university of groningen / faculty of science and engineering / mathematics and applied mathematics

Two-descent on hyperelliptic curves of genus 2

Master's Project Mathematics

28 February 2020

Student: T. Evink

First supervisor: prof. dr. J. Top

Second supervisor: dr. J.S. Müller

Contents

Acknowledgements

I would like to thank my supervisors prof. dr. J. Top and dr. J.S. Müller for their great guidance during the writing of this thesis. I would also like to thank prof. dr. P. Stevenhagen for his help concerning the relevance of Redei symbols to this thesis, and dr. P.A. Helminck for many comments about the thesis and fruitful discussions.

Chapter 1

Jacobians of hyperelliptic curves

1.1 Hyperelliptic curves

Fix a field k with algebraic closure $\overline{k}$.

Definition 1.1.1. *A curve over k is a scheme C of finite type over k with irreducible components all of dimension* 1*. Additionally:*

1. *The curve C is complete if it is proper over k.*
2. *The curve C is regular if all stalks $\mathcal{O}_{C,x}$ are regular local rings, and smooth if the base extension $C_{\overline{k}}$ is regular.*
3. *The curve C is normal if it is irreducible and all its stalks are normal integral domains.*

Note that a scheme of finite type over a Noetherian ring is Noetherian, so a scheme of finite type over k has finitely many irreducible components. A projective scheme over k is proper, and the converse holds for curves, so properness over k is the same as projective over k.

A smooth curve is regular, but the converse may not hold when k is not perfect. A regular local ring of dimension 1 is the same as a discrete valuation ring. As these are reduced, we see that a regular curve is reduced, hence each irreducible component is integral. Thus a curve is regular if and only if its irreducible components can be covered by finitely many spectra of Dedekind domains R. Similarly, such a curve is smooth if the various rings $R \otimes_k \overline{k}$ are also Dedekind domains. We also see that a normal curve is the same thing as an irreducible regular curve.

From [Liu 7.3.13] and the equivalence of properness and projectiveness for curves over k we obtain

Proposition 1.1.2. *We have an anti-equivalence between the category of complete normal curves over k with finite k-morphisms and the category of field extensions K/k of transcendence degree 1 with k-algebra homomorphisms.*
Concretely: a finite k-morphism $C \to C'$ of complete normal curves over k corresponds with the induced map on function fields $k(C') \to k(C)$.

Note that for a finite k-morphism $\phi : C \to C'$ of integral curves the generic point of C maps to the generic point of C' (for otherwise ϕ maps all points of C to a closed point x_0 of C', but then the induced map on residue fields $k(x_0) \to k(C)$ would be finite, which contradicts that $k(C)$ has transcendence degree 1 over k), so we indeed have an induced map on function fields.

Definition 1.1.3. *A hyperelliptic curve over k is a geometrically irreducible, smooth complete curve C over k, that admits a finite separable morphism $\phi : C \to \mathbb{P}^1_k$ of degree 2. Thus on the level of function fields we have that $k(C)$ is a separable, quadratic extension of the rational function field $k(x)$.*

Remark 1.1.4. Our definition of a hyperelliptic curve is a bit more restrictive than usual. In general one allows a finite separale morphism of degree 2 of C to a geometrically integral 0 curve of genus 0, i.e. we could have a conic without k-rational points replacing $\mathbb{P}^1_k$, see [7, Prop. 7.4.1].

To make our definition of the hyperelliptic curve C explicit, assume $\mathrm{char}(k) \neq 2$ and write $k(C) = k(x, y)$ with $y^2 = f(x)$, for some square-free $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in k[x]$ of degree d.
If $\mathbb{P}^1_k = U \cup V$ for $U \cong \mathrm{Spec}(k[x])$ and $V \cong \mathrm{Spec}(k[u])$, with $u = x^{-1}$, then $X = \phi^{-1}(U) \cup \phi^{-1}(V)$ with $\phi^{-1}(U) \cong \mathrm{Spec}(A)$ and $\phi^{-1}(V) \cong \mathrm{Spec}(B)$ for A and B the integral closures of $k[x]$ and $k[u]$ in $k(C)$, respectively.

Note that $k[x, y] \subset A$, and one can check that f being square-free implies that $k[x, y]$ is normal so that $A = k[x, y]$.
To compute B, note that only normality at the points of B lying over the ideal (u) of $k[u]$ need to be considered. Let

$$f^*(u) = a_d + \cdots + a_1 u^{d-1} + a_0 u^d = u^d f(u^{-1})$$

be the reciprocal polynomial of f. We consider two cases based on the parity of d. If $d = 2k + 1$, then

$$\begin{aligned}\left(\frac{y}{x^{k+1}}\right)^2 &= \sum_{i=0}^{d} a_i x^{i-2k-2} \\ &= u \sum_{i=0}^{d} a_i u^{2k+1-i} = u f^*(u),\end{aligned}$$

shows that $k[u, v] \subset B$ for $v = y/x^{k+1}$. We see that $\mathrm{Spec}(k[u, v])$ has (u, v) as unique point lying over $(u) \subset k[u]$. As $f^*(0) = a_d \neq 0$, the relation $v^2 = u f^*(u)$ shows that (u, v) is locally generated by v, proving that $k[u, v]$ is normal, hence

$B = k[u, v]$.
If $d = 2k + 2$, then similarly we see that $k[u, v] \subset B$ for $v = y/x^{k+1}$ satisfying $v^2 = f^*(u)$. Since $k[u, v]/(u) \cong k(\sqrt{a_d})$, we see that (u) is a maximal ideal of $k[u, v]$, which is already globally principal, so that $B = k[u, v]$.

Letting $\varepsilon = 1$ if d is odd and 0 if d is even, and letting k with $2k + 1 \leq d \leq 2k + 2$, we have that C is the curve obtained by gluing the two affine schemes

$$U = \mathrm{Spec}(k[x, y]/(y^2 - f(x)))$$
$$V = \mathrm{Spec}(k[u, v]/(v^2 - u^\varepsilon f^*(v))),$$

Along $D(x) \cong D(u)$ with the relation $u = x^{-1}$ and $v = y/x^{k+1}$.

Replacing k with $\overline{k}$ we obtain the description for $C_{\overline{k}}$, and we see that regularity of $C_{\overline{k}}$ means precisely that $f \in \overline{k}[x]$ is square-free, i.e. that f is separable. Note that separability of f follows from f being square-free if k is perfect. For k not perfect it can happen that the equation $y^2 = f(x)$ determines a regular normal curve that is not smooth, and hence is not a hyperelliptic curve according to our definition.

For $f \in k[x]$ separable and square-free, we will use the phrase 'let C be the hyperelliptic curve determined by the equation $y^2 = f(x)$' to mean the hyperelliptic curve with function field $k(x, y)$.

Collecting the relevant information we obtain

Proposition 1.1.5. *Suppose that* $\mathrm{char}(k) \neq 2$ *and that* $f \in k[x]$ *is non-constant, square-free and separable. Then there is (up to isomorphism) a unique hyperelliptic curve* C *with affine patch defined by the equation*

$$y^2 = f(x).$$

If K/k *is a field extension then* $C(K)$ *can be identified with pairs* $(a, b) \in K^2$ *such that* $b^2 = f(a)$*, together with one point at infinity if* $\deg(f)$ *is odd, and two points at infinity if* $\deg(f)$ *is even precisely when the leading coefficient of* f *is a square in* K*.*

As a final point for this section we compute the genus of a hyperelliptic curve.

Proposition 1.1.6. *Suppose that* $\mathrm{char}(k) \neq 2$ *and let* C/k *be the hyperelliptic curve of genus* g *defined by the equation*

$$y^2 = f(x).$$

Then $2g + 1 \leq \deg(f) \leq 2g + 2$*.*

Proof. As C is smooth and geometrically connected its genus equals the arithmetic genus $p_a(C) = \dim_k H^1(C, \mathcal{O}_C)$, which we can calculate using Riemann-Hurwitz [7, p. 7.4.3] on the tamely ramified, finite separable map $\phi : C \to \mathbb{P}^1_k$.

$$2p_a(C) - 2 = 2(2p_a(\mathbb{P}^1_k) - 2) + \sum_x (e_x - 1)[k(x) : k],$$

the sum running over the closed points of C. As $p_a(\mathbb{P}^1_k) = 0$ we obtain

$$2p_a(C) + 2 = \sum_x (e_x - 1)[k(x) : k].$$

The only ramified primes of the Dedekind domain $k[x, y]/(y^2 - f(x))$ (as extension of $k[x]$) are $(y, g(x))$ for g an irreducible factor of f. As $[k(x) : k] = \deg(g)$ for x corresponding to $(y, g(x))$, we obtain $\sum_{x \in U}(e_x - 1)[k(x) : k] = \deg(f)$ with $U = \mathrm{Spec}(k[x, y])$.
It remains to check ramification at infinity. From the calculation of the normalisation we quickly see that only when $\deg(f)$ odd the point at infinity is ramified, which proves the result. □

As a corollary we have that whatever the degree of f is, the corresponding morphism $C \to \mathbb{P}^1_k$ is ramified at exactly $2g + 2$ points. Moreover, if f is of even degree (so that all ramification comes from the roots of f), and has a k-rational root, then after a suitable change of coordinates we can find a model for the curve with defining polynomial of *odd* degree. For $g = 1$ this is just 'finding a Weierstrass equation for your elliptic curve'.

Remark 1.1.7. Contrary to what is common in the literature, an elliptic curve is also hyperlliptic in our case. This will be convenient since the theory we will set up for 2-descent applies equally well to the case of genus 1.

1.2 Jacobians

Our main reference for this section is [Liu 7.4.4].

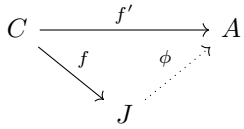
Definition 1.2.1. *An Abelian variety over k is a k-group scheme A that is of finite type, proper and geometrically integral.*

The meaning of A being a k-group scheme is that A is a group object in the category of k-schemes. Without going in too much detail this means that there are k-morphisms $m : A \times_k A \to A$ and $i : A \to A$ and $e : \mathrm{Spec}(k) \to A$ satisfying the axioms that guarantee that for any k-scheme T, the set of T-valued points $A(T)$ is a group and the association $T \mapsto A(T)$ gives a functor from the category of k-schemes to the category of groups.

It is known that an Abelian variety is necessarily smooth, abelian and projective.

Definition 1.2.2. *Let C be a complete, geometrically connected, smooth curve over k of genus g, together with a base point $P_0 \in C(k)$. The Jacobian variety of C, is an Abelian variety J over k together with a map $f : C \to J$ sending P_0 to 0, such that whenever A is another abelian variety, and $f' : C \to A$ also sends P_0 to 0, then there is a unique homomorphism of k-group schemes $\phi : J \to A$*

such that



Thus loosely speaking, the Jacobian is the minimal abelian variety associated to the curve that sends the base point to 0.

A very non-trivial result is

Proposition 1.2.3. *The Jacobian variety J of C with $P_0 \in C(k)$ exists, has dimension g, and for any field extension K/k we have a natural isomorphism $J(K) \cong \mathrm{Pic}^0(C_K)$.*

Proof. From [7, Theorem 7.4.39] we see the existence of an Abelian variety A of dimension g with natural isomorphism $A(K) \cong \mathrm{Pic}^0(C_K)$ for field extensions K/k. In [8, Ch. III Proposition 6.1] we see that such an Abelian variety satisfies the same universal property we used as definition for the Jacobian, hence they are equal. □

Naturality means that for a tower of fields $L/K/k$ we have a commutative diagram

$$\begin{array}{ccc} J(K) & \xrightarrow{\sim} & \mathrm{Pic}^0(C_K) \\ \downarrow & & \downarrow \\ J(L) & \xrightarrow{\sim} & \mathrm{Pic}^0(C_L) \end{array}$$

We remark that L/K gives a map $C_L \to C_K$, and then we obtain $\mathrm{Pic}^0(C_K) \to \mathrm{Pic}^0(C_L)$ by pullback of invertible sheaves.
Assuming in addition that C is geometrically integral, we can apply corollary 7.1.19 and proposition 7.2.16 of [7] to see that $\mathrm{Pic}(C_K) \cong \mathrm{Cl}(C_K)$ whenever K/k is algebraic. Moreover, with pullback maps along $C_L \to C_K$ for $L/K/k$, we see that the isomorphisms $\mathrm{Pic}(C_K) \cong \mathrm{Cl}(C_K)$ are natural in K and respect degrees.

If $x \in C$ is a closed point with residue field $k(x)$ separable over k, then we have $[k(x) : k]$ embeddings of k-algebra's $k(x) \to k^{\mathrm{sep}}$, i.e. we have $[k(x) : k]$ points in $C(\overline{k})$ corresponding to x. Moreover $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ acts transitively on $\mathrm{Hom}_{k\text{-alg}}(k(x), k^{\mathrm{sep}})$, hence the sum of these points in the free abelian group on $C(\overline{k})$ is G_k-invariant.
If we assume that k is a perfect field, then $k(x)/k$ is always separable, hence we can identify a closed point $x \in C$ of degree $[k(x) : k]$ with a G_k-invariant sum of $[k(x) : k]$ points in the free abelian group on $C(\overline{k})$, which allows us to identify a Weil divisor on C with a G_k-invariant element of the free abelian group on $C(\overline{k})$, which we will call a k-rational divisor on C.
Giving a point of $C(\overline{k})$ degree 1, this identification respects degrees. On the level of principal divisors, the identification becomes

$$(f) = \sum_x \mathrm{ord}_x(f)[x] = \sum_{P \in C(\overline{k})} \mathrm{ord}_P(f)[P]$$

taking $\mathrm{ord}_P(f) = \mathrm{ord}_x(f)$ for x the closed point corresponding to P. With this identification we have that the degree 0 part of $\mathrm{Cl}(C)$ is the divisor class group of C as in [2, Def. 4.129], where it is also called the Picard group of C.

Lastly, considering $L/K/k$ for k perfect, we see that applying this identification to both C_K and C_L (and using that $\overline{k}$ is an algebraic closure for the perfect fields L and K), that pullback of Weil divisors along $C_L \to C_K$ simply amounts to noting that a G_K-invariant element of the free group on $C(\overline{k})$ is also G_L-invariant. This justifies the naturality of the identification, and we obtain

Proposition 1.2.4. *Let k be a perfect field with $\mathrm{char}(k) \neq 2$, consider the hyperelliptic curve C of genus $g \geq 1$ defined by the equation*

$$y^2 = f(x),$$

for $f \in k[x]$ separable of degree $2g+1$, and let J denote its Jacobian with base point $\infty \in C(k)$. Then for K/k algebraic, we may canonically identify

$$J(K) = \mathrm{Div}^0_K(C)/\mathrm{Prin}_K(C),$$

where $\mathrm{Div}^0_K(C)$ consists of G_K-invariant elements of the degree 0 subgroup of the free abelian group on $G(\overline{k})$, and $\mathrm{Prin}_K(C)$ consists of the principal divisors

$$(f) = \sum_{P \in C(\overline{k})} \mathrm{ord}_P(f)[P]$$

defined over K, i.e. $f \in K(x,y)$, the function field of C base extended to K.

If C/k is a hyperelliptic curve defined by $y^2 = f(x)$ for f of odd degree, we will implicitly take the k-rational point at infinity $\infty \in C(k)$ as base point for the Jacobian when talking about 'the Jacobian of C'. Additionally: we will identify the points of $C(K) \setminus \{\infty\}$ for K/k algebraic with pairs $(a,b) \in K^2$ satisfying $b^2 = f(a)$ as in proposition 1.1.5.

Proposition 1.2.5. *With the same notation as proposition 1.2.4, then elements of $J(K)$ can be written uniquely as $[D - d \cdot \infty]$ for some $0 \leq d \leq g$ and D an effective K-rational divisor of degree d in general position.*

Proof. This is part of the Mumford representation of points in $J(K)$. See [2, Thm. 4.135]. The divisor being in general position means that $D \not\geq P + i(P)$ for all $P \in C$ and $P \not\geq \infty$, here i is the hyperelliptic involution defined by $(x,y) \mapsto (x,-y)$. Note that this condition is necessary: if $(a,b) \in C(K)$ then $\mathrm{div}(x-a) = [(a,b) + (a,-b) - 2\infty]$.

□

Note that for $g = 1$, the divisor D has as only option consisting of a single point, which constitutes the fact that an elliptic curve equals its own Jacobian. For $g = 2$ we see that we have two options: a point of $J(K)$ corresponds with an effective K-rational divisor of degree 1 or 2. In the first case D is just a

K-rational point, whilst in the second case D is either the sum of two distinct K-rational points, or a sum $D = P + Q$ for P, Q two distinct L/K-conjugate points of $C(L)$ for L/K a quadratic extension. Note that in this last case, we cannot have $P = i(Q)$, which is the same thing as $x(P) \notin K$.

Corollary 1.2.6. *For K/k algebraic we have an injection $C(K) \to J(K)$ defined by $P \mapsto [P - \infty]$.*

Chapter 2

Theory of 2-descent

In this chapter we will consider some general theory about 2-descent on Abelian varieties A over K, quickly specializing to the case where A is the Jacobian of a hyperelliptic curve. We then make the situation more explicit to allow computations.

2.1 Introduction

Let J be the Jacobian of the hyperelliptic curve C defined over a number field K by the equation $y^2 = f(x)$, where $f \in K[x]$ is has odd degree. Thus $\deg(f) = 2g + 1$, where g is the genus of C.

Theorem 2.1.1 (Mordell-Weil)**.** *The group $J(K)$ is finitely generated.*

Proof. See Manin's appendix in [9]. □

We are interested in the structure of the group $J(K)$. In particular, we are interested in computing the rank: the integer $r \geq 0$ such that

$$J(K)/J(K)_{\text{tor}} \cong \mathbb{Z}^r.$$

We will often use the notation $\text{rank}(J/K)$ for the rank of $J(K)$. As an illustration of the utility of having information about the rank, suppose that $J(K)$ has rank 0, then $J(K) = J(K)_{\text{tor}}$, and one can quickly determine the torsion elements via reduction techniques as is done for elliptic curves. With corollary 1.2.6 we can then detect points of $J(K)$ that arise from $C(K)$, which solves a Diophantine equation.

The theory of 2-descent revolves around studying $J(K)/2J(K)$. This quotient contains information about the rank, for if $J(K) \cong \mathbb{Z}^r \times J(K)_{\text{tors}}$, then

$$J(K)/2J(K) \cong (\mathbb{Z}/2\mathbb{Z})^r \times J(K)_{\text{tor}}/2J(K_{\text{tor}})$$

As $J(K)_{\mathrm{tor}}$ is finite, we have $\dim_{\mathbb{F}_2}(J(K)_{\mathrm{tor}})/2J(K_{\mathrm{tor}}) = \dim_{\mathbb{F}_2} J(K)[2]$, hence we obtain the formula

$$\mathrm{rank}(J/K) = \dim_{\mathbb{F}_2}(J(K)/2J(K)) - \dim_{\mathbb{F}_2} J(K)[2]. \tag{2.1}$$

The computation of $\dim_{\mathbb{F}_2} J(K)[2]$ is not hard:

Proposition 2.1.2. *Allowing K to be any perfect field, we have*

$$\dim_{\mathbb{F}_2}(J(K)[2]) = \#\{\textit{irreducible factors of } f \textit{ in } K[x]\} - 1$$

More specifically, if $g_1, \ldots, g_r$ are the monic irreducible factors of f of degrees r_i, then $J(K)[2]$ is generated by $D_i = \sum_{g_i(\alpha)=0}[(\alpha, 0) - \infty]$, with the relation $D_1 + \cdots + D_r = 0$.

Proof. With the Mumford representation (see [2, Thm. 14.5]) we have a quick proof for this: if $P \in J(K)$ is represented by the pair of polynomials (a, b), then $-P$ is represented by $(a, -b)$. Thus $J(K)[2]$ consists precisely of those points represented by $(a, 0)$ where a is a product of irreducible factors of f. As $\deg(a) \leq g$, we see that the order of $J(K)[2])$ equals the number of sets $S \subset \{1, \ldots, r\}$ such that $\sum_{i \in S} \deg(g_i) \leq g$, which is 2^{r-1} as for any subset $S' \subset \{1, \ldots, r\}$ we have $\sum_{i \in S} \deg(g_i) \leq g$ for S exactly one of $\{S', \{1, \ldots, r\} \setminus S'\}$. Thus we now know that the D_i generate $J(K)[2]$, which is of dimension $r - 1$. To see the relation $D_1 + \cdots + D_r = 0$ in $J(K)$ one simply observes that $\mathrm{div}(y) = \sum_{i=1}^{r} D_i$. □

To work with the group $J(K)/2J(K)$, we first find an embedding of this group in another group by means of Galois cohomology, which we will treat for an arbitrary Abelian variety over K.

2.2 Some Galois cohomology

Let A be an Abelian variety over K. Multiplication by 2 is an isogeny on A, and hence surjective. As surjectivity is preserved under base change to $\overline{K}$ (see for example [13, Lemma 29.9.4]), and $A(\overline{K}) = A_{\overline{K}}(\overline{K})$ can be identified with the closed points of $A_{\overline{K}}$ via the weak nullstellensatz, we see that multiplication by 2 on $A(\overline{K})$ is surjective, i.e. we have the exact sequence

$$0 \to A(\overline{K})[2] \to A(\overline{K}) \to A(\overline{K}) \to 0 \tag{2.2}$$

of $G_K := \mathrm{Gal}(\overline{K}/K)$-modules. Taking invariants yields the following long exact sequence due to cohomology

$$0 \to A(K)[2] \to A(K) \to A(K) \to H^1(G_K, A(K)[2]) \to H^1(G_K, A(K)) \to H^1(G_K, A(K)) \tag{2.3}$$

The induced map $H^1(G_K, A(K)) \to H^1(G_K, A(K))$ is also just multiplication by 2, so exactness of this long exact sequence at $H^1(G_K, A(\overline{K})[2])$ results in the short exact sequence

$$0 \to A(K)/2A(K) \to H^1(G_K, A(\overline{K})[2]) \to H^1(G_K, A(\overline{K}))[2] \to 0.$$

For a (finite or infinite) prime $\mathfrak{p}$ of K we similarly obtain a long exact sequence by considering multiplication by 2 on the $G_{K_\mathfrak{p}}$-module $A(\overline{K_\mathfrak{p}})$. We can identify $G_{K_\mathfrak{p}}$ with a decomposition group $D_\mathfrak{p} \subset G_K$, so we can also consider (2.2) as a short exact sequence of $G_{K_\mathfrak{p}}$-modules. The resulting long exact sequence obtained by taking $G_{K_\mathfrak{p}}$-invariants is compatible with (2.3) through restriction maps $H^1(G_K, -) \to H^1(G_{K_\mathfrak{p}}, -)$ on cohomology, meaning that from the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\overline{K})[2] & \longrightarrow & A(\overline{K}) & \longrightarrow & A(\overline{K}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\overline{K_\mathfrak{p}})[2] & \longrightarrow & A(\overline{K_\mathfrak{p}}) & \longrightarrow & A(\overline{K_\mathfrak{p}}) & \longrightarrow & 0, \end{array}$$

we obtain the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(G_K, A(\overline{K})[2]) & \longrightarrow & H^1(G_K, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(K_\mathfrak{p})/2A(K_\mathfrak{p}) & \longrightarrow & H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})[2]) & \longrightarrow & H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}}))[2] & \longrightarrow & 0 \end{array} \tag{2.4}$$

Studying (the size of) the group $A(K)/2A(K)$ is equivalent to studying its image in the cohomology group $H^1(G_K, A(\overline{K})[2])$. One remark is that an element of this image maps vertically into the image of $A(K_\mathfrak{p})/2A(K_\mathfrak{p})$ in $H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})[2])$, or equivalently into the kernel of

$$H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})[2]) \to H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})),$$

for *every* completion $K_\mathfrak{p}$ of K.
We can combine the diagrams (2.4) for all completions into a single diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(G_K, A(\overline{K})[2]) & \longrightarrow & H^1(G_K, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_\mathfrak{p} A(K_\mathfrak{p})/2A(K_\mathfrak{p}) & \longrightarrow & \prod_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})[2]) & \longrightarrow & \prod_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}}))[2] & \longrightarrow & 0. \end{array}$$

We now define respectively the 2-Selmer group, and the Tate-Shafarevich group of J/K as follows:

$$\begin{aligned} S^2(A/K) &:= \ker\left(H^1(G_K, A(\overline{K})[2]) \to \prod\nolimits_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}}))\right), \\ Ш(A/K) &:= \ker\left(H^1(G_K, A(\overline{K})) \to \prod\nolimits_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}}))\right). \end{aligned}$$

Proposition 2.2.1. *The 2-Selmer group $S^2(A/K)$ fits in the following short exact sequence.*

$$0 \to A(K)/2A(K) \to S^2(A/K) \to Ш(A/K)[2] \to 0, \tag{2.5}$$

and moreover, this sequence is natural in A.

Proof. Let $A \to A'$ be a morphism of Abelian varieties over K, and consider the following commutative diagram of G_K-modules with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\overline{K})[2] & \longrightarrow & A(\overline{K}) & \longrightarrow & A(\overline{K}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A'(\overline{K})[2] & \longrightarrow & A'(\overline{K}) & \longrightarrow & A'(\overline{K}) & \longrightarrow & 0. \end{array}$$

By naturality of the long exact sequence of cohomology, this yields the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(G_K, A(\overline{K})[2]) & \longrightarrow & H^1(G_K, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A'(K)/2A'(K) & \longrightarrow & H^1(G_K, A'(\overline{K})[2]) & \longrightarrow & H^1(G_K, A'(\overline{K}))[2] & \longrightarrow & 0 \end{array}$$

Extending this diagram 'in 3D' with

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(G_K, A(\overline{K})[2]) & \longrightarrow & H^1(G_K, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & \longrightarrow & \prod_{\mathfrak{p}} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})) & \xrightarrow{\mathrm{id}} & \prod_{\mathfrak{p}} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})) & \longrightarrow & 0. \end{array} \tag{2.6}$$

and the same diagram with A replaced by A', we see that the snake lemma and its naturality yields the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & S^2(A/K) & \longrightarrow & Ш(A/K)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A'(K)/2A'(K) & \longrightarrow & S^2(A'/K) & \longrightarrow & Ш(A'/K)[2] & \longrightarrow & 0 \end{array} \tag{2.7}$$

noting that exactness at the Tate-Shafarevich groups is due to the two connecting homomorphisms being 0. □

The group $S^2(A/K)$ gathers all local information on a global level. Note that $A(K)/2A(K) \xrightarrow{\sim} S^2(A/K)$ means that elements of $H^1(G_K, A(\overline{K})[2])$ that map to all local images of $A(K_\mathfrak{p})/2A(K_\mathfrak{p})$ are in fact globally in the image. Thus the group $Ш(A/K)[2]$ measures the obstruction to a local-global principle for the maps $A(K)/2A(K) \to A(K_\mathfrak{p})/2A(K_\mathfrak{p})$.

Let us conclude this abstract setting with the following.

Proposition 2.2.2. *Let L/K be an extensions of number fields and A an Abelian varierty over K. Then we have a natural commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & S^2(A/K) & \longrightarrow & Ш(A/K)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(L)/2A(L) & \longrightarrow & S^2(A/L) & \longrightarrow & Ш(A/L)[2] & \longrightarrow & 0 \end{array} \tag{2.8}$$

Proof. We have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & H^1(G_K, A(\overline{K})[2]) & \longrightarrow & H^1(G_K, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(L)/2A(L) & \longrightarrow & H^1(G_L, A(\overline{L})[2]) & \longrightarrow & H^1(G_L, A(\overline{L}))[2] & \longrightarrow & 0, \end{array}$$

which results in the desired diagram by comparing the relevant diagrams like (2.6) with the natural map

$$\prod_{\mathfrak{p}} H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})) \to \prod_{\mathfrak{q}} H^1(G_{L_\mathfrak{q}}, A(\overline{L_\mathfrak{q}})),$$

which is constructed through the maps

$$H^1(G_{K_\mathfrak{p}}, A(\overline{K_\mathfrak{p}})) \to \prod_{\mathfrak{q}|\mathfrak{p}} H^1(G_{L_\mathfrak{q}}, A(\overline{L_\mathfrak{q}})). \qquad \square$$

Let us now specialize to the case where A is the Jacobian of a hyperelliptic curve C defined by the equation $y^2 = f(x)$, for f of odd degree. We will see that the 2-Selmer group $S^2(J/K)$ is finite, hence from the equations (2.1) and (2.5) we obtain

$$\operatorname{rank}(J/K) + \dim_{\mathbb{F}_2} Ш(J/K)[2] = \dim_{\mathbb{F}_2} S^2(J/K) - \dim_{\mathbb{F}_2} J(K)[2]. \qquad (2.9)$$

Proposition 2.2.3. *If $Ш(J/K)$ is finite, then $Ш(J/K) \cong T \times T$ for a finite group T.*

Proof. Because of the K-rational point at infinity, there is a $K_\mathfrak{p}$-rational divisor of degree $g-1$ for every prime $\mathfrak{p}$ of K, which means that C has no deficient primes in the language of [11]. The result then follows from corollary 9 and 12 of [11]. $\square$

It is conjectured that $Ш(J/K)$ is indeed finite, so that conditionally we have $\dim_{\mathbb{F}_2} Ш(J/K)[2] \equiv 0 \bmod 2$.

The first step in computing $S^2(J/K)$ consists of a computation of $J(K_\mathfrak{p})/2J(K_\mathfrak{p})$ for various completions.

Proposition 2.2.4. *Let F be a finite extension of $\mathbb{Q}_p$ for some finite or infinite prime p of $\mathbb{Q}$, let C/F be a hyperelliptic curve of genus g of odd degree, and let J be its Jacobian. Then*

$$\dim_{\mathbb{F}_2}(J(F)/2J(F)) = \begin{cases} \dim_{\mathbb{F}_2} J(F)[2] + g[F:\mathbb{Q}_2] & \text{if } p = 2, \\ \dim_{\mathbb{F}_2} J(F)[2] & \text{if } 2 < p < \infty \\ \dim_{\mathbb{F}_2} J(F)[2] - g & \text{if } F = \mathbb{R} \\ 0 & \text{if } F = \mathbb{C} \end{cases}$$

Proof. The proof is based on lemma 4.4 and 4.8 of [16]. Suppose that $p < \infty$ and let $R = \mathcal{O}_F$. Then $J(F)$ has a subgroup H of finite index isomorphic to g copies of the additive group R^+. Letting T be the quotient we have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & J(F) & \longrightarrow & T & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot 2} & & \downarrow{\scriptstyle \cdot 2} & & \downarrow{\scriptstyle \cdot 2} & & \\ 0 & \longrightarrow & H & \longrightarrow & J(F) & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

We have $|T[2]| = |T/2T|$ as T is finite, and $H[2] = 0$ as H is torsion-free. Thus when counting $\mathbb{F}_2$-dimensions in the long exact sequence obtained from the snake lemma applied to the above diagram, we obtain

$$\dim_{\mathbb{F}_2}(J(F)/2J(F)) = \dim_{\mathbb{F}_2} J(F)[2] + \dim_{\mathbb{F}_2}(H/2H).$$

Now if $p \neq 2$, then multiplication by 2 is an isomorphism on H as $2 \in \mathcal{O}_F^*$, so that $\dim_{\mathbb{F}_2}(H/2H)=0$.
If $p = 2$ then R^+ is free of rank $[F : \mathbb{Q}_2]$ as $\mathbb{Z}_2$-module, hence $R^+/2R^+ \cong (\mathbb{Z}/2\mathbb{Z})^{[F:\mathbb{Q}_2]}$ as groups, hence $\dim_{\mathbb{F}_2}(H/2H) = g[F : \mathbb{Q}_2]$.
When $F = \mathbb{C}$ the result follows as $\mathbb{C}$ is algebraically closed (compare (2.2)). When $F = \mathbb{R}$, the result follows similarly from the fact that $J(\mathbb{R})$ has a subgroup of finite index isomorphic to $(\mathbb{R}/\mathbb{Z})^g$, on which multiplication by 2 is surjective and has kernel $(\mathbb{Z}/2\mathbb{Z})^g$. □

2.3 An explicit embedding

In this section we make the situation more explicit following [12]. For simplicity of exposition we additionally assume f to be monic.
Consider the K-algebra $A = K[x]/(f(x))$ and the $\overline{K}$-algebra $\overline{A} = \overline{K}[x]/(f(x))$. Then $A^* \to \overline{A}^*$ is an injection, and $\overline{A}^*$ becomes a G_K-module by letting x mod (f) act trivially, with G_K-invariants precisely A^*. We also have norm maps $A \to K$ and $\overline{A} \to \overline{K}$. Write $f = g_1 \cdots g_r$ for g_i the monic irreducible factors of f and set $A_i = K[x]/(g_i)$. Then with the Chinese remainder theorem we have the commutative diagram

$$\begin{array}{ccc} A^* & \xrightarrow{\sim} & \prod_{i=1}^{r} A_i^* \\ & \searrow^{N} & \downarrow{\scriptstyle \prod_i N_i} \\ & & K^* \end{array}$$

for $N_i : A_i^* \to K^*$ the norm maps.

Let α_i denote the roots of f in $\overline{K}$, and write $D_i = [(\alpha_i, 0)] - [\infty]$, so that the D_i span $J(\overline{K})[2]$ with the single relation $\sum_{i=1}^{2g+1} D_i = 0$. Then $\mu_2(\overline{A}) \cong$

$\mu_2(\overline{K})^{2g+1}$, and we have a map $w : J(\overline{K})[2] \to \mu_2(\overline{A})$ defined by

$$D \mapsto (e_2(D, D_1), \ldots, e_2(D, D_{2g+1})),$$

where e_2 is the Weil pairing. This map also induces a map $w^* : H^1(G_K, \mu_2(\overline{A})) \to H^1(G_K, \mu_2(\overline{K}))$. Denote by k the isomorphism $H^1(G_K, \mu_2(A)) \to A^*/A^{*2}$ from Kummer theory. We then have

Proposition 2.3.1. *The composition $k \circ w^*$ induces an isomorphism*

$$H^1(G_K, J(\overline{K})[2]) \xrightarrow{\sim} \ker(A^*/A^{*2} \to K^*/K^{*2}),$$

and in terms of this isomorphism, our embedding $J(K)/2J(K) \to H^1(G_K, J(\overline{K})[2])$ takes the form

$$D = \sum_P n_P[P] \mapsto \prod_P (x(P) - x)^{n_P} \in A^*/A^{*2} \tag{2.10}$$

whenever D is a K-rational degree 0 divisor without Weierstrass points in its support, where $x(P)$ denotes the x-coordinate of P.

Proof. This is theorem 1.1 and 1.2 from [12]. □

We remark that $x(P) - x \in \overline{A}^*$ for P in the support of D in (2.10), but the product over such P is G_K-invariant, so that $\prod_P (x(P) - x)^{n_P} \in A^*$, which we can then take modulo squares.

Proposition 2.3.2. *Suppose that $D \in J(K)$ is represented by $[P_1 + \cdots + P_d - d\infty]$. Then the map* (2.10) *sends*

$$D \mapsto \begin{cases} \prod_{i=1}^d (x(P_i) - x) & \text{if } P \text{ is not a Weierstrass point} \\ \prod_{i=1}^d (\alpha_i - x) + \prod_{i=d+1}^{2g+1} (\alpha_i - x) & \text{if } P_1 = (\alpha_1, 0) \end{cases}$$

Proof. This is lemma 2.2 of [12]. □

The morale of proposition 2.3.2 is that for P not Weierstrass the image of D can still be deduced from (2.10) by just 'ignoring' the $d\infty$ part. If $P = (\alpha_1, 0)$, then to determine the image of D in $A^*/A^{*2} = \prod_{i=1}^r A_i^*/A_i^{*2}$ as r-tuple, note that $\prod_{i=1}^d (\alpha_i - x)$ in A_1, while $\prod_{i=d+1}^{2g+1} (\alpha_i - x) = 0$ in A_i for $i > 1$. We see the image of D in A_i^*/A_i^{*2} for $i > 1$ is again simply obtained by omitting the $d\infty$ part and then applying (2.10). Only for A_1 we have a special case. Considering the roots of a different g_i we have exactly the same: the images at A_j for $j \neq i$ are 'as usual', but at A_i we have a special case.

Now suppose that f splits completely over k so that $g_i = x - \alpha_i$ for $1 \leq i \leq r = 2g + 1$. Then we obtain

$$A^*/A^* \cong \prod_{i=1}^r A_i^*/A_i^{*2} \cong \prod_{i=1}^{2g+1} K^*/K^{*2}, \tag{2.11}$$

and under this isomorphism, the norm maps $N_i : A_i^* \to K^*$ become trivial, so that we obtain an embedding

$$J(K)/2J(K) \hookrightarrow \ker\left(\prod_{i=1}^{2g+1} K^*/K^{*2} \to K^*/K^{*2}\right) \tag{2.12}$$

with the kernel just being the 'hyperplane' consisting of those $(2g+1)$-tuples for which the product of all coordinates are trivial. Tracing the isomorphisms from (2.11) we see that for $D = \sum_P n_P[P]$ having no Weierstrass points in its support, that the embedding (2.12) sends

$$D \mapsto \left(\prod_P (x(P) - \alpha_1)^{n_P}, \ldots, \prod_P (x(P) - \alpha_{2g+1})^{n_P}\right)$$

In this case the image of the divisor $D_1 = [(\alpha_1, 0) - \infty]$ is especially simple: recall from the discussion about the morale of proposition 2.3.2 that in any case we have

$$D_1 \mapsto (?, \alpha_1 - \alpha_2, \ldots, \alpha_1 - \alpha_{2g+1}).$$

But the first coordinate of this image is determined[1] by the rest as the product is trivial in K^*/K^{*2}. For D_i a similar argument holds.

We can repeat this section replacing K with a completion $K_\mathfrak{p}$, which results in

$$J(K_\mathfrak{p})/2J(K_\mathfrak{p}) \hookrightarrow H^1(G_K, J(\overline{K_\mathfrak{p}})[2]) \xrightarrow{\sim} \ker\left(A_\mathfrak{p}^*/A_\mathfrak{p}^{*2} \to K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}\right)$$

where $A_\mathfrak{p} = A \otimes_K K_\mathfrak{p} = K_\mathfrak{p}[x]/(f)$. We then have a commutative diagram

$$\begin{array}{ccc} J(K)/2J(K) & \xrightarrow{\delta} & \ker\left(A^*/A^{*2} \to K^*/K^{*2}\right) \\ \downarrow & & \downarrow \\ J(K_\mathfrak{p})/2J(K_\mathfrak{p}) & \xrightarrow{\delta_\mathfrak{p}} & \ker\left(A_\mathfrak{p}^*/A_\mathfrak{p}^{*2} \to K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}\right), \end{array}$$

with the right vertical map induced from the canonical map $K \to K_\mathfrak{p}$. From now on we will view the 2-Selmer group $S^2(J/K)$ as a subgroup of A^*/A^{*2}. In many cases we will write the above diagram with just A^*/A^{*2} and $A_\mathfrak{p}^*/A_\mathfrak{p}^{*2}$, remembering that the images actually land inside the kernel of the relevant norm maps.

2.4 Finiteness of the 2-Selmer group

We specialise further by assuming $f \in \mathcal{O}_K[x]$, and that f splits completely over K, i.e.

$$f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i),$$

[1] Note that in the general case, only the norm of a coordinate is determined by the other coordinates. If the algebra corresponding to the coordinate is non-trivial we need proposition 2.3.2 for the value itself.

for $\alpha_i \in K$. As f is monic the α_i are integral over $\mathcal{O}_K$, hence $\alpha_i \in \mathcal{O}_K$.
Thus we now have $S^2(J/K) \subset \bigoplus_{i=1}^{2g+1} K^*/K^{*2}$.

Let S be the set of all real primes of K and the finite primes of K that lie over 2 or divide $\Delta(f)$.

Lemma 2.4.1. *Let $\mathfrak{p}$ be a finite prime of K not in S, and let $F = K_{\mathfrak{p}}^{\mathrm{unr}}$ be the maximal unramified extension of the completion $K_{\mathfrak{p}}$. Then $J(F)/2J(F) = 0$.*

Proof. We sketch the idea: the fact that $\mathfrak{p} \notin S$ guarantees that J has good reduction at $\mathfrak{p}$, which gives us an exact sequence

$$0 \to H \to J(F) \to \widetilde{J}(\overline{\mathbb{F}}_p) \to 0,$$

where p is the rational prime lying under $\mathfrak{p}$. One then argues that multiplication by 2 is surjective on $\widetilde{J}(\overline{\mathbb{F}}_p)$ because $\overline{\mathbb{F}}_p$ is algebraically closed, and also on H because of a formal group argument. Applying the snake lemma on the diagram obtained by applying multiplication by 2 on the above exact sequence, we see that this implies $J(F)/2J(F) = 0$.
For a formal proof one uses corollary and lemma 2.1 of Manin's Appendix in [9]. □

Proposition 2.4.2. *Let $\mathfrak{p}$ be a finite prime of K not in S. Then $(x_1, \ldots, x_{2g+1}) \in \ker\left(\bigoplus_{i=1}^{2g+1} K^*/K^{*2} \to K^*/K^{*2}\right)$ maps into $\mathrm{im}(\delta_{\mathfrak{p}})$ if and only if $\mathrm{ord}_{\mathfrak{p}}(x_i) \equiv 0 \bmod 2$ for all i.*

Proof. Let $F = K_{\mathfrak{p}}^{\mathrm{unr}}$ be the maximal unramified extension of $K_{\mathfrak{p}}$. Then we have a commutative diagram

$$\begin{array}{ccc}
J(K)/2J(K) & \xrightarrow{\delta} & \bigoplus_{i=1}^{2g+1} K^*/K^{*2} \\
\downarrow & & \downarrow \\
J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}}) & \xrightarrow{\delta_{\mathfrak{p}}} & \bigoplus_{i=1}^{2g+1} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2} \\
\downarrow & & \downarrow \\
J(F)/2J(F) & \hookrightarrow & \bigoplus_{i=1}^{2g+1} F^*/F^{*2}.
\end{array}$$

We have $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2} = \langle \pi, r \rangle$, where π is uniformizer and $r \in \mathcal{O}_{K_{\mathfrak{p}}}^*$ is a non-square. As $J(F)/2J(F) = 0$ we see that

$$\mathrm{im}(\delta_{\mathfrak{p}}) \subset \ker\left(\bigoplus_{i=1}^{2g+1} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2} \to \bigoplus_{i=1}^{2g+1} F^*/F^{*2}\right)$$

But $F^*/F^{*2} = \langle \pi \rangle$, so this implies that $\mathrm{im}(\delta_{\mathfrak{p}}) \subset \ker\left(\bigoplus_{i=1}^{2g+1}\langle r\rangle \to \langle r\rangle\right)$. As $J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}})$ has dimension $2g$ by proposition 2.2.4, this inclusion in fact an equality, which implies the desired result. □

Combining this with the fact that the complex primes need not be considered by proposition 2.2.4 we obtain

Corollary 2.4.3. *If we define*

$$K(S) := \{x \in K^*/K^{*2} : \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \bmod 2 \text{ for all finite } \mathfrak{p} \notin S\},$$

then $S^2(J/K) \subset \bigoplus_{i=1}^{2g+1} K(S)$, *and*

$$S^2(J/K) = \left\{ x \in \bigoplus_{i=1}^{2g+1} K(S) : x \text{ maps into } \mathrm{im}(\delta_{\mathfrak{p}}) \text{ for all } \mathfrak{p} \in S \right\}.$$

The description of $K(S)$ depends on the ring R_S of S-integers, some basic properties of which are collected in Appendix section A.1. In the appendix the ring R_S is only considered for a finite set S of *finite* primes, but we have included the real primes as well, let us define $R_S := R_{S_0}$ where $S_0 = \{\mathfrak{p} \in S : \mathfrak{p} \text{ finite}\}$.

Proposition 2.4.4. *There is an exact sequence*

$$0 \longrightarrow R_S^*/R_S^{*2} \xrightarrow{\alpha} K(S) \xrightarrow{\beta} \mathrm{Cl}(R_S)[2] \longrightarrow 0,$$

where β *sends an* xK^{*2} *to the ideal class* $[IR_S]$, *where* $(x) = \mathfrak{a}I^2$ *for* $\mathfrak{a}$ *and* I *co-prime fractional* $\mathcal{O}_K$*-ideals such that* $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0$ *for all* $\mathfrak{p} \notin S$.

Proof. Exactness at R_S^*/R_S^{*2} holds as the natural map $R_S^* \to K(S)$ has kernel $\{y^2 \in R_S^* : y \in K^*\} = R_S^{*2}$.
For the rest, let us first see that the map β is well-defined. Consider the auxiliary set $K_S := \{x \in K^* : \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \bmod 2 \text{ for all } \mathfrak{p} \notin S\}$, so that $K(S) = K_S/K^{*2}$. If $x \in K_S$, then we can write uniquely $(x) = \mathfrak{a}I^2$ for $\mathfrak{a}$ and I co-prime fractional ideals and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all $\mathfrak{p} \notin S$. We have $\mathfrak{a}R_S = R_S$ as $\mathfrak{p}R_S = R_S$ for $\mathfrak{p} \in S$, hence the identity $(x) = \mathfrak{a}I^2$ gives $[IR_S] \in \mathrm{Cl}(R_S)[2]$. We thus have a well-defined map $K_S \to \mathrm{Cl}(R_S)[2]$, which is clearly a homomorphism. If $x \in K^*$ we can write $(x) = \mathfrak{b}I$ for $\mathfrak{b}$ and I co-prime fractional $\mathcal{O}_K$-ideals such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0$ for all $\mathfrak{p} \notin S$. From $(x^2) = \mathfrak{b}^2I^2$ we see that $x^2 \mapsto [IR_S]$, which is trivial as $(x) = \mathfrak{b}I$ and $\mathfrak{b}R_S = R_S$. It follows that K^{*2} is in the kernel of $K_S \to \mathrm{Cl}(R_S)[2]$, hence we have the desired induced map $\beta : K(S) \to \mathrm{Cl}(R_S)[2]$.

To prove exactness at $K(S)$, let $\overline{x} \in K(S)$ be represented by $x \in R_S^*$ and let $\mathfrak{a} = (x)$. Then $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all $\mathfrak{p} \in S$, so it is immediate that $\overline{x} \in \ker(\beta)$, i.e. $\mathrm{im}(\alpha) \subset \ker(\beta)$. Conversely, suppose that $\overline{x} \in \ker(\beta)$. Writing $(x) = \mathfrak{a}I^2$ as in the definition we see that IR_S is principal. As β factors via the isomorphism

$\mathrm{Cl}(\mathcal{O}_K)/\langle\overline{S}\rangle \xrightarrow{\sim} \mathrm{Cl}(R_S)$ from lemma A.1.3 and $\mathrm{Cl}(\mathcal{O}_K)/\langle\overline{S}\rangle \cong \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)\cdot\langle S\rangle$, this implies that $I = (y)\mathfrak{b}$ for certain $y \in K^*$ and $\mathfrak{b} \in \langle S\rangle$. Thus

$$(x) = \mathfrak{a}I^2 = (y^2)\mathfrak{a}\mathfrak{b}^2, \quad \Rightarrow \quad (xy^{-2}) = \mathfrak{a}\mathfrak{b}^2 \in \langle S\rangle.$$

This means that $xy^{-2} \in R_S^*$, so that $\overline{x} = \overline{xy^{-2}} = \alpha(xy^{-2})$ and $\ker(\beta) \subset \mathrm{im}(\alpha)$.

It remains to show surjecitivity of β. If $[J] \in \mathrm{Cl}(R_S)[2]$ then using lemma A.1.3 we see that J is the extension of some ideal I of $\mathcal{O}_K$, and as primes $\mathfrak{p} \in S$ extend trivially, we may asssume without loss of generality that I contains no primes of S in its factorisation. Using the isomorphism from lemma A.1.3 again, we see that triviality of $[I^2R_S]$ in $\mathrm{Cl}(R_S)$ implies that $I^2 = (x)\mathfrak{a}$ for certain $x \in K^*$ and $\mathfrak{a} \in \langle S\rangle$. From $(x) = \mathfrak{a}^{-1}I^2$ we see that $[J] = [IR_S] = \beta(x)$, i.e. β is surjective. □

Corollary 2.4.5. *The 2-Selmer group $S^2(J/K)$ is finite.*

Proof. As R_S^* is finitely generated and $\mathrm{Cl}(R_S)$ is finite, this proves the finiteness of $K(S)$ and hence also the finiteness of $S^2(J/K)$. □

Remark 2.4.6. If f does not split completely then $S^2(J/K)$ is still finite, as corollary 2.4.3 holds similarly, see [12, p. 226].

Actually, this is the way in which the weak Mordell-Weil theorem (finiteness of $J(K)/mJ(K)$ for some $m \geq 2$) is proven. To extract the full Mordell-Weil theorem from this one needs the theory of heights.

We will in fact only need to compute $K(S)$ when K has odd class number. In this case a basis for $K(S)$ can be found as follows.

Corollary 2.4.7. *If K has odd class number then the map $R_S^*/R_S^{*2} \to K(S)$ is an isomorphism. Moreover, if for each $\mathfrak{p} \in S_0$ we have $\mathfrak{p}^{k_\mathfrak{p}} = (x_\mathfrak{p})$ with $k_\mathfrak{p}$ the order of $\mathfrak{p}$ in Cl_K, then the $x_\mathfrak{p}$ together with an $\mathbb{F}_2$-basis for $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ form an $\mathbb{F}_2$-basis for $K(S)$.*

Proof. As $\mathrm{Cl}(\mathcal{O}_K)$ has odd order and surjects onto $\mathrm{Cl}(R_S)$, also $\mathrm{Cl}(R_S)$ has odd order, hence $R_S^*/R_S^{*2} \xrightarrow{\sim} K(S)$.
For each $\mathfrak{p} \in S_0$ we have $\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}) \equiv 1 \bmod 2$, while $\mathrm{ord}_\mathfrak{q}(x_\mathfrak{p}) = 0$ for all finite primes $\mathfrak{q} \neq \mathfrak{p}$. As units of $\mathcal{O}_K$ have trivial valuations, we see that the $x_\mathfrak{p}$ together with a basis for $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ yield linear independent elements. From corollary A.1.4 we see that $\dim_{\mathbb{F}_2} K(S) = \dim_{\mathbb{F}_2}(\mathcal{O}_K^*/\mathcal{O}_K^{*2}) + |S_0|$, hence these elements form a basis. □

2.5 An algorithm

Let us recall the result so far. Let K be a number field and C the hyperelliptic curve defined by $y^2 = f(x)$, for $f \in K[x]$ square-free and of odd degree $2g+1$. Furthermore assume $f \in \mathcal{O}_K[x]$, monic and completely split over K, i.e. $f =$

$\prod_{i=1}^{2g+1}(x-\alpha_i)$.
Let S consist of the real primes of K, together with the finite primes dividing $2\Delta(f)$. Then $K(S) = \{x \in K^*/K^{*2} : \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \bmod 2 \text{ for all finite } \mathfrak{p} \notin S\}$ fits in the exact sequence

$$0 \to R_S^*/R_S^{*2} \to K(S) \to \mathrm{Cl}(R_S)[2] \to 0, \tag{2.13}$$

and we have

$$S^2(J/K) \subset \ker\left(\bigoplus_{i=1}^{2g+1} K(S) \to K(S)\right), \tag{2.14}$$

where $S^2(J/K)$ consists of those elements in the kernel of (2.14) that map into $\mathrm{im}(\delta_{\mathfrak{p}})$ for each $\mathfrak{p} \in S$ in the following diagram.

$$\begin{array}{ccc} J(K)/2J(K) & \xrightarrow{\delta} & \bigoplus_{i=1}^{2g+1} K^*/K^{*2} \\ \downarrow & & \downarrow \\ J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}}) & \xrightarrow{\delta_{\mathfrak{p}}} & \bigoplus_{i=1}^{2g+1} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2} \end{array}$$

To compute $S^2(J/K)$ we need to do the following.

(a) Compute for each $\mathfrak{p} \in S$ the local image $\mathrm{im}(\delta_{\mathfrak{p}})$.
This is done as follows: with either Hensel's lemma or the intermediate value theorem, we can search for points in $C(F)$ for F a suitable finite extension of $K_{\mathfrak{p}}$, yielding points in $J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}})$ according to Prop. 1.2.5. One can check for linear independence using the embedding $\delta_{\mathfrak{p}}$. As one knows beforehand the $\mathbb{F}_2$-dimension of $J(K_{\mathfrak{p}})/2J(K_{\mathfrak{p}})$ from proposition 2.2.4, this allows for a computation of $\mathrm{im}(\delta_{\mathfrak{p}})$.

(b) Compute generators for $K(S)$ using the exact sequence (2.13).

(c) For each generator for $K(S)$, compute its image under the maps $K^*/K^{*2} \to K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}$ for $\mathfrak{p} \in S$.

With this information the computation is 'just linear algebra': $S^2(J/K)$ is the intersection of the inverse images of $\mathrm{im}(\delta_{\mathfrak{p}})$ under the right vertical map of the above diagram for $\mathfrak{p} \in S$.

Chapter 3

A family of examples

We consider for a prime $p \neq 2, 3$ the hyperelliptic curve C_p defined over $\mathbb{Q}$ by the equation

$$y^2 = f(x) = x(x^2 - p^2)(x^2 - 4p^2).$$

Let J_p denote its Jacobian. Our goal in this chapter is to find as much information as possible about the rank of $J_p/\mathbb{Q}$ and the group $Ш(J_p/\mathbb{Q})[2]$.

3.1 A basic 2-descent

We follow the algorithm from section 2.5: one computes $\Delta(f) = 2^{10} \cdot 3^4 \cdot p^{20}$, hence we take $S = \{2, 3, p, \infty\}$, where $\infty : \mathbb{Q} \to \mathbb{R}$ is the real embedding. As $\mathbb{Q}$ has class number one, either by the exact sequence (2.13) or directly from unique factorisation, we see that $K(S) = \langle -1, 2, 3, p \rangle$.

Let $\alpha_1 = -2p$, $\alpha_2 = -p, \ldots, \alpha_5 = 2p$ be the roots of f, so that the embedding

$$J(\mathbb{Q})/2J(\mathbb{Q}) \to \bigoplus_{i=1}^{5} \mathbb{Q}^*/\mathbb{Q}^{*2}$$

of (2.12) takes the form

$$D = \prod_P n_P[P] \mapsto \left(\prod_P (x(P) + 2p)^{n_P}, \ldots, \prod_P (x(P) - 2p)^{n_P} \right)$$

for D with no Weierstrass points in its support.

The local images $J_p(\mathbb{Q}_q)/2J_p(\mathbb{Q}_q)$ depends on p mod 8 for $q = 2$, on p mod 3 for $q = 3$, and on p mod 24 for $q = p$. For $q = \infty$ the image is independent of p. These images for the various cases of p mod 24 can be found in [5, Ch. 4.1].

The last ingredient is the images of the generators of $K(S)$ in $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$ for $q \in \{2, 3, p, \infty\}$. If $r \in \mathbb{Z}$ is a non-square mod$p$, we have

$$\begin{aligned}\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} &= \langle 2, -1, 3\rangle,\\ \mathbb{Q}_3^*/\mathbb{Q}_3^{*2} &= \langle 3, -1\rangle,\\ \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} &= \langle p, r\rangle,\\ \mathbb{R}^*/\mathbb{R}^{*2} &= \langle -1\rangle.\end{aligned}$$

And we want to fill in the following table

	2	3	p	∞
-1	-1	-1		-1
2	2	-1		1
3	3	3		1
p			p	1

where the entries consist of the images of the various generator of $K(S)$ in $\mathbb{Q}_q^{*2}/\mathbb{Q}_q^{*2}$ for $q \in \{2, 3, p, \infty\}$. We note that the image of p at 2 and 3 depend on $p \bmod 8$ and $p \bmod 3$, and thanks to quadratic reciprocity, the images of $-1, 2$ and 3 at p depend on $p \bmod 4$, $p \bmod 8$ and $p \bmod 12$ respectively. We see that the relevant ingredients for the calculation all depend on $p \bmod 24$. The remaining linear algebra is where van der Heiden in [5] makes mistakes, a correction can be found in Appendix section B. The results are then as follows:

Proposition 3.1.1. *From $J_p(\mathbb{Q})[2]$ we obtain the linearly independent elements $(2, -6p, -p, 2, 6)$, $(3, -3p, -1, 3p, 3)$, $(p, -6, -p, -2p, -3p)$ and $(1, -2p, -2, -2, -2p)$. The 2-Selmer group $S^2(J_p/\mathbb{Q})$ depends on $p \bmod 24$ as follows.*

$p \bmod 24$	$\dim S^2(J_p/\mathbb{Q})$	*other generators*
1	8	$(1,1,1,p,p), (1,p,p,1,1), (1,p,1,p,1), (1,-6,-1,-2,-3)$
5	5	$(1, 6p, 2p, 2p, 6p)$
7	4	*none*
11	5	$(1, 3p, 1, 1, 3p)$
13	5	$(1, p, 1, p, 1)$
17	6	$(1, p, 1, 1, p), (1, -6, -p, -2, -3p)$
19	5	$(1, 2p, p, -2p, -p)$
23	6	$(1, -p, -p, 1, 1),), (1, 1, 1, -p, -p)$

From proposition 2.1.2 and equation (2.9) we obtain

$$\operatorname{rank}(J_p/\mathbb{Q}) + \dim_{\mathbb{F}_2}(Ш(J_p/\mathbb{Q})[2]) = \dim_{\mathbb{F}_2}(S^2(J_p/\mathbb{Q})) - 4, \qquad (3.1)$$

hence in any case we have that $\dim_{\mathbb{F}_2}(S^2(J_p/\mathbb{Q})) - 4$ is an upper bound for the rank. In particular, we see that $\operatorname{rank}(J_p/\mathbb{Q}) = 0$ whenever $p \equiv 7 \bmod 24$.

Assuming that $Ш(J_p/\mathbb{Q})$ is finite implies that $\operatorname{rank}(J_p/\mathbb{Q})$ and $\dim S^2(J_p/\mathbb{Q})$ have the same parity (see proposition 2.2.3), so we have the following conjectural

result about the ranks.

$p \bmod 24$	$\dim S^2(J_p/\mathbb{Q})$	$\operatorname{rank}(J_p/\mathbb{Q})$
1	8	0, 2 or 4
5	5	1
7	4	0
11	5	1
13	5	1
17	6	0 or 2
19	5	1
23	6	0 or 2

Note that the primes p with $\dim S^2(J/\mathbb{Q}) = 5$ are the primes $p \equiv 3, 5 \bmod 8$, which are the primes that are inert in $\mathbb{Q}(\sqrt{2})$.

3.2 The group $\mathrm{Aut}(C)$

We will compute the geometric automorphism group $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ of $C = C_p$, and then see what the minimal field is over which all automorphisms are defined, i.e. the field K for which the natural map $\mathrm{Aut}(C_K) \to \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ is an isomorphism.

Proposition 3.2.1. *All automorphisms of $C = C_p$ are defined over $\mathbb{Q}(\zeta_8)$, with $\mathrm{Aut}(C_{\mathbb{Q}(\zeta_8)}) \cong D_4$ generated by ρ and σ of order 4 and 2 respectively, given on the function field by*

$$\rho(x, y) = (-x, \zeta_4 y)$$
$$\sigma(x, y) = \left(\frac{2p^2}{x}, \frac{2\sqrt{2}p^3 y}{x^3}\right)$$

Proof. It is straightforward to check that ρ and σ are indeed automorphisms of order 4 and 2 respectively, and they satisfy the relation $\rho\sigma = \sigma\rho^{-1}$. It remains to see why there are no more automorphisms, which is more delicate.
Setting

$$y^2 = x(x^2 - p^2)(x^2 - 4p^2).$$

Setting $\eta = x/p$ and $\xi = y/p^3$ we obtain $p\xi^2 = \eta(\eta^2 - 1)(\eta^2 - 4)$, so over $\overline{\mathbb{Q}}$ the curve is simply isomorphic to

$$\tilde{\xi}^2 = \eta(\eta^2 - 1)(\eta^2 - 4).$$

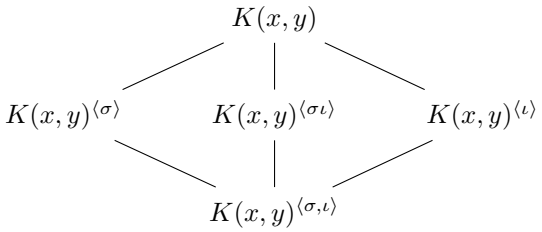
Now setting $x' = \frac{\eta+1}{\eta-1}$ and $y' = \frac{4\tilde{\xi}}{\sqrt{-3}(\eta-1)^3}$, we obtain

$$(y')^2 = x'(x' - 1)(x' + 1)(x' - 3)(x' - 1/3). \tag{3.2}$$

According to [6, p. 644] this implies that $\mathrm{Aut}_{\overline{\mathbb{Q}}}(C_{\overline{\mathbb{Q}}})/\langle\iota\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where ι is the hyperelliptic involution defined by $(x, y) \mapsto (x, -y)$. It follows that $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ has order 8.

□

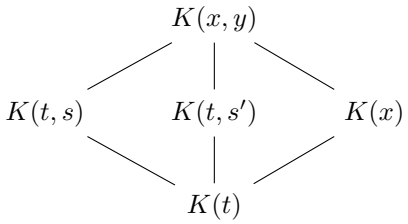
We will work with the automorphism σ, which is defined over $K = \mathbb{Q}(\sqrt{2})$. Consider the function field $K(x, y)$ of C_K. Then $\langle \sigma, \iota \rangle$ is a non-cyclic subgroup of $\mathrm{Aut}_K(K(x, y))$ of order 4, so that from Galois theory we have that $K(x, y)/K(x, y)^{\langle \sigma, \iota \rangle}$ is a Galois extension with group $(\mathbb{Z}/2\mathbb{Z})^2$, with the following subfields



To compute these invariant fields, first observe that clearly $K(x, y)^{\langle \iota \rangle} = K(x)$. For the rest, consider $t = x + \frac{2p^2}{x}$. Then $t \in K(x, y)^{\langle \sigma, \iota \rangle}$, which gives

$$K(t) \subset K(x, y)^{\langle \sigma, \iota \rangle} \subset K(x).$$

As the degree of the latter extension is 2, and we have $x^2 - tx + 2p^2 = 0$, we see that $K(t) = K(x, y)^{\langle \sigma, \iota \rangle}$.
With a similar argument it follows that $K(x, y)^{\langle \sigma \rangle} = K(t, s)$ where $s = y + \frac{2\sqrt{2}p^3 y}{x^3}$, and $K(x, y)^{\langle \sigma\iota \rangle} = K(t, s')$ for $s' = y - \frac{2\sqrt{2}p^3 y}{x^3}$. We now have



We can consider $K(t)$ as the function field of a $\mathbb{P}^1_K$, so that $K(t, s)$ and $K(t, s')$ correspond with hyperelliptic curves (note that K perfect yields that the curves associated to the function fields are in fact smooth). With Riemann-Hurwitz one can calculate that the curves have genus 1, but one can also just direct produce a Weierstrass equation as follows.
Note that $s^2 \in K(t)$ as s^2 is invariant under ι, so we already know beforehand that s^2 is a rational function in t. We compute:

$$s^2 = y^2 \left(1 + \frac{2\sqrt{2}p^3}{x^3}\right)^2 = x(x^2 - p^2)(x^2 - 4p^2)\left(1 + \frac{4\sqrt{2}p^3}{x^3} + \frac{8p^6}{x^6}\right)$$

We see that the expression expands into a sum of terms containing x^i for $|i| \leq 5$. Note that the coefficient of x^5 is 1 and that of x^{-5} is $32p^{10}$. Note that t^5 has

the same coefficients for x^5 and x^{-5} respectively, so $s^2 - t^5$ is a sum of terms containing x^i for $|i| \leq 4$. Continuing in this way we obtain the relation

$$\begin{aligned} s^2 &= t^5 - 15p^2t^3 + 4\sqrt{2}p^3t^2 + 54p^4t - 36\sqrt{2}p^5 \\ &= (t-3p)(t+3p)(t+2\sqrt{2}p)(t-\sqrt{2}p)^2 \end{aligned}$$

Letting $\mathrm{Gal}(K/\mathbb{Q})$ act on $K(x,y)$ by the natural action on K and fixing x and y, we note that s' is the conjugate of s, and that t is invariant under this action. This implies

$$\begin{aligned} (s')^2 &= t^5 - 15p^2t^3 - 4\sqrt{2}p^3t^2 + 54p^4t + 36\sqrt{2}p^5 \\ &= (t-3p)(t+3p)(t-2\sqrt{2}p)(t+\sqrt{2}p)^2 \end{aligned}$$

This yields two elliptic curves E and $\overline{E}$ defined by

$$\begin{aligned} E: &\quad y^2 = (x^2 - 9p^2)(x + 2\sqrt{2}p) \\ \overline{E}: &\quad y^2 = (x^2 - 9p^2)(x - 2\sqrt{2}p) \end{aligned}$$

together with maps $C_K \to E$ and $C_K \to \overline{E}$.

Proposition 3.2.2. *We have an isogeny $J_K \to E \times_K \overline{E}$.*

Proof. This is a generality because E and $\overline{E}$ have as function fields the invariant of the function field of C_K under $\langle\sigma\rangle$ and $\langle\sigma\iota\rangle$, see [6, p. 644]. □

Proposition 3.2.3. *We have* $\mathrm{rank}(J/\mathbb{Q}) = \mathrm{rank}(E/K)$.

Proof. Suppose that $\overline{\mathbb{Q}}/L/K$ is an intermediate field. Then from 3.2.2 (and the fact that $J(L) = J_K(L)$ canonically) we have a commutative diagram

$$\begin{array}{ccc} C(L) & \xrightarrow{\quad\pi\times\overline{\pi}\quad} & E(L)\times\overline{E}(L) \\ & \searrow \quad \nearrow & \\ & J(L) & \end{array} \tag{3.3}$$

with $J(L) \to E(L) \times \overline{E}(L)$ a group homomorphism with finite kernel.
Setting $K = L$ and precomposing $J(\mathbb{Q}) \to J(K)$, we obtain a group homomorphism $\phi : J(\mathbb{Q}) \to E(K) \times \overline{E}(K)$.
I claim that

$$\mathrm{im}(\phi) \subset \{(P,Q) \in E(K) \times \overline{E}(K) : \overline{P} = Q\}.$$

To see this note that if $P \in C(K)$ then from (3.3) with $L = K$ then we see immediately that $[P - \infty] \in J(K)$ maps to a pair of conjugate points. This that $\phi(D) \subset \{(P,Q) \in E(K) \times \overline{E}(K) : \overline{P} = Q\}$ whenever $D \in J(\mathbb{Q})$ is the sum of at most two distinct divisors class of the form $[P - \infty]$ for $P \in C(\mathbb{Q})$, or when $D = [P + Q - 2\infty]$ for $P, Q \in C(K)$ conjugate.
It remains to consider the case where $D = [P + Q - 2\infty]$ for $P \neq Q$ in $C(L)$

conjugate for $L/\mathbb{Q}$ quadratic and $L \neq K$. Consider $\sigma \in \mathrm{Gal}(LK/\mathbb{Q})$ with $\sigma|_K \neq \mathrm{id}_K$ and $\sigma|_L \neq \mathrm{id}_L$, so that $\overline{x} = \sigma(x)$ for $x \in K$, but also $\sigma(P) = Q$. Using (3.3) for this L we see that

$$D \mapsto (\pi(P) + \pi(Q), \overline{\pi}(P) + \overline{\pi}(Q)),$$

and

$$\overline{\pi(P) + \pi(Q)} = \sigma(\pi(P) + \pi(Q)) = \overline{\pi}(\sigma(P)) + \overline{\pi}(\sigma(Q)) = \overline{\pi}(P) + \overline{\pi}(Q),$$

which proves the claim.

Thus we in fact have a map $J(\mathbb{Q}) \to E(K)$ which has finite kernel, which implies $\mathrm{rank}(J/\mathbb{Q}) \leq \mathrm{rank}(E/K)$. To prove the reverse inequality, let us consider $r = \mathrm{rank}(E/K)$ independent points $P_1, \ldots, P_r \in E(K)$ of infinite order. Then over at most a quadratic extension L of K, we can find points $Q_i \in C(L)$ that map to P_i.
Letting $\mathrm{Gal}(L/K)$ be generated by σ of order at most 2, we see that $[Q_i + \sigma(Q_i) - 2\infty] \in J(K)$ maps to $2P_i$. Again we can take the sum of the $\mathrm{Gal}(K/\mathbb{Q})$-orbit of these points to obtain points $D_i \in J(\mathbb{Q})$ that map to $4P_i \in E(K)$.
But as $4P_1, \ldots, 4P_r$ are r independent points of infinite order, we see that also $D_1, \ldots, D_r \in J(\mathbb{Q})$ are r independent points of infinite order, which proves $\mathrm{rank}(J/\mathbb{Q}) = \mathrm{rank}(E/K)$. □

Remark 3.2.4. The way we obtained a map $J(\mathbb{Q}) \to E(K)$ in the proof of proposition 3.2.3 may seem rather ad hoc. What is going on 'under the hood' is Weil restriction. Specifically, we have a functor from the category of K-schemes to the category of $\mathbb{Q}$-schemes, denoted on objects by $\mathrm{Res}^K_{\mathbb{Q}}(T)$ for a K-scheme T, which is adjoint to the base extensions functor that sends a $\mathbb{Q}$-scheme T to $T \times_K \mathrm{Spec}(K)$. In our case this means that we have

$$\mathrm{Mor}_{K\text{-Sch}}(J_K, E) \leftrightarrow \mathrm{Mor}_{\mathbb{Q}\text{-Sch}}(J, \mathrm{Res}^K_{\mathbb{Q}}),$$

Our map $J_K \to E$ thus yields a map $J \to \mathrm{Res}^K_{\mathbb{Q}}(E)$ that is a morphisms of schemes over $\mathbb{Q}$. Now an explicit construction of $\mathrm{Res}^K_{\mathbb{Q}}(E)$ is to take the product of E with its conjugate, and then quotient out by the action of $\mathrm{Gal}(K/\mathbb{Q})$ that interchanges the factors, see [3, § 1.2]. The $\mathbb{Q}$-valued points $\mathrm{Res}^K_{\mathbb{Q}}(E)$ are then precisely

$$\{(P, Q) \in E(K) \times \overline{E}(K) : \overline{P} = Q\},$$

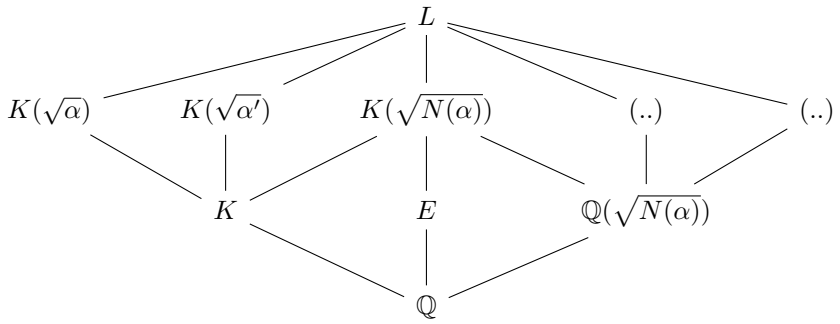
and the induced map on $J(\mathbb{Q})$ to the above coincides with the map which we considered in the proof of proposition 3.2.3.

Now that we know that $\mathrm{rank}(J/\mathbb{Q}) = \mathrm{rank}(E/K)$, we can also perform a 2-descent on E/K and achieve rank bounds for $J(\mathbb{Q})$ with (2.9). If the rank bound is smaller than the one obtained by a compution of $S^2(J/\mathbb{Q})$, then this forces a non-trivial $Ш(J/\mathbb{Q})[2]$.

3.3 2-descent on $E/\mathbb{Q}(\sqrt{2})$

First a lemmas to smooth calculations later on.

Lemma 3.3.1. *Let $K/\mathbb{Q}$ be a quadratic, and let $\alpha \in K$ a non-square. Then the Galois closure L of $K(\sqrt{\alpha})/\mathbb{Q}$ is $K(\sqrt{\alpha}, \sqrt{N(\alpha)})$, which is a D_4 extension provided that $N(\alpha) = \alpha\alpha'$ is not a square in K. The subfield lattice takes the following form*



Moreover, suppose that a rational prime p is unramified in L, and that p is not completely split in $K(\sqrt{N(\alpha)})$. Then the inertia degree f_p depends on the splitting behaviour of p in E as follows:

i) If p splits in E then $f_p = 4$.

ii) If p is inert in E then $f_p = 2$.

Proof. The first part is basic Galois theory, where one observes that $L/\mathbb{Q}(\sqrt{N(\alpha)})$ is not cyclic by checking that no automorphism of $\mathrm{Gal}(L/\mathbb{Q})$ of order 4 fixes $\sqrt{N(\alpha)}$.

As $L/\mathbb{Q}$ is not cyclic we cannot have $f_p = 8$, so $f_p \in \{2, 4\}$, hence it suffices to prove that p splits in E if and only if $f_p = 4$.
If p splits in E then since p is not completely split in $K(\sqrt{N(\alpha)})$, this forces E to be the decomposition field $Z_{\mathfrak{p}/p}$ of a prime $\mathfrak{p}$ over p, whence $f_p = [L : Z_{\mathfrak{p}/p}] = 4$. Conversely, if $f_p = 4$ then the decomposition group $D_{\mathfrak{p}/p}$ is cyclic of order 4, so its invariant field must be E, hence p splits in E. □

We now continue with the descent. To repeat: let $p \neq 2, 3$ be a prime and consider the elliptic curve E defined over $K = \mathbb{Q}(\sqrt{2})$ defined by the Weierstrass equation

$$y^2 = f(x) = (x^2 - 9p^2)(x + 2\sqrt{2}p)$$

One computes that $\Delta(f) = 2^2 \cdot 3^2 \cdot p^6$, hence the set S we need to consider consists of the infinite primes, together with the primes lying over $2, 3$ and p.

We may identify E with its Jacobian according to proposition 1.2.5. With this identification, and using $(\alpha_1, \alpha_2, \alpha_3) = (-3p, 3p, -2\sqrt{2}p)$ for the roots of f, the embedding of (2.12) becomes

$$\begin{aligned} E(K)/2E(K) &\to K^*/K^* \times K^*/K^* \times K^*/K^* \\ P &\mapsto \left(x(P) + 3p, x(P) - 3p, x(P) + 2\sqrt{2}p\right), \end{aligned}$$

for $P \in E(K)$ with $2P \neq 0$, and

$$\begin{aligned} (-3p, 0) &\mapsto (3, -3p, -p) \\ (3p, 0) &\mapsto (3p, 3, p) \\ (-2\sqrt{2}p, 0) &\mapsto (p, -p, -1) \end{aligned}$$

note that we have used that 2 and $3 \pm 2\sqrt{2}$ are squares in K. Our first step in the computation is the determination of the local images.

3.3.1 Local images

We need the local images of the map

$$E_p(F)/2E_p(F) \hookrightarrow F^*/F^* \times F^*/F^* \times F^*/F^*$$

for the completions F of K at the infinite primes and the finite primes lying over $2, 3$ and p. These are $\mathbb{R}$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_3(i)$, and either $\mathbb{Q}_p$ when p is split in K or $\mathbb{Q}_p(\sqrt{2})$ for p inert in K. As $\dim_{\mathbb{F}_2}(E(F)[2]) = 2$ for all these F, we obtain from proposition 2.2.4 that $\dim_{\mathbb{F}_2}(E(F)/2E(F))$ equals 4 when $F = \mathbb{Q}_2(\sqrt{2})$, 1 for $F = \mathbb{R}$ and 2 otherwise.

We first consider $F = \mathbb{Q}_2(\alpha)$ for $\alpha = \sqrt{2}$, which is a wildly ramified quadratic extension of $\mathbb{Q}_2$. Also write $\mathcal{O} = \mathcal{O}_F = \mathbb{Z}_2[\alpha]$ for the ring of integers for F. Then a basic application of a general version of Hensel's lemma (see [14, Ex. 2.9]) implies that

Lemma 3.3.2. *Let $x \in \mathcal{O}^*$. Then x is a square in $\mathcal{O}$ if and only if $\overline{x} \in (\mathcal{O}/\alpha^5\mathcal{O})^*$ is a square.*

Also, a basic calculation shows that elements of $(\mathcal{O}/\alpha^5\mathcal{O})^*$ can be written uniquely as $a + b\alpha \bmod \alpha^5$ for $a \in \{1, 3, 5, 7\}$ and $b \in \{0, 1, 2, 3\}$. Moreover, we have $(\mathcal{O}/\alpha^5\mathcal{O})^* \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with generators $1 + \alpha, 3 + \alpha, 5$ of order $4, 2, 2$ respectively. Consequently, the squares in $(\mathcal{O}/\alpha^5\mathcal{O})^*$ are 1 and $(1 + \alpha)^2 = 3 + 2\alpha$, and one can check that any coset in $(\mathcal{O}/\alpha^5\mathcal{O})^*/\langle 3 + 2\alpha\rangle$ has a unique representative of the form $a + b\alpha \bmod \alpha^5$ for $a \in \{1, 3, 5, 7\}$ and $b \in \{0, 1\}$. Then

$$F^*/F^{*2} \cong \langle\alpha\rangle/\langle\alpha^2\rangle \times (\mathcal{O}/\alpha^5\mathcal{O})^*/\langle 3 + 2\alpha\rangle,$$

and we will write elements of F^*/F^{*2} uniquely in the form $\alpha^i(a + b\alpha)$ for $a \in \{-3, -1, 1, 3\}$ and $b, i \in \{0, 1\}$.

Note that the image of a $k \in \mathbb{Z}$ odd in F^*/F^{*2} depends on k mod 8 since $8 = \alpha^6$.

In any case, we see that from $E(F)[2]$ that $(3, -3p, -p)$ and $(3p, 3, p)$ are linearly independent elements in the image, no matter what p is. To search for more, note that working in F^*/F^{*2} we have

$$f(1/4) = f(1/\alpha^4) = \left(\frac{1 - 9\alpha^8 p^2}{\alpha^8}\right)\left(\frac{1 - \alpha^7 p}{\alpha^4}\right) = (1 - 9\alpha^8 p^2)(1 - \alpha^7 p) = 1,$$

hence $P = (1/4, \sqrt{f(1/4)}) \in E(F)$. Its image consists of

$$\begin{aligned}(1/4 + 3p, 1/4 - 3p, 1/4 + 2\alpha p) &= (1 + 12p, 1 - 12p, 1 + 8\alpha p) \\ &= (1 + 4p, 1 + 4p, 1) \\ &= (-3, -3, 1),\end{aligned}$$

Similarly we find the point $P = (20 + p^2/10, ?) \in E(F)$ which has image

$$(3(2p-1), -3(1+2p), -3) = \begin{cases}(3, -1, 3) & \text{if } p \equiv 1 \bmod 4 \\ (-1, 3, -3) & \text{if } p \equiv 3 \bmod 4\end{cases}$$

One checks that only when $p \equiv 1, 7 \bmod 8$, this element is not in the span of the previous three elements. Luckily, precisely when $p \equiv 3, 5 \bmod 8$ we have that $(3 + a, ?)$ gives a point of $E(F)$: for $x = 3 + \alpha$ in F^*/F^{*2} we have

$$(x^2 - 9p^2) = 9 + 6\alpha + 2 - 9p^2 = 1 + 3\alpha + 9 \cdot \frac{1 - p^2}{2} = 5 + 3\alpha,$$

in F^*/F^{*2}, where we have used that $p^2 \equiv 9 \bmod 16$, whence $\frac{1-p^2}{2} \equiv 4 \bmod 8$. One directly computes that $(5 + 3\alpha)(3 + \alpha + 2\alpha p) = 1$ in F^*/F^{*2}, so that we indeed obtain a point, which has image

$$(3 + 3p + \alpha, 3 - 3p - \alpha, 3 + (1 + 2p)\alpha) = \begin{cases}(4 + \alpha, 2 + \alpha, 3 - \alpha) & \text{if } p \equiv 3 \bmod 8 \\ (2 + \alpha, 4 + \alpha, 3 - \alpha) & \text{if } p \equiv 5 \bmod 8\end{cases}$$

In summary, the local images of $E_p(F)/2E_p(F)$ have the following generators, depending on p mod 8 as follows.

$p \equiv 1 \bmod 8$			$p \equiv 3 \bmod 8$			$p \equiv 5 \bmod 8$			$p \equiv 7 \bmod 8$		
3	-3	-1	3	-1	-3	3	1	3	3	3	1
3	3	1	1	3	3	-1	3	-3	-3	3	-1
-3	-3	1	-3	-3	1	-3	-3	1	-3	-3	1
3	-1	-3	$4 + \alpha$	$2 + \alpha$	$3 - \alpha$	$2 + \alpha$	$4 + \alpha$	$3 - \alpha$	-1	3	-3

For $F = \mathbb{Q}_3(i)$ we have $F^*/F^{*2} = \langle 3, r\rangle$ with $r = 1 + i$. The corresponding image is spanned by

$$\begin{matrix}3 & 3 & 1 \\ r & r & 1\end{matrix}$$

where $(3,3,1)$ comes from $E(F)[2]$, and $(r,r,1)$ comes from a point $(1+pr,?)$.

The local images for the primes of K over p all come from the 2-torsion. For $F=\mathbb{Q}_p$ the image is spanned by

$$\begin{matrix} 3 & -3p & -p \\ p & -p & -1 \end{matrix}$$

For $F=\mathbb{Q}_p(\sqrt{2})$ quadratic over $\mathbb{Q}_p$ we have $F^*/F^{*2}=\langle p,s\rangle$ for s a lift of a non-square of $\mathbb{F}_{p^2}$. The image in this case is spanned by

$$\begin{matrix} 1 & p & p \\ p & p & 1 \end{matrix}$$

And lastly, over the reals the image is spanned by $(1,-1,-1)$ which comes from for example $(-3p,0)$.

3.3.2 The calculations

Let $\varepsilon=1+\alpha$, which is a fundamental unit of K. Let $\mathfrak{p}_2=(\alpha)$, $\mathfrak{p}_3=(3)$ and let σ_1,σ_2 be the two real embeddings of K, chosen such that $\sigma_1(\sqrt{2})>0$.

Let us first consider the cases with $p\equiv 3,5 \bmod 8$. In that case p is inert in K, and we have $S=\{\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p},\sigma_1,\sigma_2\}$, where $\mathfrak{p}=(p)$, and

$$K(S)=\langle -1,\varepsilon,\alpha,3,p\rangle.$$

For the calculations we need the entries of the following table.

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	σ_1	σ_2
-1	-1	1	1	-1	-1
ε	$1+\alpha$			1	-1
α	α			1	-1
3	3	3	1	1	1
p		1	p	1	1

The entry of p at $\mathfrak{p}_2$ depends simply on $p \bmod 8$. The remaining four entries also depend on $p \bmod 8$ thanks to lemma 3.3.1: the image of ε at $\mathfrak{p}$ depends on the splitting behaviour of p in the (normal closure) of $K(\sqrt{\varepsilon})$. We see that $\mathrm{im}_{\mathfrak{p}}(\varepsilon)=1$ precisely when p is inert in $\mathbb{Q}(\sqrt{-2})$, i.e. when $p\equiv 5,7 \bmod 8$. Similarly $\mathrm{im}_{\mathfrak{p}}(\alpha)=1$ precisely when p is inert in $\mathbb{Q}(\zeta_4)$, i.e. for $p\equiv 3 \bmod 4$.

Consider

$$A=\{x\in S^2(E/K) : \mathrm{im}_{\mathfrak{p}}(x)=(1,1,1)\}.$$

As the 2-torsion of $E(K)$ yields a subspace of $S^2(E/K)$ that surjects onto the $\mathfrak{p}$-adic image, we have

$$S^2(E/K)=A\oplus \mathrm{im}(E(K)[2]).$$

(i) $p \equiv 3 \bmod 8$. In this case the table becomes

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	σ_1	σ_2
-1	-1	1	1	-1	-1
ε	$1+\alpha$	r	s	1	-1
α	α	1	1	1	-1
3	3	3	1	1	1
p	3	1	p	1	1

Let $x = (e_1, e_2, e_3) \in A$. As x has trivial $\mathfrak{p}$-adic image we obtain $e_i \in \langle -1, \alpha, 3\rangle$ for all i. As e_1 is totally positive we have $e_1 \in \langle 3\rangle$. Looking $\mathfrak{p}_2$-adically this forces $e_3 \in \langle -1, 3\rangle$, but as $\mathrm{im}_{\mathfrak{p}_3}(e_3)$ is trivial this then forces $e_3 \in \langle -1\rangle$, hence x maps $\mathfrak{p}_2$-adically in the span of $(3, -3, -1)$, hence $e_1 = 1$ if and only if $e_3 = 1$. It follows that only $x = (3, -3, -1)$ is a non-trivial option, and one checks that indeed $(3, -3, -1) \in A$. This proves that $S^2(E/K)$ is 3-dimensional.

(ii) $p \equiv 5 \bmod 8$. The table now becomes

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	σ_1	σ_2
-1	-1	1	1	-1	-1
ε	$1+\alpha$	r	1	1	-1
α	α	1	s	1	-1
3	3	3	1	1	1
p	-3	1	p	1	1

let $x = (e_1, e_2, e_3) \in A$. Then $e_i \in \langle -1, \varepsilon, 3\rangle$ for all i. Then again as e_1 is totally positive we have $e_1 \in \langle 3\rangle$. As e_3 has trivial $\mathfrak{p}_3$-adic image we have $e_3 \in \langle -1\rangle$, which forces the $\mathfrak{p}_2$-adic image of x to lie in the span of $(-3, 3, -1)$ and $(-3, -3, 1)$. This forces $e_1 = 1$, and $e_2 = e_3 \in \langle -1\rangle$. One checks that indeed $(1, -1, -1) \in A$, whence $\dim_{\mathbb{F}_2} S^2(E/K) = 3$ in this case as well.

Now let us consider the cases $p \equiv 1, 7 \bmod 8$, so that p splits in K. Say $\mathfrak{p}$ and $\mathfrak{q}$ are the primes over p. Suppose that $\mathfrak{p} = (\pi_1)$, and multiply π_1 with ε if necessary such that $N(\pi) > 0$, and multiply with -1 if necessary so that π becomes totally positive. Also write $\pi_1 = a + b\alpha$. Letting $\pi_2 = \overline{\pi_1}$ we have $\pi_2 = a - b\alpha$, $\mathfrak{q} = (\pi_2)$, $S = \{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}, \mathfrak{q}, \sigma_1, \sigma_2\}$ and $K(S) = \langle -1, \varepsilon, \alpha, 3, \pi_1, \pi_2\rangle$. We must now consider the following table

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	$\mathfrak{q}$	σ_1	σ_2
-1	-1	-1			-1	-1
ε	$1+\alpha$	r			1	-1
α	α	1			1	-1
3	3	3			1	1
π_1			π_1		1	1
π_2				π_2	1	1

(3.4)

Some remarks: the images of -1 and 3 under $\mathfrak{p}$ and $\mathfrak{q}$ depend with quadratic reciprocity on $p \bmod 4$ and $p \bmod 12$ respectively. The images of π_i under $\mathfrak{p}_3$

depend on $p \bmod 3$ by lemma 3.3.1: if $p \equiv 1 \bmod 3$ then p is inert in $\mathbb{Q}(\sqrt{2p})$, hence $\mathrm{im}_{\mathfrak{p}_3}(\pi_i) = 1$, while for $p \equiv 2 \bmod 3$ we get $\mathrm{im}_{\mathfrak{p}_3}(\pi_i) = -1$.

For the calculations, note that $S^2(E/K) = A \oplus \mathrm{im}(E(K)[2])$ with

$$A = \{x \in S^2(E/K) : \mathrm{im}_{\mathfrak{p}_3}(x) \subset \langle (r, r, 1) \rangle \text{ and } \mathrm{im}_{\sigma_1}(x) = (1, 1, 1)\}.$$

Let $x = (e_1, e_2, e_3) \in A$. Then in any case, the $\mathfrak{p}_2$-adic image implies that $\mathrm{ord}_\alpha(e_i) \equiv 0 \bmod 2$. Combining this with information at σ_1 and $\mathfrak{p}_3$ we see that $e_i \in \langle \varepsilon, \pi_1, \pi_2 \rangle$ for all i. We also see that in fact $e_1 \in \langle \pi_1, \pi_2 \rangle$ because e_1 is totally positive. For the rest of the calculations we now specialize according to $p \equiv 1, 7, 17, 23 \bmod 24$, and will omit in table (3.4) the rows corresponding to -1, α and 3 as we don't need those anymore.

(iii) $p \equiv 1 \bmod 24$. In this case the table becomes

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	$\mathfrak{q}$	σ_1	σ_2
ε	$1+\alpha$	r			1	-1
π_1		1	π_1		1	1
π_2		1		π_2	1	1

As $\mathrm{im}_{\mathfrak{p}_3}(e_1) = 1$, we see that x has trivial $\mathfrak{p}_3$-adic image, so $e_i \in \langle \pi_i, \pi_2 \rangle$ for all i.

Reducing the norm equation

$$a^2 - 2b^2 = p$$

modulo 8 we see that b is even. As $\pi_2 = a - b\alpha$, we see from our description of elements of $\mathbb{Q}_2(\alpha)^*/\mathbb{Q}_2(\alpha)^{*2}$ that all 16 possibilities for x map into the 2-adic image. The images of x under $\mathfrak{p}_3$, σ_1 and σ_2 are all trivial, so it remains to consider the images under $\mathfrak{p}$ and $\mathfrak{q}$, for which we distinguish two cases.

Suppose that π_i is a square mod π_j for $i \neq j$, i.e. $\mathrm{im}_{(\pi_i)}(\pi_j) = 1$ for $i \neq j$. Then for a fixed i, the (π_i)-adic image is spanned by

$$\begin{matrix} 1 & \pi_i & \pi_i \\ \pi_i & \pi_i & 1 \end{matrix}$$

and we see that all 16 possibilities for x map into the (π_i)-adic image, hence yield elements of A. Thus $S^2(E/K)$ has dimension 6. As generators for A one can take $(\pi_1, \pi_1, 1)$, $(\pi_1, 1, \pi_1)$, $(\pi_2, \pi_2, 1)$ and $(\pi_2, 1, \pi_2)$.

Suppose that $\mathrm{im}_{(\pi_i)}(\pi_j) \neq 1$ for $i \neq j$, then for a fixed i, the (π_i)-adic image is spanned by

$$\begin{matrix} 1 & \pi_i\pi_j & \pi_i\pi_j \\ \pi_i\pi_j & \pi_i\pi_j & 1 \end{matrix}$$

where $K^*_{(\pi_i)}/K^{*2}_{(\pi_i)} = \langle \pi_i, \pi_j \rangle$, which forces $e_k \in \langle \pi_1\pi_2 \rangle = \langle p \rangle$ for all k. It follows that $A = \langle (p, p, 1), (p, 1, p) \rangle$, and that $S^2(E/K)$ has dimension 4.

(iv) $p \equiv 7 \bmod 24$. In this case we have the same (truncated) table as for the previous case.

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	$\mathfrak{q}$	σ_1	σ_2
ε	$1+\alpha$	r			1	-1
π_1		1	π_1		1	1
π_2		1		π_2	1	1

Then $e_i \in \langle \pi_i, \pi_2 \rangle$ for all i exactly as in the previous case. We again consider the norm equation

$$a^2 - 2b^2 = p$$

modulo 8, but $p \equiv 7 \bmod 8$ now implies that b is odd. Now if we would have $e_k = \pi_i$ for certain k and i, then b odd is incompatible with the $\mathfrak{p}_2$-adic image, so we conclude $e_k \in \langle p \rangle$ for all k. Now using p as uniformizer at $K_{\mathfrak{p}} = \mathbb{Q}_p$, we see that the $\mathfrak{p}$-adic image is spanned by

$$\begin{matrix} -1 & p & -p \\ p & -p & -1 \end{matrix}$$

This implies that x is trivial, and we conclude that $A = 0$ and that $S^2(E/K)$ has dimension 2.

(v) $p \equiv 17 \bmod 24$. In this case we see

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	$\mathfrak{q}$	σ_1	σ_2
ε	$1+\alpha$	r			1	-1
π_1		r	π_1		1	1
π_2		r		π_2	1	1

Just as with $p \equiv 1 \bmod 24$, we see from reducing $p = a^2 - 2b^2 = p$ modulo 8 that b is even. This implies that x maps into the $\mathfrak{p}_2$-adic image precisely when $e_i \in \langle \pi_1, \pi_2 \rangle$ for all i, so we indeed have $e_i \in \langle \pi_1, \pi_2 \rangle$, and need only worry about the (π_i)-adic images.

Suppose that $\mathrm{im}_{(\pi_i)}(\pi_j) = 1$ for $i \neq j$. Then for fixed i the (π_i)-adic image is spanned by

$$\begin{matrix} 3 & 3\pi_i & \pi_i \\ \pi_i & \pi_i & 1 \end{matrix}$$

It follows that $\mathrm{im}_{(\pi_i)}(x)$ is contained in the span of $(\pi_i, \pi_i, 1)$, which results A being generated by $(\pi_1, \pi_1, 1)$ and $(\pi_2, \pi_2, 1)$. Thus $S^2(E/K)$ has dimension 4.

If however $\mathrm{im}_{(\pi_i)}(\pi_j) = 3$ for $i \neq j$ then for fixed i the (π_i)-adic image is spanned by

$$\begin{matrix} 3 & \pi_i & 3\pi_i \\ 3\pi_i & 3\pi_i & 1 \end{matrix}$$

This forces $e_3 \in \langle p \rangle$, yielding four options in total. One checks in that (π_1, π_2, p) and (π_2, π_1, p) give elements of A, so also in this case we see that $S^2(E/K)$ has dimension 4.

(v) $p \equiv 23 \bmod 24$. In this case $\varepsilon\overline{\varepsilon} = -1$, which is not a square mod $\mathfrak{p}$, so $\mathrm{im}_{(\pi_i)}(\varepsilon) = 1$ for exactly one i. Interchanging π_1 and π_2 if necessary (we have not made any distinction between π_1 and π_2 yet so we can do this), we may assume that $\mathrm{im}_{\mathfrak{p}}(\varepsilon) = 1$. The table then becomes

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}$	$\mathfrak{q}$	σ_1	σ_2
ε	$1+\alpha$	r	1	-1	1	-1
π_1		r	π_1		1	1
π_2		r		π_2	1	1

Just as for the case $p \equiv 7 \bmod 24$, we see from $a^2 - 2b^2 \equiv 7 \bmod 8$ that b is odd, hence the $\mathfrak{p}_2$-adic image forces $e_1 \in \langle p \rangle$. Then e_1 has trivial $\mathfrak{p}_3$-adic image, which forces $e_i \in \langle \varepsilon\pi_1, \varepsilon\pi_2 \rangle$ for all i. As both ε and the π_i have 'odd α-coordinate' in $\mathbb{Q}_2(\alpha)^*/\mathbb{Q}_2(\alpha)^{*2}$, we see that all these options are compatible with the $\mathfrak{p}_2$-adic image. It thus remains to consider the images of $\mathfrak{p}$, $\mathfrak{q}$ and σ_2.

Suppose that $\mathrm{im}_{(\pi_i)}(\pi_j) = 1$ for $i \neq j$. Then for fixed i the (π_i)-adic image is spanned by

$$\begin{matrix} 1 & -\pi_i & -\pi_i \\ \pi_i & -\pi_i & -1 \end{matrix}$$

For $i = 1$ this implies $e_2 \in \langle \varepsilon\pi_2 \rangle$ and also that $\mathrm{im}_{(\pi_1)}(x)$ is in the span of $(\pi_1, 1, \pi_1)$. This give at most four options, and they all yield elements of A, one can take the generators $(p, 1, p)$ and $(p, \varepsilon\pi_2, \varepsilon\pi_1)$ for A.

Suppose that $\mathrm{im}_{(\pi_i)}(\pi_j) = -1$ for $i \neq j$. Then for fixed i the (π_i)-adic image is spanned by

$$\begin{matrix} 1 & \pi_i & \pi_i \\ -\pi_i & \pi_i & -1 \end{matrix}$$

For $i = 2$ this implies $e_2 \in \langle \varepsilon\pi_1 \rangle$, so we again have four options, and we see that all of them give elements of A, this time one can take $(p, 1, p)$ and $(p, \varepsilon\pi_1, \varepsilon\pi_2$ as generators for A. We see that $S^2(E/K)$ has dimension 4 in both cases.

Collecting the results of all these calculations, we have

Proposition 3.3.3. *For a prime $p \neq 2, 3$, let E be the elliptic curve over $K = \mathbb{Q}(\sqrt{2})$ defined by the equation*

$$y^2 = (x^2 - 9p^2)(x + 2\sqrt{2}p).$$

Then $S^2(E/K)$ depends partially on $p \bmod 24$ as follows.

$p \bmod 24$	$\dim S^2(E/K)$
1	4 *or* 6
5	3
7	2
11	3
13	3
17	4
19	3
23	4

And for $p \equiv 1 \bmod 24$, we have $\dim S^2(E/K) = 6$ precisely when π_1 is a square mod π_2, where $\pi_1, \pi_2 \in \mathbb{Z}[\sqrt{2}]$ are totally positive, conjugate elements of norm p.

If we compare this with the calculation of $S^2(J/K)$ and the resulting rank bounds for $J(\mathbb{Q})$ and $E(K)$, we see that for $p \not\equiv 1 \bmod 24$ we get the exact same rank bound. When $p \equiv 1 \bmod 24$ and π_1 is not a square mod π_2 however, we see with proposition 3.2.3 that

$$\operatorname{rank}(J/\mathbb{Q}) \leq 2.$$

Then as $\operatorname{rank}(J/\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(J/\mathbb{Q})[2] = 4$ by equation ((3.1)), this forces

$$(\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(J/\mathbb{Q})[2].$$

We would like to know how often this happens. We can see that π_1 is not a square mod π_2 precisely when $f_p = 2$ in the normal closure of $K(\sqrt{\pi_1})/\mathbb{Q}$, but one cannot apply Chebotarëv's density theorem directly because the field in question depends on the prime p. We can circumvent this issue however with the following lemma.

Lemma 3.3.4. *Let $p \equiv 1 \bmod 8$ be a prime and let π, π' be totally positive, conjugate elements in $\mathbb{Z}[\sqrt{2}]$ such that $\pi\pi' = p$. Then equivalent are*

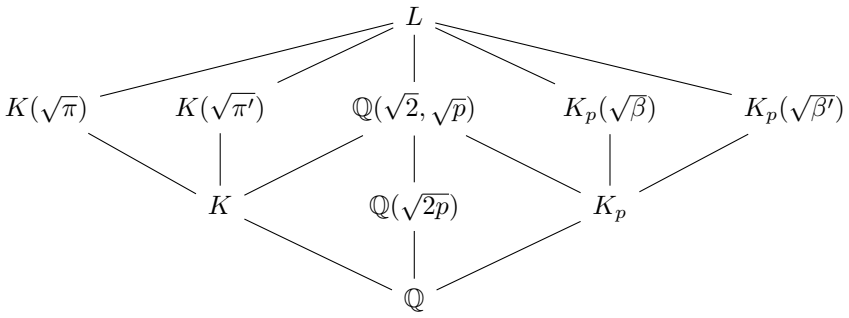
a) π is a square mod π', and π' is a square mod π.

b) p splits completely in $\mathbb{Q}(\sqrt[4]{2})$.

Proof. The normal closure L of $K(\sqrt{\pi})/\mathbb{Q}$ is obtained by adjoining $\sqrt{p}$. As π' has valuation zero with respect to the prime (π) and doesn't lie over 2, the prime (π') of K is unramified in $K(\sqrt{\pi})$. This implies that in the D_4-extension $L/\mathbb{Q}$ we have $e_p = 2$, and one readily sees that for (e_p, f_p, g_p) we have two options: $(2,1,4)$ or $(2,2,2)$. The first occurs precisely when (a) holds.
Writing $\pi = x + y\sqrt{2}$ we have $x^2 - 2y^2 = p$, which we can rewrite as $x^2 - p = 2y^2$, hence the element $\beta = x + \sqrt{p}$ in $\mathbb{Q}(\sqrt{p})$ has norm $\overline{2} \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. Let $K_p = \mathbb{Q}(\sqrt{p})$. Then L is also the normal closure of $K_p(\beta)$ as β is not a square in $\mathbb{Q}(\sqrt{p})$, while it is a square in L:

$$(\sqrt{\pi} + \sqrt{\pi'})^2 = \pi + \pi' + 2\sqrt{p} = (\sqrt{2})^2\beta$$

Letting β' be the $K_p/\mathbb{Q}$-conjugate of β we obtain the following subfield lattice.



Let $\mathfrak{p}$ be the unique prime of norm p in K_p. We see that (a) holds precisely when $\mathfrak{p}$ splits in $K_p(\sqrt{\beta})$. As $p \equiv 1 \bmod 8$ we have that 2 splits in K_p. Consider a prime $\mathfrak{p}_2|2$ in K_p. The core of the argument shows that $\mathfrak{p}$ splits in $K_p(\sqrt{\beta})$ if and only if $\mathfrak{p}_2$ splits in another quadratic extension of K_p, by invoking the product formula for quadratic Hilbert symbols in K_p.
For this, consider the unique quartic subfield E of $\mathbb{Q}(\zeta_p)$, which is quadratic over K_p and ramified only over $\mathfrak{p}$. Note that it is unramified at the infinite primes of K_p as $p \equiv 1 \bmod 8$ guarantees that $E \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. We have $E = K_p(\sqrt{\gamma})$ for $\gamma \in K_p$ a non-square of norm p (up to multiplication by squares). For β and γ we now use the product formula for quadratic Hilbert symbols in K_p:

$$1 = \prod_{\mathfrak{q}} (\beta, \gamma)_{\mathfrak{q}}$$

As γ and β have positive norm, the factors in this product corresponding to the two infinite primes are equal, hence the product reduces to

$$(\beta, \gamma)_{\mathfrak{p}_2} (\beta, \gamma)_{\mathfrak{q}_2} (\beta, \gamma)_{\mathfrak{p}} = 1,$$

where $\mathfrak{p}_2$ and $\mathfrak{q}_2$ are the primes of K_p lying over 2. Without loss of generality we may assume that $\mathrm{ord}_{\mathfrak{p}_2}(\beta) \equiv 1 \bmod 2$. When $\mathfrak{q} \neq \mathfrak{p}$, we have that $F(\sqrt{\gamma})/F$ is unramified for $F = (K_p)_{\mathfrak{q}}$ as E/K_p only ramifies over $\mathfrak{p}$, so $(\beta, \gamma)_{\mathfrak{q}_2} = 1$ as $\mathrm{ord}_{\mathfrak{q}_2}(\beta) \equiv 0 \bmod 2$, hence we have

$$(\beta, \gamma)_{\mathfrak{p}_2} = (\gamma, \beta)_{\mathfrak{p}}.$$

Which implies that $\mathfrak{p}_2$ splits in $K_p(\sqrt{\gamma})$ if and only if $\mathfrak{p}$ splits in $K_p(\sqrt{\beta})$.

Thus we see that (a) holds if and only if $\mathfrak{p}_2$ splits in F. We finish the proof by using another reciprocity argument. Note that $\mathfrak{p}_2$ splits in F precisely when 2 splits completely in F. By Galois theory, F is the invariant field of the subgroup H of fourth powers in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$. Letting D_2 and Z_2 be the decomposition group and decomposition field of 2 in this extension, we see that $F \subset Z_2$ if and only if $D_2 \subset H$. As $D_2 = \langle \mathrm{Frob}_2 \rangle = \langle 2 \bmod p \rangle$ we see that 2 splits completely in F if and only if 2 is a fourth power in $\mathbb{F}_p$, i.e. when p splits completely in $\mathbb{Q}(\sqrt[4]{2})$. $\square$

Combining the result of the computation of $S^2(E/K)$ for $p \equiv 1 \bmod 24$ with lemma 3.3.4 we obtain

Corollary 3.3.5. *Let $p \equiv 1 \bmod 24$ be a prime that does not split completely in $\mathbb{Q}(\sqrt[4]{2})$. Then if J is the Jacobian of the hyperelliptic curve defined by*

$$y^2 = x(x^2 - p^2)(x^2 - 4p^2),$$

we have

$$\operatorname{rank}(J/\mathbb{Q}) \leq 2, \quad \textit{and} \quad (\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(J/\mathbb{Q})[2].$$

To see how often this occurs, we apply

Proposition 3.3.6 (Chebotarëv's density theorem)**.** *Let $L/\mathbb{Q}$ be a finite Galois extension with group G, and let $C \subset G$ be a subset that is stable under conjugation (that is $\sigma C \sigma^{-1} = C$ for all $\sigma \in G$). Then*

$$\lim_{X \to \infty} \frac{\#\{\textit{primes } p \leq X : p \textit{ is unramified in } L \textit{ and } \operatorname{Frob}_p \in C\}}{\#\{\textit{primes } p \leq X\}} = \frac{\#C}{[L : \mathbb{Q}]}$$

Proof. See [10, Ch.VII, Thm. 13.4]. □

Note that in general, the Frobenius element $\operatorname{Frob}_p \in G$ depends on the prime $\mathfrak{p}$ of L lying over p, but the varying Frobenius elements as $\mathfrak{p}$ ranges over the primes over p are all conjugate, so the condition $\operatorname{Frob}_p \in C$ is well-defined by the assumption that C is stable under conjugation. A special case of Chebotarëv's density theorem is obtained when taking $C = \{1\}$:

$$\lim_{X \to \infty} \frac{\#\{\text{primes } p \leq X : p \text{ splits completely in } L\}}{\#\{\text{primes } p \leq X\}} = \frac{1}{[L : \mathbb{Q}]}$$

Proposition 3.3.7. *We have*

$$\lim_{X \to \infty} \frac{\#\{\textit{primes } p \leq X : p \equiv 1 \bmod 24 \textit{ and } p \textit{ doesn't split completely in } \mathbb{Q}(\sqrt[4]{2})\}}{\#\{\textit{primes } p \leq X : p \equiv 1 \bmod 24\}} = \frac{1}{2}$$

Proof. Let $L = \mathbb{Q}(\sqrt[4]{2})$. Then to prove the proposition it is equivalent to show that

$$\lim_{X \to \infty} \frac{\#\{\text{primes } p \leq X : p \equiv 1 \bmod 24 \text{ and } p \text{ splits completely in } L\}}{\#\{\text{primes } p \leq X : p \equiv 1 \bmod 24\}} = \frac{1}{2}.$$

If p is a prime that splits completely in L, then $p \equiv 1 \bmod 8$ as $\mathbb{Q}(\zeta_8) \subset L$. As p splits completely in $\mathbb{Q}(\zeta_3)$ if and only if $p \equiv 1 \bmod 3$ we obtain

$$p \equiv 1 \bmod 24 \text{ and } p \text{ splits completely in } L \quad \Leftrightarrow \quad p \text{ splits completely in } L(\zeta_3). \tag{3.5}$$

Applying Chebotarëv to both $L(\zeta_3)$ and $\mathbb{Q}(\zeta_{24})$ we obtain

$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \text{ splits completely in } L(\zeta_3)\}}{\#\{\text{primes } p \le X\}} = \frac{1}{16},$$
$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \text{ splits completely in } \mathbb{Q}(\zeta_{24})\}}{\#\{\text{primes } p \le X\}} = \frac{1}{8}.$$

A prime p splits completely in $\mathbb{Q}(\zeta_{24})$ if and only if $p \equiv 1 \bmod 24$, hence taking the quotient of the two limits above and applying (3.5), we obtain the result. □

Corollary 3.3.8. *There are infinitely many primes $p \equiv 1 \bmod 24$ for which the Jacobian J of the hyperelliptic curve defined by $y^2 = x(x^2 - p^2)(x^2 - 4p^2)$ satisfies*

$$(\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(J/\mathbb{Q})[2].$$

Proof. If $p \equiv 1 \bmod 24$ does not split completely in $\mathbb{Q}(\sqrt[4]{2})$ then $(\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(J/\mathbb{Q})[2]$ from corollary 3.3.5. As there are infinitely many primes $p \equiv 1 \bmod 24$ (which one can see by invoking Chebotarev to $\mathbb{Q}(\zeta_{24})$), we see that a finite number of primes $p \equiv 1 \bmod 24$ that do not split completely in $\mathbb{Q}(\sqrt[4]{2})$ would imply that the limit of proposition 3.3.7 is 0, which is not the case. □

3.3.3 $S^2(J/\mathbb{Q}) \to S^2(E/K)$

Let us recall: we have a prime $p \neq 2, 3$ and the hyperelliptic curve C over $\mathbb{Q}$ defined by the equation $y^2 = f(x) = x(x^2-p)^2(x^2-4p^2)$, and the elliptic curve E over $K = \mathbb{Q}(\sqrt{2})$ defined by $y^2 = g(x) = (x^2 - 9p^2)(x + 2\sqrt{2}p)$. By now we have explicitely computed the 2-Selmer groups $S^2(J/\mathbb{Q})$ and $S^2(E/K)$. In this section we will compare the two. This will not give us definitive extra results, but will be the basis for formulating a conjecture.

Using proposition 2.2.2 for J and $K/\mathbb{Q}$, and proposition 2.2.1 for $J_K \to E$ we have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & S^2(J/\mathbb{Q}) & \longrightarrow & Ш(J/\mathbb{Q})[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J(K)/2J(K) & \longrightarrow & S^2(J/K) & \longrightarrow & Ш(J/K)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/2E(K) & \longrightarrow & S^2(E/K) & \longrightarrow & Ш(E/K)[2] & \longrightarrow & 0
\end{array}$$

How do the maps to and between the Selmer groups look explicitly as in section 2.3? One quickly sees with the naturality of restriction of cohomology and the Kummer isomorphisms that considering $S^2(J/\mathbb{Q}) \subset \bigoplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2}$ similarly for $S^2(J/K)$, that the map $S^2(J/\mathbb{Q}) \to S^2(J/K)$ is simply induced by the canonical map $\bigoplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2} \to \bigoplus_{i=1}^5 K^*/K^{*2}$. The 'explicit version' of the map $S^2(J/K) \to S^2(E/K)$ is more involved however, as it depends on the map

$J(\overline{K})[2] \to E(K)[2]$ and on how the Weil pairings relate.

Set $A_J = K[x]/(f)$ and $\overline{A_J} = \overline{K}[x]/(f)$, and similarly $A_E = K[x]/(g)$ and $\overline{A_E} = \overline{K}/(g)$. Also identify $\mu_2(\overline{A_J}) = \mu_2^5$ and $\mu_2(\overline{A_E}) = \mu_2^3$ as (trivial!) G_K-modules.

Lemma 3.3.9. *If we define a group homomorphism $\alpha : \mu_2^5 \to \mu_2^3$ by*

$$\begin{aligned}
(-1,1,1,1,1) &\mapsto (-1,1,1)\\
(1,-1,1,1,1) &\mapsto (-1,1,1)\\
(1,1,-1,1,1) &\mapsto (-1,-1,-1)\\
(1,1,1,-1,1) &\mapsto (1,-1,1)\\
(1,1,1,1,-1) &\mapsto (1,-1,1)
\end{aligned}$$

then we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(\overline{K})[2] & \xrightarrow{w_J} & \mu_2^5 & \longrightarrow & \mu_2 & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \\
0 & \longrightarrow & E(\overline{K})[2] & \xrightarrow{w_E} & \mu_2^3 & \longrightarrow & \mu_2 & \longrightarrow & 0.
\end{array} \tag{3.6}$$

where w_J and w_E are the maps obtained from the respective Weil pairings as in section

Proof. Writing $D_\xi = [(\xi, \sqrt{f(\xi)}) - \infty]$, for $\xi \in \overline{\mathbb{Q}}$, the relevant images of generators of $J(\overline{K})[2]$ can be summarized in the following table.

Divisor	image in μ_2^5	image in $E(K)[2]$	image in μ_2^3
D_{-2p}	$(1,-1,-1,-1,-1)$	$(-3p,0)$	$(1,-1,-1)$
D_{-p}	$(-1,1,-1,-1,-1)$	$(-3p,0)$	$(1,-1,-1)$
D_0	$(-1,-1,1,-1,-1)$	∞	$(1,1,1)$
D_p	$(-1,-1,-1,1,-1)$	$(3p,0)$	$(-1,1,-1)$
D_{2p}	$(-1,-1,-1,-1,1)$	$(3p,0)$	$(-1,1,-1)$

Noting that $\alpha(-1,-1,-1,-1,-1) = (-1,-1,-1)$, it is easy to check that diagram (3.6) indeed commutes. □

Applying the functor $H^1(G_K, -)$ to diagram (3.6) results in the diagram

$$\begin{array}{ccccc}
H^1(G_K, J(\overline{K})[2]) & \xrightarrow{w_J^*} & H^1(G_K, \mu_2(\overline{A_J})) & \longrightarrow & H^1(G_K, \mu_2(K^*))\\
\downarrow & & \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \mathrm{id}}\\
H^1(G_K, E(\overline{K})[2]) & \xrightarrow{w_E^*} & H^1(G_K, \mu_2(\overline{A_E})) & \longrightarrow & H^1(G_K, \mu_2(K^*)),
\end{array}$$

How does α^* behave when applying the Kummer isomorphisms? We have

$$A_J^*/A_J^{*2} \xrightarrow{\sim} H^1(G_K, \mu_2(\overline{A_J})) \xrightarrow{\alpha} H^1(G_K, \mu_2(\overline{E_K})) \xrightarrow{\sim} A_K^*/A_K^{*2}$$

The first map sends $a \mapsto \left(\sigma \mapsto \frac{\sigma(a)}{a}\right)$. Considering A_J^*/A_J^{*2} as five copies of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ and similarly for A_K^*/A_K^{*2}, we see that for example the map sends

$$(a,1,1,1,1) \mapsto \left(\sigma \mapsto \left(\tfrac{\sigma\sqrt{a}}{\sqrt{a}},1,1,1,1\right)\right) \mapsto \left(\sigma \mapsto \left(\tfrac{\sigma\sqrt{a}}{\sqrt{a}},1,1\right)\right) \mapsto (a,1,1)$$

Doing the same 'for the other coordinates' we see that $(a,b,c,d,e) \mapsto (abc, cde, c)$, hence we have a commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q})/2J(\mathbb{Q}) & \hookrightarrow & \bigoplus_{i=1}^5 \mathbb{Q}^*/\mathbb{Q}^{*2} \\ \downarrow & & \downarrow \\ E(K)/2E(K) & \hookrightarrow & \bigoplus_{i=1}^3 K^*/K^{*2} \end{array}$$

where the right vertical map is given by $(a,b,c,d,e) \mapsto (abc, cde, e)$. This gives us a way to explicitly compare the 2-Selmer groups in the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & S^2(J/\mathbb{Q}) & \longrightarrow & Ш(J/\mathbb{Q})[2] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & E(K)/2E(K) & \longrightarrow & S^2(E/K) & \longrightarrow & Ш(E/K)[2] & \longrightarrow & 0 \end{array}$$

Before looking at specific cases according to the 2-Selmer group computations, note that applying the snake lemma to this diagram yields the long exact sequence

$$0 \to \ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0$$

Note that if $r = \operatorname{rank}(J/\mathbb{Q}) = \operatorname{rank}(E/K)$, then $\dim(J(\mathbb{Q})/2J(\mathbb{Q})) = r+4$, while $\dim(E(K)/2E(K)) = r+2$, which implies that $\dim\ker(\alpha) = 2 + \dim\operatorname{coker}(\alpha)$. Counting dimensions in the long exact sequence we thus obtain the relation

$$2 + \dim\ker(\gamma) + \dim\operatorname{coker}(\beta) = \dim(\ker(\beta)) + \dim(\operatorname{coker}(\gamma)). \tag{3.7}$$

The computation of $\ker(\beta)$ only depends on p mod 24, and is a matter of simple linear algebra. Note that from $J(\mathbb{Q})[2]$ we always obtain a two-dimensional subspace in $\ker(\beta)$: generators are $(2p,p,1,-p,-2p)$ and $(6p,6p,2,6,3)$.

p mod 24	$\dim_{\mathbb{F}_2} S^2(J/\mathbb{Q})$	$\dim_{\mathbb{F}_2}\ker(\beta)$	additional generators
1	8	4	$(p,p,1,1,1),(1,1,1,p,p)$
5	5	2	none
7	4	2	none
11	5	2	none
13	5	2	none
17	6	3	$(p,p,1,p,p)$
19	5	2	none
23	6	3	$(1,1,1,-p,-p)$

Now let us consider the case $p \equiv 1 \bmod 24$ where p does not split completely in $\mathbb{Q}(\sqrt[4]{2})$, so that $\dim S^2(E/K) = 4$. We see that β is surjective in this case, hence also γ is surjective, and with (3.7) we obtain $\dim(\ker(\gamma)) = 2$, which coincides with our knowledge that in any case $(\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(J/\mathbb{Q})[2]$. Surjectivity of $\ker(\beta) \to \ker(\gamma)$ means precisely that $(p, p, 1, 1, 1), (1, 1, 1, p, p)$ give independent, non-trivial elements in $Ш(J/\mathbb{Q})[2]$, and from the long exact sequence we see that $\ker(\beta) \to \ker(\gamma)$ is surjective precisely when α is surjective.

Conjecture 3.3.10. *If $p \equiv 1 \bmod 24$ does not split completely in $\mathbb{Q}(\sqrt[4]{2})$, then $\langle (p, p, 1, 1, 1), (1, 1, 1, p, p) \rangle \subset S^2(J/\mathbb{Q})$ injects into $Ш(J/\mathbb{Q})[2]$.*

We will return to the issue of numerical evidence for this conjecture later.

3.4 More 2-descents

In this section we use another approach to determine the rank of $J_p(\mathbb{Q})$ for J_p the Jacobian of the hyperelliptic curve C_p defined by

$$y^2 = x(x^2 - p^2)(x^2 - 4p^2)$$

Namely we use the fact that the curves are all quadratic twists of each other. Let $C/\mathbb{Q}$ be the hyperelliptic curve defined by the equation $y^2 = x(x^2 - 1)(x^2 - 4)$. Then C_p is a quadratic twist of C over *both* $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$. This follows from the fact that an equivalent model for C_p is determined by the equation

$$py^2 = x(x^2 - 1)(x^2 - 4)$$

and the fact that $(x, y) \mapsto (-x, \zeta_4 y)$ is an automorphism. It follows that we have the formula

$$\operatorname{rank}(J/\mathbb{Q}) + \operatorname{rank}(J_p/\mathbb{Q}) = \operatorname{rank}(J/\mathbb{Q}(\sqrt{p})) = \operatorname{rank}(J/\mathbb{Q}(\sqrt{-p})). \tag{3.8}$$

We will see that $\operatorname{rank}(J/\mathbb{Q}) = 0$, so that an alternative way of obtaining information about $\operatorname{rank}(J_p/\mathbb{Q})$ is by computing $S^2(J/\mathbb{Q}(\sqrt{\pm p}))$.

Computations with Magma for primes $p \leq 3000$ suggest that the following results hold.

$p \bmod 24$	$\dim(S^2(J_p/\mathbb{Q}))$	$\dim(S^2(J/\mathbb{Q}(\sqrt{p})))$	$\dim(S^2(J/\mathbb{Q}(\sqrt{-p})))$
1	8	4, 6 or 8	8
5	5	5	7
7	4	4	4
11	5	7	5
13	5	5	9
17	6	4 or 6	6
19	5	5	7
23	6	6	4 or 6

We will calculate $S^2(J/\mathbb{Q}(\sqrt{p}))$ for $p \equiv 1, 17 \bmod 24$ and $S^2(J/\mathbb{Q}(\sqrt{-p}))$ for $p \equiv 23 \bmod 24$, and obtain for each case a *governing field*. That is (the size of) the 2-Selmer group will depend on the splitting behaviour of p in some number field that is independent of p. This will allow us to use Chebotarëv´s density theorem, which for example will allow us to prove that $\mathrm{rank}(J/\mathbb{Q}) = 0$ occurs infinitely often in each of the cases for $p \equiv 1, 17, 23 \bmod 24$.

Note that in each of the three cases we are dealing with $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$ for an odd prime p. Proposition A.2.4 implies that these number fields have *odd* class number, and a fundamental unit of norm -1 in case the field is real.

3.4.1 Local images and image of 2-torsion

The 2-torsion yields elements in the 2-Selmer group regardless over which number field we work. The image of $J(\mathbb{Q})[2]$ is

	$X+2$	$X+1$	X	$X-1$	$X-2$
D_{-2}	6	-1	-2	-3	-1
D_{-1}	1	-6	-1	-2	-3
D_0	2	1	1	-1	-2
D_1	3	2	1	-6	-1

Over the number fields $\mathbb{Q}(\sqrt{p^*})$ we will consider this image is still 4-dimensional.

Those local fields F that occur as completions of the fields $\mathbb{Q}(\sqrt{p^*})$ for which we need the local images are $\mathbb{Q}_2$,$\mathbb{Q}_3$,$\mathbb{Q}_3(i)$ and $\mathbb{R}$. For each such F we have an embedding $J(F)/2J(F) \hookrightarrow \bigoplus_{i=1}^{5} F^*/F^{*2}$. Note that for $F = \mathbb{Q}_3(i)$ we have $F^*/F^{*2} = \langle 3, r \rangle$, where $r = 1 + i$.

$\mathbb{Q}_2$	$X+2$	$X+1$	X	$X-1$	$X-2$
D_{-2}	6	-1	-2	-3	-1
D_{-1}	1	-6	-1	-2	-3
D_0	2	1	1	-1	-2
D_1	3	2	1	-6	-1
D_6	2	-1	6	-3	1
D_7	1	2	-1	6	-3

$\mathbb{Q}_3$	$X+2$	$X+1$	X	$X-1$	$X-2$
D_{-2}	-3	-1	1	-3	-1
D_{-1}	1	3	-1	1	-3
D_0	-1	1	1	-1	1
D_4	1	-3	-1	1	3

$\mathbb{Q}_3(i)$	$X+2$	$X+1$	X	$X-1$	$X-2$
D_{-2}	3	1	1	3	1
D_{-1}	1	3	1	1	3
D_i	r	r	1	r	r
D_{4+3i}	$3r$	1	1	$3r$	1

$\mathbb{R}$	$X+2$	$X+1$	X	$X-1$	$X-2$
D_{-1}	1	-1	-1	-1	-1
D_0	1	1	1	-1	-1

The first thing we do with these local images is to prove

Proposition 3.4.1. *We have* $\mathrm{rank}(J/\mathbb{Q}) = 0$*, so that*

$$\mathrm{rank}(J_p/\mathbb{Q}) = \mathrm{rank}(J/\mathbb{Q}(\sqrt{p})) = \mathrm{rank}(J/\mathbb{Q}(\sqrt{-p})) \tag{3.9}$$

Proof. It suffices to show that $S^2(J/\mathbb{Q})$ has $\mathbb{F}_2$-dimension 4, for then $\mathrm{rank}(J/\mathbb{Q}) = 0$, so that (3.9) follows from (3.8). The primes we need to consider are $2, 3$ and ∞, and we can take $K(S) = \langle -1, 2, 3\rangle$. It follows that $S^2(J/\mathbb{Q})$ injects into the 2-adic image. It follows that

$$S^2(J/\mathbb{Q}) = A \oplus \mathrm{im}(J(\mathbb{Q})[2])$$

where A consists of those $x \in S^2(J/\mathbb{Q})$ for which $\mathrm{im}_2(x)$ is contained in the span of

$$\begin{matrix} 2 & -1 & 6 & -3 & 1 \\ 1 & 2 & -1 & 6 & -3 \end{matrix}$$

Now if $x = (e_1, \ldots, e_5) \in A$, then the 3-adic image forces $\mathrm{im}_3(e_3) \subset \langle -1\rangle$, hence the $\mathrm{im}_2(x)$ is in the span of $(1, 2, -1, 6, -3)$, hence x is in the span of $(1, 2, -1, 6, -3)$, which forces x to be trivial as $(1, 2, -1, 6, -3)$ maps 3-adically to $(1, -1, -1, 3, -3)$, which is not in the 3-adic image. Thus $A = 0$ and $S^2(J/\mathbb{Q})$ has $\mathbb{F}_2$-dimension 4. □

3.4.2 $J/\mathbb{Q}(\sqrt{-p})$ for $p \equiv 23 \bmod 24$

Let $K = \mathbb{Q}(\sqrt{-p})$ for $p \equiv 23 \bmod 24$. Then as K is complex and both 2 and 3 split in K, we need to consider four primes, and only need the local images for $\mathbb{Q}_2$ and $\mathbb{Q}_3$.

Suppose that $(3) = \mathfrak{p}_3\mathfrak{q}_3$ and let k_3 be the order of $[\mathfrak{p}]$ (or $[\mathfrak{q}]$) in Cl_K. Then $\mathfrak{p}_3^{k_3} = (x_3)$ for some x_3. Then x_3 maps to ± 1 under $K^*_{\mathfrak{q}_3}/K^{*2}_{\mathfrak{q}_3}$, so that by multiplying x_3 by -1 if necessary, we may assume that x_3 has trivial image under $\mathfrak{q}_3$. Let y_3 be the conjugate of x_3, so that $\mathfrak{q}_3^{k_3} = (y_3)$ and $x_3y_3 = 3^{k_3}$.

If $\mathfrak{p}$ is a prime over 2, then x_3 and y_3 map under the $\mathfrak{p}$-adic completion into $\{1, 3, 5, 7\} \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, while their product maps to 3, thus either x_3 or y_3 is mapped into $\{1, 5\}$ while the other is not. As $\mathrm{im}_{\mathfrak{p}}(y_3) = \mathrm{im}_{\mathfrak{q}}(x_3)$, with $\mathfrak{q}$ the other prime over 2, this implies that x_3 maps into $\{1, 5\} \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ for precisely one prime of K over 2, say $\mathfrak{p}_2$. This means that $\mathfrak{p}_2$ is unramified in $K(\sqrt{x_3})$.

Let $\mathfrak{q}_2$ be the conjugate of $\mathfrak{p}_2$. Let $x_2 \in \mathfrak{p}_2$ be a generator for $\mathfrak{p}_2^{k_2}$, with k_2 the

order of $[\mathfrak{p}_2]$. Similarly as for x_3, multiplying x_2 with -1 if necessary we may assume that x_2 maps $\mathfrak{q}_2$-adically into $\{1,5\} \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Finally we also let y_2 be the conjugate of x_2, so that also $x_2 y_2 = 2^{k_2}$.

Now from proposition A.2.4 we know that $k_2, k_3 \equiv 1 \bmod 2$, and hence from corollary 2.4.7 we see that $K(S) = \langle -1, x_2, y_2, x_3, y_3 \rangle$. We can compute the 2-Selmer group if we know the images of these generators in $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^*$ for the primes $\mathfrak{p}$ over 2 and 3. Evaluating the product formula for quadratic Hilbert symbols over K at x_2 and x_3 we obtain

$$(x_2, x_3)_{\mathfrak{p}_2}(x_2, x_3)_{\mathfrak{q}_2}(x_2, x_3)_{\mathfrak{p}_3} = 1$$

Now $(x_2, x_3)_{\mathfrak{q}_2} = (x_3, x_2)_{\mathfrak{q}_2} = 1$ as $\mathfrak{q}_2$ is unramfied in $K(\sqrt{x_2})$ and $\mathrm{ord}_{\mathfrak{q}_2}(x_3) = 0$, so that

$$(x_3, x_2)_{\mathfrak{p}_3} = (x_2, x_3)_{\mathfrak{p}_2},$$

As $\mathfrak{p}_3$ is unramified in $K(\sqrt{x_2})$ and $\mathfrak{p}_2$ is unramified in $K(\sqrt{x_3})$, this means that $x_3 \overset{\mathfrak{p}_2}{\longmapsto} 1$ if and only if $x_2 \overset{\mathfrak{p}_3}{\longmapsto} 1$.

Define

$$A = \{(e_1, \ldots, e_5) \in S^2(J/K) : e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1 \text{ and } e_4 \overset{\mathfrak{p}_2}{\longmapsto} 1\}.$$

Then $S^2(J/K) = A \oplus \mathrm{im}(J(K)[2])$. Elements of A land in smaller local images. For $\mathfrak{p}_2$ we see that the fourth coordinate of the local image hits everything in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, hence the subspace of the local image with fourth coordinate 1 is three dimensional. Independent elements are the images of $D_0 + D_1 + D_7, D_{-2} + D_6$ and $D_{-1} + D_6 + D_7$, which gives us the following local image for $\mathfrak{p}_2$.

$$\begin{array}{ccccc} 6 & 1 & -1 & 1 & -6 \\ 3 & 1 & -3 & 1 & -1 \\ 2 & 3 & 6 & 1 & 1 \end{array}$$

The corresponding local image for $\mathfrak{p}_3$ is spanned by

$$\begin{array}{ccccc} -3 & -1 & 1 & -3 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 \end{array} \tag{3.10}$$

There are now four cases, depending on $\mathrm{im}_{\mathfrak{q}_2}(x_2)$ and $\mathrm{im}_{\mathfrak{p}_2}(x_3)$.

Case (i)

For the first case of calculations we consider $\mathrm{im}_{\mathfrak{q}_2}(x_2) = 1$ and $\mathrm{im}_{\mathfrak{p}_2}(x_3) = 1$, which gives us the following table.

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$
-1	-1	-1	-1	-1
x_2	2	1	1	-1
y_2	1	2	-1	1
x_3	1	3	3	1
y_3	3	1	1	3

Let $x = (e_1, \ldots, e_5) \in A$. Since $e_4 \overset{\mathfrak{p}_2}{\longmapsto} 1$ we have $e_4 \in \langle y_2, x_3 \rangle$. As e_1, e_2 and e_5 are mapped $\mathfrak{p}_2$-adically into $\langle 2, 3 \rangle, \langle 3 \rangle$ and $\langle -1, 6 \rangle$, respectively, we obtain $e_1 \in \langle x_2, y_2, x_3, y_3 \rangle, e_2 \in \langle y_2, x_3, y_3 \rangle$ and $e_5 \in \langle -1, x_2 y_3, y_2, x_3 \rangle$. As e_3 maps into $\langle -1 \rangle$ both $\mathfrak{p}_3$-adically and $\mathfrak{q}_3$-adically, we have $v_{x_3}(e_3) = v_{y_3}(e_3) = 0$. As $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$, we have $e_3 \in \langle x_2, -y_2 \rangle$. From the smaller $\mathfrak{p}_3$-adic table we also see that $v_{x_3}(e_2) = v_{x_3}(e_5) = 0$, resulting in the following options for the e_i:

$$\begin{aligned} e_1 &\in \langle x_2, y_2, x_3, y_3 \rangle \\ e_2 &\in \langle y_2, y_3 \rangle \\ e_3 &\in \langle x_2, -y_2 \rangle \\ e_4 &\in \langle y_2, x_3 \rangle \\ e_5 &\in \langle -1, x_2 y_3, y_2 \rangle \end{aligned}$$

Because $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle 2 \rangle$ we see that x maps $\mathfrak{q}_2$-adically in the span of

$$\begin{array}{ccccc} 2 & 1 & 1 & -1 & -2 \\ 3 & 1 & -3 & 1 & -1 \\ 3 & 1 & -1 & -1 & 3 \\ 3 & 2 & 1 & -6 & -1 \end{array}$$

which further implies $e_3 \in \langle x_2 \rangle$ as $-y_2 \overset{\mathfrak{q}_2}{\longmapsto} -2$. But now e_3 maps $\mathfrak{q}_2$-adically to 1, and e_4 is mapped into $\langle 2, 3 \rangle$, which implies that the $\mathfrak{q}_2$-image of x lies in the span of $(6, 2, 1, 6, 2)$. It follows that $e_1 \in \langle x_2, y_2 x_3, y_3 \rangle, e_4 \in \langle y_2 x_3 \rangle$ and $e_5 \in \langle x_2 y_3, y_2 \rangle$.

As $e_4 \overset{\mathfrak{q}_3}{\longmapsto} 1$ and $\mathrm{im}_{\mathfrak{q}_3}(e_5) \subset \langle -3 \rangle$, we see that x maps $\mathfrak{q}_3$-adically into the span of $(1, 3, -1, 1, -3)$. This implies that $e_1 \in \langle y_2 x_3 \rangle$, resulting in the options

$$\begin{aligned} e_1 &\in \langle y_2 x_3 \rangle \\ e_2 &\in \langle y_2, y_3 \rangle \\ e_3 &\in \langle x_2 \rangle \\ e_4 &\in \langle y_2 x_3 \rangle \\ e_5 &\in \langle x_2 y_3, y_2 \rangle \end{aligned}$$

One can easily check that $(1, y_3, x_2, 1, x_2 y_3) \in A$, so that a complement inside A of the span of $(1, y_3, x_2, 1, x_2 y_3)$ consists of those elements with trivial third coordinate. Thus working inside this complement amounts to setting $e_3 = 1$ in the above options for the e_i. This forces our x to have trivial $\mathfrak{p}_2$-adic image, which implies $e_2, e_5 \in \langle y_2 \rangle$. The $\mathfrak{q}_2$-adic image now immediately forces x to be either $(y_2 x_3, y_2, 1, y_2 x_3, y_2)$ or trivial, that is this complement is one-dimensional. This proves that A is two-dimensional, with generators $(1, y_3, x_2, 1, x_2 y_3), (y_2 x_3, y_2, 1, y_2 x_3, y_2)$.

Case (ii)

For the second case we consider $\mathrm{im}_{\mathfrak{q}_2}(x_2) = 1$ and $\mathrm{im}_{\mathfrak{p}_2}(x_3) = -3$, so the table becomes

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$
-1	-1	-1	-1	-1
x_2	2	1	-1	1
y_2	1	2	1	-1
x_3	-3	-1	3	1
y_3	-1	-3	1	3

Let $x = (e_1, \ldots, e_5) \in A$, then $e_4 \overset{\mathfrak{p}_2}{\longmapsto} 1$ and $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$, which gives $e_3 \in \langle -x_2, y_2, y_3\rangle$ and $e_4 \in \langle y_2, -y_3\rangle$. From $\mathfrak{q}_3$-adic we see $e_3 \in \langle -x_2, y_2\rangle$. Then $\mathrm{im}_{\mathfrak{p}_2}(e_3) \subset \langle -2\rangle$, which forces the $\mathfrak{p}_2$-adic image of x_2 to be in the span of $(6, 3, -2, 1, -1)$, which implies $e_2 \in \langle y_2, -x_3, x_3y_3\rangle$. With $\mathfrak{p}_3$-adic information we see $e_2 \in \langle y_2, -y_3\rangle$, hence $\mathrm{im}_{\mathfrak{p}_2}(x)$ is trivial, so that $e_i \in \langle y_2, -y_3\rangle$ for all i. From $\mathfrak{p}_3$-adic image we see additionally $e_3 \in \langle y_2\rangle$. As $\mathrm{im}_{\mathfrak{q}_2}(e_i) \subset \langle 2, 3\rangle$ and $\mathrm{im}_{\mathfrak{q}_2}(e_i) \subset \langle 2\rangle$ we see that $\mathrm{im}_{\mathfrak{q}_2}(x)$ is in the span of

$$\begin{matrix} 6 & 2 & 1 & 6 & 2 \\ 6 & 6 & 2 & 6 & 3 \end{matrix}$$

This implies that $e_4 \in \langle -y_2y_3\rangle$, hence the $\mathfrak{q}_3$-adic image of x is contained in the span of

$$\begin{matrix} 3 & -1 & 1 & 3 & -1 \\ 1 & 3 & -1 & 1 & -3 \\ 1 & -3 & -1 & 1 & 3 \end{matrix}$$

Hence also $e_1 \in \langle -y_2y_3$. From the $\mathfrak{q}$-adic image we see that $e_1 = e_4$. One checks that $n_1 = (-y_2y_3, y_2, 1, -y_2y_3, y_2) \in A$, hence we obtain a complement inside A for $\langle n_1\rangle$ by setting $e_1 = e_4 = 1$, which forces the $\mathfrak{q}_2$-adic image to be in the span of $(1, 3, 2, 1, 6)$. This implies $e_2\langle -y_3\rangle$, $e_3 \in \langle y_2$ and $e_5 \in \langle -y_2y_3\rangle$, hence we see that the only non-trivial option remaining is $n_2 = (1, -y_3, y_2, 1, -y_2y_3)$, which is indeed in A, hence we see in this case that A two-dimensional.

Case (iii)

For this case we consider $\mathrm{im}_{\mathfrak{q}_2}(x_2) = -3$ and $\mathrm{im}_{\mathfrak{p}_2}(x_3) = 1$.

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$
-1	-1	-1	-1	-1
x_2	-6	-3	1	-1
y_2	-3	-6	-1	1
x_3	1	3	3	1
y_3	3	1	1	3

Let $x = (e_1, \ldots, e_5) \in A$. Then $e_4 \in \langle x_3, -y_2y_3\rangle$ and $e_3 \in \langle x_2, -y_2\rangle$. From the smaller $\mathfrak{p}_2$-adic image, we obtain just as with the previous case $e_1 \in \langle x_3, -y_2y_3, x_2y_2, y_3\rangle$,

$e_2 \in \langle -y_2, x_3, y_3\rangle$ and $e_5 \in \langle -1, x_2, y_2y_3, x_3\rangle$.
As $\mathrm{im}_{\mathfrak{p}_3}(e_2), \mathrm{im}_{\mathfrak{p}_3}(e_4) \subset \langle 3\rangle$, we see that x has trivial $\mathfrak{p}_3$-adic image, which implies $e_i \in \langle x_2, -y_2, y_3\rangle$ for all i, resulting in the following options

$$\begin{aligned} e_1 &\in \langle x_2, -y_2y_3\rangle \\ e_2 &\in \langle -y_2, y_3\rangle \\ e_3 &\in \langle x_2, -y_2\rangle \\ e_4 &\in \langle -y_2y_3\rangle \\ e_5 &\in \langle x_2, -y_2y_3\rangle \end{aligned}$$

With this we see $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle 6\rangle$, so that x maps $\mathfrak{q}_2$-adically in the span of

$$\begin{array}{ccccc} 2 & 1 & 1 & -1 & -2 \\ 3 & 1 & -3 & 1 & -1 \\ 3 & 1 & -1 & -1 & 3 \\ 6 & 6 & 2 & 6 & 3 \end{array}$$

Since also $\mathrm{im}_{\mathfrak{q}_2}(e_4) \subset \langle 6\rangle$, we see that x maps $\mathfrak{q}_2$-adically in the span of

$$\begin{array}{ccccc} 6 & 1 & -1 & 1 & -6 \\ 3 & 1 & -3 & 1 & -1 \\ 6 & 6 & 2 & 6 & 3 \end{array}$$

This forces $\mathrm{im}_{\mathfrak{q}_2}(e_1) \subset \langle 2, 3\rangle$, hence $e_1 \in \langle -y_2y_3\rangle$, so that we may remove the second row as well. But then $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -1, 2\rangle$, which implies $e_3 \in \langle -x_2y_2\rangle$, which in turn implies that the x maps $\mathfrak{q}_2$-adically into the span of $(1, 6, -2, 6, -2)$. We see that $e_1 = 1$, and also $e_3 \in \langle -x_2y_2\rangle$ and $e_5 \in \langle -x_2y_2y_3\rangle$. But then $e_3 \overset{\mathfrak{q}_3}{\longmapsto} 1$, so that with $e_1 = 1$ we see that x has trivial $\mathfrak{q}_3$-adic image.
In particular, this implies that $e_5 = 1$, so that the $\mathfrak{q}_2$-adic image of x is trivial, which implies $x = (1, 1, 1, 1, 1)$, i.e. $A = 0$.

Case (iv)

For the last case we have $\mathrm{im}_{\mathfrak{q}_2}(x_2) = -3$ and $\mathrm{im}_{\mathfrak{p}_2}(x_3) = -3$, so the table becomes

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$
-1	-1	-1	-1	-1
x_2	-6	-3	-1	1
y_2	-3	-6	1	-1
x_3	-3	-1	3	1
y_3	-1	-3	1	3

Let $x = (e_1, \ldots, e_5) \in A$. Then $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$ and $e_4 \overset{\mathfrak{q}_2}{\longmapsto} 1$, hence $e_3 \in \langle -x_2, y_2, y_3\rangle$ and $e_4 \in \langle y_2x_3, -y_3\rangle$. From $\mathfrak{q}_3$-adic info we see $e_3 \in \langle -x_2, y_2\rangle$, and from $\mathfrak{p}_2$-adic and $\mathfrak{p}_3$-adic information we obtain $e_2 \in \langle -y_2, -y_3\rangle$ and $e_5 \in \langle -1, y_3\rangle$.
Then e_2 and e_4 map $\mathfrak{q}_2$-adically into $\langle 2, 3\rangle$, while $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -2, 3\rangle$ and

$\mathrm{im}_{\mathfrak{q}_2}(e_5) \subset \langle -1, 3\rangle$, which results in the fact that $\mathrm{im}_{\mathfrak{q}_2}(x)$ is contained in the span of

$$\begin{matrix} 6 & 3 & -2 & 1 & -1 \\ 3 & 2 & 3 & 6 & 3 \end{matrix}$$

This forces $e_4 \in \langle -y_2x_3y_3\rangle$, which forces $\mathrm{im}_{\mathfrak{p}_3}(x)$ in the span of

$$\begin{matrix} 3 & -1 & 1 & 3 & -1 \\ 1 & -1 & 1 & 1 & -1 \end{matrix}$$

and $\mathrm{im}_{\mathfrak{q}_3}(x)$ in the span of

$$\begin{matrix} -3 & -1 & 1 & -3 & -1 \\ 1 & 3 & -1 & 1 & -3 \\ 1 & -3 & -1 & 1 & 3 \end{matrix}$$

Combining the local images at $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{q}_3$ we obtain $e_1 \in \langle -x_2y_2x_3, y_2y_3\rangle$. This maps $\mathfrak{q}_2$-adically into $\langle 2\rangle$, hence $\mathrm{im}_{\mathfrak{q}_2}(x)$ is in the span of $(2, 6, -6, 6, -3)$, which forces $e_2 \in \langle -y_2\rangle$, $e_3 \in \langle y_2$ and $e_5 \in \langle y_3\rangle$. From e_3 we see that $\mathrm{im}_{\mathfrak{p}_2}(x)$ is in the span of $(3, 1, -3, 1, -1)$, which forces $e_2 = 1$, hence $\mathrm{im}_{\mathfrak{q}_2}(x)$ is trivial, which then also forces $e_3 = e_5 = 1$, and also $e_4 = 1$. We conclude that $A = 0$.

Collecting the results from the four cases we obtain the following.

$\mathrm{im}_{\mathfrak{q}_2}(x_2)$	$\mathrm{im}_{\mathfrak{p}_2}(x_3)$	$\dim_{\mathbb{F}_2} S^2(J/K)$	additional generators
1	1	6	$(1, y_3, x_2, 1, x_2y_3), (y_2x_3, y_2, 1, y_2x_3, y_2)$
1	-3	6	$(-y_2y_3, y_2, 1, -y_2y_3, y_2), (1, -y_3, y_2, 1, -y_2y_3)$
-3	1	4	none
-3	-3	4	none

Proposition 3.4.2. *For the $\mathbb{F}_2$-dimension of $S^2(J/\mathbb{Q}(\sqrt{-p}))$ for $p \equiv 23 \bmod 24$ we have*

$$\dim_{\mathbb{F}_2} S^2(J/\mathbb{Q}(\sqrt{-p})) = \begin{cases} 6 & \text{if } p \equiv 15 \bmod 16 \\ 4 & \text{if } p \equiv 7 \bmod 16 \end{cases}$$

Proof. From the calculation we see that $\dim_{\mathbb{F}_2}(S^2(J/K)) = 6$ if and only if $\mathrm{im}_{\mathfrak{q}_2}(x_2) = 1$, which happens precisely when $\mathfrak{q}_2$ splits in $K(\sqrt{x_2})$, or when $(e_2, f_2, g_2) = (2, 1, 4)$ in the normal closure L of $K(\sqrt{x_2})/\mathbb{Q}$, which is $K(\sqrt{x_2}, \sqrt{2})$. Letting $K' = \mathbb{Q}(\sqrt{2})$, we see that L is also the normal closure of $K'(\sqrt{\gamma})/\mathbb{Q}$, where γ is an element of norm $\overline{-p} \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. Let $\mathfrak{p}$ be the prime of K' with $\mathrm{ord}_{\mathfrak{p}}(\gamma)$ odd, and let $\mathfrak{p}_2' = (\sqrt{2})$ the prime over 2 of K'. Then we see that $(e_2, f_2, g_2) = (2, 1, 4)$ in $L/\mathbb{Q}$ precisely when $\mathfrak{p}_2$ splits in $K'(\sqrt{\gamma})$. Let $\varepsilon = 1+\sqrt{2}$, which is a fundamental unit of K'. Then $\varepsilon\sqrt{2}$ is a totally positive generator for $\mathfrak{p}_2'$, hence in the product formula for Hilbert symbols

$$1 = \prod_{\mathfrak{q}} (\varepsilon\sqrt{2}, \gamma)_{\mathfrak{q}}$$

we see that the factors corresponding to the infinite primes vanish, and we end up with

$$(\varepsilon\sqrt{2},\gamma)_{\mathfrak{p}_2'} = (\gamma,\varepsilon\sqrt{2})_{\mathfrak{p}}.$$

It follows that $\mathfrak{p}_2'$ splits in $K'(\sqrt{\gamma})$ precisely when $\mathfrak{p}$ splits in $E = K'(\sqrt{\varepsilon\sqrt{2}})$. As $E/\mathbb{Q}$ is Galois (note that $\varepsilon\sqrt{2}$ has norm 2, which is already a square in K'), it is abelian, of degree 4, and only ramified over 2. As it is also totally real one quickly sees with Kronecker-Weber that $E = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$. We see that $\mathfrak{p}$ splits in E if and only if p splits completely in E, which happens precisely when $p \equiv \pm 1 \bmod 16$. As $p \not\equiv 1 \bmod 16$ we see that p splits in E if and only if $p \equiv 15 \bmod 16$, which proves the result. □

Corollary 3.4.3. *Let $p \equiv 23 \bmod 48$ be a prime. Then for the Jacobian J_p of the hyperelliptic curve defined by $y^2 = x(x^2 - p^2)(x^2 - 4p^2)$ we have*

$$\operatorname{rank}(J_p/\mathbb{Q}) = 0, \quad Ш(J_p/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2.$$

Proof. We have $\operatorname{rank}(J_p/\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(J_p/\mathbb{Q})[2] = 2$ from equation (3.1). With equation 3.9 and proposition 3.4.2 we see $\operatorname{rank}(J_p/\mathbb{Q}) = \operatorname{rank}(J/\mathbb{Q}(\sqrt{-p})) = 0$, hence the result. □

3.4.3 $J/\mathbb{Q}(\sqrt{p})$ for $p \equiv 17 \bmod 24$

Let $K = \mathbb{Q}(\sqrt{p})$ for $p \equiv 17 \bmod 24$. Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$ be the real embeddings, chosen in some order. Take a fundamental unit ε with $\sigma_1(\varepsilon) > 0$. Then as $\varepsilon\bar{\varepsilon} = -1$, there is exactly one prime $\mathfrak{p}_2$ over 2 in K that is unramified in $K(\sqrt{\varepsilon})$. Let $\mathfrak{q}_2$ be the other prime over 2. If k is the order of $\mathfrak{p}_2$ (or $\mathfrak{q}_2$) in Cl_K, we have $\mathfrak{p}_2^k = (x_2)$ for some $x_2 \in \mathcal{O}_K$. After multiplication by ε if necessary, we may assume that x_2 has positive norm, whence $x_2 y_2 = 2^k$, with y_2 the conjugate of x_2. We may also multiply x_2 with -1 if necessary so that $\mathfrak{q}_2$ is unramified in $K(\sqrt{x_2})$.
If $\mathfrak{p}_3 = (3)$ we have $S = \{\mathfrak{p}_2, \mathfrak{q}_2, \mathfrak{p}_3, \sigma_1, \sigma_\}$ and $K(S) = \langle -1, \varepsilon, x_2, y_2, 3\rangle$. With lemma 3.3.1 for the entries at $\mathfrak{p}_3$ we have the following table.

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	σ_1	σ_2
-1	-1	-1	1	-1	-1
ε			r	1	-1
x_2			r		
y_2			r		
3	3	3	3	1	1

We apply the product formula again to find a relation:

$$\begin{aligned} 1 = \prod_{\mathfrak{q}} (\varepsilon, x_2)_{\mathfrak{q}} &= (x_2,\varepsilon)_{\mathfrak{p}_2}(\varepsilon,x_2)_{\mathfrak{q}_2}(\varepsilon,x_2)_{\sigma_1}(\varepsilon,x_2)_{\sigma_2} \\ &= (x_2,\varepsilon)_{\mathfrak{p}_2}(\varepsilon,x_2)_{\sigma_2}. \end{aligned}$$

It follows that $\sigma_2(x_2) > 0$ if and only if $\varepsilon \overset{\mathfrak{p}_2}{\longmapsto} 1$. There are now four cases, based on $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon), \mathrm{im}_{\mathfrak{p}_2}(y_2) \in \{1, -3\}$.

To compute the 2-Selmer group, one checks that $S^2(J/K) = A \oplus \mathrm{im}(J(K)[2])$ with

$$A := \{(e_1, \ldots, e_5) \in S^2(J/K) : e_2 \overset{\mathfrak{p}_2}{\longmapsto} 1, e_4 \overset{\sigma_1}{\longmapsto} 1\}.$$

The $\mathfrak{p}_2$-adic image of A is contained in the subspace spanned by

$$\begin{array}{ccccc} 3 & 1 & -3 & 1 & -1 \\ 2 & 1 & 1 & -1 & -2 \\ 3 & 1 & -1 & -1 & 3 \end{array}$$

and the image under σ_1 lands inside the span of $(1, -1, -1, 1, 1)$.

Case (i)

The first case we consider is that $\varepsilon, y_2 \overset{\mathfrak{p}_2}{\longmapsto} 1$.

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	σ_1	σ_2
-1	-1	-1	1	-1	-1
ε	1	-1	r	1	-1
x_2	2	1	r	1	1
y_2	1	2	r	1	1
3	3	3	3	1	1

Let $x = (e_1, \ldots, e_5) \in A$. As $e_2 \overset{\mathfrak{p}_2}{\longmapsto} 1$ we have $e_2 \in \langle \varepsilon, y_2 \rangle$, which immediately implies that $\mathrm{im}_{\sigma_1}(x)$ is trivial, which implies $v_{-1}(e_i) = 0$ for all i. The $\mathfrak{p}_2$-adic image also implies that $v_{x_2}(e_3) = 0$, which combined with $v_{-1}(e_1) = 0$ and $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$ yields $e_3 \in \langle \varepsilon y_2 \rangle$.
As $v_{-1}(e_i) = 0$ for all i we have $\mathrm{im}_{\mathfrak{p}_2}(e_i) \subset \langle 2, 3 \rangle$ for all i, which together with $e_3 \overset{\mathfrak{p}_2}{\longmapsto} 1$ implies that x has trivial $\mathfrak{p}_2$-adic image, which in turn implies that $e_i \in \langle \varepsilon, y_2 \rangle$ for all i. But then $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle -1, 2 \rangle$ for all i, which implies that $\mathrm{im}_{\mathfrak{q}_2}(x)$ lies in the span of

$$\begin{array}{ccccc} 2 & -2 & -2 & 2 & 1 \\ 2 & 1 & 1 & -1 & -2 \end{array}$$

which yields the restrictions

$$\begin{aligned} e_1 &\in \langle y_2 \rangle \\ e_2, e_3, e_5 &\in \langle \varepsilon y_2 \rangle \\ e_4 &\in \langle \varepsilon, y_2 \rangle \end{aligned}$$

As $e_2, e_3, e_5 \overset{\mathfrak{p}_3}{\longmapsto} 1$, and $\mathrm{im}_{\mathfrak{p}_3}(e_1) \subset \langle r \rangle$, we see that $\mathrm{im}_{\mathfrak{p}_3}(x)$ lies in the span of $(r, 1, 1, r, 1)$. One can now quickly see that $(y_2, 1, 1, \varepsilon, \varepsilon y_2) \in A$, so that

a complement for the span of $(y_2, 1, 1, \varepsilon, \varepsilon y_2)$ are those elements with $e_1 = 1$. Setting $e_1 = 1$ in the restrictions above implies that x has trivial $\mathfrak{p}_3$-adic image, whence $e_i \in \langle \varepsilon y_2 \rangle$ for all i. Looking at $\mathrm{im}_{\mathfrak{q}_2}(e_4)$ we see that if $e_4 = 1$, then $\mathrm{im}_{\mathfrak{q}_2}(x)$ is trivial, while if $e_4 = \varepsilon y_2$, then $\mathrm{im}_{\mathfrak{q}_2}(x) = (1, -2, -2, -2, -2)$, which implies that $x = (1, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2)$, which indeed lies in the 2-Selmer group. This proves that A is two-dimensional, with generators $(y_2, 1, 1, \varepsilon, \varepsilon y_2)$ and $(1, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2)$.

Case (ii)

For this case we have $\varepsilon \overset{\mathfrak{p}_2}{\longmapsto} 1$ and $y_2 \overset{\mathfrak{p}_2}{\longmapsto} -3$, which yields

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	σ_1	σ_2
-1	-1	-1	1	-1	-1
ε	1	-1	r	1	-1
x_2	-6	-3	r	1	1
y_2	-3	-6	r	1	1
3	3	3	3	1	1

Let $x = (e_1, \ldots, e_5) \in A$. From σ_1-adic information we have $v_{-1}(e_i) = 0$ for $i \in \{1, 4, 5\}$. Combining this with $\mathfrak{p}_2$-adic information we obtain $e_1 \in \langle \varepsilon, x_2 y_2, 3 \rangle$, $e_2 \in \langle \varepsilon, -y_2 3 \rangle$, $e_3 \in \langle -1, \varepsilon, x_2, 3 \rangle$ and $e_4 \in \langle \varepsilon, y_2 3 \rangle$. From $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -1, 3 \rangle$ and $\mathrm{im}_{\mathfrak{q}_2}(e_4) \subset \langle -1, 2 \rangle$ it follows that $\mathrm{im}_{\mathfrak{q}_2}(x)$ lies in the span of

$$\begin{array}{ccccc} 3 & 1 & -3 & 1 & -1 \\ 1 & -6 & -1 & -2 & -3 \\ 2 & 1 & 1 & -1 & -2 \\ 3 & 1 & -1 & -1 & 3 \end{array}$$

But $e_2 \in \langle \varepsilon, -y_2 3 \rangle$ implies that $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle -1, 2 \rangle$, which forces $e_2 = 1$.
This implies that $\mathrm{im}_{\sigma_1}(x)$ is trivial, and that $\mathrm{im}_{\sigma_2}(x)$ is spanned by $(1, 1, 1, -1, -1)$. In particular, this implies that $v_{-1}(e_i) = v_\varepsilon(e_i) = 0$ for $i \leq 3$, so that $e_1 \in \langle x_2 y_2, 3 \rangle$, $e_3 \in \langle x_2, 3 \rangle$. As $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$ we obtain $e_3 = 1$. From $e_2 = e_3 = 1$ we see that both $\mathrm{im}_{\mathfrak{p}_2}(x)$ and $\mathrm{im}_{\mathfrak{q}_2}(x)$ are contained in the span of $(2, 1, 1, -1, -2)$, which implies $e_1 \in \langle x_2 y_2 \rangle$. We now also see that $\mathrm{im}_{\mathfrak{p}_3}(x)$ is trivial, which in turn implies that $e_4 = 1$, and hence that $\mathrm{im}_{\mathfrak{p}_2}(x)$ is trivial, so that also $e_1 = 1$. It follows that $A = 0$.

Case (iii)

For this case we have $\varepsilon \overset{\mathfrak{p}_2}{\longmapsto} -3$ and $y_2 \overset{\mathfrak{p}_2}{\longmapsto} 1$, which yields

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	σ_1	σ_2
-1	-1	-1	1	-1	-1
ε	-3	3	r	1	-1
x_2	2	1	r	-1	-1
y_2	1	2	r	-1	-1
3	3	3	3	1	1

Let $x = (e_1, \dots, e_5) \in A$. As $\mathrm{im}_{\mathfrak{p}_2}(x)$ and $\mathrm{im}_{\mathfrak{q}_2}(x)$ are contained in $\langle 2, 3\rangle$, we have $e_1 \in \langle x_2, y_2, 3\rangle$. From the $\mathfrak{p}_2$-adic information we further obtain $e_2 \in \langle -\varepsilon 3, y_2\rangle$, and also $v_{x_2}(e_3) = 0$, which combined with $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$ implies that $e_3 \in \langle -1, \varepsilon y_2\rangle$. From $\mathrm{im}_{\mathfrak{p}_2}(e_4) \subset \langle -1\rangle$ we obtain $e_4 \in \langle -1, \varepsilon 3, y_2\rangle$.
From $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle -1, 2\rangle$, $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -1, 6\rangle$ and $\mathrm{im}_{\mathfrak{q}_2}(e_4) \subset \langle -1, 2\rangle$ it follows that $\mathrm{im}_{\mathfrak{q}_2}(x)$ is in the span of

$$\begin{array}{ccccc} 2 & 1 & 1 & -1 & -2 \\ 3 & 1 & -1 & -1 & 3 \\ 6 & -2 & 6 & 2 & -1 \end{array}$$

It follow that $e_2 \in \langle -\varepsilon y_2 3\rangle$, and hence that $\mathrm{im}_{\sigma_1}(x)$ is trivial, which implies that $e_1 \in \langle x_2 y_2, 3\rangle$, $e_3 \in \langle -\varepsilon y_2\rangle$ and $e_4 \in \langle -y_2, \varepsilon 3\rangle$. But then $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -6\rangle$ and $\mathrm{im}_{\mathfrak{q}_2}(e_4) \subset \langle -2\rangle$ implies that $\mathrm{im}_{\mathfrak{q}_2}(x)$ is contained in the span of $(2, -2, -6, -2, -3)$. This then implies that $e_1 \in \langle x_2 y_2\rangle$ and $e_5 \in \langle -\varepsilon, x_2, -3\rangle$.
We now have that $e_1 \overset{\mathfrak{p}_3}{\longmapsto} 1$ and $\mathrm{im}_{\mathfrak{p}_3}(e_2) \subset \langle 3\rangle$, which implies that $\mathrm{im}_{\mathfrak{p}_3}(x)$ is contained in the span of $(1, 3, 1, 1, 3)$, which implies $e_4 = 1$, which implies that $\mathrm{im}_{\mathfrak{q}_2}(x)$ is trivial. This quickly implies that $e_1 = e_2 = e_3 = 1$ as well, which shows that $A = 0$.

Case (iv)

For the last we have $\varepsilon \overset{\mathfrak{p}_2}{\longmapsto} -3$ and $y_2 \overset{\mathfrak{p}_2}{\longrightarrow} -3$, which yields

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	σ_1	σ_2
-1	-1	-1	1	-1	-1
ε	-3	3	r	1	-1
x_2	-6	-3	r	-1	-1
y_2	-3	-6	r	-1	-1
3	3	3	3	1	1

Let $x = (e_1, \dots, e_5) \in A$. As $e_2 \overset{\mathfrak{p}_2}{\longmapsto} 1$ we have $e_2 \in \langle -\varepsilon \cdot 3, \varepsilon y_2\rangle$. Then $e_2 \overset{\sigma_2}{\longmapsto} 1$, which implies that $\mathrm{im}_{\sigma_2}(x)$ is in the span of $(1, 1, 1, -1, -1)$. Combining this with $e_3 \overset{\mathfrak{p}_3}{\longmapsto} 1$ and $v_{x_2}(e_3) = 0$ from the $\mathfrak{p}_2$-adic information, we obtain $e_3 \in \langle \varepsilon y_2\rangle$. It follows that $\mathrm{im}_{\mathfrak{p}_2}(x)$ is contained in the span of $(2, 1, 1, -1, -2)$. Combining this with the $e_1, e_4 \overset{\sigma_1}{\longmapsto} 1$, we obtain $e_1 \in \langle x_2 y_2, -x_2 \cdot 3\rangle$ and $e_4 \in \langle -\varepsilon y_2, \varepsilon \cdot 3\rangle$.
As $\mathrm{im}_{\mathfrak{q}_2}(e_3) \subset \langle -2\rangle$, we see that $\mathrm{im}_{\mathfrak{q}_2}(x)$ lies in the span of

$$\begin{array}{ccccc} 1 & -3 & 1 & -3 & 1 \\ 2 & 1 & 1 & -1 & -2 \\ 3 & 2 & 1 & -6 & -1 \\ 6 & -1 & -2 & -3 & -1 \end{array}$$

From $\mathrm{im}_{\mathfrak{q}_2}(e_1) \subset \langle 2\rangle$, $\mathrm{im}_{\mathfrak{q}_2}(e_2) \subset \langle -1, 2\rangle$ and $\mathrm{im}_{\mathfrak{q}_2}(e_4) \subset \langle 2\rangle$, we in fact see that $\mathrm{im}_{\mathfrak{q}_2}(x)$ lies in the span of $(2, -2, -2, 2, 1)$. In particular this implies that $e_2 \in \langle \varepsilon y_2\rangle$. Because now $\mathrm{im}_{\mathfrak{p}_3}(e_1) \subset \langle \varepsilon \cdot 3\rangle$ and $e_2 \overset{\mathfrak{p}_3}{\longmapsto} 1$, we see that $\mathrm{im}_{\mathfrak{p}_3}(x)$ lies

in the span of $(3r, 1, 1, 3r, 1)$. As e_5 has trivial image under $\mathfrak{q}_2, \mathfrak{p}_3$ and σ_1 we deduce $e_5 \in \langle -\varepsilon x_2 \rangle$. In summary we have the following restrictions:

$$\begin{aligned} e_1 &\in \langle x_2 y_2, -x_2 \cdot 3 \rangle \\ e_2, e_3 &\in \langle \varepsilon y_2 \rangle \\ e_4 &\in \langle -\varepsilon y_2, \varepsilon \cdot 3 \rangle \\ e_5 &\in \langle -\varepsilon x_2 \rangle \end{aligned}$$

We can see that $n_1 := (x_2 y_2, \varepsilon y_2, \varepsilon y_2, -\varepsilon y_2, -\varepsilon x_2) \in A$, so that a complement for $\langle n_1 \rangle$ inside A is obtained by setting $e_2 = 1$. This forces $\mathrm{im}_{\mathfrak{q}_2}(x)$ to be trivial, which implies $e_1 \in \langle -x_2 \cdot 3 \rangle$, $e_3 = 1$, $e_4 \in \langle \varepsilon \cdot 3 \rangle$. As $\prod_i e_i = 1$ it follows that $n_2 = (-x_2 \cdot 3, 1, 1, \varepsilon \cdot 3, -\varepsilon x_2)$ is the only non-trivial possibility, and one checks that indeed $n_2 \in A$. This proves that A is two-dimensional, with generators n_1 and n_2.

Collecting cases, we have the following result of the calculation.

$\mathrm{im}_{\mathfrak{p}_2}(\varepsilon)$	$\mathrm{im}_{\mathfrak{p}_2}(y_2)$	$\dim_{\mathbb{F}_2} S^2(J/K)$	additional generators
1	1	6	$(y_2, 1, 1, \varepsilon, \varepsilon y_2), (1, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2, \varepsilon y_2)$
1	-3	4	none
-3	1	4	none
-3	-3	6	$(x_2 y_2, \varepsilon y_2, \varepsilon y_2, -\varepsilon y_2, -\varepsilon x_2), (-x_2 \cdot 3, 1, 1, \varepsilon \cdot 3, -\varepsilon x_2)$

Proposition 3.4.4. *For the $\mathbb{F}_2$-dimension of $S^2(J/\mathbb{Q}(\sqrt{p}))$, where $p \equiv 17 \bmod 24$ is a prime we have*

$$\dim_{\mathbb{F}_2} S^2(J/\mathbb{Q}(\sqrt{p})) = \begin{cases} 6 & \text{if } p \text{ splits completely in } \mathbb{Q}(\sqrt[4]{2}) \\ 4 & \text{if } p \text{ does not split completely in } \mathbb{Q}(\sqrt[4]{2}) \end{cases}$$

Proof. From the calculation we see that $\dim_{\mathbb{F}_2}(S^2(J/K)) = 6$ if and only if $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon y_2) = 1$, which happens precisely when $\mathfrak{p}_2$ splits in $K(\sqrt{\varepsilon y_2})$. I claim that this happens precisely when p is completely split in $\mathbb{Q}(\sqrt[4]{2})$, which requires a reciprocity argument over $\mathbb{Q}(\sqrt{-2})$.
Noting that εy_2 has norm -2^k for k an odd number, we see that the normal closure of $K(\sqrt{\varepsilon y_2})/\mathbb{Q}$ is obtained by adjoining $\sqrt{-2}$. The element $\sqrt{\varepsilon y_2}$ yields an element of norm $p \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ in $K' := \mathbb{Q}(\sqrt{-2})$, say α, and we see that $\mathfrak{p}_2$ splits in $K(\sqrt{\varepsilon y_2})$ if and only the prime $\mathfrak{p}_2' = (\sqrt{-2})$ of K' splits in $K'(\sqrt{\alpha})$. Now p splits in K' as say $p\mathbb{Z}[\sqrt{-2}] = \mathfrak{pq}$, and without loss of generality we may assume that $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ is odd, so that $\mathrm{ord}_{\mathfrak{q}}(\alpha)$ is even. The product formula now simply reduces to

$$(\sqrt{-2}, \alpha)_{\mathfrak{p}_2'} (\sqrt{-2}, \alpha)_{\mathfrak{p}} = 1,$$

And as $(\sqrt{-2}, \alpha)_{\mathfrak{p}} = (\alpha, \sqrt{-2})_{\mathfrak{p}}$, we see that $\mathfrak{p}_2$ splits in $K'(\sqrt{\alpha})$ if and only if $\mathfrak{p}$ splits in $\mathbb{Q}(\sqrt[4]{-2})$. The normal closures of $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(\sqrt[4]{-2})$ over $\mathbb{Q}$ are the same (both contain ζ_8), which then proves the result. □

Corollary 3.4.5. *Let $p \equiv 17 \bmod 24$ be a prime that does not split completely in $\mathbb{Q}(\sqrt[4]{2})$. Then for the Jacobian J of the hyperelliptic curve defined by $y^2 = x(x^2-p^2)(x^2-4p^2)$ we have*

$$\operatorname{rank}(J/\mathbb{Q}) = 0, \quad Ш(J/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2.$$

Now just as for the case $p \equiv 1 \bmod 24$ and the descent on $E/\mathbb{Q}(\sqrt{2})$, we have the following

Proposition 3.4.6. *We have*

$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24 \text{ and } p \text{ doesn't split completely in } \mathbb{Q}(\sqrt[4]{2})\}}{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24\}} = \frac{1}{2}$$

Proof. Let $K = \mathbb{Q}(\sqrt[4]{2}, \zeta_4)$. Then it is equivalent to prove that

$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24 \text{ and } p \text{ splits completely in } \mathbb{Q}(\sqrt[4]{2})\}}{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24\}} = \frac{1}{2}$$

As $\mathbb{Q}(\zeta_8) \subset K$, we have $p \equiv 1 \bmod 8$ whenever p splits completely in K. Let C consist of the generator of the subgroup of order 2 corresponding to K in the Galois extension $K(\zeta_3)/\mathbb{Q}$. Then $\mathrm{Frob}_p \in C$ means exactly that p splits completely in K, but not in $K(\zeta_3)$, i.e. $p \equiv 2 \mod 3$, i.e. $p \equiv 17 \bmod 24$. It follows that

$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24 \text{ and } p \text{ splits completely in } \mathbb{Q}(\sqrt[4]{2})\}}{\#\{\text{primes } p \le X\}} = \frac{1}{16}.$$

With a similar argument for $\mathbb{Q}(\zeta_{24})$ we obtain

$$\lim_{X\to\infty} \frac{\#\{\text{primes } p \le X : p \equiv 17 \bmod 24\}}{\#\{\text{primes } p \le X\}} = \frac{1}{8},$$

hence taking the quotient of the limits gives the result. □

Corollary 3.4.7. *There are infinitely many primes $p \equiv 17 \bmod 24$ for which the Jacobian J of the hyperelliptic curve defined by $y^2 = x(x^2-p^2)(x^2-4p^2)$ satisfies*

$$\operatorname{rank}(J/\mathbb{Q}) = 0, \quad Ш(J/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

3.4.4 $J/\mathbb{Q}(\sqrt{p})$ for $p \equiv 1 \bmod 24$

Let $K = \mathbb{Q}(\sqrt{p})$ for $p \equiv 1 \mod 24$. As 2 and 3 split in K, we now consider 6 primes. Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$ be the real embeddings, chosen in some order. Take a fundamental unit ε with $\sigma_1(\varepsilon) > 0$. Then as $\varepsilon\bar{\varepsilon} = -1$, there is exactly one prime $\mathfrak{p}_2$ over 2 in K that is unramified in $K(\sqrt{\varepsilon})$. Let $\mathfrak{q}_2$ be the other prime over 2. If k_2 is the order of $\mathfrak{p}_2$ (or $\mathfrak{q}_2$) in Cl_K, we have $\mathfrak{p}_2^{k_2} = (x_2)$ for some $x_2 \in \mathcal{O}_K$. After multiplication by ε if necessary, we may assume that x_2 has positive norm, whence $x_2 y_2 = 2^{k_2}$, with y_2 the conjugate of x_2. We may

also multiply x_2 with -1 if necessary so that $\mathfrak{q}_2$ is unramified in $K(\sqrt{x_2})$.
Let $\mathfrak{p}_3$ be the prime that splits in $K(\sqrt{x_2})$, and let $\mathfrak{q}_3$ be its conjugate. Let $\mathfrak{p}_3^{k_3} = (x_3)$ for $k_3 = \mathrm{ord}([\mathfrak{p}_3])$ and x_3 of positive norm, and multiply x_3 with -1 if necessary so that $\mathfrak{p}_2$ is unramified in $K(\sqrt{x_3})$. If y_3 is the conjugate of x_3, we see that $x_3 y_3 = 3^{k_3}$. Then $S = \{\mathfrak{p}_2, \mathfrak{q}_2, \mathfrak{p}_3, \mathfrak{q}_3, \sigma_1, \sigma_2\}$ and $K(S) = \langle -1, \varepsilon, x_2, y_2, x_3, y_3\rangle$.

We apply the product formula for quadratic Hilbert symbols a few times to find some relevant relations.

a) Just as in the case for $p \equiv 17 \bmod 24$, evaluating $\prod_{\mathfrak{q}}(\varepsilon, x_2)_{\mathfrak{q}} = 1$ implies that $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon) = 1$ if and only if $\sigma_2(x_2) > 0$.

b) As $\mathfrak{q}_2$ is unramified in $K(\sqrt{x_2})$ and x_2 and x_3 both have positive norm we have

$$\begin{aligned} 1 = \prod_{\mathfrak{q}}(x_2, x_3)_{\mathfrak{q}} &= (x_2, x_3)_{\mathfrak{p}_2}(x_3, x_2)_{\mathfrak{q}_2}(x_3, x_2)_{\mathfrak{p}_3}(x_2, x_3)_{\sigma_1}(x_2, x_3)_{\sigma_2} \\ &= (x_2, x_3)_{\mathfrak{p}_2}(x_3, x_2)_{\mathfrak{p}_3}, \end{aligned}$$

As $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are, respectively, unramified in $K(\sqrt{x_3})$ and $K(\sqrt{x_2})$, it follows that $\mathrm{im}_{\mathfrak{p}_2}(x_3) = 1$ if and only if $\mathrm{im}_{\mathfrak{p}_3}(x_2) = 1$. But we have chosen $\mathfrak{p}_3$ such that it splits in $K(\sqrt{x_2})$, i.e. we have $\mathrm{im}_{\mathfrak{p}_3}(x_2) = 1$ and hence also $\mathrm{im}_{\mathfrak{p}_2}(x_3) = 1$.

c) Note that as $\mathfrak{p}_2$ is unramified in $K(\sqrt{x_3})$ we have that $\mathfrak{q}_2$ is unramified $K(\sqrt{-x_3})$. Using in addition that $\mathfrak{p}_2$ is unramified in $K(\sqrt{\varepsilon})$ we have

$$\begin{aligned} 1 = \prod_{\mathfrak{q}}(\varepsilon, -x_3)_{\mathfrak{q}} &= (-x_3, \varepsilon)_{\mathfrak{p}_2}(\varepsilon, -x_3)_{\mathfrak{q}_2}(-x_3, \varepsilon)_{\mathfrak{p}_3}(-x_3, \varepsilon)_{\sigma_1}(-x_3, \varepsilon)_{\sigma_2} \\ &= (-x_3, \varepsilon)_{\mathfrak{p}_3}(-x_3, \varepsilon)_{\sigma_2}. \end{aligned}$$

This implies that $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon) = 1$ if and only if $\sigma_2(x_3) < 0$.

This results in the following table.

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$	σ_1	σ_2
-1	-1	-1	-1	-1	-1	-1
ε					1	-1
x_2			1	-1		
y_2			-1	1		
x_3	1	3				
y_3	3	1				

As $\varepsilon\overline{\varepsilon} = -1$, $x_2 y_2 = 2^{k_2}$ and $x_3 y_3 = 3^{k_3}$, the table can be filled in based on $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon)$, $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon)$, $\mathrm{im}_{\mathfrak{p}_2}(y_2)$ and $\mathrm{im}_{\mathfrak{p}_3}(y_3)$, resulting in sixteen cases. We will however skip the laborious linear algebra of all these cases, and state the result

of the linear algebra in the cases. The results are as follows.

$\mathrm{im}_{\mathfrak{p}_2}(\varepsilon)$	$\mathrm{im}_{\mathfrak{p}_2}(y_2)$	$\mathrm{im}_{\mathfrak{p}_3}(\varepsilon)$	$\mathrm{im}_{\mathfrak{p}_3}(y_3)$	$\dim S^2(J/K)$
1	1	1	1	8
1	1	1	−1	8
1	1	−1	1	4
1	1	−1	−1	4
1	−3	1	1	6
1	−3	1	−1	6
1	−3	−1	1	4
1	−3	−1	−1	4
−3	1	1	1	4
−3	1	1	−1	4
−3	1	−1	1	6
−3	1	−1	−1	6
−3	−3	1	1	6
−3	−3	1	−1	6
−3	−3	−1	1	4
−3	−3	−1	−1	4

We observe that the dimension of $S^2(J/K)$ depends on $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon)$, $\mathrm{im}_{\mathfrak{p}_2}(y_2)$ and $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon)$. To be able to apply Chebotarëv we apply a couple of reciprocity arguments.

Proposition 3.4.8. *The following equivalences hold.*

a) We have $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon y_2) = 1$ *if and only if* p *splits completely in* $\mathbb{Q}(\sqrt[4]{2})$.
b) We have $\mathrm{im}_{\mathfrak{p}_2}(y_2) = 1$ *if and only if* $p \equiv 1 \bmod 16$.
c) We have $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon x_2) = 1$ *if and only if* p *splits completely in* $\mathbb{Q}(\sqrt{1+\sqrt{3}})$.

Proof. The proof of the first is completely contained in the proof of proposition 3.4.4. Although the proof assumes $p \equiv 17 \bmod 24$, only $p \equiv 1 \bmod 8$ is used in the reciprocity argument.
To prove b), note that the normal closure L of $K(\sqrt{y_2})/\mathbb{Q}$ is also the normal closure of $K'(\sqrt{\gamma})/\mathbb{Q}$, where $K' = \mathbb{Q}(\sqrt{2})$ and γ has norm p modulo squares. Thus $\mathrm{im}_{\mathfrak{p}_2}(y_2) = 1$ if and only if $\mathfrak{p}_2' = (\sqrt{2})$ in $K'(\sqrt{\gamma})$. From the product formula

$$1 = \prod_{\mathfrak{q}} (\varepsilon\sqrt{2}, \gamma),$$

where $\varepsilon = 1 + \sqrt{2}$), we then see that $\mathfrak{p}_2'$ splits in $K'(\sqrt{\gamma})$ precisely when p splits completely in $K'(\sqrt{\varepsilon\sqrt{2}}) = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ (recall the proof of proposition 3.4.2). Lastly, and resetting the notations introduced for the proof of b), we note that $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon x_2) = 1$ precisely when 3 splits completely in $K(\sqrt{\varepsilon x_2})$. As with the other argument, symmetry in the normal closure yields that this is equivalent to 3 splitting completely in $K'(\sqrt{\gamma})$, with γ of norm p in $K' = \mathbb{Q}(\sqrt{-2})$, and with the product formula applied to γ and $\beta = 1 + \sqrt{-2}$ (note that β generates

a prime over 3), we see that this is equivalent to p splitting completely in $\mathbb{Q}(\sqrt{1+\sqrt{-2}})$. This field has the same normal closure over $\mathbb{Q}$ as $\mathbb{Q}(\sqrt{1+\sqrt{3}})$, hence the result. □

Noting that $\mathrm{im}_{\mathfrak{p}_3}(\varepsilon x_2) = \mathrm{im}_{\mathfrak{p}_3}(\varepsilon)) = 1$, we obtain.

Corollary 3.4.9. *Let $p \equiv 1 \bmod 24$. Then the size of $S^2(J/K)$ depends on the splitting behaviour of p as in the following table. A yes or no indicates whether the prime p splits completely in the corresponding field or not.*

$\mathbb{Q}(\zeta_{16})$	$\mathbb{Q}(\sqrt[4]{2})$	$\mathbb{Q}(\sqrt{1+\sqrt{3}})$	$\dim S^2(J/K)$
yes	*yes*	*yes*	8
yes	*yes*	*no*	4
yes	*no*	*yes*	4
yes	*no*	*no*	6
no	*yes*	*yes*	6
no	*yes*	*no*	4
no	*no*	*yes*	6
no	*no*	*no*	4

Applying Chebotarëv to the compositum $\mathbb{Q}(\zeta_{16}), \sqrt[4]{2}, \sqrt{1+\sqrt{3}})$ we obtain

Corollary 3.4.10. *We have*

$$\lim_{X\to\infty} \frac{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24 \textit{ and } \dim S^2(J/K) = 4\}}{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24\}} = \frac{1}{2}$$
$$\lim_{X\to\infty} \frac{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24 \textit{ and } \dim S^2(J/K) = 6\}}{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24\}} = \frac{3}{8}$$
$$\lim_{X\to\infty} \frac{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24 \textit{ and } \dim S^2(J/K) = 8\}}{\#\{\textit{primes } p \le X : p \equiv 1 \bmod 24\}} = \frac{1}{8}$$

Corollary 3.4.11. *There are infinitely many primes $p \equiv 1 \bmod 24$ for which the Jacobian J of the hyperelliptic curve defined by $y^2 = x(x^2-p^2)(x^2-4p^2)$ satisfies*

$$\mathrm{rank}(J/\mathbb{Q}) = 0, \quad Ш(J/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

3.5 Positive rank

Let $p \neq 2, 3$ be a prime and let J be the Jacobian of the hyperelliptic curve C defined by the equation

$$y^2 = x(x^2-p^2)(x^2-4p^2).$$

In this section we mention some results about positive rank on the curve for specific primes.

When $p \equiv 3, 5 \bmod 8$ we have seen that conjecturally (that is assuming finiteness of $Ш(J/\mathbb{Q})$), we have $\text{rank}(J/\mathbb{Q}) = 1$. For specific primes, Magma can find $K = \mathbb{Q}(\sqrt{2})$-rational points on the elliptic curve E defined by

$$y^2 = (x^2 - 9p^2)(x - 2\sqrt{2}p)$$

more efficiently then on $J(\mathbb{Q})$, but points of infinite order quickly become large. For example, already for $p = 19$ we have the following point of infinite order on $E(K)$

$$\left(\frac{-113850191446377-12254855228512\sqrt{2}}{305005^2}, \frac{-6999941561804396202 08+46134034860568410 6100\sqrt{2}}{305005^3}\right).$$

In the cases $p \equiv 1, 17, 23 \bmod 24$, we can in principle have rank 2, and even rank 4 for $p \equiv 1 \bmod 24$.

Let us focus on the case $p \equiv 1 \bmod 24$, which is the only prime $p \equiv 1 \bmod 24$ for which the author could prove unconditionally a positive rank. $\text{rank}(E/K)$. After many hours of searching, MAGMA was able to find two independent points of infinite order on $E(K)$ for $p = 241$. The x-coordinates of the points are

$$\frac{-3430098882\sqrt{2} - 478517032600}{670758201}$$
$$\frac{295126964042354\sqrt{2} + 1104228958035051}{913222065800}$$

One can use these points to construct points of infinite order on $J(\mathbb{Q})$ following the proof of $\text{rank}(J/\mathbb{Q}) = \text{rank}(E/K)$. It is interesting to note that in this case, the map α preceeding 3.3.10 is indeed surjective.
Even more curious, is the for many of the primes $p \equiv 1 \bmod 24$ at most 10000 for which $\text{rank}(J/\mathbb{Q})$ can be 4 according to the descents, MAGMA can relatively quickly find 1 or 2 points of infinite order, but *all* of points these points map into $\ker(\beta)$.

Chapter 4

Comments

4.1 Redei symbols

In the thesis there are various reciprocity arguments involved over quadratic number fields. Recently, P. Stevenhagen proved a very flexible reciprocity law concerning Redei symbols, see [15]. We briefly explain the connection with the thesis here.
Given $a, b, c \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ all with relatively co-prime quadratic Hilbert symbols

$$(a, b)_p = (a, c)_p = (b, c)_p = 1, \quad \text{for all primes } p$$

there is a tri-linear symbol $[a, b, c]$ taking values in $\{\pm 1\}$. The first two arguments are used to construct a quadratic extension of $\mathbb{Q}(\sqrt{ab})$, by adjoining to $\mathbb{Q}(\sqrt{a})$ the square root of an element β of norm b modulo-squares (whose existence is guarenteed by the condition $(a, b)_p = 1$ by Hasse-Minkowski). This gives a cyclic extension of $\mathbb{Q}(\sqrt{ab})$ of degree 4, which is dihedral over $\mathbb{Q}$ when $a \neq b$. The argument c then defines an Artin symbol in the extension based on its prime divisors and its sign, thus encoding splitting behaviour of D_4 extensions (and sometimes 'simply' quartic abelian extensions) of $\mathbb{Q}$.

The Redei symbols satisfy a wonderful reciprocity law, namely that the symbol $[a, b, c]$ is symmetric in all permutations of its arguments. The symmetry of a and b reflects the symmetry of D_4-extensions that we have seen at numerous occasions in this thesis, but the symmetry $[a, b, c] = [a, c, b]$ is a true reciprocity, and is proven by invoking the product formula for quadratic Hilbert symbols in $\mathbb{Q}(\sqrt{a})$.
A lot of the reciprocity arguments proven in this thesis are special cases of this Redei reciprocity. For example, proposition 3.4.8 can be interpreted by the

equalities

$$[p,-2,2]=[2,-2,p],$$
$$[p,2,2]=[2,2,p],$$
$$[p,-3,2]=[3,-2,p].$$

Similarly, the content of lemma 3.3.4 can be restated as the equality $[2,p,p]=[2,-2,p]$ of Redei symbols. In fact the proof of the lemma is done in two steps, first the equality

$$[2,p,p]=[p,2,p]=[p,p,2]$$

is shown, and then with a 'quartic reciprocity' over $\mathbb{Q}$ we see $[p,p,2]=[2,-2,p]$. We note however that some reciprocity arguments of this thesis can not (directly) be equated to a Redei reciprocity. For example in the preparation of the 2-descent on $J/\mathbb{Q}(\sqrt{-p})$ for $p\equiv 23 \bmod 24$, we use the product formula over $\mathbb{Q}(\sqrt{-p})$ on elements of norm 2 and 3, respectively, modulo squares. One might think of this as '$[-p,2,3]=[-p,3,2]$', but this symbol is not well-defined. The reason is that $\mathbb{Q}(\sqrt{2},\sqrt{3})$ cannot be extended to a D_4-extension as required for the Redei symbols: note for example that $\mathbb{Q}(\sqrt{2})$ has no element of norm 3.

4.2 Connection between 4-descent and 2-descent of twists?

With MAGMA one can obtain 4-descent information on Elliptic curves over number fields. It appears to be the case that performing a 4-descent on $E_p/\mathbb{Q}(\sqrt{2})$ yields *exactly* the same rank bounds as those we have obtained by 2-descents on both $J/\mathbb{Q}(\sqrt{p})$ and $J/\mathbb{Q}(\sqrt{-p})$. It is unclear to the author whether there is some theoretical relationship between these two, or if it can be reasonably thought of as a coincidence because the relevant governing fields happen to yield the same information.

Appendix A

Some number theory

A.1 S-integers

Throughout this section, will will call a finite prime of a number field K simply a prime. Let S be a possible empty, finite set of primes of K. The subring of K defined by

$$R_S := \{x \in K : \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\} = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{K,\mathfrak{p}}$$

is called the ring of S-integers. Note that the unit group R_S^* consists of those $x \in K^*$ with $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. In particular, taking $S = \emptyset$ we obtain the ordinary unit group $\mathcal{O}_K^*$.

Lemma A.1.1. *The ring of S-integers R_S equals $\Sigma^{-1}\mathcal{O}_K$ for $\Sigma = \mathcal{O}_K \setminus \bigcup_{\mathfrak{p} \notin S} \mathfrak{p}$.*

Proof. Since $\Sigma = \bigcap_{\mathfrak{p} \notin S}(\mathcal{O}_K \setminus \mathfrak{p})$ it is clear that Σ is a multiplicative set. Moreover, $s \in \mathcal{O}_K \setminus \mathfrak{p}$ for a prime $\mathfrak{p}$ means that $\mathrm{ord}_{\mathfrak{p}}(s) = 0$. This implies that also $\mathrm{ord}_{\mathfrak{p}}(s^{-1}) = 0$ for all those $\mathfrak{p}$, whence the inclusion $\Sigma^{-1}\mathcal{O}_K \subset R_S$.
The reverse inclusion is non-trivial and uses the finiteness of the class group. Let $x \in R_S$ and fix some $\mathfrak{p} \in S$. As some power of $\mathfrak{p}$ is principal, there exists $s_{\mathfrak{p}} \in K^*$ with $\mathrm{ord}_{\mathfrak{q}}(s_{\mathfrak{p}}) = 0$ if $\mathfrak{q} \neq \mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(s_{\mathfrak{p}}) > 0$. Replacing $s_{\mathfrak{p}}$ with a suitable power if necessary, we may assume that $\mathrm{ord}_{\mathfrak{p}}(s_{\mathfrak{p}}) \geq -\mathrm{ord}_{\mathfrak{p}}(x)$, so that $\mathrm{ord}_{\mathfrak{p}}(s_{\mathfrak{p}}x) \geq 0$. It is then clear that $sx \in \mathcal{O}_K$ for $s = \prod_{\mathfrak{p} \in S} s_{\mathfrak{p}} \in \Sigma$, proving the inclusion $R_S \subset \Sigma^{-1}\mathcal{O}_K$. □

Corollary A.1.2. *The ring of S-units R_S is a Dedekind domain, and the association $\mathfrak{p} \mapsto \mathfrak{p}R_S$ gives a bijective correspondence between the primes of K not in S and the primes of R_S.*

Proof. The statement about the primes of R_S follows as a prime $\mathfrak{p} \in S$ meets Σ, and prime $\mathfrak{p} \notin S$ does not meet Σ: if $\mathfrak{p} \in S$ and $\mathfrak{p}^k = (x)$ then $x \in \mathfrak{p} \cap \Sigma$, while if $\mathfrak{p} \notin S$ then we have $\mathcal{O}_K \subset R_S \subset \mathcal{O}_{K,\mathfrak{p}}$, so that $\mathfrak{p}R_S \neq R_S$ as $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \neq \mathcal{O}_{K,\mathfrak{p}}$,

hence $\mathfrak{p}$ cannot meet Σ.

We also see from this that $\mathcal{O}_{K,\mathfrak{p}}$ is the localisation of R_S at the prime $\mathfrak{p}R_S$, hence R_S is everywhere locally a DVR. As R_S is a localisation of $\mathcal{O}_K$ we see that R_S is also Noetherian and of dimension at most 1. As K has infinitely many primes we cannot have dimension 0, so R_S is a Dedekind domain. □

Knowing that R_S is a Dedekind domain, we can study its class group.

Lemma A.1.3. *Extension of ideals along the natural map $\mathcal{O}_K \to R_S$ induces a surjection $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(R_S)$ with kernel generated by the classes of the primes in S.*

Proof. Consider the following commutative diagram of abelian groups.

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & K^* & \xrightarrow{\mathrm{id}} & K^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \langle S \rangle & \longrightarrow & \mathcal{I}(\mathcal{O}_K) & \longrightarrow & \mathcal{I}(R_S) & \longrightarrow & 0 \end{array}$$

Here $\langle S \rangle$ is the subgroup of $\mathcal{I}(\mathcal{O}_K)$ generated by S, and the two rightmost vertical maps send an $x \in K^*$ respectively to the fractional $\mathcal{O}_K$-ideal or the fractional R_S-ideal generated by x.
The bottom row is exact because the primes of K form a $\mathbb{Z}$-basis for $\mathcal{I}(\mathcal{O}_K)$ and $\{\mathfrak{p}R_S : \mathfrak{p} \notin S\}$ is a $\mathbb{Z}$-basis for $\mathcal{I}(R_S)$. Applying the snake lemma yields the following long exact sequence

$$0 \to \mathcal{O}_K^* \to R_S^* \to \bigoplus_{\mathfrak{p} \in S} \mathbb{Z} \xrightarrow{\psi} \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(R_S) \to 0, \tag{A.1}$$

where ψ maps the generator corresponding to $\mathfrak{p} \in S$ to the class $[\mathfrak{p}]$. Exactness of this sequence at the two class groups yield the desired result. □

By counting free ranks in the long exact sequence (A.1) we also obtain

Corollary A.1.4. *If r is the free rank of the unit group $\mathcal{O}_K^*$, then R_S^* has free rank $r + |S|$.*

A.2 Some number theory

Throughout, $K = \mathbb{Q}(\sqrt{d})$ is a quadratic number field, with class group Cl_K of order h_K and narrow class group Cl_K^+ of order h_K^+, i.e. the ray class group $Cl_{\mathfrak{f}}$ for $\mathfrak{f}$ consisting of the real primes of K. It is the ideal group of K with the quotient by all principal ideals that admit a generator of positive norm. There is an exact sequence

$$0 \to [(\sqrt{d})] \to Cl_K^+ \to Cl_K \to 0 \tag{A.2}$$

as $\sqrt{d}$ has sign 1 or -1 depending on the real embeddings for K real. The class $[(\sqrt{d})]$ is trivial when K is complex or K is real with fundamental unit of norm -1. If K is real with fundamental unit of norm 1 then $[(\sqrt{d})]$ has order 2 and Cl_K^+ has order $2h_K$.

Lemma A.2.1. *Let H^+ be the narrow Hilbert class field of K. Then $H^+/\mathbb{Q}$ is Galois with group fitting in the exact sequence*

$$0 \to Cl_K^+ \to \mathrm{Gal}(H^+/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 0. \tag{A.3}$$

Moreover, this sequence is split, with the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ *acting on Cl_K^+ by inversion.*

Proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ then $\sigma(H^+)$ is an Abelian extension of K that is unramified at all finite primes of K. As H^+ is the maximal Abelian extension with this property we must have $\sigma(H^+) \subset H^+$, hence we see that $H^+/\mathbb{Q}$ is Galois. The exact sequence then follows from the Artin isomorphism $Cl_K^+ \xrightarrow{\sim} \mathrm{Gal}(H^+/K)$.

For the splitting of the sequence, choose primes $\mathfrak{B}|\mathfrak{p}|p$ in $H^+/K/\mathbb{Q}$ with $e(\mathfrak{p}|p) = 2$. The inertia group $I_{\mathfrak{B}/p}$ has order 2 as $\mathfrak{p}$ is unramified in H^+, and since K is not contained in the corresponding inertia field $T_{\mathfrak{p}/p}$ we have that $I_{\mathfrak{B}/p}$ does not fix K, so mapping $\mathrm{Gal}(K/\mathbb{Q})$ onto $I_{\mathfrak{B}/p}$ yields a section of the surjection in (A.3).
Letting $I_{\mathfrak{B}/p} = \langle\sigma\rangle$ and noting that $\sigma\mathrm{Frob}_{\mathfrak{q}}\sigma = \mathrm{Frob}_{\sigma\mathfrak{q}}$ for primes $\mathfrak{q}$ of K, and that σ restricts to the non-trivial automorphism in $\mathrm{Gal}(K/\mathbb{Q})$, we see that that the action of $\mathrm{Gal}(K/\mathbb{Q})$ on Cl_K^+ induced by the section coincides with the natural action. Furthermore, the non-trivial automorphism of K acts by inversion because the ideal $p\mathcal{O}_K$ for any rational prime p is trivial in Cl_K^+. □

Remark A.2.2. Similarly one can show that a ray class field $H_{\mathfrak{f}}$ for a cycle $\mathfrak{f}$ in K is Galois over $\mathbb{Q}$ provided that $\mathfrak{f}$ is $\mathrm{Gal}(K/\mathbb{Q})$-invariant, and the argument that the resulting exact sequence splits still works provided that there exist primes $\mathfrak{B}|\mathfrak{p}|p$ in $H_{\mathfrak{f}}/K/\mathbb{Q}$ with $(e_{\mathfrak{B}/\mathfrak{p}}, e_{\mathfrak{p}/p}) = (1, 2)$. When such primes do not exist the sequence need not split, a simple counterexample is obtained taking $K = \mathbb{Q}(\sqrt{2})$ and $\mathfrak{f} = \mathfrak{p}_2^4$: in that case $0 \to Cl_{\mathfrak{f}} \to \mathrm{Gal}(H_{\mathfrak{f}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 0$ does not split as $H_{\mathfrak{f}} = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ is cyclic over $\mathbb{Q}$.

Corollary A.2.3. *If E/K is an Abelian extension unramified at all finite primes of K, then $E/\mathbb{Q}$ is Galois.*

Proof. We have $K \subset E \subset H^+$ with $\mathrm{Gal}(H^+/\mathbb{Q}) \cong Cl_K^+ \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$, where $\overline{1}$ acts by inversion on Cl_K^+. Then E corresponds with a subgroup contained in Cl_K^+, which is necessarily normal because it is stable under inversion. □

For an odd prime p we write $p^* = (-1)^{(p-1)/2}p$.

Proposition A.2.4. *Let p be an odd prime and let $K = \mathbb{Q}(\sqrt{p^*})$. Then K has odd class number, when K is real, has a fundamental unit of norm of -1.*

Proof. Let H^+ be the narrow Hilbert class field of K. As $h_K^+ = 2h_K$ when K is real with a fundamental unit of norm 1, the result follows by proving that h_K^+ is odd. If it is even, then H^+/K contains an intermediate field E that is quadratic over K, which is Galois over $\mathbb{Q}$ by corollary A.2.3. As $[E : \mathbb{Q}] = 4$ it is Abelian, and with Kronecker-Weber we see that $E \subset \mathbb{Q}(\zeta_p)$, which contradicts that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is totally ramified over p. □

Appendix B

Corrections to van der Heiden

This goal of this Appendix is to give a corrected version of [5, § 4.2]. To verify the computations of this appendix the reader is assumed to have a copy of the thesis as almost all the tables used for the calculation are correct, and those will not be copied here. All the tabels up to par 4.2 are correct, but inside the paragraph some are not.

For the computation one notices that there is a surjection $S^2(J/\mathbb{Q}) \to \langle 2,3,q\rangle$ by projection onto the first coordinate. Surjectivity follows as the 2-torsion yields elements in the Selmer group and the first coordinate is positive by local considerations for the archimedian place. This reduces the study of the Selmer group to the study of the kernel S_1^2 of this map, which must contain a one-dimensional subspace as the 2-torsions yields a four-dimensional subspace of the Selmergroup. This done in the first paragraph of section 4.2: from the 2-torsion we also obtain $m_1 = (1, -2q, -2, -2, -2q) \in S_1^2$.

The mistake v.d. Heiden makes is that he removes all local images of m_1 from consideration, which is of course not valid: one can have elements in S_1^2 not equal to m_1 but having the same local image as m_1 for some prime.
One notices that for each case $q \neq 2, 3$, the projection onto the last coordinate of the 2-adic image is 1 or 2-dimensional, while the 2-adic image of m_1 has non-trivial last coordinate, which allows a direct sum decomposition $S_1^2 = G_1 \oplus \langle m_1\rangle$.

(**i**) $q \equiv 1 \bmod 24$. In this case m_1 maps 2-adically to $y_{2,2}$, which has last coordinate -2. The image of projection onto the last coordinate of this local image is spanned by -2 and -3, so we have $S_1^2 = G_1 \oplus \langle m_1\rangle$ where G_1 consists of $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -3\rangle$.
Now if $x = (1, e_2, \ldots, e_5) \in G_1$, then e_4 maps 3-adically to 1 and hence $e_4 \in \langle -2, q\rangle$. Suppose that $e_4 \in \langle q\rangle$. Then 2-adically we have $e_4 \mapsto 1$, hence x maps 2-adically into the span of $y_{2,1} + y_{2,2}$. As this element has last coordinate

not inside $\langle -3\rangle$, we see that x has trivial 2-adic image. This implies that $e_i \in \langle q\rangle$ for $i = 2, 3, 4, 5$. As the product of the e_i must equal 1 this gives 8 options, all of which give elements of G_1. Three linearly independent elements are:

$$n_1 = (1, 1, 1, q, q)$$
$$n_2 = (1, q, 1, q, 1)$$
$$n_3 = (1, q, q, 1, 1)$$

We have shown that the subgroup of G_1 for which $e_4 \in \langle q\rangle$ has dimension 3. This subgroup maps isomorphically onto $\langle y_{q,1}, y_{q,2}, y_{q,3}\rangle$, hence a complement for this subgroup consists of those elements in G_1 that map q-adically to the identity. For $x = (1, e_2, \ldots, e_5)$ in this complement this forces $e_i \in \langle -1, 2, 3\rangle$ for $i = 2, \ldots 5$. Looking 3-adically we see $e_4 \in \langle -2\rangle$, and looking 2-adically we see that $e_5 \in \langle -3\rangle$. By real considerations, e_4 and e_5 have the same sign so if $e_5 = -3$ also $e_4 = -2$, which implies x maps 2-adically to $y_{2,1}$, and hence forces $(1, e_2, \ldots, e_5) = (1, -6, -1, -2, -3)$, which indeed gives an element in the Selmer group.
If $e_5 = 1$ then also $e_4 = 1$ and we see that 2-adically $(1, e_2, e_3, 1, 1,)$ maps to the identity, hence it is the identity. This proves the complement is one-dimensional and generated by $n_4 = (1, -6, -1, -2, -3)$. In conclusion, we see that S_1^2 has dimension 5, so the Selmer group has dimension 8 with generators $\{m_1, m_2, m_3, m_q, n_1, n_2, n_3, n_4\}$.

(**ii**) $q \equiv 5 \bmod 24$. As $q \equiv -3 \bmod 8$ we see that in this case the last coordinate of m_1 maps 2-adically to 6, and hence $S_1^2 = G_1 \oplus \langle m_1\rangle$ where G_1 consists of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -2\rangle$. Let $x = (1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -2, -3q\rangle$. As e_3 and e_4 map 3-adically to 1 we have $e_3, e_4 \in \langle -2, -q\rangle$. As e_3 maps 2-adically into $\langle -6\rangle$ we obtain $e_3 \in \langle 2q\rangle$. Suppose that $e_3 = 2q$. Then x maps q-adically to $(1, q, 2q, 2q, q)$. This together with $e_4 \in \langle -2, -q\rangle$ and $e_5 \in \langle -2, -3q\rangle$ forces $e_4 = 2q$ and $e_5 = 6q$. As the coordinates multiply to 1 we obtain $e_2 = 6q$ also, and one sees that $n_1 = (1, 6q, 2q, 2q, 6q) \in G_1$. A complement inside G_1 for the subgroup generated by n_1 is the subgroup of those elements with $e_3 = 1$. Such elements map q-adically to the identity, so we have $e_i \in \langle -1, 6\rangle$ for $i = 2, 4, 5$. As e_4 maps 3-adically to 1 we obtain $e_4 = 1$ as well, and as $e_5 \in \langle -2, -3q\rangle$ we also obtain $e_5 = 1$, and hence $e_2 = 1$.
We conclude that this complement is trivial and that $\dim(S^2(J/\mathbb{Q})) = 5$, with generators being $\{m_1, m_2, m_3, m_q, n_1\}$.

(**iii**) $q \equiv 7 \bmod 24$. In this case the subspace of the 2-adic image with first coordinate 1 is different from what van der Heiden claims, the correct one is as follows.

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

The last coordinate of m_1 maps 2-adically to 2, and hence $S_1^2 = G_1 \oplus \langle m_1\rangle$ where

G_1 consists of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 has trivial 2-adic image. Suppose that $x = (1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -q \rangle$, which forces the 3-adic image of x to lie in the span of $(1, -1, 1, 1, -1)$, which implies $e_3, e_4 \in \langle -2, q \rangle$. Looking 2-adically we see that $e_3 = e_4 = 1$. This forces the q-adic image of x to be trivial, hence from $e_2 = e_5 \in \langle -q \rangle$ we see that also $e_2 = e_5 = 1$. Thus $G_1 = \langle m_1 \rangle$ and the 2-Selmer group has dimension 4.

(**iv**) $q \equiv 11 \bmod 24$. The last coordinate of m_1 maps 2-adically to -6, hence $S_1^2 = G_1 \oplus \langle m_1 \rangle$ for G_1 consisting of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -3 \rangle$. Let $(1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -3, -q \rangle$. From 3-adic image we see $e_3, e_4 \in \langle -2, -q \rangle$. As e_3 maps 2-adically into $\langle -3 \rangle$, we see that $e_3 \in \langle -q$, but then the q-adic image forces $e_3 = 1$. From the q-adic image we also see $e_4 \in \langle -2 \rangle$, but then the 2-adic image forces $e_4 = 1$ as well. But then the 2-adic image is trivial, so that $e_2 = e_5 \in \langle 3q \rangle$, and one checks that indeed $n_1 = (1, 3q, 1, 1, 3q) \in G_1$, so that the 2-Selmer group has dimension 5.

(**v**) $q \equiv 13 \bmod 24$. The last coordinate of m_1 maps 2-adically to 6, hence $S_1^2 = G_1 \oplus \langle m_1 \rangle$ for G_1 consisting of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -2 \rangle$. Let $(1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -2, 6q \rangle$, and looking q-adically reduces this to $e_5 \in \langle 6q \rangle$. From 3-adic and q-adic information we see that $e_3 \in \langle -1, 2 \rangle$, and then 2-adically we see that $e_3 = 1$. But e_5 maps 3-adically into $\langle -1 \rangle$, which forces $e_5 = 1$. The 3-adic image forces $e_2 = e_4 \in \langle -2, q \rangle$, and then 2-adically we get $e_4 \in \langle q \rangle$. We see indeed that $n_1 = (1, q, 1, q, 1) \in G_1$, hence we see that the 2-Selmer group has dimension 5.

(**vi**) $q \equiv 17 \bmod 24$. The last coordinate of m_1 maps 2-adically to -2, hence $S_1^2 = G_1 \oplus \langle m_1 \rangle$ for G_1 consisting of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -3 \rangle$. Let $x = (1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -3, q \rangle$. Now e_4 has trivial 3-adic and q-adic image, which forces $e_4 \in \langle -2 \rangle$, and also that the 2-adic image of x is spanned by $y_{2,1} = (1, -6, -1, -2, -3)$. As e_3 has trivial 3-adic image we see $e_3 \in \langle -2, -q \rangle$, which reduces to $e_3 \in \langle -q \rangle$ from the 2-adic image. We also see that $e_2 \in \langle -6, q \rangle$ by the 2-adic image.
We see that $n_1 = (1, -6, -q, -2, -3q)$ maps 2-adically to $(1, -6, -1, -2, -3)$ and is an element of G_1, so we obtain a complement of $\langle n_1 \rangle$ inside G_1 by demanding that the 2-adic image is trivial. This forces $e_3 = e_4 = 1$, and $e_2 = e_5 \in \langle q \rangle$. One also sees that $n_2 = (1, q, 1, 1, q) \in G_1$, so $G_1 = \langle n_1, n_2 \rangle$, and the 2-Selmer group has dimension 6.

(**vii**) $q \equiv 19 \bmod 24$. The last coordinate of m_1 maps 2-adically to -6, hence $S_1^2 = G_1 \oplus \langle m_1 \rangle$ for G_1 consisting of those $x = (1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 maps 2-adically into $\langle -3 \rangle$. Let $(1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -3, -q \rangle$. From 2-adic and 3-adic information we see $e_3 \in \langle q \rangle$, from 3-adic information we have $e_4 \in \langle -2, q \rangle$, and then from 2-adic information we see that $e_4 \in \langle -2q \rangle$ and that the 2-adic image of x is contained in the span of $(1, 6, 3, -6, -3)$. This gives $e_2 \in \langle 6, 2q \rangle$. One sees that $n_1 = (1, 2q, q, -2q, -q) \in G_1$, which maps 2-adically to $(1, 6, 3, -6, -3)$, so we obtain a complement of $\langle n_1 \rangle$ inside G_1 by demanding

that the 2-adic image is trivial. This forces $e_3 = e_4 = 1$, and $e_2 \in \langle 3q \rangle$, and looking q-adically we see that also $e_2 = e_5 = 1$, hence $G_1 = \langle n_1 \rangle$ and the 2-Selmer group is 5-dimensional.

(**viii**) $q \equiv 23 \bmod 24$. Similarly as for $q \equiv 7 \bmod 24$, the suspace of the 2-adic image with first coordinate 1 is spanned by

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

The q-adic image from van der Heiden is also incorrect. The correct one is

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

The last coordinate of m_1 maps 2-adically to 2, and hence $S_1^2 = G_1 \oplus \langle m_1 \rangle$ where G_1 consists of those $(1, e_2, \ldots, e_5) \in S_1^2$ for which e_5 has trivial 2-adic image. Suppose that $x = (1, e_2, \ldots, e_5) \in G_1$. Then $e_5 \in \langle -q \rangle$, and from 3-adic information we see $e_3, e_4 \in \langle -2, -q \rangle$. As e_3 and e_4 cannot map 2-adically to -2 we see that $e_3, e_4 \in \langle -q \rangle$, and that x has trivial 2-adic image, i.e. $e_i \in \langle -q \rangle$ also for e_2 and e_5. One checks that $n_1 = (1, -q, -q, 1, 1)$ and $n_2 = (1, 1, 1, -q, -q) \in G_1$, and since the ∞-adic images of n_1 and n_2 span the ∞-image, we obtain a complement inside G_1 of $\langle n_1, n_2 \rangle$ by demanding the ∞-adic image to be trivial. As $e_i \in \langle -q \rangle$ for all i this immediately forces the complement to be trivial, so $G_1 = \langle n_1, n_2 \rangle$ and $S^2(J/\mathbb{Q})$ has dimension 6.

Bibliography

[1] John William Scott Cassels, E Victor Flynn, et al. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Cambridge University Press, 1996.

[2] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall/CRC, 2005.

[3] Claus Diem and N. Naumann. *On the Structure of the Weil Restriction of Abelian Varieties*. 2005. arXiv: `math/0504359 [math.AG]`.

[4] Robin Hartshorne. *Algebraic Geometry. Graduate Texts in Math. 52*. 1977.

[5] Gert-Jan van der Heiden. *Computing the* 2*-descent over* $\mathbb{Q}$ *for curves of genus* 2. `http://fse.studenttheses.ub.rug.nl/8657`. 1998.

[6] Jun-Ichi Igusa. "Arithmetic variety of moduli for genus two". In: *Annals of Mathematics* (1960), pp. 612–649.

[7] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford University Press on Demand, 2002.

[8] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[9] David Mumford. *Abelian Varieties*. Oxford Univesity press, 1985. ISBN: 9780195605280.

[10] Jürgen Neukirch. *Algebraic number theory*. Springer, 1999.

[11] Bjorn Poonen and Michael Stoll. "The Cassels-Tate pairing on polarized abelian varieties". In: *Annals of Mathematics* 150.3 (1999), pp. 1109–1149.

[12] Edward F. Schaefer. "2-descent on the Jacobians of hyperelliptic curves". In: *Journal of number theory* 51.2 (1995), pp. 219–232.

[13] The Stacks project authors. *The Stacks project*. `https://stacks.math.columbia.edu`. 2020.

[14] Peter Stevenhagen. *Local Fields*. `http://websites.math.leidenuniv.nl/algebra/`. Accessed February 2020. 2002.

[15] Peter Stevenhagen. *Redei reciprocity, governing fields, and negative Pell*. 2018. arXiv: `1806.06250 [math.NT]`.

[16] Michael Stoll. "Implementing 2-descent for Jacobians of hyperelliptic curves". eng. In: *Acta Arithmetica* 98.3 (2001), pp. 245–277. URL: `http://eudml.org/doc/279762`.