Computing the 2-descent over $\mathbb{Q}$ for curves of genus 2

Gert-Jan van der Heiden

Department of
Mathematics

RuG

Master's thesis

Computing the 2-descent over $\mathbb{Q}$ for curves of genus 2

Gert-Jan van der Heiden

University of Groningen
Department of Mathematics
P.O. Box 800
9700 AV Groningen

October 1998

Contents

Introduction

A wide range of problems in number theory is concerned with so called Diophantine problems. These are the kind of problems in which you look at a polynomial equation with rational coefficients and you wonder whether there exist any rational solutions and if so, whether you can find all these solutions. In this paper we will look at an algorithm which could give us some information about the rational solutions to a certain type of Diophantine equation.
The main subject of this paper will be the problem of finding the rational points on the Jacobian J of an hyperelliptic curve C of genus 2, which is defined over $\mathbb{Q}$. This problem is correlated to and motivated by the problem of finding the rational points of this curve C. Because there exists an easy embedding of the rational points of C into those of J and because there exists an easy way of representing the rational points of J, we can, with sufficient knowledge about $J(\mathbb{Q})$, in principle find the rational points of C. We denote the set of rational points of C and J by $C(\mathbb{Q})$ and $J(\mathbb{Q})$ respectively.

In this paper we will restrict ourselves to the class of curves of genus 2 defined over $\mathbb{Q}$, whose affine part, the Diophantine equation, is given by the model:

$$Y^2 = f_5(X),$$

where f_5 is a monic polynomial of degree 5 in $\mathbb{Z}[X]$, with distinct roots.

In the rest of this chapter we will define some elementary notions concerning divisors and we will introduce $J(\mathbb{Q})$. Notice that for our problem we only need this group and not the variety J itself. So we restrict ourselves to the introduction of $J(\mathbb{Q})$ and $J(\overline{\mathbb{Q}})$ and leave the Jacobian a mysterious object. In chapter 2 we will turn our attention to the quotient $J(\mathbb{Q})/2J(\mathbb{Q})$. We use this quotient for computing the Mordell-Weil rank. Computing it this way is called the 2-descent method. The main object of chapter 2 and 3 will be the development of an algorithm as exposed in [10] and we will consider its theoretical background. In this algorithm we will actually compute $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, embed this in a direct sum of fields in which computing is slightly easier and lift this local information to $\mathbb{Q}$. This results in the di-

mension and the generators of the so-called Selmer-group. This computation gives us an upperbound for the Mordell-Weil rank of the group of rational points on the Jacobian. And with a bit of luck this Selmer-group even turns out to be equal to $J(\mathbb{Q})/2J(\mathbb{Q})$. In that case the algorithm gives us the Mordell-Weil rank of $J(\mathbb{Q})$.
In chapter 4 we will try our luck by applying the algorithm to the curve $Y^2 = (X^2 - 4q^2)(X^2 - q^2)X$, with q a prime. We will see that a classification of q modulo 24 gives information of the number of points on this curve. For the main result we refer the impatient reader to theorem (4.3.4).

Chapter 1

Elementary notions

1.1 The curve C

As we already mentioned, we will restrict ourselves to the class of curves of genus 2 whose affine part is given by the model:

$$Y^2 = f_5(X) = a_0 + a_1 X + \cdots + a_4 X^4 + X^5, \tag{1.1}$$

with f_5 a monic polynomial in $\mathbb{Z}[X]$, and with distinct roots. Over $\overline{\mathbb{Q}}$, we have that f_5 splits as $f_5(X) = \prod_{i=1}^{5}(X - \alpha_i)$. Throughout this paper α_i will denote a root of f_5 in $\overline{\mathbb{Q}}$. The corresponding points $(\alpha_i, 0)$ on C will always be referred to as P_i.

We have that model (1.1) is an affine model, so it doesn't tell us what happens at infinity. Therefore we look at the birational transformation

$$\xi = \frac{Y}{X^3}, \eta = \frac{1}{X}. \tag{1.2}$$

After dividing the equation by x^6 the model (1.1) transforms into (1.3):

$$\xi^2 = \eta(a_0\eta^5 + \cdots + a_4\eta + 1). \tag{1.3}$$

If $x \to \infty$ then $\eta \to 0$. This gives us in (1.3) exactly one point at infinity, namely $(\eta, \xi) = (0, 0)$. This point will be denoted as ∞. Notice that this point at infinity is a point over $\mathbb{Q}$, which gives us $\infty \in C(\mathbb{Q})$, so there exists at least one rational point on C.
The points P_i and ∞ are called the *Weierstrass* points of C.
Furthermore we see in general that once we have a point (x, y) on this curve C, then we also have $(x, -y)$ on C. This gives us a bijective map on C, the *hyperelliptic involution*, $\varphi : C \to C$, which is given by $\varphi : (x, y) \mapsto (x, -y)$.

1.2 Divisors on C

We are interested in the computation of the rational points on the Jacobian. To be able to define this object, we first need to introduce *divisors*. In

this paragraph, we give some elementary notions and notations concerning divisors.

Definition 1.2.1

(i) We define a divisor *on C as a finite, formal sum*

$$D = \sum_{P \in C} n_P[P], \tag{1.4}$$

with $n_P \in \mathbb{Z}$ and finitely many $n_P \neq 0$.

(ii) Let D be a divisor on C, given by (1.4), then we call the set $\{P \in C \mid n_P \neq 0\}$ the support *of D, denoted by $Supp(D)$. Moreover we define the* degree *of D as*

$$deg(D) := \sum_{P \in C} n_P.$$

(iii) We denote with $Div(C)$ the set of all divisors on C and with

$$Div^0(C) = \{D \in Div(C) \mid deg(D) = 0\},$$

the set of divisors on C of degree 0.

We can now define the *divisor of a function*. Therefore we need the introduction of a *function field* and a notion of *order*.

Let $\mathbb{C}[X,Y] \ni h = Y^2 - f_5(X)$, then we have that h is irreducible. We can see that as follows. All zeroes of $f_5(X)$ are simple, thus if $p(X)$ is a prime divisor of $f_5(X)$, then $p(X) \not| 1, (p(X))^2 \not| f_5(X)$, thus h is Eisenstein and hence irreducible.
Let now $C(\mathbb{C}) = V(h) := \{P \in \mathbb{C}^2 \mid h(P) = 0\} \cup \{\infty\}$, then we have that its *function field* is $\mathbb{C}(C) = \text{Quot}(\mathbb{C}[V(h)])$, where $\mathbb{C}[V(h)] = \mathbb{C}[X,Y]/(I(V(h)))$. (We use the notations I and V as in [8].)
Because of the irreducibility of h, we have $\text{rad}(h) = (h)$ ([8], pp. 54) and so it follows with the Nullstellensatz that $I(V(h)) = \text{rad}(h) = (h)$.
This gives us $\mathbb{C}[V(h)] = \mathbb{C}[X,Y]/(h)$. Thus the function field is $\mathbb{C}(C) = \text{Quot}(\mathbb{C}[X,Y]/(h)) = \mathbb{C}(X)[\sqrt{f_5(X)}]$.

Let $P \in C(\mathbb{C})$. If $\frac{\partial f_5}{\partial X}(P) = 0$, then $f_5(P) \neq 0$, because $f_5(X)$ has distinct roots. Thus for $P \in C(\mathbb{C})$, we never have that $Y(P)$ and $\frac{\partial f_5}{\partial X}(P)$ are both 0, thus

$$\text{rk}\left(\frac{\partial h}{\partial X} \quad \frac{\partial h}{\partial Y}\right)(P) = \text{rk}\left(\frac{\partial f_5}{\partial X} \quad 2Y\right)(P) = 1 \quad \forall P \in C(\mathbb{C}).$$

Henceforth C is smooth everywhere.
This implies that we have a valuation ring at every point P, which comes from the affine coordinate ring and is given by

$$\mathcal{O}_{C,P} = \{f \in \mathbb{C}(C) \mid f = \frac{f_1}{f_2}, f_1, f_2 \in \mathbb{C}[C], f_2(P) \neq 0\}.$$

We can make an *order-function* ord_P on this ring.
Let's assume $P \in C(\mathbb{C})$ and $P \neq \infty$.

(*i*) *P is not a Weierstrass point.* In this case we have that $(X - X(P))$ is a maximal ideal in $\mathcal{O}_{C,P}$. We can see this as follows. First notice $Y \notin (X - X(P))$, otherwise $f_5(X) = Y^2 \in (X - X(P))$, which contradicts the assumption that P is not a Weierstrass point. Furthermore an arbitrary element in $\mathcal{O}_{C,P}$ is given by $\frac{f_1}{f_2}$, where $f_1 = (X - X(P))g(X,Y) + Y - a$. This implies that $(X - X(P), \frac{f_1}{f_2}) = (X - X(P), Y - a)$. Now we have that if $a \neq Y(P)$, then $\frac{1}{Y-a} \in \mathcal{O}_{C,P}$, hence $(X - X(P), Y - a) = \mathcal{O}_{C,P}$. If $a = Y(P)$, then we have that $(Y - a)(Y + a) = Y^2 - a^2 = f_5(X) - Y(P)^2 \in (X - X(P))$ and now $\frac{1}{Y+a} \in \mathcal{O}_{C,P}$, hence $Y - a \in (X - X(P))$ and thus $(X - X(P), Y - a) = (X - X(P))$.
For every element $0 \neq f_1 \in \mathbb{C}[C]$ we have a unique decomposition of f_1 of the form $f_1 = (X - X(P))^n g$, with $g \in \mathbb{C}[C], g \notin (X - X(P)), n \in \mathbb{N}_0$. Moreover if $f_1(P) \neq 0$, this n is 0. Thus for an $f = \frac{f_1}{f_2} \in \mathcal{O}_{C,P}$, we have a unique decomposition $f = \frac{(X-X(P))^n g}{f_2}$, with $g, f_2 \notin (X - X(P))$ and $n \in \mathbb{N}_0$. We define the order of f at P to be:

$$\mathrm{ord}_P(f) := n.$$

(*ii*) *P is a Weierstrass point.* Over $\mathbb{C}$ we have that f_5 decomposes as $f_5(X) = \prod_{i=1}^{5}(X - \alpha_i)$. We know that P is a Weierstrass point, thus it is of the form $P = (\alpha_i, 0)$, say for simplicity $P = (\alpha_1, 0)$. In this case we don't have that $(X - \alpha_1)$ is a maximal ideal, instead we have that (Y) is a maximal ideal, with $X - \alpha_1 \in (Y)$, because $Y^2 = f_5(X) = \prod_{i=1}^{5}(X - \alpha_i) \Rightarrow X - \alpha_1 = \frac{Y^2}{\prod_{i=2}^{5}(X-\alpha_i)}$.
We can write every $0 \neq f \in \mathcal{O}_{C,P}$ uniquely as $f = Y^n g$, with $g \notin (Y)$. and $n \in \mathbb{N}_0$. Now we define the order at P of f by:

$$\mathrm{ord}_P(f) := n.$$

Note that we have that $\mathrm{ord}_P(X - \alpha_1) = \mathrm{ord}_P(\frac{Y^2}{\prod_{i=2}^{5}(X-\alpha_i)}) = 2$.

For all P we define $\mathrm{ord}_P(0) = \infty$. Let now $\frac{f}{g} \in \mathbb{C}(C), f, g \in \mathbb{C}[C], g \neq 0$, then we can extend the map ord_P to $\mathbb{C}(C)$, by defining

$$\mathrm{ord}_P\left(\frac{f}{g}\right) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g).$$

Remark 1.2.2 Notice that, because we explicitly wrote our maximal ideals in terms of principal ideals, we have found uniformizers at all points $P \neq \infty$. A *uniformizer at* P is a function $f \in \mathbb{C}(C)$ with $\mathrm{ord}_P(f) = 1$. So for Weierstrass points P we have that Y is a uniformizer and for non-Weierstrass points P we have that $X - X(P)$ is a uniformizer.

Finally we define the order at $P = \infty$, for this point we will use the transformation (1.2), which we also used to obtain model (1.3) out of model (1.1). We already saw that ∞ in the latter model corresponds to $(0,0)$ in the former. Thus we define

$$\mathrm{ord}_\infty(f(X,Y)) := \mathrm{ord}_{(0,0)}(f(\frac{1}{\eta}, \frac{\xi}{\eta^3})).$$

Notice that ∞ is also a Weierstrass point. As in the case of the Weierstrass points above, we get as a uniformizer ξ and again we have $\mathrm{ord}_{(0,0)}(\eta) = 2$. This gives us for every $P \in C(\mathbb{C})$ a map

$$\mathrm{ord}_P : \mathbb{C}(C) \longrightarrow \mathbb{Z} \cup \{\infty\},$$

with the properties:

$$\begin{aligned} 0 &\longmapsto \infty, \\ \mathrm{ord}_P(f_1 f_2) &= \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2), \\ \mathrm{ord}_P(f_1 + f_2) &\geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)). \end{aligned}$$

And the useful property

$$\sum_{P \in C(\mathbb{C})} \mathrm{ord}_P(f) = 0, \tag{1.5}$$

which is proved in [7], lemma 1.1, because we can see a smooth curve as a compact Riemann surface.
With all this we can define the divisor of a function, a *principal divisor*, as follows.

Definition 1.2.3 *Let $f \in \mathbb{C}(C)$ be a non-constant function, then we can associate with f a* principal divisor, *notation $div(f)$ or (f), by:*

$$div(f) = \sum_{P \in C} ord_P(f)\ [P].$$

We denote the set of principal divisors as

$$Div(\mathbb{C}(C)) = \{(f) \mid f \in \mathbb{C}(C) \backslash \mathbb{C}\}.$$

Because of property (1.5) we have that a principal divisor is of degree 0, and henceforth $\mathrm{Div}(\mathbb{C}(C)) \subset \mathrm{Div}^0(C)$. This $\mathrm{Div}(\mathbb{C}(C))$ is a group.
The next proposition illustrates the explicit computation of a principal divisor.

Proposition 1.2.4 *Let $P = (x, y) \in C$ and let $f \in \mathbb{C}(C)$ s.t. $f = (X - x)$, then we have $(f) = [P] + [\varphi(P)] - 2[\infty]$.*

Proof. First suppose that P is not a Weierstrass point. Then we know that $f(Q) = 0 \Leftrightarrow X(Q) = x \Leftrightarrow Q \in \{P, \varphi(P)\}$. In the definition of the order function we saw that $X - x$ is a uniformizer at P and henceforth $\mathrm{ord}_P(X - x) = 1$. The same is true for $\varphi(P)$, thus $\mathrm{ord}_{\varphi(P)}(X - x) = 1$. With (1.2) $X - x$ transforms in $\frac{1}{\eta} - x = \frac{1}{\eta}(1 - x\eta)$, which has order -2 in $(0, 0)$, thus $\mathrm{ord}_\infty(X - x) = -2$. For other points $(v, w) \in C(\mathbb{C})$ we have that the order at Q of $(X - x)$ is 0, because $X - v \nmid X - x$ and $Y \nmid X - x$. Henceforth $(f) = [P] + [\varphi(P)] - 2[\infty]$.
If P is a Weierstrass point, then the only zero of $X - x$ is P and $\mathrm{ord}_P(X - x) = 2$, hence $(X - x) = 2[P] - 2[\infty]$. Moreover we have in this case that $P = \varphi(P)$, hence we get $(X - x) = [P] + [\varphi(P)] - 2[\infty]$. ⊠

Suppose we have a function $f \in \mathbb{C}(C)$ and $D = \sum_{P \in C} n_P[P]$ a divisor s.t. the support of D is disjoint from the support of (f). Then we define the evaluation of f at D by $f(D) := \prod_{P \in C}(f(P))^{n_P}$. And we have for this kind of evaluation the Weil-reciprocity.

Theorem 1.2.5 (Weil-reciprocity) *Let $f, g \in \mathbb{C}(C)$ with the support of (f) disjoint from the support of (g) then $f((g)) = g((f))$.*

Proof. For a proof see [12], chapter 2. ⊠

1.3 The group $J(\mathbb{Q})$

Because the group of principal divisors is a subgroup of the group of divisors of degree 0, it makes sense to define the *Picard group* (over $\mathbb{C}$) as:

$$\mathrm{Pic}^0(C) := \frac{\mathrm{Div}^0(C)}{\mathrm{Div}(\mathbb{C}(C))}.$$

Actually we will only be looking at the Picard group over a closure of $\mathbb{Q}$.

Finally we can define the group $J(\mathbb{Q})$ of the curve C. It is the group consisting of all elements in $\mathrm{Pic}^0(C)$ over $\overline{\mathbb{Q}}$, denoted by $\mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C)$ that are invariant under the action of the Galois-group $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

$$J(\mathbb{Q}) := \left(\mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C)\right)^G. \tag{1.6}$$

Similar, we can define $J(K)$ for a field K over $\mathbb{Q}$ as

$$J(K) := \left(\mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C)\right)^{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}.$$

We see that $\mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C) = J(\overline{\mathbb{Q}})$.

Expression (1.6) looks rather complicated, but there is a theorem which gives the group $J(\mathbb{Q})$ a more friendly appearance.

Theorem 1.3.1 *For the class of genus 2 curves whose affine model is given by (1.1), we have:*

$$J(\mathbb{Q}) \simeq \frac{(Div^0_{\overline{\mathbb{Q}}}(C))^G}{Div(\mathbb{Q}(C))}.$$

Remark 1.3.2 Actually this theorem is true for curves of genus 2 in general, but this is rather hard to prove. In our case we always have a point over $\mathbb{Q}$, which is not true in general. It is exactly this property which saves us from real difficulties. However, for the proof of this theorem we have to wait until the development of some group cohomology in the next chapter.

To clearify notations concerning the computation in the Picard group and in $J(\mathbb{Q})$, we introduce linear equivalency of divisors.

Definition 1.3.3 *Let $D_1, D_2 \in Div_{\overline{\mathbb{Q}}}(C)$, then we call D_1 and D_2 linearly equivalent over a field $K \subset \overline{\mathbb{Q}}$, denoted by $D_1 \sim_K D_2$, if there exists an $f \in K(C)$, s.t. $D_1 - D_2 = (f)$.*

Notice that when we just say 'linearly equivalent', we mean 'linearly equivalent over $\mathbb{Q}$'. Also we denote linear equivalence over $\mathbb{Q}$ by $\sim$.
We see, e.g., that from proposition (1.2.4) it follows that $-[P] \sim_{\overline{\mathbb{Q}}} [\varphi(P)] - 2[\infty]$. And if $P \in C(\mathbb{Q})$ we even have $-[P] \sim [\varphi(P)] - 2[\infty]$.
The new expression for $J(\mathbb{Q})$ in theorem (1.3.1) enables us to describe the elements of $J(\mathbb{Q})$. We see that if we have two elements $D_1, D_2 \in (\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G$, then they represent the same elements of $J(\mathbb{Q})$ if and only if they are linearly equivalent. Moreover we see that every element in $J(\mathbb{Q})$ can be represented by a $D_1 \in (\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G$. This is more than we know *a priori*. We only knew $D_1 \sim_{\overline{\mathbb{Q}}} \sigma(D_1)$ for all $\sigma \in G$. The theorem states that there always is a representation in $(\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G$.

Instead of the somewhat confusing notation for an element $D_1 + (\mathrm{Div}(\mathbb{Q}(C)))$ $\in J(\mathbb{Q})$, we denote this element simply by D_1. And if D_1 and D_2 are the same element in $J(\mathbb{Q})$, then we denote this as $D_1 \sim D_2$.

With this information we want to describe the elements of $J(\mathbb{Q})$ more properly.

Proposition 1.3.4 *Let $P,Q \in C(\overline{\mathbb{Q}})$, $P \neq Q$ and let $D \in (Div^0_{\overline{\mathbb{Q}}}(C))^G$, s.t. $D \sim [P]+[Q]-2[\infty]$. Then we have that either $P,Q \in C(\mathbb{Q}(\sqrt{d}))$ with $d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $Q = \sigma(P)$ for σ the non-trivial element of $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, or $P,Q \in C(\mathbb{Q})$.*

Proof. D is G-invariant, so for every $\sigma \in G$, we have $\sigma(D) = D$. Moreover $D \sim [P]+[Q]-2[\infty]$, hence there exists an $f \in \mathbb{Q}(C)$, s.t. $-D+[P]+[Q]-2[\infty] = (f)$. Because $f = \sigma(f)$, for all $\sigma \in G$, we also have $\sigma((f)) = (f)$ for all $\sigma \in G$. Hence $[P]+[Q]-2[\infty] = \sigma([P]+[Q]-2[\infty]) = [\sigma(P)]+[\sigma(Q)]-2[\infty]$. This implies that

$$[P]+[Q] = [\sigma(P)]+[\sigma(Q)] \quad \forall \sigma \in G. \tag{1.7}$$

Now there are two possibilities: either $\sigma(P) = P$ for all $\sigma \in G$ or there exists at least one $\sigma \in G$ with $\sigma(P) = Q$.
In the former case we have $P,Q \in C(\mathbb{Q})$, because $\sigma(P) = P$ and $\sigma(Q) = Q$ for all $\sigma \in G$.
In the latter case we consider the σ's with $\sigma(P) = Q$. According to equation (1.7) we have for such σ's that $\sigma(Q) = P$. This implies that for all extensions K of $\mathbb{Q}$ we have that $P \in C(K) \Leftrightarrow Q \in C(K)$. This smallest extension K for which $P \in C(K)$ with this property is at least quadratic, because $P \notin C(\mathbb{Q})$, but also at most quadratic, because otherwise there would exist a $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \subset G$, s.t. $\sigma(P)$ is neither P nor Q, which contradicts equation (1.7).
Thus there exists an extension K of $\mathbb{Q}$, s.t. $P,Q \in C(K)$, with $[K:\mathbb{Q}] = 2$, which gives the desired result: indeed $P,Q \in C(\mathbb{Q}(\sqrt{d})), d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $\sigma(P) = Q$ for σ the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. ⊠

Theorem 1.3.5 *Let C be a genus 2 curve, whose affine part is given by model (1.1), and let $D \in J(\mathbb{Q})$. Then we have that $D \sim [P]+[Q]-2[\infty]$, with either*

$$P,Q \in C(\mathbb{Q}),$$

or

$$P,Q \in C(\mathbb{Q}(\sqrt{d})), d \in \mathbb{Q}^*/\mathbb{Q}^{*2},$$

s.t. $P \neq \sigma(P) = Q$ for σ the non-trivial element in $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.
We call those elements the generators of $J(\mathbb{Q})$.

Proof. The line of argument will be as follows. First we will show that every $D \in J(\mathbb{Q})$ is linearly equivalent to a sum of generators. Subsequently we will show that the sum of two generators is a generator.
Let $D \in J(\mathbb{Q})$, then in general $D \sim \sum_{P \in C(\overline{\mathbb{Q}})} n_P[P]$, with $\sigma(D) = D \ \forall \sigma \in G$. Define for all $n \in \mathbb{Z}, n \neq 0$, $D_n := \sum_{P \in S_n}([P]-[\infty])$, with $S_n = \{P \in \mathrm{supp}(D) \mid n_P = n\}$, then we have $D \sim \sum_{n \in \mathbb{Z}}(nD_n)$. Because

$\sigma(n_P[P]) = n_P[\sigma(P)]$, the G-invariance of D and hence of $\sum n_P[P]$ implies $\sigma(D_n) = D_n$ for all $\sigma \in G$.
We only need to show that the D_n are sums of generators, i.e. for divisors with $n_P = 1$ for every P in its support. Let now D be such an element of $J(\mathbb{Q})$, thus $D \sim \sum_{P \in C(\overline{\mathbb{Q}})}(n_P[P] - n_P[\infty])$ with finitely many $n_P = 1$ and the other $n_P = 0$. Moreover we can assume without loss of generality that $P \notin C(\mathbb{Q})$ if $n_P = 1$, because if $P \in C(\mathbb{Q})$ and $D = [P] - [\infty] + D_1$, then we only have to write D_1 as the sum of generators, which implies that D is a sum of generators.
It is possible that both Q and $\varphi(Q)$ are in the support of D. In that case we can look at the minimal polynomial of $X(Q)$ over $\mathbb{Q}$, say f_Q. We know that the support of $(Y - f_Q)$ is the set $\{\sigma(Q), \sigma(\varphi(Q)) \mid \sigma \in G\}$. All the points in this set are also in the support of $\sum_{P \in C(\overline{\mathbb{Q}})}(n_P[P] - n_P[\infty])$, because by assumption Q and $\varphi(Q)$ in its support and this divisor is G-invariant. Hence $D \sim \sum_{P \in C(\overline{\mathbb{Q}})}(n_P[P] - n_P[\infty]) \sim \sum_{P \in C(\overline{\mathbb{Q}})}(n_P[P] - n_P[\infty]) - (Y - f_Q) =: B$.
We can do this for every point Q, for which also $\varphi(Q)$ is in the support of D. This gives us that D is linearly equivalent to a divisor B, with $n_P = 0$ or 1 and if $P \in \operatorname{supp}(B)$ then $\varphi(P) \notin \operatorname{supp}(B)$. Thus the support of B consists of, say k, distinct points P with all $X(P)$ distinct.
If $k \leq 2$, we have $D \sim [P] + [Q] - 2[\infty]$, and now we can apply proposition (1.3.4), which gives D the desired representation.
If $k > 2$, we have to do something more. Now we can construct a unique polynomial $g(X) \in \mathbb{C}[X]$ of degree at most $k - 1$, say m, through the points P in the support, s.t. for all P we have $Y(P) = g(X(P))$. Let $g(X) = \sum_{i=0}^{m} b_i X^i$.
Because B is G-invariant we have that $\sigma \in G$ acts as a permutation on the P in the support of B and if $Q = \sigma(P)$, then we have $g(X(Q)) = Y(Q) = \sigma(Y(P)) = \sigma(g(X(P))) = \sigma(g)(\sigma(X(P))) = \sigma(g)(X(Q))$. Hence $\sum_{i=0}^{m}(b_i - \sigma(b_i))X(Q)^i = 0$ for every Q in the support of B. There are k of such distinct Q's, so this gives k zeroes of the polynomial $\sum_{i=0}^{m}(b_i - \sigma(b_i))X^i = 0$, hence this polynomial is 0, which gives $b_i = \sigma(b_i)$ for all $\sigma \in G$ and hence $g(X) \in \mathbb{Q}[X]$.
Now we can substitute $Y = g(X)$ into $Y^2 - f_5(X)$, which gives us a polynomial of degree $n = \max(2m, 5) \leq \max(2k - 2, 5)$ in $\mathbb{Q}[X]$. We already know k of these roots and hence there are still $\max(2m - k, 5 - k) \leq \max(k - 2, 5 - k) < k$ other roots. Let $B_2 = \sum_{Q \in C(\overline{\mathbb{Q}})}(n_Q[Q] - [\infty])$ with $n_Q = \operatorname{ord}_Q(g(X)^2 - f_5(X))$ if Q not in the support of B. Because $g(X) \in \mathbb{Q}[X]$, we have that $B + B_2 \sim (g(X)^2 - f_5(X)) \sim 0$. Thus $B \sim -B_2 \sim \sum_{Q \in C(\overline{\mathbb{Q}})}(n_Q[\varphi(Q)] - [\infty])$ Again we may assume that $n_Q \in \{0, 1\}$. If this isn't the case, we can apply the operations we used at the beginning of this proof. Thus we have that $D \sim B \sim \sum_{Q \in C(\overline{\mathbb{Q}})} n_Q([Q] - [\infty]) = B_2$, and B_2 has the same properties as B, but has less than k points Q in its support and for those points $n_Q = 1$.

We can repeat this step until $k \leq 2$ and we have found an expression $D \sim [P] + [Q] - 2[\infty]$ and then we can apply proposition (1.3.4) and we get the desired representation.

Let now $D_1, D_2 \in J(\mathbb{Q})$ both be given by a generator as stated in the theorem. If $D_1 = [P] + [\sigma(P)] - 2[\infty], D_2 = [Q] + [\tau(Q)] - 2[\infty]$, with $P \neq Q$, then we see that there exists a polynomial of degree at most 3 through $P, \sigma(P), Q, \tau(Q)$. If we substitute this polynomial for Y in $Y^2 - f_5(X)$, we get two new points, R_1, R_2 (or in case the degree is smaller than 3, one point R_1, which must be in $C(\mathbb{Q})$, so we are done in this case). Hence we know that $D_1 + D_2 \sim [R_1] + [R_2] - 2[\infty]$, so we get our demanded form again out of proposition (1.3.4).
If $P = Q$ we have to create the polynomial $g(X)$ a bit more subtle by not only demanding that $Y(P) = g(X(P))$, but also that the curve $Y - g(X)$ has the same derivative in P as $Y^2 - f_5(X)$. This gives us the polynomial we need and again we get two new points R_1, R_2 after substituting g for Y in $Y^2 - f_5(X)$. For generators of the form $[P] + [Q] - 2[\infty], P \in C(\mathbb{Q})$ the argument is similar. ⊠

With this theorem we have not only described the elements of $J(\mathbb{Q})$, but in the proof we have also seen how the *group law* acts on those elements. In the latter part of the proof we showed that the sum of two generators is linearly equivalent to a generator. The way in which this is done describes exactly how the group law acts on elements of $J(\mathbb{Q})$.
Moreover, this theorem shows how $C(\mathbb{Q})$ is mapped to $J(\mathbb{Q})$. This map is an embedding.

Chapter 2

Embedding $J(\mathbb{Q})/2J(\mathbb{Q})$

In this chapter we will do the first step towards computing $J(\mathbb{Q})$. This first step consists in a 2-descent, i.e. we will try to compute $J(\mathbb{Q})/2J(\mathbb{Q})$. By using group cohomology we will construct a map from $J(\mathbb{Q})$ to L, a direct sum of fields we need to define, which gives rise to an embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$ into L. This map is rather complicated, so in the third paragraph we will find an easier description of this map. In chapter 3 we will see that the new description of this map simplifies computations.

2.1 The rank of the 2-torsion of $J(\mathbb{Q})$

In the previous chapter we described $J(\mathbb{Q})$ in terms of generators. Besides this approach, we can look at $J(\mathbb{Q})$ in a more abstract sense. This gives us a description of $J(\mathbb{Q})$ which gives us the information we need for the 2-descent method. We will state this other description as a fact.

Theorem 2.1.1 (Mordell Weil) *With the assumptions above we have*

$$J(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_t\mathbb{Z},$$

with $n_t \mid n_{t-1} \mid \ldots \mid n_1$.

$J(\mathbb{Q})$ is the direct sum of a group of infinite order and a finite group. This finite group is called the *torsion* of $J(\mathbb{Q})$. The infinite part is characterised by r, the *Mordell-Weil rank* of $J(\mathbb{Q})$.
The computation of this rank will be the problem of the rest of this chapter. In this paragraph we will describe $J(\mathbb{Q})/2J(\mathbb{Q})$.

We write $J(\mathbb{Q})[2] := \{D \in J(\mathbb{Q}) \mid D + D = 0\}$ for the 2-torsion of $J(\mathbb{Q})$. We can look at $J(\mathbb{Q})[2]$ as a vector space over $\mathbb{F}_2$. In this vectorspace linear dependency is the same as linear equivalency.

Proposition 2.1.2 *We have $J(\mathbb{Q})/2J(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^r \oplus (\mathbb{Z}/2\mathbb{Z})^s$, where r is the Mordell-Weil rank and $s = \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$.*

Proof. From the Mordell-Weil theorem (2.1.1) we know that

$$J(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_t\mathbb{Z},$$

with $n_1|n_2|\ldots|n_t$.
Now we look at multiplication by 2. Defined as map from $\mathbb{Z}$ to $\mathbb{Z}$, we have that $\mathbb{Z}/\mathrm{im}(2) \simeq \mathbb{Z}/2\mathbb{Z}$.
If $\gcd(2, n_i) = 1$, then we have that $2 \in (\mathbb{Z}/n_i\mathbb{Z})^*$, hence $2\mathbb{Z}/n_i\mathbb{Z} = \mathbb{Z}/n_i\mathbb{Z}$. So we have $(\mathbb{Z}/n_i\mathbb{Z})/2(\mathbb{Z}/n_i\mathbb{Z}) = 0$.
If $2|n_i$, and we look at multiplication by 2 on $\mathbb{Z}/n_i\mathbb{Z}$, we have that $\ker(2) = \langle \frac{n_i}{2} \rangle$, which has order 2, then also $(\mathbb{Z}/n_i\mathbb{Z})/\mathrm{im}(2)$ has order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
There are exactly s n_i's for which $2|n_i$, because $J(\mathbb{Q})[2] \simeq \oplus_{2|n_i} \mathbb{Z}/n_i\mathbb{Z}$.
Hence $J(\mathbb{Q})/2J(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^r \oplus (\mathbb{Z}/2\mathbb{Z})^s$. ⊠

The computation of this s is rather easy.

Proposition 2.1.3 *Let $P_i = (\alpha_i, 0), D_i = [P_i] - [\infty]$, then $D_1, \ldots, D_4$ are not linearly equivalent and $D_1, \ldots, D_5$ are linearly equivalent.*

Proof. First notice that for an element $D \in J(\overline{\mathbb{Q}})$, we have that $D \not\sim_{\overline{\mathbb{Q}}} 0 \Rightarrow D \not\sim 0$.
We know that if $D = (f)$, then $2D = (f^2)$ so if $D_i = (f)$, then $2D_i = (f^2) = (X - \alpha_i)$, but $(X - \alpha_i)$ is not a square in $\overline{\mathbb{Q}}[X]$, so we have $D_i \not\sim_{\overline{\mathbb{Q}}} 0$, hence $D_i \not\sim 0$. Obviously the latter conclusion of the proposition is true, for we have $(Y) \sim D_1 + \cdots + D_5$. Furthermore we have $0 \not\sim -D_5 = D_1 + \cdots + D_4$, so suppose $c_1D_1 + \cdots + c_4D_4 \sim 0$, then if 3 of the $c_i = 1$, say only $c_4 = 0$ then $0 \sim c_1D_1 + \cdots + c_4D_4 \sim D_4 + D_5$ But this cannot be true for $(X - \alpha_4)(X - \alpha_5)$ is not a square in $\overline{\mathbb{Q}}[X]$, so $D_4 + D_5 \not\sim_{\overline{\mathbb{Q}}} 0$, hence $D_4 + D_5 \not\sim 0$. If 2 of the $c_i = 1$ we use the same argument. ⊠

This proposition in fact states that the D_i are independent over $\mathbb{F}_2$.

Theorem 2.1.4 *We have*

$$\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = -1 + \#(\textit{irreducible factors of } f_5(X) \textit{ in } \mathbb{Q}[X]).$$

Proof. We have $f_5(X) = \prod_{i=1}^5 (X - \alpha_i), X - \alpha_i \in \overline{\mathbb{Q}}[X]$ and $f_5(X) = \prod_{j=1}^d h_j(X)$ with $h_j(X) \in \mathbb{Q}[X]$ irreducible. Every h_j is the product of some $(X - \alpha_i)$'s. Consider for some j the set $\{\alpha_i \mid h_j(\alpha_i) = 0\}$, then we know with some Galois-theory that this set is G-invariant. Denote this set as $\{\beta_1, \ldots, \beta_k\}$ (so $h_j(X) = \prod_{i=1}^k (X - \beta_i)$) and $Q_i = (\beta_i, 0)$. Let D_j be the divisor $D_j = \sum_{i=1}^k ([Q_i] - [\infty])$ which is in $J(\mathbb{Q})$, because $\{\beta_1, \ldots, \beta_k\}$ is G-invariant.

We have $Q_i = \varphi(Q_i)$, which gives $0 \sim (h_j(X)) \sim (\prod_{i=1}^{k}(X-\beta_i)) \sim \sum_{i=1}^{k}([Q_i]+[\varphi(Q_i)]-2[\infty]) \sim \sum_{i=1}^{k}(2[Q_i]-2[\infty]) \sim 2D_j$, so even $D_j \in J(\mathbb{Q})[2]$.
So every h_j gives rise to a divisor D_j of order 2. On the other hand we have that $D_1, \ldots, D_{d-1}$ are linearly independent over $\mathbb{F}_2$, as stated in the former proposition. This gives us that $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$ is at least $d-1$.
To prove that this dimension is also $\leq d-1$, we note that from theorem (1.3.5) we know that an element $D \in J(\mathbb{Q})$ can be written as $D \sim [P]+[Q]-2[\infty]$. Now suppose $2D \sim 0$, hence $2[P]+2[Q]-4[\infty] \sim 0$, thus we know that $2[P]+2[Q]-4[\infty] = (f)$ for some $f \in \mathbb{Q}(C)$, with $\mathrm{ord}_\infty(f) \geq -4, \mathrm{ord}_P(f) \geq 0$ for all other points P. We introduce the vector space $\mathcal{L}(n) := \{f \in \mathbb{Q}(C) \mid \mathrm{ord}_\infty(f) \geq -n, \mathrm{ord}_P \geq 0 \quad \forall P \in C(\overline{\mathbb{Q}})\backslash\{\infty\}\} \subset \mathbb{Q}[C]$. This is a vector space, because ord_P has the property $\mathrm{ord}_P(f_1+f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$. First notice that $\mathcal{L}(1)$ consists of the constant functions, because $f_1 \in \mathcal{L}(1)$ implies that f_1 has exactly one pole, which gives an isomorphism from C to $\mathbb{P}^1$ (we refer to [7], lemma 1.1). But this is impossible for a genus 2 curve (in fact this is impossible for every curve of genus > 0), hence f_1 is constant. Clearly we are interested in $\mathcal{L}(4)$, because $f \in \mathcal{L}(4)$. First notice that every function of the form $\sum a_i X^i$ is in $\mathcal{L}(4)$ if and only if its degree is at most 2.
Let now $f_1 \in \mathbb{Q}[C]$, we can write this uniquely as $f_1 = Y g_1(X) + g_2(X)$. If $g_1(X) = 0$, then $f_1 \in \mathcal{L}(4)$ if and only if $g_2 = aX^2+bX+c$. If $g_1(X) \neq 0$, then we have at least 5 zeroes (counted with multiplicity), hence $f_1 \notin \mathcal{L}(4)$. This gives us $\mathcal{L}(4) = \{aX^2+bX+c \mid a,b,c \in \mathbb{Q}\}$.
Thus there exist $\beta_1, \beta_2 \in \overline{\mathbb{Q}}$, s.t. $f = (X-\beta_1)(X-\beta_2)$. Let $Q_i \in C(\overline{\mathbb{Q}})$, s.t. $X(Q_i) = \beta_i$, then we have that $(f) = [Q_1]+[\varphi(Q_1)]+[Q_2]+[\varphi(Q_2)]-4[\infty] = 2[P]+2[Q]-4[\infty]$. Without loss of generality, we can now assume $P = Q_1, Q = Q_2$. This means $\varphi(P) = P$ (when $\varphi(P) = Q$, then already $D \sim 0$) and hence $Y(P) = 0$. The same is true for Q, hence $Y(Q) = 0$. Hence P and Q are both Weierstrass points. Hence there exists a j with $D \sim D_j$, which means that $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] \leq \dim_{\mathbb{F}_2} \mathrm{span}((D_j)) = d-1$.
This gives that $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = d-1$. Recall that d is the number of irreducible factors of $f_5(X)$ in $\mathbb{Q}[X]$, so we are done. ⊠

With this theorem we have an expression for the order of the torsion part of $J(\mathbb{Q})/2J(\mathbb{Q})$, so, once we know $J(\mathbb{Q})/2J(\mathbb{Q})$, we can simply compute the Mordell-Weil rank. From this we can maybe find $J(\mathbb{Q})$, therefore we need to compute the torsion points which are not 2-torsion.
For the computation of the Mordell-Weil rank we will turn our attention to the group $J(\mathbb{Q})/2J(\mathbb{Q})$. To compute this group we will bound it by a smaller and a larger group. With a bit of luck these two groups are equal and we find $J(\mathbb{Q})/2J(\mathbb{Q})$.
The smaller group will be the torsion group, possibly extended with some known points of infinite order in $J(\mathbb{Q})$. We have just seen that this group

is easy to compute. The larger group will be the so-called 2-Selmergroup, $S^2(\mathbb{Q}, J)$. The definition of this group and the way $J(\mathbb{Q})/2J(\mathbb{Q})$ embeds in this group is our next problem. For that purpose we need some group cohomology.

2.2 Group cohomology

We will start with the introduction of some notions and propositions concerning group cohomology.
We will be looking at a group M on which we assume a topology and a Galois-group $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which acts on M.

Definition 2.2.1 *We call M a G-module, when there exists a map $G \times M \to M$ written as $(\sigma, m) \mapsto \sigma(m)$, with*

(i) $id(m) = m$;

(ii) $\sigma(m_1 + m_2) = \sigma(m_1) + \sigma(m_2)$;

(iii) $(\sigma\tau)(m) = \sigma(\tau(m))$.

Definition 2.2.2 *The* 0th cohomology group *of the G-module M, denoted by $H^0(G, M)$ is the group consisting of the G-invariant elements of M. Furthermore we define the group of* 1-cochains

$$C^1(G, M) = \{\textit{mappings } \xi : G \longrightarrow M\},$$

the group of continuous 1-cocycles

$$Z^1(G, M) = \{\xi \in C^1(G, M) \mid \xi(\sigma\tau) = \sigma(\xi(\tau)) + \xi(\sigma) \quad \forall \sigma, \tau \in G\},$$

and the group of 1-coboundaries

$$B^1(G, M) = \{\xi \in C^1(G, M) \mid \exists m \in M, s.t. \;\; \xi(\sigma) = \sigma(m) - m \quad \forall \sigma \in G\}.$$

Because $B^1(G, M) \subset Z^1(G, M)$ we can introduce the 1st cohomology group *as the group 1-cocycles divided out by the group of coboundaries:*

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

With this definitions we construct a rather powerful tool, namely *exact sequences.*

Definition 2.2.3 *If M_1 and M_2 are G-modules, we define a* G-homomorphism *to be a homomorphism $\psi : M_1 \longrightarrow M_2$, which commutes with the action of G.*
We also define an exact sequence *of G-modules M_1, M_2, M_3 to be a sequence*

$$0 \longrightarrow M_1 \xrightarrow{\psi_1} M_2 \xrightarrow{\psi_2} M_3 \longrightarrow 0,$$

with ψ_i G-homomorphisms, $im(\psi_1) = ker(\psi_2)$, ψ_1 injective and ψ_2 surjective.

With these definitions we can construct a long exact sequence out of the short one as follows:

Proposition 2.2.4 *Let*

$$0 \longrightarrow M_1 \xrightarrow{\psi_1} M_2 \xrightarrow{\psi_2} M_3 \longrightarrow 0$$

be an exact sequence of G-modules. This sequence gives rise to the next long exact sequence:

$$\begin{aligned} 0 \longrightarrow H^0(G,M_1) &\xrightarrow{\psi_1} H^0(G,M_2) \xrightarrow{\psi_2} H^0(G,M_3) \xrightarrow{\delta} \\ H^1(G,M_1) &\xrightarrow{\psi_1} H^1(G,M_2) \xrightarrow{\psi_2} H^1(G,M_3), \end{aligned}$$

where the map δ is defined as follows. Let $m_3 \in H^0(G,M_3) = M_3^G$, then there exists an $m_2 \in M_2$, such that $\psi_2(m_2) = m_3$. Now define a cochain $\xi \in C^1(G,M_2)$ by $\xi(\sigma) = \sigma(x) - x$, then we have $\xi \in Z^1(G,M_1)$ and $\delta(n)$ is an element of the cohomology class $H^1(G,M_1)$ of the cocycle ξ.

Proof. First we prove that $\xi \in Z^1(G,M_1)$. We know that $\xi(\sigma) = \sigma(m_2) - m_2$. The question is whether for all σ there exists a $m_1 \in M_1$, s.t. $\psi_1(m_1) = \sigma(m_2) - m_2$. We know that ψ_1 is injective and that $\mathrm{im}(\psi_1) = \ker(\psi_2)$. Notice that by construction $\psi_2(m_2) \in M_3^G$, hence $\psi_2(\sigma(m_2) - m_2) = \sigma(\psi_2(m_2)) - \psi_2(m_2) = 0$, thus $\sigma(m_2) - m_2 \in \ker(\psi_2) = \mathrm{im}(\psi_1)$. So indeed such an m_1 exists and so $\xi \in Z^1(G,M_1)$.
We will only prove that (i) $\mathrm{im}(\psi_2) = \ker(\delta)$ and (ii) $\mathrm{im}(\delta) = \ker(\psi_1)$.

(i) Let $m_3 \in \mathrm{im}(\psi_2)$, then $m_3 = \psi_2(m_2)$ and so $\xi = \delta(m_3) = 0$, because $m_2 \in M_2^G$ implies $\xi(\sigma) = \sigma(m_2) - m_2 = 0$. For the other inclusion, let $m_3 \in \ker(\delta)$, then $\xi = \delta(m_3)$ with $0 = \xi(\sigma) = \sigma(m_2) - m_2$ for some $m_2 \in M_2$ with $\psi_2(m_2) = m_3$ and for all $\sigma \in G$, so m is G-invariant and thus $m_2 \in M_2^G = H^0(G,M_2)$, so $m_3 = \psi_2(m_2) \in \mathrm{im}(\psi_2)$.

(ii) By construction we have $\psi_1(\xi)(\sigma) = \sigma(m_2) - m_2$ for some $m_2 \in M_2$, so indeed $\mathrm{im}(\delta) \subset \ker(\psi_1)$. The other inclusion goes analogously to the proof of $\xi \in Z^1(G,M_1)$.

⊠

A very useful lemma is the application of Hilbert '90 to the group $H^1(G,\overline{\mathbb{Q}}^*)$.

Lemma 2.2.5 *With the previous definition we have $H^1(G,\overline{\mathbb{Q}}^*) = 0$.*

Proof. By definition we have $H^1(G,\overline{\mathbb{Q}}^*) = Z^1(G,\overline{\mathbb{Q}}^*)/B^1(G,\overline{\mathbb{Q}}^*)$. The group $Z^1(G,\overline{\mathbb{Q}}^*)$ consists of the maps $\xi : G \to \overline{\mathbb{Q}}^*$ with $\xi(\sigma\tau) = \sigma(\xi(\tau))\xi(\sigma)$ (we use multiplication because $\mathbb{Q}^*$ is a multiplicative group). We know then by Hilbert '90 that there exists an $x \in \overline{\mathbb{Q}}^*$ with $\xi(\sigma) = \frac{\sigma(x)}{x}$ for all $\sigma \in G$, so $\xi \in B^1(G,\overline{\mathbb{Q}}^*)$ and thus $Z^1(G,\overline{\mathbb{Q}}^*) = B^1(G,\overline{\mathbb{Q}}^*) \Rightarrow H^1(G,\overline{\mathbb{Q}}^*) = 0$. ⊠

Before we will use this cohomology theory for finding a suitable and computable embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$, we will first give the proof of theorem (1.3.1).

Proof. (theorem (1.3.1))
We want to prove

$$J(\mathbb{Q}) \simeq \frac{(\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G}{\mathrm{Div}(\mathbb{Q}(C))}.$$

By definition we have

$$J(\mathbb{Q}) = \mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C) = \left(\frac{\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C)}{\mathrm{Div}(\overline{\mathbb{Q}}(C))}\right)^G.$$

So it seems rather logical to look at the sequence

$$0 \longrightarrow \mathrm{Div}(\overline{\mathbb{Q}}(C)) \longrightarrow \mathrm{Div}^0_{\overline{\mathbb{Q}}}(C) \longrightarrow \mathrm{Pic}^0_{\overline{\mathbb{Q}}}(C) \longrightarrow 0.$$

This gives us a long sequence

$$\begin{aligned} 0 \longrightarrow \quad & (\mathrm{Div}(\overline{\mathbb{Q}}(C)))^G \longrightarrow (\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G \longrightarrow J(\mathbb{Q}) \\ & \longrightarrow H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C)). \end{aligned}$$

If we can prove that $H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C)) = 0$, we get that

$$J(\mathbb{Q}) \simeq (\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G/(\mathrm{Div}(\overline{\mathbb{Q}}(C)))^G \tag{2.1}$$

To prove this we look at the sequence

$$0 \longrightarrow \overline{\mathbb{Q}}^* \longrightarrow \overline{\mathbb{Q}}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(\overline{\mathbb{Q}}(C)) \longrightarrow 0.$$

This gives the long sequence

$$\begin{aligned} 0 \longrightarrow \quad & \mathbb{Q}^* \longrightarrow \mathbb{Q}(C)^* \xrightarrow{\mathrm{div}} (\mathrm{Div}(\overline{\mathbb{Q}}(C)))^G \\ & \longrightarrow H^1(G, \overline{\mathbb{Q}}^*) \longrightarrow \ldots. \end{aligned}$$

Note that by lemma (2.2.5) we have $H^1(G, \overline{\mathbb{Q}}^*) = 0$, hence we have that $(\mathrm{Div}(\overline{\mathbb{Q}}(C)))^G = \mathrm{im}(\mathrm{div}) = \mathrm{Div}(\mathbb{Q}(C))$. Firstly we can substitute this in equation (2.1), which gives us

$$J(\mathbb{Q}) \simeq \frac{(\mathrm{Div}^0_{\overline{\mathbb{Q}}}(C))^G}{\mathrm{Div}(\mathbb{Q}(C))}.$$

Hence if we have $H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C)) = 0$, we are done.
Secondly we can rewrite the long sequence as

$$0 \longrightarrow \mathbb{Q}^* \longrightarrow \mathbb{Q}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(\mathbb{Q}(C)) \longrightarrow 0.$$

And the rest of the long sequence is now

$$0 \longrightarrow H^1(G, \overline{\mathbb{Q}}(C)^*) \longrightarrow H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C))$$
$$\longrightarrow H^2(G, \overline{\mathbb{Q}}^*) \longrightarrow H^2(G, \overline{\mathbb{Q}}(C)^*).$$

Noether has proved, as a variant of Hilbert '90, that $H^1(G, \overline{\mathbb{Q}}(C)^*) = 0$. We haven't defined what H^2 means, but it is something that can be defined in the same manner as H^1, which we will not do here (we refer to [13], pp. 4-8). Of this H^2 group we need that the embedding ψ of $\overline{\mathbb{Q}}^*$ into $\overline{\mathbb{Q}}(C)^*$ induces the map from $H^2(G, \overline{\mathbb{Q}}^*)$ to $H^2(G, \overline{\mathbb{Q}}(C)^*)$ in a similar way as it induces a map from $H^1(G, \overline{\mathbb{Q}}^*)$ to $H^2(G, \overline{\mathbb{Q}}(C)^*)$. Let's denote this map by Ψ. This gives an isomorphism

$$H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C))) \simeq \ker\left(\Psi : H^2(G, \overline{\mathbb{Q}}^*) \to H^2(G, \overline{\mathbb{Q}}(C)^*)\right).$$

So if we prove that this kernel is 0, then $H^1(G, \mathrm{Div}(\overline{\mathbb{Q}}(C))) = 0$ and we are done.
In our 'simple' case of model (1) we have a point $P \in C(\mathbb{Q})$, so there exists a $\pi \in \mathbb{Q}(C)$ with $\mathrm{ord}_P \pi = 1$. (In fact we can take $P = \infty$ and $\pi = \xi = \frac{Y}{X^3}$.) With this we can define a function

$$\mathrm{ev} : \overline{\mathbb{Q}}(C)^* \to \overline{\mathbb{Q}}^* \quad \text{by } f \mapsto \frac{f}{\pi^{\mathrm{ord}_P f}}(P).$$

Because $P \in C(\mathbb{Q})$, we have that this function commutes with the action of G. Moreover we have that $\mathrm{ev} \circ \psi = \mathrm{id}$. The function ev gives rise to $\mathrm{Ev} : H^2(G, \overline{\mathbb{Q}}(C)^*) \to H^2(G, \overline{\mathbb{Q}}^*)$. This map inherits, by the fact that ev commutes with the Galois action, the property that $\mathrm{Ev} \circ \Psi = \mathrm{Id}$, so we have that Ψ is an injection and so we have indeed that the kernel of Ψ is equal to 0. ⊠

The theory of group cohomology is very useful for our problem. First look at the short exact sequence:

$$0 \longrightarrow J(\overline{\mathbb{Q}})[2] \xrightarrow{\mathrm{id}} J(\overline{\mathbb{Q}}) \xrightarrow{2} J(\overline{\mathbb{Q}}) \longrightarrow 0.$$

With the theory we have just developed, we know how this short sequence gives a long one, (recall that: $J(\overline{\mathbb{Q}})[2]^G = J(\mathbb{Q})[2], J(\overline{\mathbb{Q}})^G = J(\mathbb{Q})$).

$$0 \longrightarrow J(\mathbb{Q})[2] \longrightarrow J(\mathbb{Q}) \xrightarrow{2} J(\mathbb{Q}) \xrightarrow{\delta} H^1(G, J(\overline{\mathbb{Q}})[2]).$$

Because this is an *exact* sequence it follows that δ induces the embedding

$$J(\mathbb{Q})/2J(\mathbb{Q}) \overset{\delta}{\hookrightarrow} H^1(G, J(\overline{\mathbb{Q}})[2]).$$

With this mapping we have an embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$ into $H^1(G, J(\overline{\mathbb{Q}})[2])$. This is the usual embedding one uses to compute the Mordell-Weil rank. We want our computations to be more simple, so we try to find another embedding and therefore we look at a few other short sequences.

2.3 The algebra $L = \mathbb{Q}[T]/(f_5(T))$

It is useful to define the algebra $L := \mathbb{Q}[T]/(f_5(T))$ and then $\overline{L} = \overline{\mathbb{Q}}[T]/(f_5(T))$. We recall the Chinese Remainder theorem.

Theorem 2.3.1 *Let K be a field and let $f \in K[X]$ be a separable polynomial, then we can write $f(X) = \prod_{i=1}^{d} f_i(X)$, with $f_i(X) \in K[X]$ irreducible, and $K[T]/(f(T))$ is a direct sum of fields, in fact*

$$K[X]/(f(X)) = \oplus_{i=1}^{d} K[X]/(f_i(X)).$$

This theorem implies that we have

$$\overline{L} \simeq \oplus_{i=1}^{5} \overline{\mathbb{Q}},$$

because $\overline{\mathbb{Q}}[X]/(X - \alpha_i) \simeq \overline{\mathbb{Q}}$. And if f_5 splits over $\mathbb{Q}$ as $f_5(T) = \prod_{j=1}^{d} h_j(T)$, with $h_j(T) \in \mathbb{Q}[T]$ irreducible, then we have

$$L \simeq \oplus_{j=1}^{d} \mathbb{Q}[T]/(h_j(T)).$$

By defining $\sigma(T) = T$ for all $\sigma \in G$, we can consider $\overline{L}$ as a G-module. With this definition we see that if we have an element $g \in L$, then obviously $\sigma(g) = g$ for all $\sigma \in G$. We can consider L as the G-invariants of $\overline{L}$.
The previous theorem states that $\overline{L}$ can be considered as 5 copies of $\overline{\mathbb{Q}}$. What is the actual action of a $\sigma \in G$ on such a 5-tuple? Let Ψ be the isomorhism $\overline{L} \mapsto \prod_{i=1}^{5} \overline{\mathbb{Q}}$. Let $g \in \overline{L}$ and $(c_1, \ldots, c_5) = \Psi(g)$, then by the definition of Ψ we have that $g = g_i(T)(T - \alpha_i) + c_i$, for some $g_i \in \overline{\mathbb{Q}}[X]$. We know how σ acts on g, this gives us $\sigma(g) = \sigma(g_i(T))(T - \sigma(\alpha_i)) + \sigma(c_i)$. We know that σ permutes the α_i. Let's denote this permutation by s, s.t. $j = s^{-1}(i)$. Then we have $\sigma(g) = \sigma(g_i(T))(T - \alpha_{s^{-1}(i)}) + \sigma(c_i)$, hence $\Psi(\sigma(g)) = (\sigma(c_{s^{-1}(1)}), \ldots, \sigma(c_{s^{-1}(5)}))$. We would like to have that $\Psi(\sigma(g)) = \sigma(\Psi(g))$, so we simply define the action of σ on a 5-tuple as the action on each of its coordinates followed by the permutation induced by σ. This all justifies the next proposition.

Proposition 2.3.2 *Every $\sigma \in G$ induces a permutation on the 5-tuple $(c_1, \ldots, c_5) = \Psi(g), g \in \overline{L}$, as described above.*

Now we can understand what it means that an element $g \in L$ is G-invariant as a 5-tuple. Because $\sigma(g) = g$ for a G-invariant element, we get 5-tuple-wise that $(c_1, \ldots, c_5) = (\sigma(c_{s^{-1}(1)}), \ldots, \sigma(c_{s^{-1}(5)}))$, hence $c_i = c_{s^{-1}(i)}$. So for a G-invariant element, the only action of σ is the coordinate permutation. Hence we can describe a G-invariant element as elements for which $(c_1, \ldots, c_5)$ is, upto the coordinate permutation of σ for all $\sigma \in G$ equal to $(\sigma(c_1), \ldots, \sigma(c_5))$. We will call this simply 'fixed upto the permutation of G'.

Remark 2.3.3 We can extend this action of G on elements of $\prod_{i=1}^{5} \overline{\mathbb{Q}}$ to an action on 5-tuples of points or divisors, simply by using the same coordinate permutation followed by the action of σ on each coordinate. Again we have that G-invariance is the same as being fixed upto the permutation of G. If we e.g. look at the 5-tuple $(P_1, \ldots, P_5)$, then we have that this 5-tuple is G-invariant, because $\sigma(P_i) \in \{P_1, \ldots, P_5\}$.

2.4 The isomorphism $k \circ w$

Because $H^1(G, J(\overline{\mathbb{Q}})[2])$ is a rather abstract object we will, in this paragraph, create an isomorphism from this group to another in which computations are more easily done.
We will start with the introduction of some groups and some maps.

Definition 2.4.1 *Let $\mu_2(\overline{\mathbb{Q}})$ be the group of second roots of unity in $\overline{\mathbb{Q}}$, hence*

$$\mu_2(\overline{\mathbb{Q}}) := \{x \in \overline{\mathbb{Q}} \mid x^2 = 1\} = \{\pm 1\}.$$

Let $\mu_2(\overline{L})$ be the group of the second roots of unity in $\overline{L}$, hence

$$\mu_2(\overline{L}) := \{l \in \overline{L} \mid l^2 = 1\}.$$

We already saw that $\overline{L}$ is isomorphic to 5 copies of $\overline{\mathbb{Q}}$, hence $\mu_2(\overline{L}) \simeq \mu_2(\overline{\mathbb{Q}})^5$. We know that $\mu_2(\overline{\mathbb{Q}}) \simeq (\pm 1)$ and hence $\mu_2(\overline{L}) \simeq (\pm 1)^5$.

Definition 2.4.2 *We define the Weil-pairing,*

$$e_2 : (J(\overline{\mathbb{Q}})[2])^2 \to \mu_2(\overline{\mathbb{Q}}),$$

as follows. Let $D_1, D_2 \in Div^0_{\overline{\mathbb{Q}}}(C)$, with disjoint support (i.e. we see D_1, D_2 as divisors of degree 0), then there exist $f_1, f_2 \in \overline{\mathbb{Q}}(C)$ such that $2D_1 = (f_1), 2D_2 = (f_2)$, and we define

$$e_2(D_1, D_2) = \frac{f_1(D_2)}{f_2(D_1)}.$$

First notice that $\left(\frac{f_1(D_2)}{f_2(D_1)}\right)^2 = \frac{f_1(2D_2)}{f_2(2D_1)} = \frac{f_1((f_2))}{f_2((f_1))} \overset{(*)}{=} \frac{f_1((f_2))}{f_1((f_2))} = 1$, where $(*)$ follows from the Weil-reciprocity, theorem (1.2.5), hence the Weil-pairing indeed maps to $\mu_2(\overline{\mathbb{Q}})$.
The question remains whether the Weil-pairing is well-defined. There are two problems in the definition. The first problem is that the representations f_i can be multiplied with some constant. So besides $2D_i = (f_i)$, we also have $2D_i = (a_i f_i)$, for some constants a_i (of course $a_i \neq 0$). If we write $D_1 = \sum_{P \in C} n_P[P]$, we get

$$a_2 f_2(D_1) = \prod_{P \in C} (a_2 f_2(P))^{n_P} = a_2^{\sum_{P \in C} n_P} f_2(D_1) = a_2^{\deg(D_1)} f_2(D_1) = f_2(D_1).$$

With the same computation we get $a_1 f_1(D_2) = f_1(D_2)$, hence for another choice of f_i, we get the same image under e_2.
The second problem is that we know that elements of $J(\overline{\mathbb{Q}})$ are divisor classes, so if we have 2 representants $D_1, \tilde{D}_1$, for the same element in $J(\overline{\mathbb{Q}})[2]$, does this actually give the same image under the Weil-pairing? Suppose $(f_1) = 2D_1, (\tilde{f}_1) = 2\tilde{D}_1$, and $D_1 - \tilde{D}_1 = (g)$, then $(\frac{f_1}{\tilde{f}_1}) = 2(g)$, in fact we can choose g, s.t. $\frac{f_1}{\tilde{f}_1} = g^2$. Hence

$$\frac{e_2(D_1, D_2)}{e_2(\tilde{D}_1, D_2)} = \frac{f_1(D_2)}{\tilde{f}_1(D_2)} \frac{f_2(D_1)}{f_2(\tilde{D}_1)} = g(D_2)^2 f_2(D_1 - \tilde{D}_1) =$$

$$g((f_2))f_2((g)) = g((f_2))^2 = 1.$$

We can use the same argument for two different representants for D_2, hence the Weil-pairing is well-defined.
We will summarize a few properties which we need.

Proposition 2.4.3 *The Weil-pairing has the following properties*

(*i*) *We have* $e_2(D_1, D_2) = e_2(D_2, D_1)$, *hence* e_2 *is symmetric in its arguments.*

(*ii*) *The map* e_2 *is bilinear and even* $e_2(-D_1, D_2) = e_2(D_1, D_2)$.

(*iii*) *We have*

$$e_2([P_j] - [\infty], [P_i] - [\infty]) = \frac{\alpha_i - \alpha_j}{\alpha_j - \alpha_i} = -1, i \neq j.$$

(*iv*) *The map* e_2 *is non-degenerate, i.e. if* $e_2(D_1, D_2) = 1$ *for all* $D_2 \in J(\overline{\mathbb{Q}})[2]$, *then* $D_1 = 0$.

(*v*) *The Weil-pairing commutes with the action of* G.

Proof.

(*i*) We know $e_2(D_2, D_1)^2 = 1$, because e_2 maps into $\mu_2(\overline{\mathbb{Q}})$. Hence

$$\frac{e_2(D_1, D_2)}{e_2(D_2, D_1)} = e_2(D_1, D_2)e_2(D_2, D_1) = \frac{f_1(D_2)}{f_2(D_1)} \frac{f_2(D_1)}{f_1(D_2)} = 1.$$

(*ii*) Let $D_1, D_2, D_3 \in J(\overline{\mathbb{Q}})[2]$, and $f_i \in \overline{\mathbb{Q}}(C)$, s.t. $2D_i = (f_i)$, then we have $2(D_1 + D_2) = (f_1 f_2)$, and $(f_1 f_2)(D_3) = f_1(D_3)f_2(D_3)$, hence

$$e_2(D_1 + D_2, D_3) = \frac{f_3(D_1 + D_2)}{(f_1 f_2)(D_3)} = \frac{f_3(D_1)f_3(D_1)}{f_1(D_3)f_2(D_3)} =$$

$$\frac{f_3(D_1)}{f_1(D_3)} \frac{f_3(D_2)}{f_2(D_3)} = e_2(D_1, D_3)e_2(D_2, D_3).$$

That e_2 is also linear in its second argument now follows from (*i*).
We immediately see that $e_2(-D_1, D_2) = e_2(D_2, D_1) = e_2(D_1, D_2)$.

(*iii*) We just evaluate $e_2([P_j]-[\infty],[P_i]-[\infty])$, this gives us:

$$e_2([P_j]-[\infty],[P_i]-[\infty]) = \frac{(X-\alpha_j)([P_i]-[\infty])}{(X-\alpha_i)([P_j]-[\infty])} = \frac{\alpha_i-\alpha_j}{\alpha_j-\alpha_i}\frac{\infty-\alpha_j}{\infty-\alpha_i} = -1.$$

Because ∞ is in the support of both $[P_i]-[\infty]$ and $[P_j]-[\infty]$ we officially need to rewrite at least one of the $[P_i]-[\infty]$, $[P_j]-[\infty]$ in such a way that we have representants with disjoint support. How this works is shown in the proof of a theorem that will be stated in the next paragraph.

(*iv*) We know that $J(\overline{\mathbb{Q}})[2]$ is generated by $[P_i]-[\infty], i = 1,\ldots,4$. Thus $e_2(D_1,D_2) = 1$ for all D_2 if $e_2(D_1,[P_i]-[\infty]) = 1$ for all i. $D_1 \sim \sum_{i=1}^4 c_i([P_i]-[\infty]), c_i \in \{0,1\}$, thus

$$e_2(D_1,[P_j]-[\infty]) = \prod_{i=1}^{4}(e_2([P_i]-[\infty],[P_j]-[\infty]))^{c_i}.$$

This gives us that $e_2(D_1,D_2) = 1$ for all D_2 if and only if $D_1 = 0$, which proves the non-degeneracy of the Weil-pairing.

(*v*) We see

$$(e_2(\sigma(D_1),\sigma(D_2)) = \frac{\sigma(f_1)(\sigma(D_2))}{\sigma(f_2)(\sigma(D_1))} = \sigma\left(\frac{f_1(D_2)}{f_2(D_1)}\right) = \sigma(e_2(D_1,D_2)).$$

⊠

Definition 2.4.4 *With the Weil-pairing we can define a map*

$$w : J(\overline{\mathbb{Q}})[2] \to \mu_2(\overline{L}) \quad by \quad P \mapsto (e_2(P,[P_1]-[\infty]),\ldots,e_2(P,[P_5]-[\infty])).$$

This is obviously an homomorphism, moreover it is an injection. We can see this as follows. If $P \in J(\overline{\mathbb{Q}})[2]$ is in the kernel of w, then we have that $e_2(P,[P_i]-[\infty]) = 1$, for all i, hence by the non-degeneracy of the Weil-pairing we get $P = 0$.
By property (v) of proposition (2.4.3), it follows that w is a G-module homomorphism.

Definition 2.4.5 *We define a norm $N : \overline{L} \to \overline{\mathbb{Q}}$ as follows. Look at $\overline{L}$ as 5 copies of $\overline{\mathbb{Q}}$ and define $N : g = (c_1,\ldots,c_5) \mapsto \prod_{i=1}^5 c_i$.*
This norm map induces a norm, also denoted by N, from $\mu_2(\overline{L})$ to $\mu_2(\overline{\mathbb{Q}})$, again defined by taking the product of the coordinates.

Proposition 2.4.6 *With all these definitions we get the short exact sequence of G-modules*

$$0 \longrightarrow J(\overline{\mathbb{Q}})[2] \xrightarrow{w} \mu_2(\overline{L}) \xrightarrow{N} \mu_2(\overline{\mathbb{Q}}) \longrightarrow 1.$$

Proof. Because N is surjective (obvious) and w is injective, we only need to prove that $\ker(N) = \mathrm{im}(w)$. Let $m \in \mathrm{im}(w)$, then there exists a $P \in J(\overline{\mathbb{Q}})[2]$, with $m = w(P) = (e_2(P,[P_i]-[\infty]),\ldots,e_2(P,[P_5]-[\infty]))$. Let now $h \in \overline{\mathbb{Q}}(C)$, s.t. $2P = (h)$. We have already seen that $[P_5]-[\infty] \sim \sum_{i=1}^{4}[P_i]-[\infty]$. This gives

$$e_2(P,[P_5]-\infty) = e_2(P,\sum_{i=1}^{4}[P_i]-[\infty]) = \prod_{i=1}^{4} e_2(P,[P_i]-[\infty]).$$

So it follows

$$N(w(P)) = \prod_{i=1}^{5} e_2(P,[P_i]-[\infty]) = \left(\prod_{i=1}^{4} e_2(P,[P_i]-[\infty])\right)^2 = 1$$

and thus indeed $m = w(P) \in \ker(N)$ and hence $\mathrm{im}(w) \subset \ker(N)$.
For the other inclusion we use that the rank of $\ker(N)$ is 4, which is the same as the rank of $J(\overline{\mathbb{Q}})[2]$ and because w is an injection, it follows that $\mathrm{im}(w) \supset \ker(N)$, which proves the proposition.
⊠

With this knowledge and our previous results about short exact sequences, this short sequence gives rise to the following long exact one:

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

From this sequence we deduce that

$$w : H^1(G,J(\overline{\mathbb{Q}})[2]) \longrightarrow H^1(G,\mu_2(\overline{L}))$$

is a homomorphism and its image is exactly

$$\ker\left(N : H^1(G,\mu_2(\overline{L})) \longrightarrow H^1(G,\mu_2(\overline{\mathbb{Q}}))\right).$$

The second w inherits the injectivity from the first w in the last long exact sequence. Hence this results in the isomorphism

$$H^1(G,J(\overline{\mathbb{Q}})[2]) \overset{w}{\simeq} \ker\left(N : H^1(G,\mu_2(\overline{L})) \longrightarrow H^1(G,\mu_2(\overline{\mathbb{Q}}))\right).$$

But we are not done yet. Take a look at the next short exact sequence.

$$1 \longrightarrow \mu_2(\overline{\mathbb{Q}}) \longrightarrow \overline{\mathbb{Q}}^* \xrightarrow{2} \overline{\mathbb{Q}}^* \longrightarrow 1.$$

This is actually an exact sequence. The squaring map is clearly surjective. The second roots of unity, $\mu_2(\overline{\mathbb{Q}}) = \{\pm 1\}$, are canonically embedded in $\overline{\mathbb{Q}}^*$

and $\ker(2) = \{x \in \overline{\mathbb{Q}}^* \mid x^2 = 1\}$, which is by definition equal to $\mu_2(\overline{\mathbb{Q}})$. So this gives rise to the long sequence

$$\begin{aligned} 1 \longrightarrow\ & \mu_2(\mathbb{Q}) \to \mathbb{Q}^* \xrightarrow{2} \mathbb{Q}^* \\ \xrightarrow{\delta_1}\ & H^1(G, \mu_2(\overline{\mathbb{Q}})) \longrightarrow H^1(G, \overline{\mathbb{Q}}^*) = 0. \end{aligned}$$

Out of this last sequence we can deduce that we have an homomorphism

$$\delta_1 : \mathbb{Q}^* \longrightarrow H^1(G, \mu_2(\overline{\mathbb{Q}})),$$

where the image of δ_1 is the kernel of the next map in the sequence, which is the zero-map. Hence the image of δ_1 is $H^1(G, \mu_2(\overline{\mathbb{Q}}))$. The kernel of δ_1 is the image of the square-mapping which is $\mathbb{Q}^{*2}$. So this long sequence gives an isomorphism

$$\mathbb{Q}^*/\mathbb{Q}^{*2} \simeq H^1(G, \mu_2(\overline{\mathbb{Q}})). \tag{2.2}$$

We can repeat what we did just now for the sequence

$$1 \to \mu_2(\overline{L}) \to \overline{L}^* \xrightarrow{2} \overline{L}^* \to 1.$$

Out of this short sequence we get again a long one. Because according to [10], pp. 221, we have that $H^1(G, \overline{L}^*) = 0$, we can use the same line of argument to get an isomorphism:

$$L^*/L^{*2} \simeq H^1(G, \mu_2(\overline{L})). \tag{2.3}$$

Remark 2.4.7 The inverse of this isomorphism is usually called the Kummer isomorphism and is denoted by k. Let's recall how the map δ_1 is defined, to see what k does. Let $l \in L^*$ and $\sqrt{l} \in L^*$, then $\delta_1(l)$ is the cocycle class, which includes the map $\xi : \sigma \mapsto \frac{\sigma(\sqrt{l})}{\sqrt{l}}$, thus the inverse k maps the cocycle class, which includes ξ to l.

Let's look at the results we have obtained so far and make a theorem out of it.

Theorem 2.4.8 *With all the previous definitions we have that $J(\mathbb{Q})/2J(\mathbb{Q})$ embeds into the group $H^1(G, J(\overline{\mathbb{Q}})[2])$ (by the map δ) and $H^1(G, J(\overline{\mathbb{Q}})[2])$ is isomorphic (by the map $k \circ w$) to $\ker\left(N : L^*/L^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}\right)$.*

Proof. It's exactly what we have been doing the last few pages. First we created an embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$ into $H^1(G, J(\overline{\mathbb{Q}})[2])$. Then we saw that this last group is isomorphic to $\ker\left(N : H^1(G, \mu_2(\overline{L})) \to H^1(G, \mu_2(\overline{\mathbb{Q}}))\right)$ by the map w. With (2.2) and (2.3) this kernel is isomorphic to $\ker\left(N : L^*/L^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}\right)$. ⊠

2.5 The map $(X - T)$

So far we have found an embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$ into the kernel of the norm-mapping. But we still haven't found an easy way to compute this embedding. To achieve this we introduce a new map:

$$(X - T) : \mathrm{Div}^0_{\mathbb{Q}}(C)^* \longrightarrow L^*,$$

$$\text{by } \sum n_i[Q_i] \longmapsto \prod (X(Q_i) - T)^{n_i},$$

$$\text{with } \prod (X(Q_i) - T)^{n_i} = (\prod (X(Q_i) - \alpha_1)^{n_i}, \ldots, \prod (X(Q_i) - \alpha_5)^{n_i}),$$

where $\mathrm{Div}^0_{\mathbb{Q}}(C)^*$ denotes the subset of $\mathrm{Div}^0_{\mathbb{Q}}(C)$, consisting of divisors with no Weierstrass points in their supports.

Proposition 2.5.1 *$(X - T)$ is well-defined as a map from $J(\mathbb{Q})$ to L^*/L^{*2}.*

Proof. First we will show that every element of $J(\mathbb{Q})$ can be represented by a divisor in $\mathrm{Div}^0_{\mathbb{Q}}(C)$ with no Weierstrass points in its support. We know that every $D \in J(\mathbb{Q})$ can be written as $D \sim [R_1] + [R_2] - 2[\infty]$ with either

(*i*) $R_i \in C(\mathbb{Q})$, or

(*ii*) $R_i \in C(\mathbb{Q}(\sqrt{d})), d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ with $R_1 = \sigma(R_2)$ for some $\sigma \in G$.

Let k be the number of Weierstrass points in $\{R_i\}$, and let $h(X) = (X - X(R_1))(X - X(R_2)) \in \mathbb{Q}[X]$, then we have

$$(Y - h(X)) = \sum_{i=1}^{k} [R_i] + \sum_{i=1}^{5-k} [Q_i] - 5[\infty].$$

We have that $\sigma(\sum_{i=1}^{k}[R_i]) = \sum_{i=1}^{k}[R_i]$, because they're all Weierstrass points and the Q_i's are not. (The Q_i's are no Weierstrass points, because if they were, they would be one of the R_i's which would give a double zero in f_5, and this is not possible.) Thus also $\sigma(\sum_{i=1}^{5-k}[Q_i]) = \sum_{i=1}^{5-k}[Q_i]$, hence $h_3(X) = \prod_{i=1}^{5-k}(X - X(Q_i)) \in \mathbb{Q}[C]$ and

$$(h_3) = \sum_{i=1}^{5-k}([Q_i] + [\varphi(Q_i)] - 2[\infty]) = D_{h_3} - 2(5-k)[\infty],$$

with no Weierstrass points in the divisor D_{h_3}. Also $g(Y) = \prod_{i=1}^{5-k}(Y - Y(Q_i)) \in \mathbb{Q}[C]$ and

$$(g) = \sum_{i=1}^{5-k} B_i - 5[\infty] = D_g - 5(5-k)[\infty],$$

where B_i is the divisor with the points for which $Y - Y(Q_i)$ is zero in its support. There are exactly 5 of such points and these points are all non-Weierstrass. In the third expression we have that D_g is a divisor with no Weierstrass points in its support.
By construction we can also write $(\frac{(Y-h)^2}{h}) = 2(Y-h) - (h) = D_r - 6[\infty]$, with D_r no Weierstrass points in its support.
What's the use of this all? We see that $D \sim D - (Y-h) \sim \sum_{i=1}^{2-k}[R_i] - \sum_{i=1}^{5-k}[Q_i] - 3[\infty]$. In this latter representation only ∞ is a Weierstrass point.

(*i*) $k = 0$. Now we can define $A = (g) - (h_3) - 2(\frac{(Y-h)^2}{h}) = D_g - D_{h_3} - 2D_r - 3[\infty]$, hence the only Weierstrass point in A is ∞ and $D \sim \sum_{i=1}^{2-k}[R_i] - \sum_{i=1}^{5-k}[Q_i] - 3[\infty] - A \sim \sum_{i=1}^{2-k}[R_i] - \sum_{i=1}^{5-k}[Q_i] + D_g - D_{h_3} - 2D_r$, which has no Weierstrass points in its support.

(*ii*) $k = 1$. Now we take $A = (g) + 2(h_3) - (\frac{(Y-h)^2}{h}) = D_g + 2D_{h_3} - D_r - 3[\infty]$, and again $D \sim \sum_{i=1}^{2-k}[R_i] - \sum_{i=1}^{5-k}[Q_i] - 3[\infty] - A$ gives a representation without Weierstrass points.

(*iii*) $k = 2$. Now we can take $A = (g) - 2(h_3)$ and we find $D \sim \sum_{i=1}^{2-k}[R_i] - \sum_{i=1}^{5-k}[Q_i] - 3[\infty] - A$, as a representation with no Weierstrass points.

This proves that every element of $J(\mathbb{Q})$ can be represented by a divisor in $\mathrm{Div}^0_{\mathbb{Q}}(C)$ with no Weierstrass points in its support. So $X - T$ can act on representants of every class in $J(\mathbb{Q})$. But we still have to prove that it is well-defined.

Two divisors of degree 0 are the same as elements of the Jacobian if and only if they are linearly equivalent. So for the rest of the proposition we have to prove that the difference of two linearly equivalent divisors will be mapped to L^{*2}.
Let $D_1, D_2 \in J(\mathbb{Q})$ be mutually linearly equivalent with no Weierstrass points in their support and let $f \in \mathbb{Q}(C)$, with $(f) = D_1 - D_2$. When we look at $(X - T)(D_1 - D_2)$ elementwise, we get $(X - \alpha_i)(D_1 - D_2) = (X - \alpha_i)((f)) = f((X - \alpha_i)) = f(2[P_i] - 2[\infty]) = (f([P_i] - [\infty]))^2 \in \overline{\mathbb{Q}}$.
We have that for every element $\sigma(f([P_i] - [\infty])) = f(\sigma([P_i] - [\infty]))$ because $f \in \mathbb{Q}(C)$. In remark (2.3.3) we already saw that the 5-tuple of points $(P_1, \ldots, P_5)$ is fixed by G upto permutation. For the same reason we have that the 5-tuple of divisors $([P_1] - [\infty], \ldots, [P_5] - [\infty])$ is fixed by G upto permutation and thus we have that $(f([P_1] - [\infty]), \ldots, f([P_1] - [\infty])) \in \overline{L}^*$ is fixed by G upto coordinate-permutation and thus we have that $(f([P_1] - [\infty]), \ldots, f([P_1] - [\infty])) \in L^*$ and thus $(f([P_1] - [\infty]), \ldots, f([P_1] - [\infty]))^2 \in L^{*2}$, which is exactly what we had to prove. ⊠

Remark 2.5.2 With same line of argument as in the latter proof, we can show how we can easily compute with this mapping $X - T$, when we have as a representant a divisor with a Weierstrass point in its support. Suppose we have a G-invariant divisor $D = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})}(\sigma(Q) - [\infty])$, with Q no Weierstrass and K the smallest Galois extension with $Q \in K$, then we have that $(X - T)(D) \equiv \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})}(X(\sigma(Q)) - T) \bmod L^{*2}$, hence we can 'forget' the ∞-term. Moreover if we have that $D = [P_1] - [\infty]$, then we get $(X - T)(D) = \prod_{i=2}^{5}(\alpha_i - T) + (\alpha_1 - T) \bmod L^{*2} = (\prod_{i=2}^{2}(\alpha_i - \alpha_1), \alpha_1 - \alpha_2, \ldots, \alpha_1 - \alpha_5)$. The idea of the proof of this is very similar to the proof we just gave. We refer to [10], lemma 2.2.

What has this mapping $X - T$ to do with the results from our previous paragraphs? What is the use of this map? The next theorem answers these questions.

Theorem 2.5.3 *The map $X - T$ is the same injection from $J(\mathbb{Q})/2J(\mathbb{Q})$ to L^*/L^{*2} as the map $k \circ w \circ \delta$.*

Proof. The idea of this proof (see [10], pp. 225) is that we represent an element in $J(\mathbb{Q})/2J(\mathbb{Q})$ by a divisor D_1 and a divisor $2D_2$, with $D_1 \in J(\mathbb{Q}), D_2 \in J(\overline{\mathbb{Q}})$, D_1 is linearly equivalent to $2D_2$. We can assume that both divisors have no Weierstrass points in their support, because this can always be achieved the way as it is done in the proof of proposition (2.5.1). Then the class of cocycles $\delta(D_1)$ includes the cocycle ξ with $\xi(\sigma) = \sigma(D_2) - D_2$ and this gives that $w \circ \delta(D_1)$ is represented by the mapping $\sigma \mapsto (e_2(\sigma(D_2) - D_2, [P_1] - [\infty]), \ldots, e_2(\sigma(D_2) - D_2, [P_5] - [\infty]))$.
Now define $(h) = D_1 - 2D_2$. With some straightforward computations this gives us

$$w \circ \delta(D_1) = \frac{(X - T)(\sigma(D_2) - D_2)}{\frac{\sigma(h)}{h}(P_1, \ldots, P_5)} = \sigma\left(\frac{(X - T)(D_2)}{h(P_1, \ldots, P_5)}\right)\frac{1}{\left(\frac{(X-T)(D_2)}{h(P_1, \ldots, P_5)}\right)}.$$

In remark (2.4.7) we saw how k maps such a cocycle class and this gives us

$$k \circ w \circ \delta(D_1) = \left(\frac{(X - T)(D_2)}{h(P_1, \ldots, P_5)}\right)^2.$$

We know that $h(P_1, \ldots, P_5)^2 \in L^{*2}$ so we have

$$k \circ w \circ \delta(D_1) = ((X - T)(D_2))^2 = (X - T)(2D_2) = (X - T)(D_1),$$

which we wanted to prove. ⊠

We have done quite a lot so far: we found a nice embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$, via δ, into $H^1(G, J(\overline{\mathbb{Q}})[2])$ which is isomorphic to L^*/L^{*2} and we have found a computable mapping, namely $X - T$, from $J(\mathbb{Q})/2J(\mathbb{Q})$ to L^*/L^{*2}, which acts the same as injection as our embedding $k \circ w \circ \delta$. Our next step is to actually compute a subgroup of $H^1(G, J(\overline{\mathbb{Q}})[2])$ which contains $J(\mathbb{Q})/2J(\mathbb{Q})$, namely the Selmer-group.

Chapter 3

Local computations and the Selmer group

The next step in our search for r, the Mordell-Weil rank, is the computation of the 2-Selmer group. In this chapter we will define this group. For that purpose we will look at some preliminary results concerning p-adic completions of $\mathbb{Q}$. Then we define the Selmer group and we will find that this definition immediately gives an algorithm for computing this Selmer group via local computations. Note that this is exactly the reason why we introduce the Selmer group: the local computations are easily done and the Selmer group contains $J(\mathbb{Q})/2J(\mathbb{Q})$.

3.1 p-adic completions

We introduce the p-adic numbers as in [11], pp. 11-18.

Definition 3.1.1 *The set of* p-adic integers, $\mathbb{Z}_p$, *is the projective limit of the sequence*

$$\cdots \xrightarrow{\phi_n} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\phi_{n-1}} \mathbb{Z}/p^{n-1}\mathbb{Z} \xrightarrow{\phi_{n-2}} \cdots \xrightarrow{\phi_1} \mathbb{Z}/p\mathbb{Z},$$

where ϕ_n *is the map* $\bmod p^{n-1}$, *with kernel* $p^{n-1}(\mathbb{Z}/p^n\mathbb{Z})$.

With this definition we can consider an element $x \in \mathbb{Z}_p$ as an infinite sequence $(x_1, x_2, \dots)$ with the property $\phi_n(x_n) = x_{n-1}$, or, which is equivalent, $x_n \equiv x_m \bmod p^n$ for all $m > n$.
We have the exact sequence

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\xi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0,$$

with $\xi_n : (x_1, x_2, \dots) \mapsto x_n$, thus we have that $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$. In particular we see that $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$.

Every element $x \in \mathbb{Z}_p$ can uniquely be written as $x = p^k y$, with y invertible in $\mathbb{Z}_p$ and we can define the *p-adic valuation* $v_p(x) := k$; and we set $v_p(0) := \infty$. This p-adic valuation gives induces the *p-adic absolute value* defined by $|x|_p := p^{-v_p(x)}$. This gives us that $\mathbb{Z}_p$ is a complete metric space and $\mathbb{Z}$ lies dense in $\mathbb{Z}_p$. We have that $\mathbb{Z}_p$ is a domain, hence the field of p-adic numbers, $\mathbb{Q}_p$, the quotient of the p-adic integers, exists, and we even have $\mathbb{Q}_p = \text{Quot}(\mathbb{Z}_p) = \mathbb{Z}_p[p^{-1}]$. Because of the latter identity, we can extend the discrete valuation v_p to $\mathbb{Q}_p$ as well as the absolute value $|.|_p$. We have that $\mathbb{Q}$ lies dense in $\mathbb{Q}_p$.
Because we have that $\mathbb{Z}$ ($\mathbb{Q}$) lies dense in $\mathbb{Z}_p$ ($\mathbb{Q}_p$), we can consider $\mathbb{Z}_p$ ($\mathbb{Q}_p$) to be the completion, with respect to the p-adic absolute value, of $\mathbb{Z}$ ($\mathbb{Q}$).

One important result is Hensel's lemma.

Theorem 3.1.2 *Let $f(X) = a_0 + a_1 X + \ldots + a_n X^n, a_i \in \mathbb{Z}_p$. Suppose that there exists an $\alpha_1 \in \mathbb{Z}_p$, such that $f(\alpha_1) \equiv 0 \bmod p\mathbb{Z}_p$ and $f'(\alpha_1) \not\equiv 0 \bmod p\mathbb{Z}_p$. Then there exists an $\alpha \in \mathbb{Z}_p$ with $\alpha \equiv \alpha_1 \bmod p\mathbb{Z}_p$ and $f(\alpha) = 0$.*

Proof. Suppose we have α_1, s.t. $f(\alpha_1) = 0 \bmod p\mathbb{Z}_p$, then we can find $x_1 \in \mathbb{Z}_p$, s.t. $x_1 \equiv \alpha_1 \bmod p\mathbb{Z}_p$. As in Newton's method, we define $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)}$ and we see that now $x_2 \equiv x_1 \bmod p\mathbb{Z}_p$ and $f(x_2) = f(x_1) - f'(x_1)\frac{f(x_1)}{f'(x_1)}p +$ terms in $p^n, n \geq 2$. This gives us that $f(x_2) \equiv 0 \bmod p^2\mathbb{Z}_p$. In the same way we define $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, with the property that $f(x_{n+1}) \equiv 0 \bmod p^{n+1}\mathbb{Z}_p$ and $x_{n+1} \equiv x_n \bmod p^n\mathbb{Z}_p$. This gives us a sequence (x_n), with $x_n \in \mathbb{Z}_p$ and $x_n - x_{n+1} \equiv 0 \bmod p^n\mathbb{Z}_p$, hence $|x_n - x_{n+1}|_p \leq p^{-n} \to 0$, so (x_n) is a Cauchy sequence and hence has a limit in $\mathbb{Z}_p$, say x. This x is a root of f, for $f(x) \equiv f(x_n) \bmod p^n\mathbb{Z}_p \equiv 0 \bmod p^n\mathbb{Z}_p$ for all n. ⊠

This theorem is very helpful for describing the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Proposition 3.1.3 *Let p be an odd prime, and let ξ be a generator of $\mathbb{F}_p^* \simeq (\mathbb{Z}_p/p\mathbb{Z}_p)^*$, then we have that the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is generated by $\langle p, \xi\rangle$ (where ξ is seen as element of $\mathbb{Z} \subset \mathbb{Z}_p$).*
If $p = 2$, then we have that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is generated by $\langle -1, 2, 3\rangle$.

Proof. If we have $p \neq 2$, then we can easily see with Hensel's lemma that $x = (x_1, x_2, \ldots) \in \mathbb{Z}_p^*$ is a square if and only if there exists a $y \in \mathbb{Z}_p^*$, s.t. $y^2 \equiv x \bmod p\mathbb{Z}_p$, or, which is the same, if and only if x_1 is a square in $\mathbb{F}_p$. We know that there is an element $\xi \in \mathbb{F}_p^*$ with $\mathbb{F}_p^* = \langle\xi\rangle$ and thus are all non-squares in $\mathbb{Z}_p^*$ represented by ξ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
In general an element $x \in \mathbb{Q}_p^*$ is a square if and only if it can be written as $x = p^{2n}y^2, y \in \mathbb{Z}_p^*$. A non-square in $\mathbb{Q}_p^*$ will thus be represented by p, ξ or $p\xi$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. This gives that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is generated by $\langle p, \xi\rangle$.
If $p = 2$, we can't use Hensel's lemma, instead we have that $x \in \mathbb{Z}_p^*$ is a square if and only if $x \equiv 1 \bmod 8$. (This is seen by straightforward computation.)

Then we have that the non-squares in $\mathbb{Z}_p^*$ are exactly those elements which are $-3, -1$ or 3 modulo 8 and its image in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is thus generated by $\langle -1, 3\rangle$. In general we have that an element $x \in \mathbb{Q}_p^*$ is a square if $x = 2^{2n}y^2$, this implies that $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is generated by $\langle -1, 2, 3\rangle$. ⊠

We can also formulate an equivalent of theorem (2.1.4) for $\mathbb{Q}_p$.

Proposition 3.1.4 *We have for the different primes p the next number of elements of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ (where g is the genus of C):*

(*i*) $p = \infty$.
$\dim_{\mathbb{F}_2} J(\mathbb{R})/2J(\mathbb{R}) = \#$*(irreducible factors of* $f_5(X)$ *over* $\mathbb{R}$*)* $- 1 - g$;

(*ii*) $p = 2$.
$\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = \#$*(irreducible factors of* $f_5(X)$ *over* $\mathbb{Q}_2$*)* $- 1 + g$;

(*iii*) *otherwise.*
$\dim_{\mathbb{F}_2} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \#$*(irreducible factors of* $f_5(X)$ *over* $\mathbb{Q}_p$*)* $- 1$.

Proof. We will only give a sketch.
If we define $n = \dim_{\mathbb{F}_2} J(\mathbb{Q}_p)[2]$, then we can prove, as in theorem (2.1.4) that $n = \#$(irreducible factors of $f_5(X)$ over $\mathbb{Q}_p) - 1$. Moreover we know that the map $[2] : D \mapsto 2D, D \in J(\mathbb{Q}_p)$ is 2^n-to-1, because if $2D_1 = 2D_2$, then $D_1 - D_2 \in J(\mathbb{Q}_p)[2]$, thus there are exactly 2^n elements with image $2D_1$ in $J(\mathbb{Q}_p)[2]$.
Furthermore we know that if we denote

$$\mathrm{Vol}(J(\mathbb{Q}_p)) = \int_{J(\mathbb{Q}_p)} d\mu,$$

then

$$\mathrm{Vol}(2J(\mathbb{Q}_p)) = \frac{1}{2^n}\int_{J(\mathbb{Q}_p)} d(\psi_2(\mu)).$$

We have that $d(\psi_2(\mu)) = |2|_p^g d\mu$. Thus we get that

$$\#(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) = \frac{\mathrm{Vol}(J(\mathbb{Q}_p))}{\mathrm{Vol}(2J(\mathbb{Q}_p))} = \frac{2^n}{|2|_p^g}.$$

And $|2|_p$ equals 2 if $p = \infty$, $\frac{1}{2}$ if $p = 2$ and 1 otherwise. Thus the dimension over $\mathbb{F}_2$ is $n - g, n + g, n$ respectively, which gives the desired result. ⊠

3.2 Decomposition and inertia

We are working in the number field $\mathbb{Q}$ with integers $\mathbb{Z}$. When we look at the closure of $\mathbb{Q}$, $\overline{\mathbb{Q}}$, there is a closure of $\mathbb{Z}$ in this new field, which we denote by

$\overline{\mathbb{Z}}$ which consists of the algebraic integers of $\overline{\mathbb{Q}}$. We can look at this closure $\overline{\mathbb{Q}}$ as a limit of finite Galois-extensions K of $\mathbb{Q}$.

$$\begin{array}{ccc} \overline{\mathbb{Z}} & \subset & \overline{\mathbb{Q}} \\ \cup & & \cup \\ \mathbb{Z}_K & \subset & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathbb{Q}. \end{array}$$

We have that p is not a unit in $\overline{\mathbb{Z}}$, hence we have $p\overline{\mathbb{Z}} \subset \overline{\mathbb{Z}}$ is an ideal and we can choose a maximal ideal M which contains $p\overline{\mathbb{Z}}$, with the property $M \cap \mathbb{Z} = p\mathbb{Z}$.
Moreover, this prime $p \in \mathbb{Z}$ this gives rise to an ideal $p\mathbb{Z}_K \subset \mathbb{Z}_K$, with the property $p\mathbb{Z}_K \cap \mathbb{Z} = p\mathbb{Z}$ and $p\mathbb{Z}_K$ decomposes in $\mathbb{Z}_K$ into the product of *prime* ideals p_i, i.e.

$$p\mathbb{Z}_K = \left(\prod_{i=1}^{q} p_i\right)^e,$$

with the e the ramification index of $p\mathbb{Z}_K$. (See [9], chapitre VI, for an extensive account of all this.)
For the maximal ideal M we have that $M \cap \mathbb{Z}_K$ is equal to one of the p_i. Each p_i lifts to an ideal in $\overline{\mathbb{Z}}$. We can choose maximal ideals M_i which contain the lift of p_i and $M_i \cap \mathbb{Z}_K = p_i$, and $M_i \cap \mathbb{Z} = p\mathbb{Z}$. We can repeat this for a finite extension of K and create maximal ideals over p_i.
This gives rise to infinitely many maximal ideals M_i, for which $M_i \cap \mathbb{Z} = p\mathbb{Z}$.
In the finite-extension-case we have that for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(p_i) = p_j$.
The same is true for the maximal ideals M_i: every $\sigma \in G$ gives $\sigma(M_i) = M_j$, for some i, j.

Definition 3.2.1 *We define the* decomposition-*group at p to be*

$$D_p = \{\sigma \in G \mid \sigma(M_i) = M_i \text{ for a chosen } M_i.\},$$

and the inertia-*group at p to be*

$$I_p = \{\sigma \in D_p \mid \sigma(x) - x \in M_i \quad \forall x \in \overline{\mathbb{Z}}\}.$$

Obviously D_p is a subgroup of G, as well as $I_p \subset D_p \subset G$.
Note that the notation D_p is somewhat confusing, because we can choose different M_i's and each choice of M_i gives rise to another subset of G (they are equal upto conjugation).
We recall that $Z^1(G, J(\overline{\mathbb{Q}})[2])$ consists of classes of mappings $\xi : G \longrightarrow J(\overline{\mathbb{Q}})[2]$ with the property $\xi(\sigma\tau) = \sigma(\xi(\tau)) + \xi(\sigma)$.

Definition 3.2.2 *We call $\xi \in Z^1(G, J(\overline{\mathbb{Q}})[2])$ unramified if $\xi|_{I_p} = \eta$ for some $\eta \in B^1(I_p, J(\overline{\mathbb{Q}})[2])$, i.e. if $\xi|_{I_p} = 0$ in $H^1(G, J(\overline{\mathbb{Q}})[2])$.*

We know in the 'finite-extension-case' $[K : \mathbb{Q}] = n$, $K/\mathbb{Q}$ Galois, that $\#D_p = \frac{n}{q}$ and that $D_p/I_p \simeq \mathrm{Gal}((\mathbb{Z}_K/p_i\mathbb{Z}_K)/(\mathbb{Z}/p\mathbb{Z}))$. If we let f be $f := \#\mathrm{Gal}((\mathbb{Z}_K/p_i\mathbb{Z}_K)/(\mathbb{Z}/p\mathbb{Z}))$, then we have that $n = efq$ and hence $\#I_p = e$. We see in general that p is unramified, if and only if $\xi|_{I_p} = 0$ for all $\xi \in H^1(G, J(\overline{\mathbb{Q}})[2])$.

Remark 3.2.3 Let's call $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, the Galois group of $\overline{\mathbb{Q}}_p$ over $\mathbb{Q}_p$. We can easily see that $G_p \hookrightarrow G$ by $\tau \mapsto \tau|_{\overline{\mathbb{Q}}}$.

We even have a nice correspondence between G_p and D_p.

Theorem 3.2.4 *With the previous definitions we have that* $G_p \simeq D_p$.

Proof. We will only prove it in case we have a finite extension K of $\mathbb{Q}$. We have $p\mathbb{Z}_K = (\prod_{i=1}^{q} p_i)^e$. We start with the next commutative diagram

$$\begin{array}{ccc} K & \longrightarrow & K_{p_1} \\ \uparrow & & \uparrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}_p. \end{array}$$

(We could replace p_1 with an arbitrary p_i.) Now we know what happens to each p_i. If we send p_i to $P_i = p_i\mathbb{Z}_{K_{p_1}}$, then we have that by the choice of our embedding $K \longrightarrow K_{p_1}$, that $P_i = (1)$, for each $i \neq 1$. Hence $p\mathbb{Z}_K$ is sent to P_1^e, which can be written as a principal ideal $(\pi)^e$, with $v_{p_1}(\pi) = \frac{1}{e}$. Now we can create an explicit map from D_p to G_p. First notice that an element $\sigma \in G$ permutes the p_i and a $\sigma \in G_p \subset G$ must keep p_1 fixed, because the $\sigma \in G_p$ permute the P_i's that are prime. In K_{p_1}, only $P_1 = (\pi)$ is a prime, hence $G_p \subset D_p$.
We have $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$ and hence

$$K_{p_1} = (K(\beta_1, \ldots, \beta_n))_{p_1} = \mathbb{Q}_p(\beta_1, \ldots, \beta_n).$$

Every $\sigma \in D_p$ is uniquely determined by its permutation of the β_i's. We can send an element in D_p to its permutation of the β_i's in K_{p_1}. This map is surjective because $G_p \subset D_p$. But of course the only element which keeps all β_i fixed is the identity, hence this map is also injective. Which proves $D_p \simeq G_p$. ⊠

We can extend $\mathbb{Q}_p$ in two steps to $\overline{\mathbb{Q}}_p$. First by finding the largest unramified extension, the extension $\mathbb{Q}_p^{\mathrm{unr}}$ with $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p) \simeq D_p/I_p$ and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}}) \simeq I_p$ and subsequently extend this extension to $\overline{\mathbb{Q}}_p$. This gives us the following diagram.

Diagram 3.2.5

$$\begin{array}{ccc} \overline{\mathbb{Q}} & \longrightarrow & \overline{\mathbb{Q}}_p \\ \uparrow & & \uparrow I_p \\ \mathbb{Q}^{\mathrm{unr}} & \longrightarrow & \mathbb{Q}_p^{\mathrm{unr}} \\ \uparrow & & \uparrow D_p/I_p \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}_p. \end{array}$$

This gives us a nice embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow \mathbb{Q}_p^{\mathrm{unr}}$, which induces embeddings $J(\mathbb{Q}) \hookrightarrow J(\mathbb{Q}_p) \hookrightarrow J(\mathbb{Q}_p^{\mathrm{unr}})$. We can use this for creating a commutative diagram which will give much information about the Selmer group that will be introduced later on. First recall that in the previous chapter we created a map δ in theorem (2.4.8), which embedded $J(\mathbb{Q})/2J(\mathbb{Q})$ into $H^1(G, J(\overline{\mathbb{Q}})[2])$. In the same way we can construct a map δ_p which gives an embedding of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ into $H^1(G_p, J(\overline{\mathbb{Q}}_p)[2])$. We already saw that we can look at G_p as a subgroup of G, in fact as D_p, thus this map δ_p gives an embedding into $H^1(D_p, J(\overline{\mathbb{Q}})[2])$.
Identically we create an embedding of $J(\mathbb{Q}_p^{\mathrm{unr}})/2J(\mathbb{Q}_p^{\mathrm{unr}})$ into $H^1(I_p, J(\overline{\mathbb{Q}})[2])$ (note that $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}}) \simeq I_p$).
Moreover we have a restriction

$$\beta_p : H^1(G, J(\overline{\mathbb{Q}})[2]) \longrightarrow H^1(D_p, J(\overline{\mathbb{Q}})[2]),$$

as well as a restriction

$$\beta_{\mathrm{unr}} : H^1(D_p, J(\overline{\mathbb{Q}})[2]) \longrightarrow H^1(I_p, J(\overline{\mathbb{Q}})[2]).$$

Furthermore we call ψ_p and ψ_{unr} the maps from $J(\mathbb{Q})/2J(\mathbb{Q})$ to $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ and from $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ to $J(\mathbb{Q}_p^{\mathrm{unr}})/2J(\mathbb{Q}_p^{\mathrm{unr}})$, respectively, which results in the next commutative diagram.

Diagram 3.2.6

$$\begin{array}{ccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G, J(\overline{\mathbb{Q}})[2]) \\ & & \downarrow \psi_p & & \downarrow \beta_p \\ 0 & \longrightarrow & J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H^1(D_p, J(\overline{\mathbb{Q}})[2]) \\ & & \downarrow \psi_{\mathrm{unr}} & & \downarrow \beta_{\mathrm{unr}} \\ 0 & \longrightarrow & J(\mathbb{Q}_p^{\mathrm{unr}})/2J(\mathbb{Q}_p^{\mathrm{unr}}) & \xrightarrow{\delta_{\mathrm{unr}}} & H^1(I_p, J(\overline{\mathbb{Q}})[2]). \end{array}$$

3.3 The 2-Selmer group

With the maps defined in diagram (3.2.6), we define the Selmer group. Note that by 'primes of $\mathbb{Q}$' we mean either a usual prime corresponding to a

discrete valuation or the infinite prime, corresponding to the Archimedean completion $\mathbb{R}$.

Definition 3.3.1 *The 2-Selmer group is defined as follows:*

$$S^2(\mathbb{Q}, J) = \{\gamma \in H^1(G, J(\overline{\mathbb{Q}})[2]) \mid \beta_p(\gamma) \in im(\delta_p) \text{ for all primes } p \text{ of } \mathbb{Q}\}.$$

Proposition 3.3.2 *We have that $J(\mathbb{Q})/2J(\mathbb{Q})$ embeds into $S^2(\mathbb{Q}, J)$.*

Proof. Let $D \in J(\mathbb{Q})/2J(\mathbb{Q})$ and let $\gamma_p = \delta_p \circ \psi_p(D)$. Diagram (3.2.6) commutes, hence $\beta_p \circ \delta(D) = \gamma_p \in \text{im}(\delta_p)$, thus $\delta(D) \in S^2(\mathbb{Q}, J)$. Because δ is injective, this gives an embedding of $J(\mathbb{Q})/2J(\mathbb{Q})$ into $S^2(\mathbb{Q}, J)$. ⊠

Remark 3.3.3 With this proposition we see that the Selmer group indeed contains $J(\mathbb{Q})/2J(\mathbb{Q})$. Furthermore we can see with diagram (3.2.6), how we can compute this Selmer group, since

$$S^2(\mathbb{Q}, J) = \bigcap_{p \text{ prime}} \beta_p^{-1}(\delta_p(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))). \tag{3.1}$$

This shows how we will try to compute the Selmer group. First we compute the local image of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, then we look from what elements in $H^1(G, J(\overline{\mathbb{Q}}_p)[2])$ this comes (later on we replace this group by L^*/L^{*2}, by using $X - T$) and then we take the intersection over all p's. In the rest of this chapter we will see how we can describe $S^2(\mathbb{Q}, J)$ under the map $X - T$. This description will show that the involved computations are easy. Moreover we need to reduce the number of δ_p's we have to compute. This will result in theorem (3.3.9), from which it follows that $S^2(\mathbb{Q}, J)$ is finite.

Let's turn our attention to this Selmer group, to see whether we can compute it. For that purpose we will first try to find another expression for $S^2(\mathbb{Q}, J)$. Let S be the set of primes of $\mathbb{Q}$ consisting of the infinite prime, which we denote by -1, the prime 2 and furthermore the primes of *bad reduction* of J, i.e. the primes which divide the discriminant of $f_5(X)$, hence

$$S = \{ \text{ primes } p \text{ of } \mathbb{Q} \text{ for which } p \mid \prod_{1 \le i < j \le 5} (\alpha_i - \alpha_j)^2 \} \cup \{-1, 2\}.$$

First we need a proposition about $J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}})$, which will enable us to use diagram (3.2.6) more effectively.

Proposition 3.3.4 *If $p \notin S$, then we have $J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}}) = 0$.*

Proof. (We only give a sketch of the proof.)
Let $p \notin S$. We have introduced $\mathbb{Z}_p$ and the maximal ideal $p\mathbb{Z}_p$ and we have that $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. Because of this isomorphism we can look at the reduction $\mathbb{Z}_p \to \mathbb{F}_p$ (as done in [1], chapter 7). In general we have that the

Jacobian J can be embedded in $\mathbb{P}^n$, for some n (in fact, in our case $n = 8$, see [1], pp. 66), thus $J(\mathbb{Q}_p^{\text{unr}}) \hookrightarrow \mathbb{P}^n(\mathbb{Q}_p^{\text{unr}})$. Hence we get the reduction $J(\mathbb{Q}_p^{\text{unr}}) \to J(\overline{\mathbb{F}}_p)$ as follows. Let $x \in J(\mathbb{Q}_p^{\text{unr}})$, then we can represent this x by $(x_1, \ldots, x_{n+1})$, s.t. $\max |x_i|_p = 1$, i.e. $x_i \in \mathbb{Z}_p^{\text{unr}}$ and the x_i have no common factor p, so that the reduction is well-defined.
Because $p \notin S$, we have that $J(\overline{\mathbb{F}}_p)$ is an abelian variety and hence a group. The reduction we just defined is surjective. Moreover, because $\overline{\mathbb{F}}_p$ is algebraically closed, we have that $J(\overline{\mathbb{F}}_p)/2J(\overline{\mathbb{F}}_p) = 0$.
Let now M be the kernel from the reduction $J(\mathbb{Q}_p^{\text{unr}}) \to J(\overline{\mathbb{F}}_p)$. For every $x \in J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}})$ there exists a representative x' with $x' \in M$. We can see this as follows. $x \notin M \Rightarrow x \mapsto y \in J(\overline{\mathbb{F}}_p)$, $y \neq 0$. We saw $J(\overline{\mathbb{F}}_p)/2J(\overline{\mathbb{F}}_p) = 0$, hence there exists a $\tilde{x}$ s.t. $\tilde{x} \mapsto z$, with $2z = y$ and thus $x - 2\tilde{x} \in M$ and in $J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}})$ are x and $x - \tilde{x}$ equal, which gives us our representative in M. This implies that we have a surjection $M/2M \to J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}})$.
Now we 'only' need to show that $M/2M = 0$. We do this by referring to [12], chapter IV and [1], chapter 7. If $\mathcal{F}$ is the formal group associated with J, then we have that $M \simeq \mathcal{F}(p\mathbb{Z}_p^{\text{unr}})$, [12] tells us also that $[2] : \mathcal{F} \to \mathcal{F}$ is an isomorphism if $p > 2$, so this induces an isomorphism $[2] : \mathcal{F}(p\mathbb{Z}_p^{\text{unr}}) \to \mathcal{F}(p\mathbb{Z}_p^{\text{unr}})$ and thus an isomorphism $[2] : M \to M$, which implies that $M/2M = 0$. ⊠

Look at a cocycle $\xi \in H^1(G, J(\overline{\mathbb{Q}})[2])$, recall that ξ is called unramified at the prime p if $\xi|_{I_p}$ is a coboundary map.

Definition 3.3.5 *We define $H^1_S(G, J(\overline{\mathbb{Q}})[2]) \subset H^1(G, J(\overline{\mathbb{Q}})[2])$ to be the subgroup of $H^1(G, J(\overline{\mathbb{Q}})[2])$ with the property that it consists of the cocycles that are unramified at primes $p \notin S$.*

Proposition 3.3.6 *With this definition of $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ we have that $S^2(\mathbb{Q}, J) \subset H^1_S(G, J(\overline{\mathbb{Q}})[2])$, and thus*

$$S^2(\mathbb{Q}, J) = \{\gamma \in H^1_S(G, J(\overline{\mathbb{Q}})[2]) \mid \beta_p(\gamma) \in im(\delta_p)\ \forall primes\ p\ of\ \mathbb{Q}\}.$$

Proof. Let $p \notin S$. Let $\xi \in S^2(\mathbb{Q}, J)$. By definition we have that $\xi \in S^2(\mathbb{Q}, J)$ if $\beta_p(\xi)$, which is the restriction of ξ to D_p, is in the image of δ_p, thus there exists a $j_p \in J(\overline{\mathbb{Q}}_p)/2J(\overline{\mathbb{Q}}_p)$ with $\delta_p(j_p) = \xi|_{D_p}$ $(*)$. Because diagram (3.2.6) is commutative, we have that $\beta_{\text{unr}} \circ \delta_p(j_p) = \delta_{\text{unr}} \circ \psi_{\text{unr}}(j_p)$. The lefthand-side of this equation is according to $(*)$ and diagram (3.2.6) exactly the restriction of ξ to I_p. The righthand-side of this equation is 0 because $J(\mathbb{Q}_p^{\text{unr}})/2J(\mathbb{Q}_p^{\text{unr}}) = 0$ according to proposition (3.3.4). Thus $\xi|_{I_p} = 0$, thus ξ is unramified over p.
This proves $S^2(\mathbb{Q}, J) \subset H^1_S(G, J(\overline{\mathbb{Q}})[2])$.
⊠

We recall some results from the previous chapter. According to theorem (2.4.8) we have an isomorphism between $H^1(G, J(\overline{\mathbb{Q}})[2])$ and

$\ker\left(N : L^*/L^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}\right)$, by the map $k \circ w : H^1(G, J(\overline{\mathbb{Q}})[2]) \to L^*/L^{*2}$. Moreover we have that $k \circ w \circ \delta$ is the same injection as $X - T$. We can consider the same maps acting on a completion of L at p, which is the same as $\mathbb{Q}_p[X]/(f_5)$, then we get a map

$$(k \circ w)_p \circ \delta_p : J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \longrightarrow L_p^*/L_p^{*2}.$$

We extend our diagram (3.2.6) as follows (it's still commutative):

Diagram 3.3.7

$$\begin{array}{ccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G, J(\overline{\mathbb{Q}})[2]) & \xrightarrow{k \circ w} & L^*/L^{*2} \\ & & \downarrow{\scriptstyle \psi_p} & & \downarrow{\scriptstyle \beta_p} & & \downarrow{\scriptstyle \zeta_p} \\ 0 & \longrightarrow & J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H^1(D_p, J(\overline{\mathbb{Q}})[2]) & \xrightarrow{(k \circ w)_p} & L_p^*/L_p^{*2}. \end{array}$$

As an injection $k \circ w \circ \delta$ is the same as $X - T$, as well as $(k \circ w)_p \circ \delta_p$ is the same as $(X - T)_p$; this gives the next diagram.

Diagram 3.3.8

$$\begin{array}{ccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{X-T} & L^*/L^{*2} \\ & & \downarrow{\scriptstyle \psi_p} & & \downarrow{\scriptstyle \zeta_p} \\ 0 & \longrightarrow & J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \xrightarrow{(X-T)_p} & L_p^*/L_p^{*2}. \end{array}$$

With theorem (2.4.8) we can describe the elements of $S^2(\mathbb{Q}, J)$ in terms of this diagram. First of all we have that the elements of $S^2(\mathbb{Q}, J)$ are in

$$\ker\left(N : L^*/L^{*2} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}\right) \overset{k \circ w}{\simeq} H^1(G, J(\overline{\mathbb{Q}})[2]).$$

And for every $\xi \in H^1(G, J(\overline{\mathbb{Q}})[2])$ we have that $\xi \in S^2(\mathbb{Q}, J)$ if and only if after restriction to D_p it is in the image of δ_p for all primes p.
After our isomorphism $k \circ w$ this sentence reads as: For every ξ in $\ker\left(N : L^*/L^{*2} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}\right)$ we have that $\xi \in S^2(\mathbb{Q}, J)$ if and only if after mapping into L_p^*/L_p^{*2} it is in the image of $(k \circ w)_p \circ \delta_p$ for all primes p. According to theorem (2.5.3) this latter map is the same as $(X - T)_p$, thus $\xi \in S^2(\mathbb{Q}, J)$ if and only if its mapping in L_p^*/L_p^{*2} is in the image of $(X - T)_p$ for all primes p.

We want to describe the Selmer group even more precise. We already embedded $S^2(\mathbb{Q}, J)$ into $H_S^1(G, J(\overline{\mathbb{Q}})[2])$. What is the image of $H_S^1(G, J(\overline{\mathbb{Q}})[2])$ under $k \circ w$? Let $\xi \in H_S^1(G, J(\overline{\mathbb{Q}})[2])$, then of course

$$k \circ w(\xi) \in \ker\left(N : L^*/L^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}\right).$$

Furthermore we know that if $\xi \in H^1_S(G, J(\overline{\mathbb{Q}})[2])$ then ξ is unramified at p for all $p \notin S$. Thus $\xi|_{I_p} = 0$ for $p \notin S$. If we have $k \circ w(\xi) = l \in L^*/L^{*2}$ and $p \notin S$, we have by remark (2.4.7) that it comes from the map $\tilde{\xi} : \sigma \to \frac{\sigma(\sqrt{l})}{\sqrt{l}}$, with $\tilde{\xi} \in H^1(G, \mu_2(\overline{L}))$. This implies $\tilde{\xi}|_{I_p} = 1$, which means that $\sigma(\sqrt{l}) = \sqrt{l}$ for all $\sigma \in I_p$.
We know from theorem (2.3.1) that $L = \oplus_{i=1}^{d} \mathbb{Q}[T]/(h_i(T))$, with $h_i(T)$ irreducible in $\mathbb{Q}[T]$, thus L is the direct sum of d fields. We can look at l as a d-tuple $(l_1, \ldots, l_d)$ and at $\sqrt{l}$ as a d-tuple $(\sqrt{l_1}, \ldots, \sqrt{l_d})$, thus every $\sigma \in I_p$ keeps this d-tuple fixed, thus $\sigma(\sqrt{l_i}) = \sqrt{l_i}$. We already saw that $I_p \simeq \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}})$, so if we look at the extension $\mathbb{Q}[T]/(h_i(T))[\sqrt{l_i}]$, it's fixed under I_p, this means that it is an unramified extension at all $p \notin S$.
This gives us that the image of $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ under the isomorphism $k \circ w$ is exactly the subset of the kernel of the norm N, viewed as d-tuples $(l_1, \ldots, l_d)$, for which each of the extensions $\mathbb{Q}[T]/(h_i(T))[\sqrt{l_i}]$ is unramified at all $p \notin S$. Thus

$$H^1_S(G, J(\overline{\mathbb{Q}})[2]) \overset{k \circ w}{\simeq} \{(l_1, \ldots, l_d) \in \ker(N) \mid \forall i \text{ is } \mathbb{Q}[T]/(h_i(T))[\sqrt{l_i}] \text{ an unramified extension at all } p \notin S\}.$$

Our Selmer group $S^2(\mathbb{Q}, J)$ consists of the elements l in this set for which the mapping into L_p^*/L_p^{*2} is in the image of $(X - T)_p$ for all primes p.

With this information we can resolve another intricate problem. We want to compute the Selmer group by evaluating it locally, subsequently we must compute the images of all our δ_p's, but there are infinitely many primes, so this tends to be a problem. Our next theorem states that we only need to compute the images of finitely many δ_p's to compute the group, namely only the primes in the set S.

Theorem 3.3.9 *We have*

$$S^2(\mathbb{Q}, J) = \{\xi \in H^1_S(G, J(\overline{\mathbb{Q}})[2]) \mid \beta_p(\xi) \in im(\delta_p) \quad \forall p \in S\}.$$

Proof. We will prove this under the assumption that the roots of f_5 are all rational. We use the notations of diagram (3.3.7):

$$\begin{array}{ccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G, J(\overline{\mathbb{Q}})[2]) & \xrightarrow{k \circ w} & L^*/L^{*2} \\ & & \downarrow \psi_p & & \downarrow \beta_p & & \downarrow \zeta_p \\ 0 & \longrightarrow & J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H^1(D_p, J(\overline{\mathbb{Q}})[2]) & \xrightarrow{(k \circ w)_p} & L_p^*/L_p^{*2}. \end{array}$$

We denote $k \circ w(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$ simply as $H^1_S(G, J(\overline{\mathbb{Q}})[2])$, because $k \circ w$ is an isomorphism. We do this also for $S^2(\mathbb{Q}, J)$.

Then we have that $L^*/L^{*2} \simeq \oplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2}$ and we know that $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ consists of the 5-tuples $(x_1, \ldots, x_5)$ with $\mathbb{Q}(\sqrt{x_i})$ unramified at all $p \notin S$. Let $S = \{p_1, \ldots, p_n\}$, (where the prime at infinity is denoted as -1) then this implies that $x_i \in \langle p_1, \ldots, p_n \rangle =: H \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$. Thus $H^1_S(G, J(\overline{\mathbb{Q}})[2]) \subset \oplus_{i=1}^5 H$. This immediately shows that $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ is a finite group.
Let now $p \notin S$. We know that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \langle p, r \rangle$, with r a non-square modulo p. Because $p \notin S$, we have that every coordinate of an element in H is mapped to either 1 or r, hence $\zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2])) \subset \oplus_{i=1}^5 \langle r \rangle$, which implies that the rank of $\zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$ is at most 5. Because $H^1_S(G, J(\overline{\mathbb{Q}})[2]) \subset \ker(N)$, we have for all $(\tilde{x}_1, \ldots, \tilde{x}_5) \in \zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$ that $\prod_{i=1}^5 \tilde{x}_i = 1$. Hence the rank of $\zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$ is at most $5 - 1 = 4$.
We already know that $\mathrm{im}(\delta_p)$ is a subset of $\zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$, moreover by proposition (3.1.4) we know that $\mathrm{im}(\delta_p)$ has rank 4, hence $\mathrm{im}(\delta_p) \supset \zeta_p(H^1_S(G, J(\overline{\mathbb{Q}})[2]))$, which implies that $\zeta_p^{-1}(\mathrm{im}(\delta_p)) \supset H^1_S(G, J(\overline{\mathbb{Q}})[2])$. By the inverse of $k \circ w$, this results in $\beta_p^{-1}(\mathrm{im}(\delta_p)) \supset H^1_S(G, J(\overline{\mathbb{Q}})[2])$.
Recall that

$$S^2(\mathbb{Q}, J) = \{\gamma \in H^1_S(G, J(\overline{\mathbb{Q}})[2]) \mid \beta_p(\gamma) \in \mathrm{im}(\delta_p) \ \forall \text{ primes } p \text{ of } \mathbb{Q}\}.$$

Hence we can forget the $p \notin S$, because these give a set of γ's which is at least $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ and we get the demanded expression for $S^2(\mathbb{Q}, J)$. ⊠

Remark 3.3.10 From the proof of this proposition we can deduce directly an upperbound for the rank of the Selmer group in terms of the number of elements of S. Because $H^1_S(G, J(\overline{\mathbb{Q}})[2]) \subset \oplus_{i=1}^5 H$, we have that $H^1_S(G, J(\overline{\mathbb{Q}})[2])$ consists of at most 2^{5n} elements, with $n = \#S$ and because the Selmer group consists of the elements in the kernel of the norm we have that the Selmer group consists of at most 2^{4n} elements, hence the dimension is at most $4n$. Moreover we have that the rank of the torsion is 4, hence the Mordell-Weil rank is at most $4n - 4$.

3.4 The algorithm

We can express the Selmer group also in terms of the map $X - T$, then we get with the notation of diagram (3.3.8)

$$S^2(\mathbb{Q}, J) = \{l \in k \circ w(H^1_S(G, J(\overline{\mathbb{Q}})[2])) \mid \zeta_p(l) \in \mathrm{im}((X - T)_p) \ \ \forall p \in S\}.$$

We can simplify this even more, because we will only look at cases for which the roots of f_5 are rational. This gives us that $L^*/L^{*2} = \oplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2}$. And as we saw in the proof of theorem (3.3.9), if we let $H = \langle \prod p_i \mid p_i \in S \rangle \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$, then we have $k \circ w(H^1_S(G, J(\overline{\mathbb{Q}})[2])) \subset \oplus_{i=1}^5 H$, hence

$$S^2(\mathbb{Q}, J) = \{l \in \oplus_{i=1}^5 H \mid \zeta_p(l) \in \mathrm{im}((X - T)_p) \ \ \forall p \in S\}.$$

With this expression and diagram (3.3.8), we can see how our algorithm works.

(*i*) Compute S, by computing the discriminant of f_5.

(*ii*) For every $p \in S$:

- compute a set A_p of generators of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. Because we already have a set of generators for $J(\mathbb{Q})[2]$, this practically comes down to finding 1 or 2 new generators;
- compute $(X-T)_p(A_p)$;
- compute the set $B_p \subset L^*/L^{*2}$, with $\zeta_p(B_p) = (X-T)_p(A_p)$.

(*iii*) Now we have $S^2(\mathbb{Q}, J) = \cap_{p \in S} \mathrm{span}(B_p)$.

In the next chapter we will compute an example.

Chapter 4

Computing an example

In this chapter we will use the theory we have developed in the previous chapter for computing the rank of $J(\mathbb{Q})$ of the next genus 2 curve.
Let $q > 3$ (the cases $q = 2, 3$ will be considered separately) be a prime and let the model of C be given by

$$Y^2 = (X^2 - 4q^2)(X^2 - q^2)X. \tag{4.1}$$

In this case we have that $f_5(X) = (X + 2q)(X + q)X(X - q)(X - 2q)$, so f_5 splits over $\mathbb{Q}$ and we see immediately 5 points in $C(\mathbb{Q})$, namely $(\alpha_1, 0) = (-2q, 0), \ldots, (\alpha_5, 0) = (2q, 0)$. This gives us 5 points in the 2-torsion of the Jacobian $J(\mathbb{Q})$, namely $D_i = [(\alpha_i, 0)] - [\infty]$, $i = 1, \ldots, 5$.
We have that the discriminant, Δ, of $f_5(X)$ is:

$$\Delta(f_5) = \prod_{1 \le i < j \le 5} (\alpha_i - \alpha_j)^2 = (q^2)^4((2q)^2)^3((3q)^2)^2((4q)^2)^1 = 2^{10}3^4q^{20}.$$

The primes that divide $\Delta(f_5)$ are $2, 3$ and q, so the set of primes p for which we need to compute the image of $(X - T)_p$ is $S = \{-1, 2, 3, q\}$.
We have that $L^*/L^{*2} = \oplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2}$. Define $H := \langle -1, 2, 3, q \rangle$. We already saw that $H^1_S(G, J(\overline{\mathbb{Q}})[2]) \subset \oplus_{i=1}^5 H$ and that the Selmer group is a subset of $H^1_S(G, J(\overline{\mathbb{Q}})[2])$. Thus $X - T$ embeds $S^2(\mathbb{Q}, J)$ into $\oplus_{i=1}^5 H$. Moreover we have for $x \in S^2(\mathbb{Q}, J)$, that the product of the 5 coordinates is a square, because the Selmer group embeds in the kernel of the norm from L^*/L^{*2} to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. As we noticed in the previous chapter, the dimension of the Selmer group is at most $4 \cdot 4 = 16$.

4.1 Computing $(X - T)_p$

In paragraph (2.5) we introduced the map $X - T$ as a mapping from the group $J(\mathbb{Q})/2J(\mathbb{Q})$ to 5 copies of $\mathbb{Q}^*/\mathbb{Q}^{*2}$, but we needed a representation for every element without Weierstrass points in its support. We refer to remark

(2.5.2) to see how we deal with representations which have a Weierstrass point in its support.

We have that $D_1, \ldots, D_4$ represent distinct divisor classes in $J(\mathbb{Q})/2J(\mathbb{Q})$ because as divisors $D_1, \ldots, D_4$ are linearly independent. And we already know that these 4 divisors span $J(\mathbb{Q})[2]$ as vectorspace over $\mathbb{F}_2$. We will use in the following the abbreviation $D_a = [(a, \sqrt{f_5(a)})] - [\infty]$, thus $D_{-2q} = [(-2q, 0)] - [\infty]$, etc.. This gives the next table.

Table 4.1.1 $X - T$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	$-q$	$-2q$	$-3q$	$-q$
D_{-q}	q	-6	$-q$	$-2q$	$-3q$
D_0	$2q$	q	1	$-q$	$-2q$
D_q	$3q$	$2q$	q	-6	$-q$

According to the algorithm in paragraph (3.4) we need to compute generators of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ for every $p \in S$ and subsequently the image of these generators in L_p^*/L_p^{*2}. We recall that $L_p^*/L_p^{*2} = \oplus_{i=1}^5 \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ for all $p \in S$. To be able to do these computations we need to classify our prime q, because we need to know when q is a square modulo 2 and 3. Furthermore we need to know when $-1, 2$ and 3 are squares modulo q. This classification is given by the next proposition:

Proposition 4.1.2 *Let $q \equiv a \bmod 24$, with $q > 3$ and q is a prime, thus $a \in (\mathbb{Z}/24\mathbb{Z})^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$, then we get the following classification:*

a	*squares mod q*
1	$-1, 2, 3$
5	-1
7	2
11	3
13	$-1, 3$
17	$-1, 2$
19	*none*
23	$2, 3$

Moreover we have that q is a square in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ if and only if $a \in \{1, 17\}$. And q is a square in $\mathbb{Q}_3^*/\mathbb{Q}_3^{*2}$ if and only if $a \in \{1, 7, 13, 19\}$.

Proof. Obviously we have that if $q > 3$ a prime, then $q \bmod 24 \in (\mathbb{Z}/24\mathbb{Z})^*$. From [2], pp. 66-70, we know that if p is a prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \equiv 1, 5, 13, 17 \bmod 24, \\ -1 & \text{if } p \equiv -1 \bmod 4 \equiv 7, 11, 19, 23 \bmod 24. \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \equiv 1, 7, 17, 23 \bmod 24, \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \equiv 5, 11, 13, 19 \bmod 24. \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \equiv 1, 11, 13, 23 \bmod 24, \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \equiv 5, 7, 17, 19 \bmod 24. \end{cases}$$

With this information, we get the table. The two other conclusions follow from the fact that $|q|_2 = |q|_3 = 1$ and hence this is a square in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ if $q \equiv 1 \bmod 8$ and in $\mathbb{Q}_3^*/\mathbb{Q}_3^{*2}$ if $q \equiv 1 \bmod 3$ (see proposition (3.1.3)). ⊠

This proposition gives us a classification with which we can compute the images of $(X - T)_p$.

1. Image of $J(\mathbb{R})/2J(\mathbb{R})$ under $(X - T)_{-1}$

We have that $\mathbb{R}^*/\mathbb{R}^{*2} = \langle -1 \rangle$ and that $J(\mathbb{R})/2J(\mathbb{R})$ has, by proposition (3.1.4), dimension $5 - 1 - 2 = 2$, thus we need only 2 generators, this gives us the next table.

Table 4.1.3 $(X - T)_{-1}$

	$X + 2q$	$X + q$	X	$X - q$	$X - 2q$
D_{-q}	1	-1	-1	-1	-1
D_0	1	1	1	-1	-1

To give an idea of how we will work with this data, the following remark. Because we are working in $\mathbb{R}$ we know that a coordinate x_i of an element $x = (x_1, \ldots, x_5)$ of the Selmer group is mapped to 1 if it is positive and to -1 if it is negative. We see that there is no -1 in the first column, thus we conclude that all the elements in the Selmer group have a positive first coordinate. This implies that the first coordinate is in $\langle 2, 3, q \rangle \subset H = \langle -1, 2, 3, q \rangle$. An immediate result is that the rank of the Selmer group is at most 15.

2. Image of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ under $(X - T)_2$

We have that $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \langle -1, 2, 3 \rangle$ and $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ has dimension $5 - 1 + 2 = 6$, thus we are looking for 6 generators. After some computing we find that the 4 generators over $\mathbb{Q}$ are also independent over $\mathbb{Q}_2$, hence we need to find 2 other generators.
We can see that in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, we have that $f_5(\frac{1}{4}) = \frac{1}{4^5}(1 - 8q)(1 - 4q)1(1 + 4q)(1 + 8q) \equiv (1 - 8q)(1 - 4q)1(1 + 4q)(1 + 8q) \equiv (1 - 4q)(1 + 4q) \bmod 8 \equiv (1 + 16q^2) \bmod 8 \equiv 1 \bmod 8$, thus $\sqrt{f_5(\frac{1}{4})} \in \mathbb{Q}_2$, this gives us a new point

$D_{\frac{1}{4}} \in J(\mathbb{Q}_2)$. In the same way we find that $f_5(20)$ gives a point $D_{20} \in J(\mathbb{Q}_2)$. These two points appear not to be mutually equivalent nor equivalent to the 4 generators over $\mathbb{Q}$. This can be seen from the following tables.

Table 4.1.4 $(X - T)_2$

$q \equiv 1 \bmod 8 \equiv 1, 17 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	−1	−2	−3	−1
D_{-q}	1	−6	−1	−2	−3
D_0	2	1	1	−1	−2
D_q	3	2	1	−6	−1
$D_{\frac{1}{4}}$	1	−3	1	−3	1
D_{20}	6	−3	−3	3	2

$q \equiv 3 \bmod 8 \equiv 11, 19 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	−3	−6	−1	−3
D_{-q}	3	−6	−3	−6	−1
D_0	6	3	1	−3	−6
D_q	1	6	3	−6	−3
$D_{\frac{1}{4}}$	1	−3	1	−3	1
D_{20}	−6	−1	−3	1	−2

$q \equiv -1 \bmod 8 \equiv 7, 23 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	1	2	3	1
D_{-q}	−1	−6	1	2	3
D_0	−2	−1	1	1	2
D_q	−3	−2	−1	−6	1
$D_{\frac{1}{4}}$	1	−3	1	−3	1
D_{20}	2	3	−3	−3	6

$q \equiv -3 \bmod 8 \equiv 5, 13 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	3	6	1	3
D_{-q}	−3	−6	3	6	1
D_0	−6	−3	1	3	6
D_q	−1	−6	−3	−6	3
$D_{\frac{1}{4}}$	1	−3	1	−3	1
D_{20}	−2	1	−3	−1	−6

3. Image of $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ under $(X-T)_3$

We have that $\mathbb{Q}_3^*/\mathbb{Q}_3^{*2} = \langle -1, 3\rangle$ and $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ has dimension $5-1=4$, thus we need 4 generators. Only 3 of the 4 generators over $\mathbb{Q}$ appear to be not equivalent over $\mathbb{Q}_3$, so we need to find one other generator. It turns out that this generator is only depending on the fact whether or not q is a square in $\mathbb{Q}_3$.
If $q \equiv 1 \bmod 3$, then we have that $f_5(-(q+3)) = (-3q-3)(-2q-3)(-q-3)(-3)(q-3) = 9(q+1)(2q+3)(q+3)(q-3)$. Thus $\frac{f_5(-(q+3))}{9} \equiv 2\cdot 2\cdot 1 \equiv 1 \bmod 3$, thus by Hensel's lemma $f_5(-(q+3))$ is a square in $\mathbb{Q}_3$, which gives us a new point in the Jacobian, which is linearly independent from the others.
If $q \equiv -1 \bmod 3$, then we have, in the same way, that $\frac{f_5(q-3)}{9} = q(-q^2-2q)(-2q) \equiv -1(-1+2)2 \equiv 1 \bmod 3$, this gives a new point in $J(\mathbb{Q}_3)$. This information gives us the next tables.

Table 4.1.5 $(X-T)_3$

$q \equiv 1 \bmod 3 \equiv 1, 7, 13, 19 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	−3	−1	1	−3	−1
D_{-q}	1	3	−1	1	−3
D_0	−1	1	1	−1	1
$D_{-(q+3)}$	1	−3	−1	1	3

$q \equiv -1 \bmod 3 \equiv 5, 11, 17, 23 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	−3	1	−1	3	1
D_{-q}	−1	3	1	−1	3
D_0	1	−1	1	1	−1
D_{q-3}	3	1	−1	−3	1

4. Image of $J(\mathbb{Q}_q)/2J(\mathbb{Q}_q)$ under $(X-T)_q$

We have $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2} = \langle q, r\rangle$, with r a non-square in $\mathbb{F}_q$ and $J(\mathbb{Q}_q)/2J(\mathbb{Q}_q)$ has dimension $5-1=4$, thus we are looking for 4 generators. In this case we have to distinguish between the 8 classes modulo 24 of the prime q. In each case we have that the 4 generators over $\mathbb{Q}$ give 4 generators over $\mathbb{Q}_q$. This gives us the next tables.

Table 4.1.6 $(X-T)_q$

$q \equiv 1 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	1	q	q	q	q
D_{-q}	q	1	q	q	q
D_0	q	q	1	q	q
D_q	q	q	q	1	q

$q \equiv 5 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	1	q	$2q$	$2q$	q
D_{-q}	q	1	q	$2q$	$2q$
D_0	$2q$	q	1	q	$2q$
D_q	$2q$	$2q$	q	1	q

$q \equiv 7 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	-1	$-q$	$-q$	q	$-q$
D_{-q}	q	1	$-q$	$-q$	q
D_0	q	q	1	$-q$	$-q$
D_q	$-q$	q	q	1	$-q$

$q \equiv 11 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	-1	$-q$	q	$-q$	$-q$
D_{-q}	q	1	$-q$	q	$-q$
D_0	$-q$	q	1	$-q$	q
D_q	q	$-q$	q	1	$-q$

$q \equiv 13 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	2	q	$2q$	q	q
D_{-q}	q	2	q	$2q$	q
D_0	$2q$	q	1	q	$2q$
D_q	q	$2q$	q	2	q

$q \equiv 17 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	3	q	q	$3q$	q
D_{-q}	q	3	q	q	$3q$
D_0	q	q	1	q	q
D_q	$3q$	q	q	3	q

$q \equiv 19 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	1	$-q$	q	q	$-q$
D_{-q}	q	-1	$-q$	q	q
D_0	$-q$	q	1	$-q$	q
D_q	$-q$	$-q$	q	-1	$-q$

$q \equiv 23 \bmod 24$

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	1	$-q$	$-q$	$-q$	$-q$
D_{-q}	q	-1	$-q$	$-q$	$-q$
D_0	q	q	1	$-q$	$-q$
D_q	q	q	q	-1	$-q$

4.2 The computation of the Selmer group

With these tables we can compute the Selmer group for all q and find the actual generators of this group. In this paragraph we will compute the Selmer group for every classification of q. At the end we have a table with a summary of the results of the computations. In the following we will see elements of the Selmer group as 5-tuples in $\oplus_{i=1}^{5}\mathbb{Q}^*/\mathbb{Q}^{*2}$.
We will first make some general remarks. We have already seen that the first coordinate of elements in the Selmer group is in $\langle 2,3,q\rangle$. If we look at table (4.1.1), then we see that $(X-T)(J(\mathbb{Q})/2J(\mathbb{Q}))$ spans $\langle 2,3,q\rangle$ for the first coordinate.
We consider the map $S^2(\mathbb{Q},J)\to\langle 2,3,q\rangle$, given by $(x_1,\ldots,x_5)\mapsto x_1$. This map is surjective and $\mathbb{F}_2$-linear. Define S_1^2 to be the kernel of this map, thus to be the subgroup of $S^2(\mathbb{Q},J)$ consisting of those elements $(e_1,\ldots,e_5)$ with $e_1=1$. Then we have that $\dim_{\mathbb{F}_2} S^2(\mathbb{Q},J) = 3+\dim_{\mathbb{F}_2} S_1^2$. Let $m_2=(X-T)(D_{-q}+D_0), m_3=(X-T)(D_{-q}+D_q)$ and $m_q=(X-T)(D_{-q})$, these are elements with first coordinate $2,3$ and q respectively. In the following we only need to look for the dimension of S_1^2. Moreover we know that we always have one element besides the identity in S_1^2, namely $m_1:=(X-T)(D_{-2q}+D_0+D_q)=(1,-2q,-2,-2,-2q)$, which is independent from the others. Hence the dimension of S_1^2 is at least 1.

(i) $q\equiv 1 \bmod 24$, this implies that q is 2-adically and 3-adically mapped to a square. In Table (4.1.4) we see that $\dim(\mathrm{im}((X-T)_2)))=6$. Moreover we see in this table that the dimension of the elements with first coordinate 1 is 4. This table gives us the generators of $S_1^2(\mathbb{Q}_2)$.

$$\begin{array}{lccccc} y_{2,1}= & 1 & -6 & -1 & -2 & -3\\ y_{2,2}= & 1 & -2 & -2 & -2 & -2\\ y_{2,3}= & 1 & -3 & 1 & -3 & 1\\ y_{2,4}= & 1 & -6 & -3 & 2 & 1 \end{array}$$

Let $(1,e_2,\ldots,e_5)\in S_1^2$, then e_5 is 2-adically mapped to $\langle -2,-3\rangle$, this means that $e_5\in\langle -2,-3,q\rangle$. Notice that $y_{2,2}$ comes from m_1, and this is an element for which e_5 mapped to -2, so we can look at $G_1=S_1^2=S_1^2/y_{2,2}S_1^2$, then we have that the dimension of G_1 is 1 more than that of S_1^2. Now look at the subgroup G_1 of S_1^2, for which e_5 is mapped to $\langle -3\rangle$, which means $e_5\in\langle -3,q\rangle$.
We can do the same for $p=3,q$, and then we get for $p=3$, that the set of elements in $(X-T)_3(J(\mathbb{Q}_3)/2J(\mathbb{Q}_3))$ with first coordinate 1 is spanned by

$$\begin{array}{lccccc} y_{3,1}= & 1 & 3 & -1 & 1 & -3\\ y_{3,2}= & 1 & -3 & -1 & 1 & 3 \end{array}$$

And these also span G_1. Notice that neither the third nor the fourth coordinate is divisible by 3, thus e_3 must be mapped to $\langle -1\rangle$ and, moreover, e_4

is always mapped to 1, and is thus 1 mod 3. This gives $e_4 \in \langle -2, q\rangle$. We see that 2-adically e_4 can't be 2 nor -1 nor -6, thus we can forget $y_{2,4}$.
For $p = q$, we get the table of generators of $S_1^2(\mathbb{Q}_q)$, which also generate G_1.

$$\begin{array}{rccccc} y_{q,1} = & 1 & 1 & 1 & q & q \\ y_{q,2} = & 1 & q & 1 & q & 1 \\ y_{q,3} = & 1 & q & q & 1 & 1 \end{array}$$

Now we try to construct an element in G_1 with $e_4 = q$. Such an element is 2-adically mapped to 1, thus it must 2-adically be the identity (recall that we can forget $y_{2,2}$ and $y_{2,4}$). This means that $e_i \in \langle q\rangle$ for all $i = 2, 3, 4, 5$. This maps 3-adically also to the identity. But q-adically we have three independent elements which satisfy. You can see that $y_{q,1}$ and $y_{q,3}$ are linearly independent of m_1. Thus this gives us 2 extra linearly independent elements in G_1, namely $n_1 = (1, 1, 1, q, q)$ and $n_2 = (1, q, q, 1, 1)$.
The subgroup of S_1^2 that remains consists of those elements of G_1, which map q-adically to the identity, thus $e_i \in \langle -1, 2, 3\rangle$ for all $i = 2, 3, 4, 5$. This gives $e_4 \in \langle -2\rangle$, $e_5 \in \langle -3\rangle$, $e_3 \in \langle -1, 3\rangle$. If we look at $n_3 = (1, -6, -1, -2, -3)$, then this is 2-adically mapped to $y_{2,1}$ and 3-adically to $(1, 3, -1, 1, -3) = y_{3,1}$. Moreover this element is linearly independent of m_1, n_1, n_2, thus this gives another linearly independent element in S_1^2. What remains in S_1^2 and is independent of m_1, n_1, n_2, n_3 must satisfy $e_4 = 1, e_5 = 1$, that means that it 2-adically, 3-adically and q-adically is the identity, hence it must be $(1, 1, 1, 1, 1)$. No more independent elements can be found.
We conclude that S_1^2 has dimension 4 and thus $\dim S^2(\mathbb{Q}, J) = 7$ and it is generated by $\{m_1, m_2, m_3, m_q, n_1, n_2, n_3\}$.

(ii) $q \equiv 5 \bmod 24$, then $q \equiv -3 \bmod 8$ and $q \equiv -1 \bmod 3$. We do the same as in the previous case. Now we have that the image of $(X - T)_2$ with the first coordinate 1 is generated by three elements, namely

$$\begin{array}{rccccc} y_{2,1} = & 1 & -3 & 1 & -3 & 1 \\ y_{2,2} = & 1 & 6 & -2 & -2 & 6 \\ y_{2,3} = & 1 & -2 & -6 & -6 & -2 \end{array}$$

We see again that we can consider the subgroup G_1 of S_1^2, by dividing out m_1. So we can forget $y_{2,2}$ and then we see that e_3 is mapped to $\langle -6\rangle$ thus $e_3 \in \langle 2q, -3q\rangle$ and $e_5 \in \langle -2, -3q\rangle$.
The image of $(X - T)_3$ is spanned by two elements

$$\begin{array}{rccccc} y_{3,1} = & 1 & -1 & 1 & 1 & -1 \\ y_{3,2} = & 1 & 3 & 1 & 1 & 3 \end{array}$$

We see that both e_3 and e_4 are mapped 3-adically to 1, thus $e_3, e_4 \in \langle -2, -q\rangle$. Together with the 2-adic information this gives $e_3 \in \langle 2q\rangle$.

The image of $(X-T)_q$ is spanned by two elements

$$\begin{array}{rccccc} y_{q,1} = & 1 & q & 2q & 2q & q \\ y_{q,2} = & 1 & 2 & q & q & 2 \end{array}$$

If we look at $n_1 = (1, 6q, 2q, 2q, 6q)$, then it is 2-adically mapped to $(1, -2, -6, -6, -2)$, 3-adically to $(1, 3, 1, 1, 3)$ and q-adically to $(1, q, 2q, 2q, q)$, because according to proposition (4.1.2) only -1 is a square modulo q. We have that n_1 is linearly independent of m_1, thus we have another independent element in S^2_1. What remains is a subgroup of G_1 with $e_3 = 1$ and then $e_5 \in \langle -3q \rangle$, but 3-adically this can only be mapped to $e_5 = -1$, this is impossible thus it must 3-adically be mapped to the identity, thus each e_i is 1 modulo 3. But e.g. e_2 is mapped to -3, thus this must come from q, which is 3-adically mapped to -1. Thus also 2-adically it must be the identity, this means that every e_i is 1 modulo 3 and 1 modulo 8, this means $e_i = 1$ for all i.
So we conclude that S^2_1 is generated by m_1, n_1 and $S^2(\mathbb{Q}, J)$ has dimension 5.

(iii) $q \equiv 7 \bmod 24$, then $q \equiv -1 \bmod 8$ and $q \equiv 1 \bmod 3$.

$$\begin{array}{rccccc} y_{2,1} = & 1 & -3 & 1 & -3 & 1 \\ y_{2,2} = & 1 & -2 & -2 & -2 & -2 \\ y_{2,3} = & 1 & 1 & 6 & 3 & 2 \end{array}$$

We can forget $y_{2,2}$, thus G_1 is the group with $e_5 \in \langle 2 \rangle$.

$$\begin{array}{rccccc} y_{3,1} = & 1 & 3 & -1 & 1 & -3 \\ y_{3,2} = & 1 & -3 & -1 & 1 & 3 \end{array}$$

We have $e_5 \in \langle 2 \rangle$, thus it is 3-adically mapped to -1, which can only come from $y_{3,1}y_{3,2} = (1, -1, 1, 1, -1)$. This implies that no e_i is divisible by three, but from the 2-adic table we see that besides the identity at least one e_i must be divisible by three. Thus every e_i is 2-adically mapped to 1, which implies $e_i \in \langle -q \rangle$. This means that e_i is 3-adically mapped to 1, thus also here it must be the identity.
Over $\mathbb{R}$ we see that the image must be $(1, -1, -1, 1, 1)$, thus the only non-trivial possibility is $(1, -q, -q, 1, 1)$.
Now we have that $S^2_1(\mathbb{Q}_q)$ is generated by

$$\begin{array}{rccccc} y_{q,1} = & 1 & q & -q & 1 & -1 \\ y_{q,2} = & 1 & -q & -1 & -1 & -q \end{array}$$

So we see that $(1, -q, -q, 1, 1)$ is not in $S^2_1(\mathbb{Q}_q)$. Ergo the dimension of the 2-Selmer group is 4.

(iv) $q \equiv 11 \bmod 24$, then $q \equiv 3 \bmod 8$ and $q \equiv -1 \bmod 3$.

$$\begin{array}{lccccc} y_{2,1} = & 1 & -3 & 1 & -3 & 1 \\ y_{2,2} = & 1 & -6 & -2 & -2 & -6 \\ y_{2,3} = & 1 & 6 & 3 & -6 & -3 \end{array}$$

We have that $y_{2,2}$ is the image of m_1, thus we can forget this one and we get that e_5 is 2-adically mapped to $\langle -3 \rangle$, which means $e_5 \in \langle -3, -q \rangle$.

$$\begin{array}{lccccc} y_{3,1} = & 1 & -1 & 1 & 1 & -1 \\ y_{3,2} = & 1 & 3 & 1 & 1 & 3 \end{array}$$

We have that $y_{3,1}$ is the image of m_1, so we can forget this one. This gives again $e_3, e_4 \in \langle -2, -q \rangle$, and $e_2, e_5 \in \langle 3, -q \rangle$, thus $e_5 \in \langle -q \rangle$.

$$\begin{array}{lccccc} y_{q,1} = & 1 & -q & -1 & q & 1 \\ y_{q,2} = & 1 & q & 1 & 1 & q \end{array}$$

Thus $e_5 = 1$. Hence 3-adically we're only concerned with the identity, 2-adically with $y_{2,1}$ and q-adically with $y_{q,1}$. This last fact means that e_4 is q-adically mapped to q, but this is impossible, because $e_4 \in \langle -2, -q \rangle$ which is q-adically mapped to $\langle -q \rangle$, thus $e_4 = 1$. This implies that also q-adically and 2-adically we only have to deal with the identity, thus it has only the identity besides m_1 in S_1^2.
We conclude that the 2-Selmer group has dimension 4.

(v) $q \equiv 13 \bmod 24$, then $q \equiv -3 \bmod 8$ and $q \equiv 1 \bmod 3$.

$$\begin{array}{lccccc} y_{2,1} = & 1 & -3 & 1 & -3 & 1 \\ y_{2,2} = & 1 & 6 & -2 & -2 & 6 \\ y_{2,3} = & 1 & -2 & -6 & -6 & -2 \end{array}$$

We can forget $y_{2,2}$, (image of m_1), thus e_5 is mapped to $\langle -2 \rangle$, so $e_5 \in \langle -2, -3q \rangle$

$$\begin{array}{lccccc} y_{3,1} = & 1 & 3 & -1 & 1 & -3 \\ y_{3,2} = & 1 & -3 & -1 & 1 & 3 \end{array}$$

$$\begin{array}{lccccc} y_{q,1} = & 1 & q & 1 & q & 1 \\ y_{q,2} = & 1 & 2 & 2 & 2q & 2q \end{array}$$

We immediately see that $(1, q, 1, q, 1) \in S_1^2$, because it is 2-adically mapped to $(1, -3, 1, -3, 1)$ and 3-adically to the identity.
For the remaining part we can forget $y_{2,1}$ and $y_{q,1}$. We see with 3-adic information that $e_4 \in \langle -2, q \rangle$, with q-adic information this gives $e_4 \in \langle -2q \rangle$ (-1 is a q-adic square). But $-2q$ is 2-adically mapped to 6, thus $e_4 = 1$, which implies that 2-adically it gives the identity, as well as q-adically. This implies 2-adically $e_2 \in \langle -3q \rangle$, but this is q-adically mapped to q, thus also

$e_2 = 1$, this implies that also 3-adically it gives the identity and we have that S_1^2 is generated by m_1 and n_1.
We conclude that $\dim(S^2(\mathbb{Q}, J)) = 5$.

(vi) $q \equiv 17 \bmod 24$, then $q \equiv 1 \bmod 8$ and $q \equiv -1 \bmod 3$.

$$\begin{aligned} y_{2,1} &= 1 \quad -6 \quad -1 \quad -2 \quad -3 \\ y_{2,2} &= 1 \quad -2 \quad -2 \quad -2 \quad -2 \\ y_{2,3} &= 1 \quad -3 \quad 1 \quad -3 \quad 1 \\ y_{2,4} &= 1 \quad -6 \quad -3 \quad 2 \quad 1 \end{aligned}$$

We can forget $y_{2,2}$.

$$\begin{aligned} y_{3,1} &= 1 \quad -1 \quad 1 \quad 1 \quad -1 \\ y_{3,2} &= 1 \quad 3 \quad 1 \quad 1 \quad 3 \end{aligned}$$

We can forget $y_{3,1}$, because it comes from m_1.

$$\begin{aligned} y_{q,1} &= 1 \quad 3q \quad q \quad 1 \quad 3 \\ y_{q,2} &= 1 \quad q \quad 1 \quad 1 \quad q \end{aligned}$$

We can forget $y_{q,2}$, because it comes from m_1. Then we see q-adically that $e_4 \in \langle -1, 2 \rangle$. With 3-adic info this gives $e_4 \in \langle -2 \rangle$. This implies that $(1, e_2, \ldots, e_5)$ can 2-adically only be mapped to $y_{2,1}$. This implies that $e_5 \in \langle -3, q \rangle$; q-adically this reduces to $e_5 \in \langle -3 \rangle$; this reduces 3-adically to $e_5 = 1$. Then it follows directly that only the identity remains. Thus the Selmer group has dimension 4.

(vii) $q \equiv 19 \bmod 24$, then $q \equiv 3 \bmod 8$ and $q \equiv 1 \bmod 3$.

$$\begin{aligned} y_{2,1} &= 1 \quad -3 \quad 1 \quad -3 \quad 1 \\ y_{2,2} &= 1 \quad -6 \quad -2 \quad -2 \quad -6 \\ y_{2,3} &= 1 \quad 6 \quad 3 \quad -6 \quad -3 \end{aligned}$$

We can forget $y_{2,2}$.

$$\begin{aligned} y_{3,1} &= 1 \quad 3 \quad -1 \quad 1 \quad -3 \\ y_{3,2} &= 1 \quad -3 \quad -1 \quad 1 \quad 3 \end{aligned}$$

$$\begin{aligned} y_{q,1} &= 1 \quad q \quad 1 \quad 1 \quad q \\ y_{q,2} &= 1 \quad -1 \quad q \quad q \quad -1 \end{aligned}$$

We can forget $y_{q,1}$, because it comes from m_1. We see that with the q-adic info $e_5 \in \langle -1, 2, 3 \rangle$, with 2-adic info this gives $e_5 \in \langle -3 \rangle$, thus the only element that is q-adically possible is the identity. This implies that $e_i \in \langle -2, -3 \rangle$, because $-1, 2, 3$ are all q-adic non-squares. If we look 2-adically we see that this gives $e_3 = 1$ and thus $e_5 = 1$, but then the only possibility 3-adically is the identity. That means $e_2, e_4 \in \langle -2 \rangle$. This gives 2-adically

that the only possibility is the identity, thus here we also have that the Selmer group has dimension 4.

(viii) $q \equiv 23 \bmod 24$, then $q \equiv -1 \bmod 8$ and $q \equiv -1 \bmod 3$.

$$\begin{aligned} y_{2,1} &= 1 \quad -3 \quad 1 \quad -3 \quad 1 \\ y_{2,2} &= 1 \quad -2 \quad -2 \quad -2 \quad -2 \\ y_{2,3} &= 1 \quad 1 \quad 6 \quad 3 \quad 2 \end{aligned}$$

We can forget $y_{2,2}$.

$$\begin{aligned} y_{3,1} &= 1 \quad -1 \quad 1 \quad 1 \quad -1 \\ y_{3,2} &= 1 \quad 3 \quad 1 \quad 1 \quad 3 \end{aligned}$$

We can forget $y_{3,1}$.

$$\begin{aligned} y_{q,1} &= 1 \quad -q \quad -q \quad -q \quad -q \\ y_{q,2} &= 1 \quad -q \quad -1 \quad -1 \quad -q \\ y_{q,3} &= 1 \quad -q \quad -q \quad 1 \quad 1 \end{aligned}$$

We can forget $y_{q,2}$, because it comes from m_1. For the remaining part we can say that according to 2-adic information $e_2 \in \langle -3, -q \rangle$; 3-adically this gives that e_2 is mapped to $\langle -3 \rangle$, thus $e_2 \in \langle -q \rangle$ and only the identity satisfies 3-adically, so not one of the e_i is divisible by 3, this gives 2-adically that the only possibility is the identity. If we let $n_1 = (1, -q, -q, -q, -q), n_2 = (1, -q, -q, 1, 1)$, then we see that both n_1 and n_2 are 2-adically and 3-adically mapped to the identity and q-adically to $y_{q,1}$ and $y_{q,3}$ respectively. Notice that n_1 and n_2 are mutually independent, as well as indepent of m_1, so S_1^2 has dimension 3 and is generated by m_1, n_1 and n_2. We conclude that $\dim(S^2(\mathbb{Q}, J)) = 6$.

For completeness we will also compute the cases $q = 2, 3$ here.
For $q = 2$ we have the next $(X - T)_2$-table.

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	-2	-1	-6	-2
D_{-q}	2	-6	-2	-1	-6
D_0	1	2	1	-2	-1
D_q	6	1	2	-6	-2
D_{-3}	1	-1	-3	3	1
D_{16}	-3	2	1	-2	3

We see again that the first coordinate should be in $\langle 2, 3 \rangle$ and this the case, so we only need to consider the elements with first coordinate 1. These elements are spanned by 3 elements, namely D_0, D_{-3} and $D_{-2q} + D_q$. Of these, only D_{-3} is not in the image of $J(\mathbb{Q})[2]$, so for further computations

we only need to consider this one and add to the dimension 4.
We have the next $(X-T)_3$ table:

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	-3	-2	-1	3	-2
D_{-q}	2	3	-2	-1	3
D_0	1	2	1	-2	-1
D_9	1	-1	1	-1	1

Here also we only consider the elements with first coordinate 1 and not in the image of $J(\mathbb{Q})[2]$, this gives as the only element D_9. But there cannot be an element above D_9 and D_{-3}, because the fourth coordinate should be divisible by 3 according to D_{-3} and this is impossible according to D_9, so besides the image of $J(\mathbb{Q})[2]$ there is nothing in the image of $(X-T)_p$. Thus for $q=2$, the Mordell-Weil rank is 0.

In case $q=3$, we have that the table of $(X-T)_2$ is:

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	6	-3	-6	-1	-3
D_{-q}	3	-6	-3	-6	-1
D_0	6	3	1	-3	-6	
D_q	1	6	3	-6	-3
$D_{\frac{1}{4}}$	1	-3	1	-3	-2
D_{-21}	-6	-1	-3	1	1

With the same argument as above, we only need to consider $D_{\frac{1}{4}}$. The table of $(X-T)_3$ is:

	$X+2q$	$X+q$	X	$X-q$	$X-2q$
D_{-2q}	-3	-3	3	-1	-3
D_{-q}	3	3	-3	3	-1
D_0	-3	3	1	-3	3
D_{-21}	3	1	-3	3	-3

We only have to look at $D_{-21}+D_{-q} \mapsto (1,3,1,1,3)$. Then we see that an element which is above the fourth element is not divisible by 3 and the second coordinate is divisible by 3, but then it cannot be above $D_{\frac{1}{4}}$, because then the fourth coordinate would be divisible by 3. Thus the only element is the identity, which gives that the Selmer group is equal to $J(\mathbb{Q})[2]$ and has dimension 4, and thus the Mordell-Weil rank is 0.

Theorem 4.2.1 *Let q be a prime, and C the hyperelliptic curve of genus 2 given by the model*

$$Y^2 = (X^2 - 4q^2)(X^2 - q^2)X.$$

Then we have that the Selmer group, $S^2(\mathbb{Q}, J) \subseteq \oplus_{i=1}^{5} \mathbb{Q}^*/\mathbb{Q}^{*2}$, belonging to the Jacobian of this curve has for every q as linearly independent elements $(2, -6q, -q, 2, 6)$, $(3, -3q, -1, 3q, 3)$, $(q, -6, -q, -2q, -3q)$ and $(1, -2q, -2, -2, -2q)$. The following table gives a classification of q modulo 24 and for each q the dimension of the 2-Selmer group $S^2(\mathbb{Q}, J)$ and some other generators of $S^2(\mathbb{Q}, J)$, which together with the 4 mentioned generators span the Selmer group.

q (24)	$\dim(S^2(\mathbb{Q}, J))$	MW-*rank*	*other generators*
1	7	≤ 3	$(1, 1, 1, q, q); (1, q, q, 1, 1); (1, -6, -1, -2, -3)$
2	4	0	*none*
3	4	0	*none*
5	5	≤ 1	$(1, 6q, 2q, 2q, 6q)$
7	4	0	*none*
11	4	0	*none*
13	5	≤ 1	$(1, q, 1, q, 1)$
17	4	0	*none*
19	4	0	*none*
23	6	≤ 2	$(1, -q, -q, -q, -q); (1, -q, -q, 1, 1)$

4.3 The torsion part of $J(\mathbb{Q})$

In theorem (4.2.1) we see that for many primes q the Mordell-Weil rank is equal to 0. For these primes, we can look whether the 2-torsion points are the only points in $J(\mathbb{Q})$. If this is so, we can conclude that the only points in $C(\mathbb{Q})$ are the Weierstrass points. The difficulty here is, that we don't know anything about the torsion of $J(\mathbb{Q})$ besides the 2-torsion. In this paragraph, we will prove that in the case of model (4.1), there is no torsion besides the 2-torsion.
We can reduce $J(\mathbb{Q})$ to $J(\mathbb{F}_p)$ by the reduction as defined in the proof of proposition (3.3.4). Furthermore we know that a torsion point in $J(\mathbb{Q})$ is mapped to a torsion point of $J(\mathbb{F}_p)$, in fact $J(\mathbb{F}_p) = J(\mathbb{F}_p)_{\text{tors}}$, because $\mathbb{F}_p$ is finite. In this case we have the following theorem.

Theorem 4.3.1 *Let $J(\mathbb{Q})_{\text{tors}} \longrightarrow J(\mathbb{F}_p)_{\text{tors}} = J(\mathbb{F}_p)$, be the reduction modulo a prime p. If $p > 2$ then this reduction is injective.*

Proof. Let p be a prime. We recall from the proof of proposition (3.3.4) the reduction $J(\mathbb{Q}_p^{\text{unr}}) \to J(\overline{\mathbb{F}}_p)$. Similarly we have a reduction $J(\mathbb{Q}_p) \to J(\mathbb{F}_p)$, because the residue field of $\mathbb{Q}_p$ is $\mathbb{F}_p$. As in the proof of proposition (3.3.4)

we look at the kernel M of this reduction. Again we have the formal group $\mathcal{F}$ and now with $M \simeq \mathcal{F}(p\mathbb{Z}_p)$. Moreover we have that a torsion point $P \in M$ of order m corresponds to an element $x \in \mathcal{F}$, with x in the kernel of the map $[m] : \mathcal{F} \to \mathcal{F}$, as defined in [12], chapter IV. ([12] works with elliptic curves, but according to [1], chapter 7, this works exactly the same for hyperelliptic curves we are studying in this paper, but then an element in $\mathcal{F}(p\mathbb{Z}_p)$ is given by a pair $(x_1, x_2), x_i \in p\mathbb{Z}_p$, whereas in the elliptic case we work with $x \in p\mathbb{Z}_p$.) According to [12], proposition (IV 2.3.(b)) we have that for every $m \in \mathbb{Z}_p^*$ the map $[m]$ is an isomorphism. In particular, the kernel of this image is 0. Hence there are no torsion points of order m in M. So the only torsion that can occur must be of order p^n.
Suppose now $x = (x_1, x_2) \in \mathcal{F}(p\mathbb{Z}_p)$ is an element of order p^n, then we have $v_p(x) \leq \frac{1}{p^n - p^{n-1}}$, where $v_p(x) = \max_i v_p(x_i)$. (see for this [12], theorem (IV 6.1) and [1], pp. 70.) Now we have that for $p > 2$, that $v_p(x) < 1$, hence $v_p(x_i) < 1$ for both i, but $x_i \in \mathcal{F}(p\mathbb{Z}_p)$, so by definition $v_p(x_i) \geq 1$. Hence we have a contradiction, so there are no torsion points of order p^n for $p > 2$, for all $n \geq 1$.
This proves that there are no torsion points in M, for $p > 2$, hence the reduction $J(\mathbb{Q}_p)_{\text{tors}} \to J(\mathbb{F}_p)_{\text{tors}} = J(\mathbb{F}_p)$ is injective and hence the reduction $J(\mathbb{Q})_{\text{tors}} \to J(\mathbb{F}_p)$ is injective. ⊠

We will use this theorem for the computation of the number of elements of the torsion of $J(\mathbb{Q})$ in our example. We already have that $\#J(\mathbb{Q})_{\text{tors}} \geq \#J(\mathbb{Q})[2] = 16$. Furthermore we have an expression for $\#J(\mathbb{F}_p)$ in terms of $\#C(\mathbb{F}_p)$ and $\#C(\mathbb{F}_{p^2})$.

Proposition 4.3.2 *We have*

$$\#J(\mathbb{F}_p) = 1 - t + s - pt + p^2,$$

where

$$s = \frac{(\#C(\mathbb{F}_p))^2 + \#C(\mathbb{F}_{p^2})}{2} + p - \#C(\mathbb{F}_p) - p \cdot \#C(\mathbb{F}_p)$$

and

$$t = p + 1 - \#C(\mathbb{F}_p).$$

Which is the same as

$$\#J(\mathbb{F}_p) = \frac{(\#C(\mathbb{F}_p))^2 + \#C(\mathbb{F}_{p^2})}{2} - p.$$

Proof. Take $V = T_pJ \otimes \mathbb{Q}$, then V is a $2g$-dimensional vectorspace over $\mathbb{Q}_p$, where T_pJ is the Tate module of J, given by $T_pJ = \lim_{\leftarrow n} J(\mathbb{Q}_p)[p^n]$, which is a $\mathbb{Z}_p$ module of rank $2g$.

By the Lefschetz fixed point theorem, we have an expression of $\#J(\mathbb{F}_p)$ in terms of the trace of the Frobenius map as follows:

$$\#J(\mathbb{F}_p) = \sum_{i=0}^{2g} (-1)^i \mathrm{tr}(\mathrm{Frob}\,|_{\wedge^i V}). \tag{4.2}$$

Now suppose that $\lambda_1, \ldots, \lambda_{2g}$ are the eigenvalues of the Frobenius map, then we have by (4.2) that

$$\#J(\mathbb{F}_p) = 1 - \sum \lambda_i + \sum \lambda_i\lambda_j + \ldots + \prod_{i=1}^{2g} \lambda_i,$$

with $\prod_{i=1}^{2g} \lambda_i = p^g$.
By the same theorem of Lefschetz, but now applied to the Tate module of C and Frob, Frob^2 respectively, we get

$$\#C(\mathbb{F}_p) = 1 - \sum \lambda_i + p,$$

$$\#C(\mathbb{F}_{p^2}) = 1 - \sum \lambda_i^2 + p^2.$$

This shows us that $s = \sum_{i<j} \lambda_i\lambda_j$ and $t = \sum \lambda_i$. Moreover we have that $\sum_{i<j<k} \lambda_i\lambda_j\lambda_k = \sum_i \frac{p^2}{\lambda_i} = p\sum_i \frac{p}{\lambda_i} = pt$, where the latter equality follows from the fact that if λ is an eigenvalue, then also $\frac{p}{\lambda}$ is an eigenvalue. This all proves that (recall that $g = 2$)

$$\#J(\mathbb{F}_p) = 1 - t + s - pt + p^2.$$

⊠

If we have $q \neq 5$, we can apply theorem (4.3.1) for $p = 5$, and we get an injection of $J(\mathbb{Q})_{\mathrm{tors}}$ into $J(\mathbb{F}_5)$. With proposition (4.3.2), we know that we can compute $\#J(\mathbb{F}_5)$ once we know $\#C(\mathbb{F}_5)$ and $\#C(\mathbb{F}_{25})$.
We have that our model for C is given by

$$Y^2 = (X^2 - 4q^2)(X^2 - q^2)X,$$

which reduces over $\mathbb{F}_5$ and $\mathbb{F}_{25}$ to

$$Y^2 = (X^2 + q^2)(X^2 - q^2)X = (X^4 - q^4)X.$$

Because we have that $q \not\equiv 0 \bmod 5$, we get that $q^4 \equiv 1 \bmod 5$, hence our model is even given by

$$Y^2 = (X^4 - 1)X.$$

The order of every element in $\mathbb{F}_5^*$ is divisble by 4, hence every element in $\mathbb{F}_5$ gives exactly one point in $C(\mathbb{F}_5)$. Moreover we have a point at ∞, hence $\#C(\mathbb{F}_5) = 6$.
We know that $\mathbb{F}_{25} \simeq \mathbb{F}_5[X]/(X^2+X+1) = \{a+bX \mid a, b \in \mathbb{F}_5\}$. We use some *ad hoc* implementations in `Mathematica` to evaluate $f_5(X) \equiv (X^4 - 1)X$ in every element of $\mathbb{F}_{25}$. This gives us:

```
Table[EvalF[i + j X, X], {i,0,4},{j,0,4}]

 {{0, 4 + 3 X, 3 + X, 2 + 4 X, 1 + 2 X},
  {0, 4 + 3 X, 3 + X, 2 + 4 X, 1 + 2 X},
  {0, 4 + 3 X, 3 + X, 2 + 4 X, 1 + 2 X},
  {0, 4 + 3 X, 3 + X, 2 + 4 X, 1 + 2 X},
  {0, 4 + 3 X, 3 + X, 2 + 4 X, 1 + 2 X}}
```

Hence we need to check whether one or more of $4+3X, 3+X, 2+4X, 1+2X$ is a square. With `Mathematica` we can easily see that $2X+3$ generates $\mathbb{F}_{25}^*$. The computation of the orbit of $2X+3$ gives:

```
FindOrde1[2X+3,X]

{3 + 2X, 3X     , 4 + 3X, 1 + X, 1 + 3X, 2      , 1 + 4X, X,
 3 + X , 2 + 2X, 2 + X , 4     , 2 + 3X, 2X     , 1 + 2X, 4 + 4X,
 4 + 2X, 3      , 4 + X , 4X    , 2 + 4X, 3 + 3X, 3 + 4X, 1}
```

Hence we see that $4 + 3X = (2 + 3X)^3$, $3 + X = (2 + 3X)^9$, $2 + 4X = (2 + 3X)^{21}$ and $1 + 2X = (2 + 3X)^{15}$, hence they are all non-squares in $\mathbb{F}_{25}$. So besides the points that we already found in $C(\mathbb{F}_5)$, we have no more points in $C(\mathbb{F}_{25})$. Hence $\#C(\mathbb{F}_{25}) = \#C(\mathbb{F}_5) = 6$. We can substitute these two values in the formula of proposition (4.3.2) for $p = 5$. This gives us $s = (36 + 6)/2 + 5 - 6 - 30 = -10$ and $t = 5 + 1 - 6 = 0$, hence $\#J(\mathbb{F}_5) = 1 - 0 - 10 - 0 + 25 = 16$, so $\#J(\mathbb{Q})_{\text{tors}} \leq 16$. This implies that $J(\mathbb{Q})_{\text{tors}} = J(\mathbb{Q})[2]$, which proves the following proposition.

Proposition 4.3.3 *Let C be given by model (4.1), and let $q \neq 5$, then we have that the only torsion points in $J(\mathbb{Q})$ are the 2-torsion points.*

With this proposition we can now fully describe $C(\mathbb{Q})$ for the primes q for which the Mordell-Weil rank is 0.

Theorem 4.3.4 *Let q be a prime with either $q = 2, 3$ or $q \equiv 7, 11, 17$ or 19 mod 24. Let C be given by the model*

$$Y^2 = (X^2 - q^2)(X^2 - 4q^2)X.$$

Then we have that the only rational points on C are the 6 Weierstrass points, so

$$C(\mathbb{Q}) = \{(0,0), (\pm q, 0), (\pm 2q, 0), \infty\}.$$

Proof. From the latter proposition and the fact that the Mordell-Weil rank is 0, it follows that $J(\mathbb{Q}) = J(\mathbb{Q})[2]$. Every element in $J(\mathbb{Q})[2]$ can be written as $[P] + [Q] - 2[\infty]$, with $P, Q \in \{(0,0), (\pm q, 0), (\pm 2q, 0), \infty\}$. By proposition (1.3.4) we have a representation for every element in $J(\mathbb{Q})$, which gives us that $C(\mathbb{Q}) = \{(0,0), (\pm q, 0), (\pm 2q, 0), \infty\}$. ⊠

Remark 4.3.5 For every $q \neq 5$, we have that the only torsion points are the 2-torsion points. The same is true for $q = 5$. To see this we need to do the same computations as we did for $q \neq 5$, but now for $p = 7$, and $p = 11$. We can do this after some minor adjustments, with the same algorithms in `Mathematica`. This gives us $\#C(\mathbb{F}_7) = 8, \#C(\mathbb{F}_{49}) = 46$, which gives by proposition (4.3.2) that $\#J(\mathbb{F}_7) = 48$. For $p = 11$, we have $\#C(\mathbb{F}_{11}) = 12, \#C(\mathbb{F}_{121}) = 134$, hence $\#J(\mathbb{F}_{11}) = 128$. Because both $J(\mathbb{Q})_{\text{tors}} \longrightarrow J(\mathbb{F}_7)$ and $J(\mathbb{Q})_{\text{tors}} \longrightarrow J(\mathbb{F}_{11})$ are injections by theorem (4.3.1), we have that $\#J(\mathbb{Q})_{\text{tors}} \leq \gcd(48, 128) = 16$. We already know that $\#J(\mathbb{Q})[2] = 16$, hence $J(\mathbb{Q})_{\text{tors}} = J(\mathbb{Q})[2]$.

Hence also in the case $q = 5$, the only torsion is the 2-torsion. Hence we see that we can forget the assumption $q \neq 5$ in proposition (4.3.3) and get:

Proposition 4.3.6 *Let C be given by model (4.1), then we have that the only torsion points in $J(\mathbb{Q})$ are the 2-torsion points.*

Corollary 4.3.7 *If $P \in C(\mathbb{Q})$, with $Y(P) \neq 0$, then we have that $\#J(\mathbb{Q}) = \infty$.*

Proof. This immediately follows from the fact that the only torsion is the 2-torsion and that the 2-torsion points are generated by the Weierstrass points. Hence the other point $P \in C(\mathbb{Q})$ gives rise to a point in $J(\mathbb{Q})$ of infinite order. ⊠

Remark 4.3.8 We have limited ourselves to the case of Mordell-Weil rank 0, but there are also methods known for solving $C(\mathbb{Q})$ in case the Mordell-Weil rank is 1. We refer to [3].
Another remark that can be made is that we can write the Selmer group as

$$S^2(\mathbb{Q}, J) = J(\mathbb{Q})/2J(\mathbb{Q}) \oplus Ш[2],$$

where $Ш[2]$ denotes the 2-torsion subgroup of the Shafarevich-group

$$Ш(J/\mathbb{Q}) := \text{Ker}\Big(H^1(G, J(\overline{\mathbb{Q}})) \longrightarrow \prod_p H^1(\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), J(\overline{\mathbb{Q}}_p))\Big).$$

Now we have that $\dim_{\mathbb{F}_2} S^2(\mathbb{Q}, J) = r + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш[2] = r + 4 + \dim_{\mathbb{F}_2} Ш[2]$. This reduces modulo 2 to $\dim_{\mathbb{F}_2} S^2(\mathbb{Q}, J) \equiv r + \dim_{\mathbb{F}_2} Ш[2] \bmod 2$.
It is known that if $Ш$ is finite and if there exists a prime p s.t. there exists a $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-invariant divisor of degree 1, then $\dim_{\mathbb{F}_2} Ш[2] \equiv 0 \bmod 2$.
In our case we have that $[\infty]$ is a divisor as required. Moreover, there exists a conjecture saying that $Ш$ is finite. If this conjecture is true, we get $\dim_{\mathbb{F}_2} Ш[2] \equiv 0 \bmod 2$ and hence $\dim_{\mathbb{F}_2} S^2(\mathbb{Q}, J) \equiv r \bmod 2$.

In the cases $q \equiv 1, 5$ or $13 \bmod 24$, which are in fact infinitely many primes, we have, according to theorem (4.2.1), that $\dim_{\mathbb{F}_2} S^2(\mathbb{Q}, J) \equiv 1 \bmod 2$, hence the Mordell-Weil rank r is at least 1, so there should exist at least one other point of infinite order on $J(\mathbb{Q})$.
Surprisingly we have only been able to find such a point in the case $q = 5$. We still wonder whether there exists a general method for finding those points.

4.4 An isogeny between the Jacobian and two elliptic curves

This paragraph is a remark on another way of approaching the problem we have been discussing in this paper.
Recall that our curve was given by the equation

$$C : Y^2 = (X^2 - 4q^2)(X^2 - q^2)X, \tag{4.3}$$

which over $\mathbb{Q}$ is isomorphic (by $\eta = \frac{x}{q}, \xi = \frac{y}{q^3}$) to

$$C : q\xi^2 = (\eta^2 - 4)(\eta^2 - 1)\eta. \tag{4.4}$$

If we look over $\overline{\mathbb{Q}}$, we see that the model of the curve is birational to

$$C_{\sqrt{q}} : \tilde{\xi}^2 = (\eta^2 - 4)(\eta^2 - 1)\eta. \tag{4.5}$$

According to [5], pp. 5-9, we have that this curve given by model (4.5) over $\overline{\mathbb{Q}}$ is isomorphic to

$$C_3 : y^2 = x(x^2 - 1)(x - 3)(x - \frac{1}{3}) =: f_3(x). \tag{4.6}$$

For this curve [5] tells us that there exists an isogeny between the curve's Jacobian and the product of the two elliptic curves $E_\sigma \times E_\tau$, where

$$E_\sigma : Y^2 = X(X - \frac{1}{3})(X - 6 + 4\sqrt{2}) =: f_\sigma(X) \tag{4.7}$$

$$E_\tau : Y^2 = X(X - \frac{1}{3})(X - 6 - 4\sqrt{2}) =: f_\tau(X). \tag{4.8}$$

So another way of approaching the problem of finding the Mordell-Weil rank could be by computing the ranks of the elliptic curves. Note that both elliptic curves are defined over $\mathbb{Q}(\sqrt{2})$.

Bibliography

[1] J.S. Cassels, E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic on Curves of Genus 2.* Cambridge, 1996.

[2] H. Davenport. *The Higher Arithmetic.* Cambridge University Press, 1995[6].

[3] E.V. Flynn. *A flexible method for applying Chabauty's Theorem.* In: Compositio Mathematica 105(1), january 1997, pp. 79-94.

[4] F.Q. Gouvêa. *p-adic Numbers, An Introduction.* Springer-Verlag, 1993.

[5] T. Ibukiyama, T. Katsura, F. Oort. *Supersingular curves of genus two and class numbers.* Preprint nr. 319. December 1983.

[6] M. van der Put. *Schoven en Cohomologie*, dictaat, september 1997.

[7] M. van der Put. *Riemann Surfaces*, lectures, march 1994.

[8] M. Reid. *Undergraduate Algebraic Geometry.* Cambridge University Press, 1988.

[9] P. Samuel. *Théorie algébrique des nombres.* Hermann, 1967.

[10] E.F. Schaefer. *2-Descent on the Jacobians of Hyperelliptic curves.* In: Journal of number theory 51(2), april 1995, pp. 219-232.

[11] J.P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[12] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[13] J. Top. *Introductory lectures on local fields*, november 1995.