{4.30}$$

and hence taking cohomology induces a homomorphism

$$\epsilon : H^1(G_k, J[2]) \to H^1 \left(G_k, \frac{\mu_2(A_{\bar{k}})}{\mu_2(\bar{k})} \right) \tag{4.31}$$

The exact sequence

$$1 \to \mu_2(\bar{k}) \to \mu_2(A_{\bar{k}}) \to \frac{\mu(A_{\bar{k}})}{\mu_2(\bar{k})} \to 1 \tag{4.32}$$

induces an injection

$$\iota : \frac{H^1(G_k, \mu_2(A^*_{\bar{k}}))}{H^1(\mu_2(\bar{k}^*))} \hookrightarrow H^1 \left(G_k, \frac{\mu_2(A^*_{\bar{k}})}{\mu_2(\bar{k}^*)} \right) \tag{4.33}$$

The identities $H^1(G_k, A^*_{\bar{k}}) = H^1(G_k, \bar{k}^*) = 0$ show that $H^1(G_k, \mu_2(A^*_{\bar{k}})) \cong k^*/(k^*)^2$ and $H^1(G_k, \mu_2(A^*_{\bar{k}})) \cong A^*_k/(A^*_k)^2$, hence ι can be viewed as an injection

$$\iota : A_k/k^*(A^*_k)^2 \hookrightarrow H^1 \left(G_k, \frac{\mu_2(A^*_{\bar{k}})}{\mu_2(\bar{k}^*)} \right) \tag{4.34}$$

As in the odd degree case, the short exact sequence $0 \to J[2] \to J \overset{\times 2}{\to} J \to 0$ of G_k-modules induces an injection $\delta : J(k)/2J(k) \hookrightarrow H^1(G_k, J[2])$. We are now in a position to state the Theorem giving the cohomological description of the map λ_k.

Theorem 4.4.1. *$\iota \circ \lambda_k$ and $\epsilon \circ \delta$ are identical as maps $J(k)/2J(k) \to H^1 \left(G_k, \frac{\mu_2(A^*_{\bar{k}})}{\mu_2(\bar{k}^*)} \right)$.*

Proof. This is Theorem 9.4 of [11]. □

We now finally have the description of $\ker \lambda_k$ that we require. Recall that we are assuming $C(k) \neq \emptyset$, say $P \in C(k)$.

Corollary 4.4.2. *The kernel of the map $\lambda_k : J(k)/2J(k) \to A^*_k/k^*(A^*_k)^2$ is generated by the class of $2(P) - (\infty^+) - (\infty^-)$.*

Proof. (Sketch). Since ι and δ are both injective, $\ker \lambda_k = \delta^{-1} \ker \epsilon$. The map ϵ is induced by the short exact sequence

$$0 \to J[2] \to \frac{\mu_2(A^*_{\bar{k}})}{\mu_2(\bar{k}^*)} \to \mu_2(\bar{k}^*) \to 0 \tag{4.35}$$

and hence the kernel of ϵ is the image of the connecting homomorphism $\mu_2(k^*) \to H^1(G_k, J[2])$, generated by the image of -1. It thus suffices to show that $\delta([2(P) - (\infty^+) - (\infty^-)])$ is equal to the image of -1 in $H^1(G_k, J[2])$. This is just a case of chasing through the various definitions involved, using the Weil pairing $e_2 : J[2] \times J[2] \to \mu_2(\bar{k}^*)$ in the definition of ϵ. For more details, see [11].

□

Proposition 4.4.3. *$\lambda_k : J(k)/2J(k)$ is injective if and only if one of the following two conditions holds.*

1. *f has a factor of odd degree in $k[x]$.*

2. *C has even genus, and f factors as $h \cdot {}^{\sigma}h$ over some quadratic extension L of k, where σ is the non trivial element of* $\mathrm{Gal}(L/k)$.

Proof. Taking cohomology of the exact sequence

$$0 \to J[2] \to \frac{\mu_2(A_{\bar{k}})}{\mu_2(\bar{k})} \to \mu_2(\bar{k}) \to 1 \tag{4.36}$$

and using injectivity of $\delta : J(k)/2J(k) \to H^1(G_k, J[2])$ and $q : A_k^*/k^*(A_k^*)^2 \to H^1\left(G_k, \mu_2(A_{\bar{k}}^*)/\mu_2(\bar{k}^*)\right)$, we see that λ_k is injective $\Leftrightarrow$ the norm map $\mathrm{N}_{A_{\bar{k}}/\bar{k}} : H^0\left(G_k, \mu_2(A_{\bar{k}}^*)/\mu_2(\bar{k}^*)\right) \to \mu_2(k)$ is surjective.

If f has a factor of odd degree in $k[x]$, it must have an irreducible factor of odd degree in $k[x]$, say h. Then let α be the element of $A_{\bar{k}}$ which is -1 in the components corresponding to the roots of f, and 1 elsewhere. This is clearly G_k-invariant, and has norm $(-1)^{\deg h} = -1$.

Suppose that C has even genus, and f factors as $h \cdot {}^{\sigma}h$ over L/k, as in the statement of the Proposition. Let α be the element of A_k which is 1 in the components corresponding to the roots of h and -1 in the components corresponding to the roots of ${}^{\sigma}h$. Then this represents a G_k-invariant element of $\mu_2(A_{\bar{k}}^*)/\mu_2(\bar{k}^*)$, since the effect of Galois on α is simply to multiply by ±1. The norm of α is $(-1)^{\deg h} = (-1)^{\frac{d}{2}} = (-1)^{g+1} = -1$ since g is even.

Conversely, suppose that $\mathrm{N}_{A_{\bar{k}}/\bar{k}} : H^0\left(G_k, \mu_2(A_{\bar{k}}^*)/\mu_2(\bar{k}^*)\right) \to \mu_2(k)$ is surjective. Let $\alpha \in \mu_2(A_{\bar{k}}^*)$ be such that $\mathrm{N}_{A_{\bar{k}}/\bar{k}}(\alpha) = -1$. Let the roots fo f in $\bar{k}$ be $\alpha_1, \ldots, \alpha_d$. Define $h_0 = \prod_i (x - \alpha_i)$ to be the product over those α_i such that $\alpha \in A_k$ is 1 in the component of A_k corresponding to α_i, and similarly define $h_1 = \prod_j (x - \alpha_j)$ to be the product over those α_j such that the corresponding component of α is 1. Since α has norm -1, $\deg h_1$ must be odd, thus if $h_1 \in k[x]$ we are done. If not, then G_k must transpose h_0 and h_1, so in particular $\deg h_0 = \deg h_1 = g + 1$ is odd, thus g is even, and h_0, h_1 are conjugates over a quadratic extension of k. □

Bibliography

[1] S. Bosch, W. Lütkebohmert and M. Raynaud: *Neron Models*, Ergeb. Math. Grenz. **21**, Springer, New York, 1990.

[2] A. Brumer and K. Kramer: *The Rank of Elliptic Curves*, Duke Math. J. **44** 715-743, 1977.

[3] J.W.S. Cassels: *Lectures on Elliptic Curves*, LMS Student Texts 24, Cambridge University Press, Cambridge, 1991.

[4] J.W.S. Cassels and E.V. Flynn: *Prolegomena to a Middlebrow Arithmetic on Curves of Genus 2*, LMS Lecture Note Series 230, Cambridge University Press, Cambridge, 1996

[5] E.V. Flynn, B. Poonen and E.F. Shaefer: *Cycles of Quadratic Polynomials and Rational Points on a Genus 2 Curve*, Duke Math. J. **90** 435-463, 1997

[6] J.W.S. Cassels and A. Fröhlich (eds.): *Algebraic Number Theory*, Academic Press, London, 1967

[7] N. Katz: *Galois Properties of Torsion Points on Abelian Varieties*, Invent. Math. **62**, 481-502, 1981.

[8] S. Lang: *Abelian Varieties*, Springer, New York, 1983.

[9] S. Lang and J. Tate: *Principal Homogeneous Spaces over Abelian Varieties*, Amer. J. Math. **80** No. 3, 659-684, 1958.

[10] J. S. Milne: *Abelian Varieties*, Online Course Notes, `http://www.jmilne.org/math/CourseNotes/AV.pdf`, Retrieved 31/03/2010.

[11] B. Poonen and E.F. Schaefer: *Explicit Descent for Jacobians of Cyclic Covers of the Projective Line*, J. Reine Angew. Math. **488**, 141-188, 1997.

[12] E.F. Schaefer: *2-Descent on the Jacobians of Hyperelliptic Curves*, J. Number Theory, **51** 219-232, 1995.

[13] E.F. Shaefer: *Computing a Selmer Group of a Jacobian using Functions on the Curve*, Math. Ann. **301** No. 3, 447-471, 1998.

[14] J.-P. Serre: *Local Fields*, GTM 67, Springer-Verlag, New York, 1979.

[15] J.-P. Serre: *Algebraic Groups and Class Fields*, GTM 117, Springer-Verlag, New York, 1988.

[16] J.H. Silveman: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

[17] J.H. Silverman: *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, New York, 1994.

[18] A. Weil: *The Field of Definition of a Variety*, Amer. J. Math. **78** No. 3, 509-524, 1956.

[19] **MAGMA** homepage: `http://magma.maths.usyd.edu.au/magma/`

[20] Wolfram Research Inc.: *Mathematica* Version 7.0, Wolfram Research Inc., Champaign Illinois, 2008.