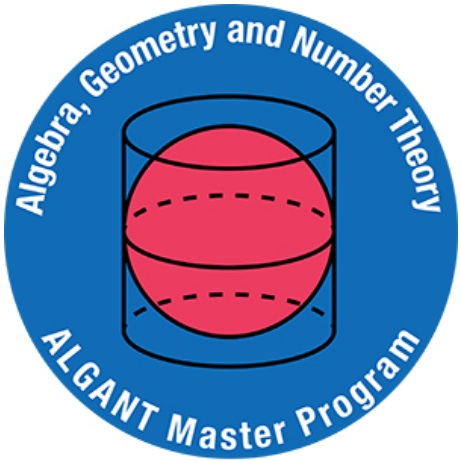


ALGANT Master Thesis in Mathematics

Rank Bounds on Some Hyperelliptic Jacobians

Gürkan Dogan, advised by Richard Griffon

14 June 2018

Universität
Regensburg

Universiteit
Leiden

Contents

Introduction

Let $C/\mathbb{Q}$ be a hyperelliptic curve, given affinely by a model

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

with $f(x) \in \mathbb{Q}[x]$ monic, squarefree and of odd degree. We consider the Jacobian variety $J/\mathbb{Q}$ attached to C. Since J is an Abelian variety, the *Mordell-Weil Theorem* shows that its $\mathbb{Q}$-rational points $J(\mathbb{Q})$ form a finitely generated Abelian group. Therefore, we have a decomposition

$$J(\mathbb{Q}) \cong \mathbb{Z}^{\operatorname{rank} J(\mathbb{Q})} \oplus \operatorname{tors}(J(\mathbb{Q})),$$

where $\operatorname{tors}(J(\mathbb{Q}))$ is a finite group containing elements in $J(\mathbb{Q})$ of finite order, and $\operatorname{rank} J(\mathbb{Q})$ is the *rank* of $J/\mathbb{Q}$. In this thesis, we are interested in bounding $\operatorname{rank} J(\mathbb{Q})$ in terms of the invariants of C.

To this end, we define the Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ of J over $\mathbb{Q}$, and find a more practical description of it. As the inequality (see Theorem 2.3.1)

$$\operatorname{rank} J(\mathbb{Q}) \leq \dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim J(\mathbb{Q})[2]$$

suggests, we study $\operatorname{rank} J(\mathbb{Q})$ by means of the Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. Here, the dimensions are taken over $\mathbb{F}_2$ and $J(\mathbb{Q})[2]$ denotes the 2-torsion subgroup of $J(\mathbb{Q})$. Moreover, we will see that the computation of $\dim J(\mathbb{Q})[2]$ depends only on the shape of the factorisation of $f(x)$ in $\mathbb{Q}[x]$ and is therefore "easy to compute".

Our main approach to studying $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ is to use Stoll's Implementation of 2-descent. Following [23], we firstly give a more concrete description of the 2-Selmer group, referring to [16] for general and complete proofs. In [16], Edward F. Schaefer replaces the cohomology groups appearing in the original definition of the Selmer group by the kernels of certain norm maps of the algebra $L = \mathbb{Q}[T]/(f(T))$ defined by $f(x)$, making $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ more tangible to work on. See Theorem 3.2.3 for the precise statement.

We will see that this concrete description of the 2-Selmer group can further be simplified so as to yield an upper bound on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ as follows:

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq m_\infty - 1 + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)),$$

where G is a group defined by finitely many local conditions at finite places of $\mathbb{Q}$ and m_∞ is the number of irreducible factors of $f(x)$ in $\mathbb{R}[x]$. The main step in deriving that bound is to find a suitable finite subgroup $\widetilde{\mathrm{Sel}} \subseteq L^\times/(L^\times)^2$ containing $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, whose dimension can be studied relatively easily. The details can be found in Chapter 3.

In the next chapter, we will concentrate on a more current consideration. Following [4], we will introduce a subgroup $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widehat{\mathrm{Sel}} \subseteq L^\times/(L^\times)^2$ with $\widehat{\mathrm{Sel}} \subseteq \widetilde{\mathrm{Sel}}$ and obtain the following bound:

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \dim \mu_\infty + \dim \mathrm{Cl}^+(L)[2] + \dim(G \cap V_\infty), \qquad (*)$$

where $\mu_\infty \subseteq \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ and $G \cap V_\infty \subseteq I(L)/I(L)^2$ are defined by certain local conditions at infinity, $I(L)$ is the group of fractional ideals of L and $\mathrm{Cl}^+(L)$ is the narrow class group of L. Furthermore, we will study the dimension of the totally positive units $\mathcal{O}_L^{\times,+}$ more carefully and will be able to make the bound (*) stronger for some families of hyperelliptic curves.

For example, when L is a cyclic number field of odd prime degree p, the order of 2 in $(\mathbb{Z}/p\mathbb{Z}^\times)$ is even and $\mathcal{O}_L^{\times,+} = (\mathcal{O}_L^\times)^2$, we will see that the bound (*) improves to the one

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) \qquad (**)$$

where $g = (p-1)/2$ is the genus of C. See Theorem 4.5.2 for details.

In the last chapter, we will present an infinite family E_n of elliptic curves for which we are able to use the bound (**) and estimate $\dim \ker(G \to \mathrm{Cl}(L_n)/2\,\mathrm{Cl}(L_n))$. This will yield the following optimal bound on $\mathrm{rank}\, E_n(\mathbb{Q})$:

$$\mathrm{rank}\, E_n(\mathbb{Q}) \leq 3 + \dim \mathrm{Cl}(L_n)[2].$$

I would like to sincerely thank my advisor, Richard Griffon, for he has constantly supported me in all of my academic pursuits during the period he has been advising.

Chapter 1

Preliminaries

This chapter is intended to contain preliminary definitions and results we will need in the next sections for our main exposition. Some proofs are omitted due to their being long or technical, but we then provide references for them. Every title has a rich literature on its own, so one probably cannot expect to get a full account of them through this chapter.

1.1 Hyperelliptic curves

We give a definition of hyperelliptic curves in this section. Let k be a field of characteristic 0 and let $f(x) \in k[x]$ be a monic, squarefree polynomial of odd degree $d = 2g + 1$ with $g \geq 1$ (so that $d \geq 3$). Write $f = \sum_{j=0}^{d} a_j x^j \in k[x]$ and consider

$$h_0(x, y) = y^2 - f(x) \in k[x, y].$$

The polynomial $f(x)$ being squarefree, we have that $h_0(x, y)$ is irreducible in $\overline{k}[x, y]$ and hence, the ideal $(h_0) \subseteq \overline{k}[x, y]$ is prime. Let $C_0 \subseteq \mathbb{A}^2$ be the affine set corresponding to the ideal $(h_0) \in k[x, y]$. One can see that C_0 is smooth because $f(x)$ is squarefree. Therefore, we conclude that $C_0 \subseteq \mathbb{A}^2$ is a smooth affine algebraic variety of dimension 1, defined over k. Let $\overline{C_0} \subseteq \mathbb{P}^2$ be the projective closure of C_0. Then one can check that there is a unique point at infinity on $\overline{C_0}$; namely, $[0 : 1 : 0]$, which is $\mathbb{Q}$-rational. One can also check that the point $[0 : 1 : 0]$ is singular if $d > 3$.

Consider the projective algebraic set $C \subseteq \mathbb{P}^{g+2}$, whose ideal is generated by the following $2g$ homogeneous polynomials of degree 2:

$$\begin{gathered}
Q_1 = x_1^2 - x_0 x_2 \\
Q_2 = x_2^2 - x_1 x_3 \\
\vdots \\
Q_g = x_g^2 - x_{g-1} x_{g+1} \\
Q_{g+1} = x_0 x_{g+1} - x_1 x_g \\
Q_{g+2} = x_1 x_{g+1} - x_2 x_g \\
\vdots \\
Q_{2g-1} = x_{g-2} x_{g+1} - x_{g-1} x_g \\
H = -x_{g+2}^2 + \sum_{j=0}^{g} a_j . x_0 x_j + \sum_{j=0}^{g} a_{j+g+1} . x_g x_j .
\end{gathered}$$

Let $\phi : \mathbb{A}^2 \to \mathbb{P}^{g+2}$ be the map given by

$$(x, y) \mapsto [1 : x : x^2 : \cdots : x^{g+1} : y].$$

We claim that ϕ is an isomorphism of algebraic varieties between C_0 and the dehomogenisation $C \cap \{x_0 = 1\}$. Indeed, an induction argument shows that for all $[x_0 : x_1 : \cdots : x_{g+2}] \in C$, one has

$$x_j x_0^{j-1} = x_1^j, \qquad (*)$$

for all $j = 1, \ldots, g+1$. By definition, $C \cap \{x_0 = 1\}$ is defined by dehomogenisations of the above equations $Q_1, \ldots Q_g$, $Q_{g+1}, \ldots Q_{2g-1}$, H with respect to the 0^{th} variable x_0; *i.e.*, by the following polynomials:

$$\begin{gathered} Q_1' = x_1^2 - x_2 \\ Q_2' = Q_2 \\ \vdots \\ Q_g' = Q_g \\ Q_{g+1}' = x_{g+1} - x_1 x_g \\ Q_{g+2}' = Q_{g+2} \\ \vdots \\ Q_{2g-1}' = Q_{2g-1} \end{gathered}$$

$$H' = -x_{g+2}^2 + \sum_{j=0}^{g} a_j . x_j + \sum_{j=0}^{g} a_{j+g+1} . x_g x_j = -x_{g+2}^2 + f(x_1).$$

Moreover, for all $j = 1, \ldots, g+1$, (*) reads $x_j = x_1^j$ for the points on the "dehomogenised curve" $C \cap \{x_0 = 1\}$. It follows that all points on $C \cap \{x_0 = 1\}$ are of the form $[1 : x_1 : x_1^2 : \cdots : x_1^{g+1} : x_{g+2}]$, meaning $\phi^{-1}(C \cap \{x_0 = 1\}) \subseteq C_0$. Moreover, the inverse of ϕ is given by

$$\phi^{-1}|_{C \cap \{x_0 = 1\}} : [1 : x_1 : x_1^2 : \cdots : x_1^{g+1}, x_{g+2}] \mapsto (x_1, x_{g+2}) \in C_0,$$

for $[1 : x_1 : x_1^2 : \cdots : x_1^{g+1} : x_{g+2}] \in C \cap \{x_0 = 1\}$. Hence $\phi|_{C_0}$ and $\phi^{-1}|_{C \cap \{x_0 = 1\}}$ are mutually inverse, and moreover, they are both given by polynomial functions. Thus, it follows that ϕ is an isomorphism of algebraic varieties, as claimed.

Notice that $C \cap \{x_0 = 0\}$ consists of a unique point $P_\infty = [0 : \cdots : 0 : 1 : 0]$, the point at infinity, and this point is k-rational. A straightforward computation shows that the rank of the Jacobian matrix of C at the point P_∞ is $g - 1$; *that is*, C is smooth at P_∞. Since C_0 is smooth and we have established an isomorphism $C_0 \cong C \cap \{x_0 = 1\}$ above, we conclude that $C = C_0 \cup \{P_\infty\} \subseteq \mathbb{P}^{g+2}$ is a smooth projective variety of dimension 1, defined over k, containing C_0 as a dense open subset.

Definition 1.1.1. *Let k be a field of characteristic 0 and let $f = \sum_{j=0}^{d} a_j x^j \in k[x]$ be a monic, squarefree polynomial of odd degree $d = 2g + 1 \geq 3$. Let C be the smooth projective variety of dimension 1 constructed above. We then call C/k the hyperelliptic curve associated to f.*

In what follows, we show that if C/k is the hyperelliptic curve over a field k of characteristic 0, associated to f with f monic, squarefree and of odd degree $d = 2g + 1 \geq 3$, then the genus of the curve C is g.

To this end, let C_0 be as above and consider the morphism $\pi_0 : C_0 \to \mathbb{A}^1$, $(x, y) \mapsto x$, defined over k. There exists a unique finite morphism

$$\pi : C \to \mathbb{P}^1,$$

extending π_0 via $P_\infty \mapsto [1 : 0]$. Let $p \in \mathbb{P}^1$ be a point such that $p \neq [1 : 0]$; *i.e.*, $p \in \mathbb{A}^1$. Then, whenever $f(p) \neq 0$ (which holds for almost all $p \in \mathbb{P}^1$), the fibre $f^{-1}(p)$ consists of two points $(p, \pm\sqrt{f(p)})$ where $\sqrt{f(p)} \in \overline{k}$. This implies that the degree of the morphism π is 2 (see [21, Proposition 2.6]). On the other hand, whenever $p \in \mathbb{P}^1$ is such that $f(p) = 0$, the fibre $\pi^{-1}(p)$ consists of a single point and the ramification index e_p is 2. Note also that $\pi^{-1}[1 : 0] = P_\infty$ and π ramifies at the point $p = [1 : 0]$, meaning that $e_p = 2$. Hence, the set of ramification points is $\Omega = \{p \in \overline{k} : f(p) = 0\} \cup \{[1 : 0]\}$.

Now, let g_C denote the genus of the hyperelliptic curve C, then the Riemann-Hurwitz formula (see [21, Chapter II, Theorem 5.9]) reads

$$\begin{aligned} 2g_C - 2 &= 2(2g_{\mathbb{P}^1} - 2) + \sum_{p \in \Omega} (e_p - 1) \\ &= 2(2g_{\mathbb{P}^1} - 2) + \deg(f)(2 - 1) + (2 - 1). \end{aligned}$$

Since the genus $g_{\mathbb{P}^1}$ of $\mathbb{P}^1$ is 0 and $\deg(f) = 2g + 1$, we get that $g_C = g$, as claimed.

1.2 Jacobians of hyperelliptic curves

Let k be a field of characteristic 0 and let $C : y^2 = f(x)$ be a a hyperelliptic curve over k with f monic, squarefree and of odd degree $2g+1$. Let P_∞ be the point at infinity of C. In this section, we want to sketch the construction of the Jacobian variety $J(C)$ attached to the curve C.

Let $\mathrm{Div}(C)$ be the group of divisors on C (over the algebraic closure $\overline{k}$) and let $\mathrm{Pic}(C)$ be the quotient of $\mathrm{Div}(C)$ by the principal divisors $\mathrm{div}(f)$ where $f \in \overline{k}(C)^\times$. Then there is a group homomorphism

$$\deg : \mathrm{Pic}(C) \to \mathbb{Z}, \left[\sum n_i P_i\right] \mapsto \sum n_i,$$

where $[D] \in \mathrm{Pic}(C)$ denotes the linear equivalence class of a divisor $D \in \mathrm{Div}(C)$. We define

Definition 1.2.1. *The Jacobian variety of C is given by*

$$J(C) = \ker(\deg : \mathrm{Pic}(C) \to \mathbb{Z}).$$

The kernel $\ker(\deg)$ *is sometimes denoted by* $\mathrm{Pic}^0(C)$ *and called the class group of C.*

Note that we have to "justify" this definition; *that is*, we must endow the Abelian group $J(C)$ with the structure of an algebraic variety. This is explicitly done in [10] by D. Mumford over an algebraically closed field. In the following, we present a sketch of this construction, closely following [10]. For two divisors $D_1, D_2 \in \mathrm{Div}(C)$, we write $D_1 \equiv D_2$ to mean $[D_1] = [D_2]$ in $\mathrm{Pic}(C)$.

- Let $C^g = C \times \cdots \times C$ be the product of g copies of C. Then C^g is an algebraic variety of dimension g. Let S_g be the symmetric group on g letters. There is an action of S_g on C^g by permutation of the factors. We can therefore form the quotient $\mathrm{Symm}^g C = C^g/S_g$ of C^g by the action of S_g. It can be shown that $\mathrm{Symm}^g C$ is also an algebraic variety of dimension g. Now if $[D]$ is any element of $J(C)$, then one can show that there are points $P_1, \ldots, P_g$ such that $D \equiv \sum_{i=1}^{g} P_i - g.P_\infty$ (see [10, p. 3.29]). This yields a surjection

  $$I : \mathrm{Symm}^g C \to J(C), \sum_{i=1}^{g} P_i \mapsto \sum_{i=1}^{g} P_i - g.P_\infty.$$

  Define Θ as the subset of $J(C)$ of divisor classes of the form $\sum_{i=1}^{g-1} P_i - (g-1).\infty$. One can explicitly define a subvariety $Z \subseteq \mathrm{Symm}^g C$ of dimension g such that the restriction

  $$I|_Z : Z \to J(C) \setminus \Theta$$

  is a bijection. Hence one can transfer the structure of algebraic variety from Z to $J(C) \setminus \Theta$.

- The aim in this step is to cover $J(C)$ by affine pieces which are in bijection with to Z which we know is an algebraic variety of dimension g from the previous step. The following type of elements of $J(C)$ is particularly important:

  Definition 1.2.2. *Let $\Omega = \{P_\alpha = (\alpha, 0) \in C(\overline{k}) : f(\alpha) = 0\} \cup \{P_\infty\}$. Let $T \subseteq \Omega$ be a subset of even cardinality. We define*

  $$e_T = \left[\sum_{P \in T} P - |T| P_\infty\right] \in J(C).$$

  The following lemma summarises some important properties of e_T. We will make a heavy use of this lemma in the next section while computing the dimension of the 2-torsion of the Jacobian.

Lemma 1.2.3. *Let $T, T_1, T_2 \subseteq \Omega$ be some subsets of even cardinality (so that the symmetric difference $T_1 \triangle T_2 = (T_1 \cup T_2) \setminus (T_1 \cap T_2)$ also has even cardinality). Then*

(i) $2e_T = 0$,

(ii) $e_{T_1} + e_{T_2} = e_{T_1 \triangle T_2}$,

(iii) $e_{T_1} = e_{T_2}$ *if and only if* $T_1 = T_2$ *or* $T_1 = \Omega \setminus T_2$.

Thus, the set of the e_T's forms a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g}$.

Proof. See [10, Lemma 2.4]. □

We achieve our aim by the following lemma:

Lemma 1.2.4. *We have*

$$\bigcup_T \left[(J(C) \setminus \Theta) + e_T\right] = J(C),$$

where T varies over the subsets $T \subseteq \Omega$ of even cardinality and e_T is defined as above.

Proof. See [10, Lemma 2.5]. □

We know from the previous step that Z and $J(C) \setminus \Theta$ are in bijection. Since $(J(C) \setminus \Theta) + e_T$ is a translation of $J(C) \setminus \Theta$ by an element e_T using the group structure of $J(C)$, we have an isomorphism $(J(C) \setminus \Theta) + e_T \cong J(C) \setminus \Theta$. Hence, Z and $(J(C) \setminus \Theta) + e_T$ are in bijection, which allows us to define the structure of an algebraic variety on $(J(C) \setminus \Theta) + e_T$. Thus, we have covered $J(C)$ with the "affine pieces" isomorphic Z, as desired.

- Take one copy of Z for each $T \subseteq \Omega$. To finalise the construction of $J(C)$, one has to show in this last step that these copies can be glued together to give $J(C)$ as a variety according to their identification as subsets of the Jacobian. This amounts to checking the compatibility of algebraic variety structure on the intersection $((J(C) \setminus \Theta) + e_T) \cap ((J(C) \setminus \Theta) + e'_T)$ with $T, T' \in \Omega$ arbitrary subsets of even cardinality. For the proofs, we refer to [10, Lemma 2.6] and [10, Proposition 2.7].

Since there exists a surjection $C^g \to J(C)$ and C is complete, it follows that $J(C)$ is a complete variety. Moreover, $J(C)$ is an Abelian variety. By an Abelian variety, we mean the following:

Definition 1.2.5. *An Abelian variety is a complete variety A with an Abelian group law such that the addition $A \times A \to A$ and inverse $A \to A$ are morphisms.*

Indeed, we just observed that $J(C)$ is a complete variety and by definition, it has an Abelian group structure. To show that the addition and inverse are morphisms, one relies on [10, Lemma 2.9].

Therefore, we conclude that given a hyperelliptic curve C over k, there exists an Abelian variety $J(C)/\overline{k}$ naturally attached to C of dimension the genus g of C; namely, the Jacobian $J(C)$. One can actually show that $J(C)$ is indeed defined over k (see [9] for more details).

1.3 2-torsion of the Jacobian

Let $k/\mathbb{Q}$ be a field extension and $C : y^2 = f(x)$ be a hyperelliptic curve over k with $f(x) \in k[x]$ monic, squarefree and of odd degree. Let

$$f = f_1 \dots f_{m_k}$$

be the factorisation of f over k into monic, irreducible factors $f_1, \dots, f_{m_k}$. Let $G_k = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group of k. Then the action of G_k on the points $P \in C(\overline{k})$ linearly extends to an action on $J(C)[2]$, the 2-torsion subgroup of $J[2]$. One can then consider the G_k-invariant points $J(C)[2]^{G_k} := J(k)[2]$ of $J(C)[2]$ under the action of G_k. One of our aims in this section is to prove the following theorem:

Theorem 1.3.1. *In the above set-up, to every factor f_i of f in $k[x]$, we associate an element $D_i \in J(k)[2]$ such that the D_i's for $i = 1, \dots, m_k$, generate $J(k)[2]$ and satisfy*

$$\sum_{i=1}^{m_k} D_i = 0.$$

Moreover, we have $\dim J(k)[2] = m_k - 1$*; i.e.,* $J(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{m_k - 1}$.

Since $J(C)/k$ is an Abelian variety of dimension g over a field k of characteristic 0, it is known (see [9]) as a general fact that

$$J(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}.$$

Note that this fact is a special instance of Theorem 1.3.1 when f factorises completely in $k[x]$ and in particular, this happens in $\overline{k}[x]$. By Lemma 1.2.3, we know that $\{e_T\}_{T \subseteq \Omega}$, where $T \subseteq \Omega$ varies over the subsets of even cardinality, form a subgroup of $J(C)$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g}$. Therefore, we conclude that the same collection $\{e_T\}_{T \subseteq \Omega}$ is the whole $J(C)[2]$.

Now, let $\Omega_0 = \{P_\alpha = (\alpha, 0) \in C(\overline{k}) : f(\alpha) = 0\}$. For any $\alpha \in \overline{k}$ such that $f(\alpha) = 0$, we define

$$e'_\alpha := e_{\{P_\alpha, \infty\}} = [P_\alpha + \infty - 2\infty] = [P_\alpha - \infty].$$

We have the following lemma:

Lemma 1.3.2. *Let e'_α where $f(\alpha) = 0$ be defined as above. We have*

(i) The classes $\{e'_\alpha\}_{f(\alpha)=0}$ generate $J(C)[2]$ as a group,

(ii) The only relation between the e'_α, where α varies over the roots of $f(x)$, is given by

$$\sum_{f(\alpha)=0} e'_\alpha = 0. \qquad (*)$$

Proof. (i) Note that if $P_{\alpha_1}, P_{\alpha_2} \in \Omega_0$ are distinct, then the part (ii) of Lemma 1.2.3 gives that $e'_{\alpha_1} + e'_{\alpha_2} = e_{\{P_{\alpha_1}, P_{\alpha_2}\}}$. This implies that if $T = \{P_{\alpha_1}, \dots, P_{\alpha_{2k}}\} \subseteq \Omega_0$, where $k \leq g$, is a subset of even cardinality, then

$$e_T = e'_{\alpha_1} + \dots + e'_{\alpha_{2k}}.$$

Likewise, if $T \subseteq \Omega$ is a subset of even cardinality of the form $T = \{P_{\alpha_1}, \dots, P_{\alpha_{2k-1}}, P_\infty\}$, where $k \leq g$, then

$$e_T = e'_{\alpha_1} + \dots + e'_{\alpha_{2k-1}}.$$

Since $\{e_T\}_{T \subseteq \Omega}$ with $T \subseteq \Omega$ varying over subsets of even cardinality generates $J(C)[2]$, it thus follows that $\{e'_\alpha\}_{f(\alpha)=0}$ also generate $J(C)[2]$, proving part (i).

(ii) Note that we can write

$$\sum_{f(\alpha)=0} e'_\alpha = e_{T_1} + e_{T_2},$$

where $T_1 = \{P_1, \ldots, P_{2g}\}$ and $T_2 = \{P_{2g+1}, \infty\}$. Since $T_1 = \Omega \setminus T_2$, part (ii) and (iii) of Lemma 1.2.3 gives the relation (*). On the other hand, the "if" part of part (iii) of Lemma 1.2.3 also implies that this is the only relation between e'_α's. Indeed, this follows because as $J(k)[2]$ is in particular a $(\mathbb{Z}/2\mathbb{Z})$-vector space, any relation between $\{e'_\alpha\}$ is given by $\sum_{\alpha \in A} e'_\alpha = 0$ with $A \subseteq \Omega$. Thus, the proof is complete. □

Recall that we put $G_k = \mathrm{Gal}(\overline{k}/k)$. Clearly there is an action of G_k on Ω_0 given by $\sigma.(\alpha, 0) = (\sigma(\alpha), 0)$ for $\sigma \in G_k$ and $\alpha \in \overline{k}$ a root of $f(x)$. This yields an action of G_k on $\{e'_\alpha\}_{f(\alpha)=0}$ via $\sigma.e'_\alpha = e'_{\sigma(\alpha)}$. Denote by O_i the orbit of an element $e'_{\alpha_i} \in \{e'_\alpha\}_{f(\alpha)=0}$ so that

$$\{e'_\alpha\}_{f(\alpha)=0} = \bigsqcup_{i=1}^{r} O_i,$$

where r is the number of orbits. For all $i = 1, \ldots, r$, we define

$$D_i := \sum_{e'_\alpha \in O_i} e'_\alpha.$$

Note that part (i) of Lemma 1.2.3 implies that

$$2D_i = 2\textstyle\sum_{e'_\alpha \in O_i} e'_\alpha = \sum_{e'_\alpha \in O_i} 2e'_\alpha = 0,$$

which means that $D_i \in J(k)[2]$. Moreover, since $\{e'_\alpha\}_{f(\alpha)=0}$ generates $J(C)[2]$, it follows that $\{D_i\}_{i=1,\ldots,r}$ generates $J(k)[2]$ as a group.

Therefore, the following lemma concludes the proof of Theorem 1.3.1:

Lemma 1.3.3. *In the above set-up, we have*

(i) $r = m_k =$ *the number of irreducible factors of* f *in* $k[x]$,

(ii) $J(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{m_k - 1}$.

Proof. (i) Note that by definition, the number r of orbits of the action of G_k on $\{e'_\alpha\}_{f(\alpha)=0}$ is the same as the number of orbits of the action of G_k on Ω_0. But this number is clearly m_k. Indeed, write $f = f_1 \ldots f_{m_k}$ in $k[x]$ with $f_i's$ monic and irreducible for $i = 1, \ldots, m_k$. If α is a root of $f(x)$, then there is a unique $i \in \{1, \ldots, m_k\}$ such that $f_i(\alpha) = 0$. Moreover since each f_i is irreducible, the orbit $G_k.\alpha$ contains all the roots of the irreducible factor f_i. Thus the result follows.

(ii) The previous part now implies that $J(k)[2]$ is generated by the elements $\{D_i\}_{i=1,\ldots,m_k}$. Moreover, part (ii) of Lemma 1.3.2 implies that the only relation between the D_i for $i = 1, \ldots, m_k$ is given by

$$\sum_{i=1}^{m_k} D_i = 0.$$

As $J(k)[2] \subseteq J(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$, it thus follows that $J(k)[2]$ is a $(\mathbb{Z}/2\mathbb{Z})$-module of rank $m_k - 1$, finishing the proof. □

We now present some results about the dimensions of the $\mathbb{F}_2$-vector spaces $J(\mathbb{R})/2J(\mathbb{R})$ and $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, where $\mathbb{Q}_p$ denotes the p-adic field for a prime number p.

Theorem 1.3.4. *Let* p *be a prime and consider the* p*-adic extension* $\mathbb{Q}_p$ *of* $\mathbb{Q}$. *Let*

$$d_p = \begin{cases} 1 & \text{if } p = 2 \\ 0 & \text{otherwise} \end{cases}.$$

Let g *be the genus of* C*; i.e.,* $g = (\deg(f) - 1)/2$, *and let* m_p *denote the number of irreducible factors of* $f(x)$ *in* $\mathbb{Q}_p[x]$. *Then we have*

$$\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \dim J(\mathbb{Q}_p)[2] + d_p g = m_p - 1 + d_p g.$$

Proof. See [8], where the author proves the fact that $J(\mathbb{Q}_p)$ contains a subgroup of finite index isomorphic to g copies of the ring of integers in $\mathbb{Q}_p$. This leads to the desired conclusion via [16, prop. 2.4]. □

Theorem 1.3.5. *Let m_∞ denote the number of irreducible factors of $f(x)$ in $\mathbb{R}[x]$ and g be the genus of C. Then we have*

$$\dim J(\mathbb{R})/2J(\mathbb{R}) = m_\infty - 1 - g.$$

Proof. See [18, Proposition 5.4]. □

1.4 Galois cohomology

We review the basics of cohomology theory of groups, avoiding technicalities and tedious constructions, and aiming at the results and constructions we will need in the subsequent sections. Our main reference for this section is [13].

Definition 1.4.1. *Let G be a group. Then an Abelian group A is a (continuous) G-module if there exists a (continuous) composition $\rho : G \times A \to A$, $(\sigma, a) \mapsto \sigma a$, which satisfies, for all $a, b \in A$, $\sigma, \sigma_1, \sigma_2 \in G$, and the unit $1 \in G$, the following conditions:*
(i) $\sigma(a + b) = \sigma a + \sigma b$,
(ii) $\sigma_1(\sigma_2 a) = (\sigma_1\sigma_2)a$,
(iii) $1a = a$.

Example 1.4.2. *Let K be a field of characteristic 0. Let $G = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. For a smooth curve C of genus $g \geq 1$ over K, let J denote its Jacobian variety $J(C)$. Then we know that J is an Abelian variety over K. Moreover $J(\overline{K})$ is a G-module. An instance of this example when $K = \mathbb{Q}$ will subsequently be of our particular interest.*

Let G be a group. For a G-module A, consider the Abelian group A^G of G-invariant elements of A. This association defines a functor $\mathcal{F}$ from the category of G-modules to the category of Abelian groups.

Theorem 1.4.3. *The functor $\mathcal{F}$ from the above discussion is a left-exact covariant functor. Hence one can construct right derived functors*

$$H^i(G, \bullet),\ i = 1, 2, \ldots,$$

of $\mathcal{F}$, from the category of G-modules to the category of Abelian groups. They are characterised by the property that, given a short exact sequece

$$0 \to A \to B \to C \to 0$$

of G-modules, there exists an associated long exact sequence, called long exact cohomolgy sequence,

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \ldots,$$

where the map δ is a connecting morphism.

Proof. See [5, p. 204, Theorem 1.1A]. □

Definition 1.4.4. *For an $i \geq 1$, the Abelian group $H^i(G, A)$ is called a cohomology group. In case where $G = \mathrm{Gal}(L/K)$ is a Galois group (of a field extension $K \subseteq L$), the cohomolgy group $H^i(G, A)$ is called a Galois cohomology group. When $G = \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group of a field K, we often abreviate $H^i(G, A)$ to $H^i(K, A)$.*

For a subgroup H of G, there are canonical morphisms $H^i(G, A) \to H^i(H, A)$ for $i = 1, 2, \ldots$, called *restriction* maps. Since we will be frequently using the *restriction* map on the first cohomology groups, we want to give a description of $H^1(G, A)$ and see how this restriction map is induced. We will also define the *inflation* map under the assumption that H is a normal subgroup of G. We will finally present a fundamental exact sequence relating these two maps.

Following [13], we define the group $Z^1(G, A)$ of *1-cocyles* as the maps $x : G \to A$ with the property that, for all $\sigma, \tau \in G$,

$$x(\sigma\tau) = \sigma x(\tau) + x(\sigma).$$

The subgroup $B^1(G, A) \subseteq Z^1(G, A)$ of *1-coboundaries* are the maps $x : G \to A$ of the form

$$x(\sigma) = \sigma a - a$$

for a fixed $a \in A$, where $\sigma \in G$. It can be shown that

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}.$$

Remark 1.4.5. *Observe that when the action of G on A is trivial, one gets*

$$H^1(G, A) = \mathrm{Hom}(G, A),$$

where $\mathrm{Hom}(G, A)$ *is the group of homomorphisms from G to A.*

Let $H \subseteq G$ be a subgroup. If $x : G \to A \in Z^1(G, A)$ is a 1-cocycle, then its restriction $x|_H$ to H is clearly a 1-cocyle in $Z^1(H, A)$. Therefore, we get a map

$$\mathrm{res} : H^1(G, A) \to H^1(H, A),$$

sending the class of a 1-cocycle to the class of its restriction to H.

Now, assume that H is a normal subgroup of G and consider the quotient G/H. Let A^H be the group of H-invariant elements of A. Then G/H acts on A^H via $\sigma H.a = \sigma(a)$ for $\sigma H \in G/H$ and $a \in A^H$. Indeed, for any $\tau \in H$,

$$\tau(\sigma(a)) = \sigma(\tau(a)) = \sigma(a).$$

So $\sigma(a) \in A^H$ and A^H has a G/H-module structure. Moreover, if $x : G/H \to A^H \in Z^1(G/H, A^H)$ is a 1-cocylcle, then it induces a 1-cocycle in $Z^1(G, A)$ via the composition

$$G \to G/H \xrightarrow{x} A^H \hookrightarrow A.$$

Hence we have obtained a map

$$\mathrm{inf} : H^1(G/H, A^H) \to H^1(G, A),$$

called inflation.

We have an *inflation-restriction exact sequence*:

Theorem 1.4.6. *Let A be a G-module and let H be a normal subgroup of G. Then the sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{inf}} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, A).$$

is exact.

Proof. See [13, p. 34, Theorem 4.6]. □

Example 1.4.7. *In line with Example 1.4.2 above, we want to write the inflation-restriction exact sequence explicitely when $G = \mathrm{Gal}(\overline{K}/K)$ and $A = J(\overline{K})$. To this end, let L/K be a Galois extension and let $H = \mathrm{Gal}(\overline{K}/L)$. Then H is a normal subgroup of G. Hence, we have an isomorphism $G/H \cong \mathrm{Gal}(L/K)$. Also, since the action of H is continuous on $J(K)$, we have $J(\overline{K})^H = J(L)$. Therefore, the exact sequence reads*

$$0 \to H^1(\mathrm{Gal}(L/K), J(L)) \xrightarrow{\mathrm{inf}} H^1(G, J(\overline{K})) \xrightarrow{\mathrm{res}} H^1(\mathrm{Gal}(\overline{K}/L), J(\overline{K})).$$

Chapter 2

Bounding the rank in terms of the Selmer group

In this chapter, we will define the 2-Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, properly introduce the notion of rank, and put a bound on the rank in terms of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. For this chapter and the rest of the thesis, we restrict attention to the hyperelliptic curves over $\mathbb{Q}$.

2.1 The 2-Selmer and Shafarevich-Tate groups

Let C be a hyperelliptic curve over $\mathbb{Q}$. Let J be the Jacobian of C. Let K be an extension of $\mathbb{Q}$ and let $\overline{K}$ denote the algebraic closure of K. Let $G = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Consider the $\overline{K}$-rational points $J(\overline{K})$ of J. We give a first definition of the *2-Selmer group* $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ *of* J *over* $\mathbb{Q}$ in terms of Galois cohomology groups. We closely follow the write up [15] of B. Poonen.

Since *multiplication by 2* map $[2]$ is surjective on the $\overline{K}$-rational points $J(\overline{K})$ of J, we have a short exact sequence

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

where $J(\overline{K})[2]$ is the group of 2-*torsion points* of $J(\overline{K})$. Recall from Example 1.4.2 that there is an action of G on $J(\overline{K})$, which turns it into a continuous G-module. By definition, we can define this action by defining it on a divisor. Indeed, if $\sigma \in G$ and $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$ is a divisor on C, then we define the action as follows:

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

It is easy to see that if D is of degree 0, then so is $\sigma(D)$. Moreover, if D is a 2-torsion, then $2\sigma(D) = \sigma(2D) = \sigma(0) = 0$. This implies that G also induces an action on the 2-torsion subgroup $J(\overline{K})[2]$ of $J(\overline{K})$.

Associated to the above short exact sequence, by Theorem 1.4.3 we have a long exact cohomolgy sequence

$$0 \to J(K)[2] \to J(K) \xrightarrow{[2]} J(K) \to H^1(G, J(\overline{K})[2]) \to H^1(G, J(\overline{K})) \xrightarrow{[2]_*} H^1(G, J(\overline{K})) \to \cdots,$$

where the map $[2]_*$ is functorially induced from the multiplication by 2 map. Thus, simplifying the notation, we obtain the following short exact sequence:

$$0 \to J(K)/2J(K) \xrightarrow{\delta} H^1(K, J[2]) \to H^1(K, J)[2] \to 0, \qquad (*)$$

where

$$\delta : J(K)/2J(K) \to H^1(K, J[2])$$

is called the *coboundary morphism.*

Let v be a place of $\mathbb{Q}$. Then v is either a finite place or is *infinity.* In the first case, v is a prime number p and $\mathbb{Q}_v = \mathbb{Q}_p$, the p-adic (local) field; and in the second, $\mathbb{Q}_v = \mathbb{R}$, the real numbers. For a discussion of this, see [12, §1].

For any place v of $\mathbb{Q}$, let $G_v = \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$ be the absolute Galois group of $\mathbb{Q}_v$. We have an injection (see [24, Section 1])

$$G_v \hookrightarrow G, \qquad \sigma \mapsto \sigma\,|_{\overline{\mathbb{Q}}},$$

giving $J(\overline{\mathbb{Q}})$ a natural G_v-module structure and yielding a restriction map on Galois cohomology groups as follows:

$$\mathrm{res}_v : H^1(G, J(\overline{\mathbb{Q}})) \to H^1(G_v, J(\overline{\mathbb{Q}})).$$

Therefore, writing the exact sequence (*) with $K = \mathbb{Q}$ and $K = \mathbb{Q}_v$ for all places v, the construction of the res_v maps defined above yields the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, J[2]) & \longrightarrow & H^1(\mathbb{Q}, J)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \overset{\phi}{\searrow} & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & \prod_v J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J[2]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J)[2] & \longrightarrow & 0
\end{array} \quad , \qquad (**)$$

where the products are over all the places v of $\mathbb{Q}$.

Definition 2.1.1. *The 2-Selmer group* $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ *of* J *over* $\mathbb{Q}$ *is defined as*

$$\begin{aligned}
\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \ker(\phi) &= \ker\Big(H^1(\mathbb{Q}, J[2]) \to \prod_v H^1(\mathbb{Q}_v, J)[2]\Big) \\
&= \bigcap_v \ker\big(H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}_v, J)[2]\big).
\end{aligned}$$

The Shafarevich-Tate group $Ш(\mathbb{Q}, J)$ *of* J *over* $\mathbb{Q}$ *is defined as*

$$\begin{aligned}
Ш(\mathbb{Q}, J) &= \ker\Big(H^1(\mathbb{Q}, J) \xrightarrow{\mathrm{Res}} \prod_v H^1(\mathbb{Q}_v, J)\Big) \\
&= \bigcap_v \ker\big(H^1(\mathbb{Q}, J) \xrightarrow{\mathrm{res}_v} H^1(\mathbb{Q}_v, J)\big),
\end{aligned}$$

where Res *is the product* $\prod_v \mathrm{res}_v$ *of restriction maps over all the places* v.

Remark 2.1.2. *The Shafarevich-Tate group* $Ш(\mathbb{Q}, J)$ *has a useful interpretation with regard to the Hasse's (Local-Global) Principle. Also it is not known in general if the Shafarevich-Tate group* $Ш(\mathbb{Q}, J)$ *is finite although it is conjectured to be so. See [6, §C.4] for a detailed discussion.*

2.2 The rank of a Jacobian

In this section, we will properly define $\mathrm{rank}\, J(\mathbb{Q})$. We obtain the following commutative diagram with exact rows from the diagram (**) above:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, J[2]) & \longrightarrow & H^1(\mathbb{Q}, J)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J)[2] & \xrightarrow{\mathrm{id}} & \prod_v H^1(\mathbb{Q}_v, J)[2] & \longrightarrow & 0
\end{array}$$

to obtain the short exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \to Ш(\mathbb{Q}, J)[2] \to 0, \qquad (***)$$

where $Ш(\mathbb{Q}, J)[2]$ is the 2-torsion of the Shafarevich-Tate group $Ш(\mathbb{Q}, J)$.

In what follows, we give a sketch of the proof to the important fact that the 2-Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ is finite group. For a detailed and general proof, we refer to [6, p. 282, Proposition C.4.2].

Definition 2.2.1. *Let J be the Jacobian of a hyperelliptic curve $C/\mathbb{Q}$. Let v be a place of $\mathbb{Q}$ and let $I_v \subseteq G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be an inertia for v. Consider the 2-torsion subgroup $J[2]$ of $J(\overline{\mathbb{Q}})$. We say that a cohomology class $\phi \in H^1(\mathbb{Q}, J[2])$ is unramified at v if the restriction map*

$$\mathrm{res} : H^1(\mathbb{Q}, J[2]) \to H^1(I_v, J[2])$$

is trivial on ϕ. For a finite set S of places of $\mathbb{Q}$, we denote by $H^1_S(\mathbb{Q}, J[2])$ the subgroup of $H^1(\mathbb{Q}, J[2])$ consisting of cohomology classes that are unramified at all places not in S.

Theorem 2.2.2. *Let $C : y^2 = f(x)$ be a hyperelliptic curve with $f(x) \in \mathbb{Q}[x]$ squarefree, and let J be its Jacobian. Then the 2-Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ is a finite group of exponent 2.*

Proof. Let S be the set

$$S = \{\infty, 2\} \cup \{p \mid p^2 \text{ divides } \mathrm{disc}(f)\}.$$

It can be shown that S contains the primes of bad reduction of J together with ∞ and 2 (see the statement of [6, C.4.2]). Then the strategy is to prove that the subgroup $H^1_S(\mathbb{Q}, J[2])$ of $H^1(\mathbb{Q}, J[2])$ containing cohomology classes which are unramified outside S is finite, and then to see that $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ is contained in $H^1_S(\mathbb{Q}, J[2])$.

Since $J[2]$ is the kernel of the isogeny $J(\overline{\mathbb{Q}}) \xrightarrow{[2]} J(\overline{\mathbb{Q}})$, it is known to be finite. Hence we have a continuous action of G on the finite set $J[2]$. This implies that G contains an open subgroup that acts trivially on $J[2]$. Since the open subgroups of G are of the form $\mathrm{Gal}(K/\mathbb{Q})$ where K is a finite extension of $\mathbb{Q}$, we conclude that there exists a finite extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K, \mathbb{Q})$ acts trivially on $J[2]$.

Let G_K be the absolute Galois group of K. An instance of Example 1.4.7 yields an exact sequence

$$0 \to H^1(G/G_K, J[2]^{G_K}) \xrightarrow{\inf} H^1(\mathbb{Q}, J[2]) \xrightarrow{\mathrm{res}} H^1(G_K, J[2]).$$

Since $\mathrm{res}(H^1_S(\mathbb{Q}, J[2])) \subseteq \mathrm{res}(H^1_S(G_K, J[2]))$, this shows that proving $H^1_S(G_K, J[2])$ is finite would imply $H^1_S(\mathbb{Q}, J[2])$ is finite. Hence, we can replace $\mathbb{Q}$ by K in the previous paragraph and assume that G acts trivially on $J[2]$. By Remark 1.4.5, this implies that

$$H^1(\mathbb{Q}, J[2]) = \mathrm{Hom}(G, J[2]).$$

Note that by definition, any element of $J[2]$ is killed by 2. This implies that the elements of $\mathrm{Hom}(G, J[2])$ correspond to finite Abelian extensions of $\mathbb{Q}$ whose Galois group has exponent 2 by means of Kummer Theory (see [13]). Hence, the elements of $H^1_S(\mathbb{Q}, J[2])$ correspond to finite Abelian extensions of $\mathbb{Q}$ of exponent 2 that are unramified outside of S. But it is known that there are only finitely many maximal Abelian extensions of exponent 2 that are unramified outside S, see [6, p. 265, Corollary C.1.8]. Thus, it follows that $H^1_S(\mathbb{Q}, J[2])$ is a finite set.

Now, let $\phi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ and let v be a place not in S. Then v is a prime $p \neq 2$, at which J has good reduction $\tilde{J}$. Furthermore, the reduction map

$$J(\mathbb{Q})[2] \to \tilde{J}(\mathbb{F}_p)$$

is injective; see [6, p. 263, Theorem C.1.4]. One can show that this implies that ϕ is unramified at v and hence, $\phi \in H^1_S(\mathbb{Q}, J)$.

Finally, it follows by definition of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ that it is a group of exponent 2. □

Having the exact sequence (***), this important theorem has two immediate finiteness consequences. The first one is that the 2-torsion $Ш(\mathbb{Q}, J)[2]$ of the Shafarevich-Tate group is finite (cf. Remark 2.1.2). And the second one is

Corollary 2.2.3 (Weak Mordell-Weil)**.** *The group $J(\mathbb{Q})/2J(\mathbb{Q})$ is a finite group.*

The Weak Mordell-Weil Theorem together with the theory of *Néron-Tate heights* (see [6, B.4]) implies the Mordell-Weil Theorem:

Theorem 2.2.4 (Mordell-Weil)**.** *$J(\mathbb{Q})$ is a finitely generated Abelian group and we have a decomposition*

$$J(\mathbb{Q}) \cong \mathbb{Z}^{\operatorname{rank} J(\mathbb{Q})} \oplus \operatorname{tors}(J(\mathbb{Q})),$$

where $\operatorname{tors}(J(\mathbb{Q}))$ *is a finite group containing elements in $J(\mathbb{Q})$ of finite order, and* $\operatorname{rank} J(\mathbb{Q})$ *is called the rank of $J/\mathbb{Q}$.*

Proof. See [3, §5, pp. 158-161]. □

Remark 2.2.5. *The proof of Mordell-Weil nevertheless does not give a recipe to compute the rank. So it still remains a mysterious invariant of the Jacobian.*

2.3 Bound on the rank

Going back to the exact sequence (***), it is now clear that the members of the sequence all have a structure of an $\mathbb{F}_2$-vector space. Therefore,

$$\dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(\mathbb{Q}, J).$$

Moreover, if $r = \operatorname{rank} J(\mathbb{Q})$, then Mordell-Weil implies that

$$J(\mathbb{Q})/2J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \oplus \operatorname{tors}(J(\mathbb{Q}))/2\operatorname{tors}(J(\mathbb{Q})).$$

On the other hand,

$$\operatorname{tors}(J(\mathbb{Q}))/2\operatorname{tors}(J(\mathbb{Q})) \cong J(\mathbb{Q})[2].$$

Therefore,

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

Thus, we have proved

Theorem 2.3.1. *Let $C/\mathbb{Q}$ be a hyperelliptic curve and let $J/\mathbb{Q}$ denote its Jacobian. Dropping the subscripts $\mathbb{F}_2$ from the notation, we obtain*

$$\operatorname{rank} J(\mathbb{Q}) \leq \dim \operatorname{Sel}^{(2)}(\mathbb{Q}, J) - \dim J(\mathbb{Q})[2].$$

Chapter 3

Stoll's implementation of 2-Descent

In this chapter, our aim is to find a practical description of the 2-Selmer group, which allows us to have an upper bound on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. Our main reference throughout this chapter is M. Stoll's article, [23].

3.1 Notation

We fix some notation and give definitions that will be used throughout the thesis. We want to restrict attention to the hyperelliptic curves $C/\mathbb{Q}$, given by $y^2 = f(x)$ such that $f(x) \in \mathbb{Z}[x]$ is monic, squarefree and of *odd degree*. However, we remark that M. Stoll also treats the case where $f(x)$ is of even degree. See [23, §5]. Observe that since $f(x)$ is of odd degree, C has a unique point at infinity that is $\mathbb{Q}$-rational. We denote this point by ∞.

For any field extension K of $\mathbb{Q}$, we consider the *algebra* $L_K = K[T]/(f(T))$ *defined by* $f(x)$ and write it as a product of finite field extensions of K as follows:

$$L_K = L_{K,1} \times \cdots \times L_{K,m_K},$$

where m_K is the number of irreducible factors of $f(x)$ in $K[x]$ and each L_{K,m_i} corresponds to an irreducible factor of $f(x)$ in $K[x]$ via the Chinese Remainder Theorem. The notions like the ring of integers, the group of fractional ideals and the class group are available for the algebra L_K; namely, we define

$$\begin{aligned} \mathcal{O}_{L_K} &= \mathcal{O}_{L_{K,1}} \times \cdots \times \mathcal{O}_{L_{K,m_K}}, \\ I(L_K) &= I(L_{K,1}) \times \cdots \times I(L_{K,m_K}), \\ \mathrm{Cl}(L_K) &= \mathrm{Cl}(L_{K,1}) \times \cdots \times \mathrm{Cl}(L_{K,m_K}). \end{aligned}$$

Moreover, for an element $\alpha = (\alpha_1, \ldots, \alpha_{m_K}) \in L_K$, we define the norm $N_K(\alpha)$ of α by

$$N_K(\alpha) = \prod_{i=1}^{m_K} N_K^{L_{K,i}}(\alpha_i),$$

where, for each $i = 1, \ldots, m_K$, $N_K^{L_{K,i}} : L_{K,i} \to K$ is the usual field norm.

Finally, we remark that all the dimensions in this thesis are taken over the finite field $\mathbb{F}_2$.

3.2 A more concrete description of the 2-Selmer group

The following group will replace the rather abstract cohomology group $H^1(\mathbb{Q}, J[2])$:

Definition 3.2.1. *We put*

$$H_K = \ker(N_K : L_K^\times/(L_K^\times)^2 \to K^\times/(K^\times)^2),$$

where the map N_K is induced by the norm map we have defined above.

At this point, we want to make some simplifications on the notation. When $K = \mathbb{Q}$, we will omit the field from subscripts, and if $K = \mathbb{Q}_v$ for a place v of $\mathbb{Q}$, we will just use the subscript v. With this convention, when we write L, for example, we actually mean $L_{\mathbb{Q}} = \mathbb{Q}[T]/(f(T))$. Or, instead of the somewhat cumbersome notation $H_{\mathbb{Q}_v} = \ker(N_{\mathbb{Q}_v} : L_{\mathbb{Q}_v}^{\times}/(L_{\mathbb{Q}_v}^{\times})^2 \to {\mathbb{Q}_v}^{\times}/({\mathbb{Q}_v}^{\times})^2)$, we will be writing $H_v = \ker(N_v : L_v^{\times}/(L_v^{\times})^2 \to {\mathbb{Q}_v}^{\times}/({\mathbb{Q}_v}^{\times})^2)$. This convention is to apply to any object in this thesis that has a field as subscript.

Let $\mathrm{Div}_{\perp}^0$ denote the degree 0 divisors on C with support disjoint from the support of the principal divisor $\mathrm{div}(y)$. Note that the support of $\mathrm{div}(y)$ contains the points with coordinates $(\alpha, 0)$, where α is a root of $f(x)$, and the point at infinity. Then for any extension K of $\mathbb{Q}$, we have a homomorphism

$$F_K : \mathrm{Div}_{\perp}^0(C)(K) \to L_K^{\times}, \qquad \sum_P n_P P \longmapsto \prod_P (x(P) - \theta)^{n_P},$$

where θ is the image of T under the reduction $K[T] \to K[T]/(f(T))$. More precisely, θ is an m_K-tuple $(\theta_1, \ldots, \theta_{m_K})$ with each θ_i being a root of the i^{th} irreducible factor of $f(x)$. Hence the map F_K is given by

$$F_K : \sum_P n_P P \mapsto \Big(\prod_P (x(P) - \theta_1), \ldots, \prod_P (x(P) - \theta_{m_K}) \Big).$$

Theorem 3.2.2. *The map F_K above induces a homomorphism*

$$\delta_K : J(K) \to H_K,$$

with kernel $2J(K)$. The induced injective map $J(K)/2J(K) \to H_K$ will be denoted by δ_K as well.

Proof. The proof essentially relies on two lemmas. The first one shows that the function F_K is a well-defined map which maps to $L^{\times}/(L^{\times})^2$. This part makes use of Weil's Reciprocity and is not very technical. And the second one shows that any point in $J(K)$ can be represented by a divisor from $\mathrm{Div}_{\perp}^0(C)(K)$. For details, see [16, Proposition 3.3] or [17, Lemma 2.1 and Lemma 2.2]. E. Schaefer's treatment in [16] is much more general, though. □

The following theorem finally establishes the important isomorphism $H \cong H^1(\mathbb{Q}, J[2])$.

Theorem 3.2.3. *For all extensions K of $\mathbb{Q}$, there exists a natural isomorphism*

$$H_K \cong H^1(K, J[2]).$$

Moreover, δ_K from Theorem 3.2.2 above composed with this isomorphism is the coboundary morphism

$$\delta : J(K)/2J(K) \to H^1(K, J[2])$$

from §2.1.

Proof. Let K be an extension of $\mathbb{Q}$. We want to relate the two seemingly different groups H_K and $H^1(K, J[2])$. To this end, assume that $\deg(f) = d$ and remember that we assume d to be odd. Let $\{\alpha_1, \ldots, \alpha_d\}$ be roots of $f(x)$ in $\overline{K}$. Then Theorem 1.3.1 implies that the classes of the divisors

$$D_1 = (\alpha_1, 0) - \infty, \ldots, D_d = (\alpha_d, 0) - \infty$$

generate $J[2]$. Define L to be the algebra $K[T]/(f(T))$ and $\overline{L}$ to be the algebra $\overline{K}[T]/(f(T))$. So we have

$$\overline{L} \cong \overline{K}[T]/(T - \alpha_1) \times \cdots \times \overline{K}[T]/(T - \alpha_n) \cong \overline{K}^d.$$

Let $\mu_2(\overline{L})$ denote the 2^{nd} roots of unity in $\overline{L}$. Clearly, $\mu_2(\overline{L}) \cong \{\pm 1\}^d$. Let

$$e_2 : J[2] \times J[2] \to \{\pm 1\}$$

denote the Weil pairing on $J[2]$. We define a map

$$w : J[2] \to \mu_2(\overline{L})$$

via

$$D \mapsto (e_2(D, D_1), \ldots, e_2(D, D_d))$$

for all $D \in J[2] \cong \mathrm{Pic}^0(C)[2]$. Then, by functoriality of Galois cohomology, w induces a map

$$w^* : H^1(K, J[2]) \to H^1(K, \mu_2(\overline{L})).$$

On the other hand, we have an isomorphism

$$k : H^1(K, \mu_2(\overline{L})) \to L^\times/(L^\times)^2.$$

Indeed, since $\overline{L}$ is a finitely generated $\overline{K}$-algebra, a generalised version of Hilbert's 90 implies that $H^1(K, \overline{L}^\times) = 0$ (see [19, p. 152]). Therefore, k is a Kummer isomorphism which is obtained from the long exact cohomology sequence associated to the following short exact sequence:

$$0 \to \mu_2(\overline{L}) \to \overline{L}^\times \xrightarrow{2} \overline{L}^\times \to 0.$$

Now, we want to prove that the composition

$$k \circ w : H^1(K, J[2]) \to L^\times/(L^\times)^2$$

maps to H_K and gives rise to a group isomorphism between $H^1(K, J[2])$ and its image H_K.

To this end, we first want to see that the sequence

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

is exact, where N denotes the norm map. The map w is injective by non-degeneracy of the Weil pairing and the norm map N is clearly surjective. Note, moreover, that

$$\dim_{\mathbb{F}_2} J[2] = d - 1, \ \dim_{\mathbb{F}_2} \mu_2(\overline{L}) = d, \text{ and } \dim_{\mathbb{F}_2} \mu_2(\overline{K}) = 1,$$

where the first equality follows from Theorem 1.3.1. Hence, to prove the exactness at the middle, it is enough to show that $N \circ w = 1$. So let $D \in J[2]$: by Theorem 1.3.1 and the additivity of the Weil pairing, we get

$$\begin{aligned} w(D) &= (e_2(D, D_1), \ldots, e_2(D, D_d)) \\ &= \Big(e_2(D, D_1), \ldots, e_2(D, D_{d-1}), e_2(D, -\sum_{i=1}^{d-1} D_i)\Big) \\ &= \Big(e_2(D, D_1), \ldots, e_2(D, D_{d-1}), \prod_{i=1}^{d-1} e_2(D, D_i)\Big). \end{aligned}$$

Therefore,

$$N(w(D)) = \Big(\prod_{i=1}^{d-1} e_2(D, D_i)\Big)^2 = 1,$$

and the sequence (*) is exact. Hence Theorem 1.4.3 yields a long exact cohomology sequence:

$$\cdots \to \mu_2(L) \xrightarrow{N} \mu_2(K) \to H^1(K, J[2]) \xrightarrow{w^*} H^1(K, \mu_2(\overline{L})) \xrightarrow{N^*} H^1(K, \mu_2(\overline{K})) \to \ldots,$$

where $H^1(K, \mu_2(\overline{L})) \xrightarrow{N^*} H^1(K, \mu_2(\overline{K}))$ is induced functorially by $\mu_2(L) \xrightarrow{N} \mu_2(K)$. But we have the following Kummer isomorphisms:

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

Moreover, $(-1, \ldots, -1) \in \mu_2(L)$ is mapped to -1 as d is odd. So the norm map N is surjective and hence $H^1(K, J[2]) \cong \ker(N^*)$, as desired. Therefore, we have proved the first assertion of the theorem.

For the second assertion, one can prove that the maps F_K and $k \circ w \circ \delta$ coincide as injections from $J(K)/2J(K)$ to $L^\times/(L^\times)^2$, where δ is the coboundary morphism. Since by Theorem 3.2.2, F_K induces δ_K, this can be shown to imply the desired result. For details and general case, refer to [16, Theorem 2.3] or [17, Theorem 1.2]. □

Suppose for simplicity that L is a number field; *i.e.* $f(x)$ is irreducible over $\mathbb{Q}$. Suppose $\alpha \in L$ with $N_{\mathbb{Q}}^{L}(\alpha) = 1$. Then, if the minimal polynomial of α over $\mathbb{Q}$ has degree d and constant term a_d, we have $N_{\mathbb{Q}}^{L}(\alpha) = (-1)^d a_d = 1$. Now, write

$$L_v = \mathbb{Q}_v[T]/(f(T)) = L_{v,1} \times \cdots \times L_{v,m_v},$$

where, as usual, m_v is the number of irreducible factors of $f(x)$ in $\mathbb{Q}_v[x]$ and $L_{v,i}/\mathbb{Q}_v$ are finite field extensions for $i = 1, \ldots, m_v$. We then have a natural inclusion map

$$L \to L_v, \qquad \alpha \mapsto (\alpha, \ldots, \alpha),$$

which is induced by the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$. Assume that the minimal polynomial of $\alpha \in L_{v,i}$ over $\mathbb{Q}_v$ has constant term $C_i \in \mathbb{Q}_v$ for all $i = 1, \ldots, m_v$ so that $N_{\mathbb{Q}_v}^{L_{v,i}}(\alpha) = (-1)^{[L_{v,i}:\mathbb{Q}_v]} C_i$. Then

$$N_v(\alpha, \ldots, \alpha) = \prod_{i=1}^{m_v} N_{\mathbb{Q}_v}^{L_{v,i}}(\alpha) = \prod_{i=1}^{m_v} (-1)^{[L_{v,i}:\mathbb{Q}_v]} C_i = (-1)^d a_d = 1.$$

Therefore, we have obtained a map of groups

$$H = \ker(N : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \to H_v = \ker(N_v : L_v^\times/(L_v^\times)^2 \to \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2).$$

This reasoning carries over to the case where L is an algebra; *i.e.*, to the case where $f(x)$ is only assumed to be squarefree. We conclude that for any place v of $\mathbb{Q}$, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ induces a map

$$\mathrm{res}_v : H \to H_v.$$

Remember that we have seen in Theorem 3.2.2 that there are induced maps $\delta_v : J(\mathbb{Q}_v) \to H_v$. We obtain

Theorem 3.2.4. *The 2-Selmer group of J over $\mathbb{Q}$ can be identified to*

$$\mathrm{Sel}^2(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all places } v\},$$

where $\mathrm{res}_v : H \to H_v$ is the restriction map defined above.

Proof. By Theorem 3.2.3 we can form the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & H & \longrightarrow & H^1(\mathbb{Q}, J)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & \searrow^{\phi} & \downarrow & & \\ 0 & \longrightarrow & \prod_v J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \xrightarrow{\prod_v \delta_v} & \prod_v H_v & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J)[2] & \longrightarrow & 0 \end{array},$$

where the products are taken over all the places v. Assume $\xi \in \ker(\phi) = \mathrm{Sel}^2(\mathbb{Q}, J)$. By commutativity of the right square, this is equivalent to requiring that

$$\prod_v \mathrm{res}_v(\xi) \in \ker\Big(\prod_v H_v \to \prod_v H^1(\mathbb{Q}_v, J)[2]\Big).$$

By exactness of the second row, this is the same as requiring that

$$\prod_v \mathrm{res}_v(\xi) \in \prod_v J(\mathbb{Q}_v)/2J(\mathbb{Q}_v).$$

Since $2J(\mathbb{Q}_v)$ is in the kernel of δ_v, this holds if and only if

$$\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)),$$

for all places v, as needed. □

3.3 A finite description of the 2-Selmer group

Although the new description of the 2-Selmer group we gave in Theorem 3.2.4 seems fairly less abstract than the original definition, it still takes us to check infinitely many conditions to determine if an element $\xi \in H$ belongs to $\mathrm{Sel}(\mathbb{Q}, J)$, simply because there are infinitely many places v of $\mathbb{Q}$. In this section, however, we will be able to reduce the set of places to consider to a finite set S. It is not a coincidence that S will turn out to be the same S that appeared in the statement of Theorem 2.2.2.

Write $L = \mathbb{Q}[T]/(f(T)) = L_1 \times \cdots \times L_m$, where $L_i/\mathbb{Q}$ are number fields for $i = 1, \ldots, m$. Recall that we have defined the group of fractional ideals of L as follows:

$$I(L) = I(L_1) \times \cdots \times I(L_m),$$

where $I(L_i)$ is the usual group of ideals of L_i for each $i = 1, \ldots, m$.

Let v be a finite place of $\mathbb{Q}$; *i.e.*, $v = p$ is a prime, and let $I_p(L)$ denote the subgroup of $I(L)$ consisting of ideals with support above p. In other words, $I_p(L)$ is the subgroup of $I(L)$ generated by ideals of the form

$$\mathfrak{p}_1 \times \cdots \times \mathfrak{p}_i \times \cdots \times \mathfrak{p}_m,$$

where, for each $i = 1, \ldots, m$, $\mathfrak{p}_i$ is a prime ideal of L_i above p. Therefore, a typical element of $I_p(L)$ can be written as

$$\Big(\prod_{i=1}^{g_1} \mathfrak{p}_{1,i}^{n_{1,i}}, \ldots, \prod_{i=1}^{g_m} \mathfrak{p}_{m,i}^{n_{m,i}}\Big),$$

where, for each $j = 1, \ldots, m$, $\mathfrak{p}_{j,i}$ is a prime ideal of L_i above p for all $i = 1, \ldots, g_j$ and $n_{j,i} \in \mathbb{Z}$. For any prime p, the norm of an element of $I_p(L)$ is given by

$$N\Big(\prod_{i=1}^{g_1} \mathfrak{p}_{1,i}^{n_{1,i}}, \ldots, \prod_{i=1}^{g_m} \mathfrak{p}_{m,i}^{n_{m,i}}\Big) = \prod_{j=1}^{m} \prod_{i=1}^{g_m} N(\mathfrak{p}_{j,i})^{n_{j,i}}.$$

This motivates the following definition:

Definition 3.3.1. *Let L be as above and p be a prime. We define*

$$I_p = \ker(N : I_p(L)/I_p(L)^2 \to I_p(\mathbb{Q})/I_p(\mathbb{Q})^2).$$

Observe that for any prime p, we have an isomorphism (see [22, Theorem 2.14])

$$I_p(L) \cong I(L_p).$$

To see this, suppose for simplicity that L is a number field. Let p be a prime number and assume $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are primes of L over p. Then we have

$$I(L_p) = I(L \otimes_{\mathbb{Q}} \mathbb{Q}_p) \cong I(L_{\mathfrak{p}_1}) \times \cdots \times I(L_{\mathfrak{p}_n}).$$

Therefore, this isomorphism assigns to an ideal $\mathfrak{I} \in I_p(L)$ the n-tuple $(\mathfrak{I}_{\mathfrak{p}_1}, \ldots, \mathfrak{I}_{\mathfrak{p}_n})$ of localisations of $\mathfrak{I}$ at the various prime ideals of L above p. One then generalises this reasoning to an algebra L.

Definition 3.3.2. *For any prime p, denote by*

$$\mathrm{val}_p : H_p \to I_p,$$

the map induced by $L_p^\times \to I(L_p)$ that sends $\alpha \in L_p^\times$ to the ideal $(\alpha) \in I(L_p)$ it generates.

Via the identification $I_p(L) \cong I(L_p)$, it is clear that the map val is well-defined. The following is the last definition of this section:

Definition 3.3.3. *Let$L = \mathbb{Q}[T]/(f(T))$ be as above.*

(i) For a finite set S of places of $\mathbb{Q}$, we put

$$I_S(L) = \prod_{p \in S \setminus \{\infty\}} I_p(L) \subseteq I(L);$$

that is, $I_S(L)$ is the group generated by ideals in $I(L)$ with support above $S \setminus \{\infty\}$.
(ii) We define

$$\mathrm{val} : H \to I(L)/I(L)^2.$$

The map val *is induced by the map associating to an element $\alpha \in H$ the principal ideal $(\alpha) \in I(L)$ it generates.*

In the following lemma, we present some useful dimension results for various spaces we have defined so far.

Lemma 3.3.4. *Let p be a prime and consider the p-adic field $\mathbb{Q}_p$. Let d_p be as in Theorem 1.3.4. We have*

(i) $\dim H_p = 2 \dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = 2(m_p - 1 + d_p g)$,

(ii) $\dim I_p = m_p - 1$.

Proof. (i) If M is a p-adic local field; *that is*, if it is a finite extension of $\mathbb{Q}_p$ for a prime p, then we know that (see [20, Chapter II, Corollary to Theorem 3.3])

$$\dim M^\times/(M^\times)^2 = 2 + d_p[M : \mathbb{Q}_p],$$

where $[M : \mathbb{Q}_p]$ is the degree of the extension $M/\mathbb{Q}_p$. Recall that $d_p = 0$ if $p \neq 2$ and $d_p = 1$ if $p = 2$. Since L_p is the product of m_p-many p-adic local fields, we obtain

$$\dim L_p^\times/(L_p^\times)^2 = 2m_p + \deg(f)d_p.$$

Moreover, as $\deg(f) = 2g + 1$ is odd by assumption, the norm map $N_p : L_p^\times/(L_p^\times)^2 \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is surjective. Thus,

$$\dim H_p = \dim L_p^\times/(L_p^\times)^2 - \dim \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = 2m_p + (2g+1)d_p - 2 - d_p = 2(m_p - 1 + d_p g),$$

as required. Finally, this is equal to $2 \dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ by Theorem 1.3.4.

(ii) Remember we noted that

$$I_p(L) \cong I(L_p) \cong I(L_{\mathfrak{p}_1}) \times \cdots \times I(L_{\mathfrak{p}_n}),$$

where $\mathfrak{p}_i$'s are the prime ideals of L lying above p. But the number of such primes is precisely m_p. Therefore

$$\dim I_p(L)/I_p(L)^2 = \dim I(L_p)/I(L_p)^2 = m_p.$$

On the other hand, the norm map $N : I_p(L)/I_p(L)^2 \to I_p(\mathbb{Q})/I_p(\mathbb{Q})^2$ is clearly surjective. Therefore,

$$\dim I_p = \dim I_p(L)/I_p(L)^2 - \dim I_p(\mathbb{Q})/I_p(\mathbb{Q})^2 = m_p - 1,$$

as needed. □

Let p be a prime. Recall that we have defined the maps $\delta_p : J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \to H_p$ (see §3.2) and $\mathrm{val}_p : H_p \to I_p$. Therefore, one can form the sequence

$$0 \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \subseteq I_p(L)/I_p(L)^2$$

and study if it is exact or not. The following technical lemma, the proof of which is omitted due to its being so, will immediately imply that this sequence is actually exact for almost all primes p.

Lemma 3.3.5. *Suppose that p is an odd prime such that p^2 does not divide* $\mathrm{disc}(f)$. *Then the composition*

$$\mathrm{val}_p \, \delta_p : J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \to I_p$$

is the trivial map.

Proof. See [23, Lemma 4.5]. □

Corollary 3.3.6. *If p is an odd prime such that p^2 does not divide the discriminant* $\mathrm{disc}(f)$ *of f, then the sequence*

$$0 \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \to 0$$

is exact.

Proof. We know that the map δ_p is injective and val_p is surjective. We also know from the previous lemma that $\mathrm{val}_p \, \delta_p = 0$.

Moreover, since p is odd, Lemma 3.3.4 together with Theorem 1.3.4 implies

$$\dim H_p = 2(m_p - 1) = \dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) + \dim I_p.$$

This proves the exactness at H_p and concludes the proof. □

The above corollary will be crucial in simplifying the description of the 2-Selmer group to a finite set S. Before we state this simplification as a theorem, we want to study a commutative diagram which will be helpful in proving it.

Suppose that L is a number field. Note that there exists an isomorphism

$$I(L) \to \prod_p I_p(L), \qquad \prod \mathfrak{p}^{n_\mathfrak{p}} \mapsto \Big(\prod_{\mathfrak{p}|p} \mathfrak{p}^{n_\mathfrak{p}} \Big)_p,$$

where the product runs over all primes p. This isomorphims induces an isomorphism

$$I(L)/I(L)^2 \to \prod_p I_p(L)/I_p(L)^2.$$

Moreover, via the natural identification

$$\Big(\prod_{\mathfrak{p}|p} \mathfrak{p}^{n_\mathfrak{p}} \Big)_p \leftrightarrow \prod_p \prod_{\mathfrak{p}|p} \mathfrak{p}^{n_\mathfrak{p}},$$

we will not distinguish between the elements of $I(L)/I(L)^2$ and $\prod_p I_p(L)/I_p(L)^2$. Therefore, we can form the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{\delta} & H & \xrightarrow{\mathrm{val}} & I(L)/I(L)^2 \\ & & \downarrow & & \downarrow{\scriptstyle \prod_p \mathrm{res}_p} & & \downarrow \\ 0 & \longrightarrow & \prod_p J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \xrightarrow{\prod_p \delta_p} & \prod_p H_p & \xrightarrow{\prod_p \mathrm{val}_p} & \prod_p I_p(L)/I_p(L)^2 \end{array} , \qquad (*)$$

where the products are over all the primes p. The commutativity of the left square is clear by the isomorphisms $H \cong H^1(\mathbb{Q}, J[2])$ and $H_p \cong H^1(\mathbb{Q}_p, J[2])$ we obtained in Theorem 3.2.3. And the commutativity of the right square follows from the isomorphism we have defined above and the identification $I_p(L) \cong I(L_p)$. Note that whenever the products are taken over odd primes p such that p^2 does not divide $\mathrm{disc}(f)$, the sequence at the bottom is exact by Corollary 3.3.6.

We have also proved

Lemma 3.3.7. *We have*

$$\mathrm{val} = \prod_p \mathrm{val}_p \, \mathrm{res}_p,$$

where p runs over all the primes.

We finally obtain the following practical description of the 2-Selmer group:

Theorem 3.3.8. *Let $S = \{\infty, 2\} \cup \{p \mid p^2$ divides* $\mathrm{disc}(f)\}$. *Then*

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2 \text{ and } \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v \in S\}.$$

Proof. Recall that from Theorem 3.2.4, we have

$$\mathrm{Sel}^2(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all places } v\}.$$

Call the set given in the theorem A. We must show that $A = \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$.

First, assume that $\xi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. This means that

$$\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v))$$

for all places v. This implies in particular that $\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v))$ for all $v \in S$. So, to show that $\xi \in A$, we only need to see that $\mathrm{val}(\xi) \in I_S(L)/I_S(L)^2$. By Lemma 3.3.7, this is equivalent to showing that

$$\prod_p \mathrm{val}_p \mathrm{res}_p(\xi) \in I(L)/I(L)^2$$

has support above S; *i.e.* that if $p \notin S$, then $\mathrm{val}_p \mathrm{res}_p = 0$. But we know that whenever $p \notin S$, the sequence at the bottom of the diagram (*) is exact. Hence, since $\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v))$ for all places v, we get $\mathrm{val}_p \mathrm{res}_p(\xi) = 0$ if $p \notin S$. Thus, $\xi \in A$ and $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq A$.

Conversely, assume that $\xi \in A$. Then to show that $\xi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, we only need to show that whenever $p \notin S$,

$$\mathrm{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p)).$$

That $\xi \in A$ implies that $\mathrm{val}(\xi) \in I_S(L)/I_S(L)^2$, which implies that $\mathrm{val}_p \mathrm{res}_p(\xi) = 0$ as $p \notin S$. Hence by Corollary 3.3.6, it follows that $\mathrm{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p))$. Thus, $\xi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ and $A \subseteq \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. □

3.4 A first bound on the dimension of the 2-Selmer group

Based on the new description of the 2-Selmer group we gave in Theorem 3.3.8, we derive a first bound on $\dim \mathrm{Sel}(\mathbb{Q}, J)$, hence on $\mathrm{rank}\, J(\mathbb{Q})$. We continue to consider L as before. Moreover, throughout this section,

$$S = \{\infty, 2\} \cup \{p \mid p^2 \text{ divides } \mathrm{disc}(f)\},$$

as above.

Definition 3.4.1. *For any prime $p \in S$, we put $J_p = \delta_p(J(\mathbb{Q}_p)) \subseteq H_p$, $G_p = \mathrm{val}_p(J_p) \subseteq I_p$, and define*

$$G = \prod_{p \in S \setminus \{\infty\}} G_p \subseteq I(L)/I(L)^2.$$

Notice that when $p \notin S$, we have $\mathrm{val}_p\, \delta_p(J(\mathbb{Q}_p)) = 0$ by Lemma 3.3.5.

We *approximate* $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ by

$$\widetilde{\mathrm{Sel}} = \{\xi \in L^\times/(L^\times)^2 \mid \mathrm{val}(\xi) \in G\} \supseteq \mathrm{Sel}^{(2)}(\mathbb{Q}, J).$$

Lemma 3.4.2. *We have*

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widetilde{\mathrm{Sel}}.$$

Moreover, $\widetilde{\mathrm{Sel}}$ is a finite group of exponent 2 and hence, has a structure of a finite-dimensional $\mathbb{F}_2$-vector space.

Proof. Let $\xi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. Then in particular, $\mathrm{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p))$ for all $p \in S \setminus \{\infty\}$. So $\mathrm{val}_p \mathrm{res}_p(\xi) \in \mathrm{val}_p\, \delta_p(J(\mathbb{Q}_p))$ for all $p \in S \setminus \{\infty\}$. Since $\mathrm{val}_p \mathrm{res}_p(\xi) = 0$ for all $p \notin S$, this means that $\mathrm{val}(\xi) \in G$, as needed.

Moreover, since it is the image of a group under a homomorphism, G_p is a group for each $p \in S \setminus \{\infty\}$. Also, since $G_p \subseteq I_p$, it is a finite group by Lemma 3.3.4. Hence, since G is a finite product of G_p's, it is a finite group. But we have $\widetilde{\mathrm{Sel}} = \mathrm{val}^{-1}(G)$ and val is a group homomorphism. Thus, $\widetilde{\mathrm{Sel}}$ is a finite group. Finally observe that $\widetilde{\mathrm{Sel}} \subseteq H$, which implies that $\widetilde{\mathrm{Sel}}$ is of exponent 2 as H is. □

In the proof of the following important lemma, we show that the containment above is a proper one:

Lemma 3.4.3. *We have*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \dim \widetilde{\mathrm{Sel}} - 1.$$

Proof. Consider the norm map

$$N : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

By Theorem 3.4.2 above, $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widetilde{\mathrm{Sel}}$ and by definition, we have $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \ker(N)$. Therefore,

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widetilde{\mathrm{Sel}} \cap \ker(N) \subseteq \widetilde{\mathrm{Sel}}. \tag{*}$$

It is clear that $-1 \in \widetilde{\mathrm{Sel}}$ as $\mathrm{val}(-1) \in G$. On the other hand, we have $N(-1) = (-1)^{\deg(f)} = -1$ as $\deg(f)$ is odd. This means that $-1 \notin \ker(N)$. Hence we have found an element, namely -1, in $\widetilde{\mathrm{Sel}}$ which is not in the intersection $\widetilde{\mathrm{Sel}} \cap \ker(N)$. Thus, the second containment in (*) is indeed proper. Since $\widetilde{\mathrm{Sel}}$ is finite over $\mathbb{F}_2$ by the above lemma, this implies that

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \dim \left(\widetilde{\mathrm{Sel}} \cap \ker(N)\right) < \dim \widetilde{\mathrm{Sel}},$$

yielding in particular

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \dim \widetilde{\mathrm{Sel}} - 1,$$

as needed. □

We derive an upper bound on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ by finding the dimension of the larger group $\widetilde{\mathrm{Sel}}$. To this end, consider the subgroup

$$W_0 = \ker(\mathrm{val} : L^\times/(L^\times)^2 \to I(L)/I(L)^2) \subseteq L^\times/(L^\times)^2,$$

where the val map is induced by the maps

$$L_i \to I(L_i), \qquad \alpha \longmapsto (\alpha)$$

on each "component" L_i of the algebra L. Since $1 \in G$, it is obvious that $W_0 \subseteq \widetilde{\mathrm{Sel}}$. Moreover, with the following lemma, the dimension of W_0 turns out to be easy to compute.

Lemma 3.4.4. *There is an exact sequence*

$$0 \to \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \to W_0 \to \mathrm{Cl}(L)[2] \to 0.$$

Proof. Apply the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} & & L^\times & \xrightarrow{\ 2\ } & L^\times & \longrightarrow & L^\times/(L^\times)^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{val}} & & \\ 0 & \longrightarrow & I(L) & \xrightarrow{\ 2\ } & I(L) & \longrightarrow & I(L)/I(L)^2 & \longrightarrow & 0 \end{array}$$

to get an exact sequence

$$\mathcal{O}_L^\times \xrightarrow{2} \mathcal{O}_L^\times \to W_0 \to \mathrm{Cl}(L) \xrightarrow{2} \mathrm{Cl}(L),$$

from which we extract the desired short exact sequence. □

Therefore, we get

$$\dim W_0 = \dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 + \dim \mathrm{Cl}(L)[2].$$

Secondly, we let

$$W = G \cap \mathrm{val}(L^\times/(L^\times)^2) \subseteq I(L)/I(L)^2.$$

We have

Lemma 3.4.5. *In the above set-up, we have*

(i) $\dim \widetilde{\mathrm{Sel}} = \dim W_0 + \dim W$,

(ii) $W = \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L))$.

Proof. (i) Consider the following group homomorphism

$$\widetilde{\mathrm{Sel}} \xrightarrow{\varphi} W = G \cap \mathrm{val}(L^\times/(L^\times)^2), \qquad \xi \mapsto \mathrm{val}(\xi).$$

The map φ is surjective by definition of $\widetilde{\mathrm{Sel}}$ and by surjectivity of val onto $\mathrm{val}(L^\times/(L^\times)^2)$. We claim that $W_0 = \ker(\varphi)$. Notice first that the inclusion $\ker(\varphi) \subseteq W_0$ is clear.

To show that $W_0 \subseteq \ker(\varphi)$, suppose $\xi \in W_0$. This means that $\mathrm{val}(\xi) = 0$. Looking at its image under the right-most vertical map in the commutative diagram (*) from the previous section, we see that at each $p \in S \setminus \{\infty\}$, $\mathrm{val}(\xi)$ maps to 0 in $I_p(L)/I_p(L)^2$. This means, by commutativity of the diagram (*), that $\mathrm{val}_p \mathrm{res}_p(\xi) = 0$ for all $p \in S \setminus \{\infty\}$. But obviously for each $p \in S \setminus \{\infty\}$, $1 \in \delta_p(J(\mathbb{Q}_p))$ as $\delta_p(J(\mathbb{Q}_p))$ is a group. Thus, $\mathrm{val}(\xi) \in G$. This implies that $\xi \in \ker(\varphi)$ and hence $W_0 \subseteq \ker(\varphi)$.

Therefore, it follows that

$$\dim \widetilde{\mathrm{Sel}} = \dim \ker(\varphi) + \dim \mathrm{im}(\varphi) = \dim W_0 + \dim W,$$

as needed.

(ii) First we claim that $W \subseteq \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L))$. So let $\mathrm{val}(\xi) \in W$ be arbitrary where $\xi \in \widetilde{\mathrm{Sel}}$. Since $\mathrm{val}(\xi)$ is the class of the principal (ξ) ideal generated by ξ, we see that $\mathrm{val}(\xi) \in \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L))$, as claimed.

Conversely, if $\mathfrak{I} \in \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L))$, then $\mathfrak{I}$ is the square of a principal ideal, hence is a itself principal ideal, say, (ζ). Then $\zeta \in \widetilde{\mathrm{Sel}}$ with $\mathrm{val}(\zeta) = \mathfrak{I}$ and hence $\mathfrak{I} \in G \cap \mathrm{val}(L^\times/(L^\times)^2)$. Thus, $\ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) \subseteq W$. □

The following number-theoretical lemma is the last result we prove in this section before the main theorem.

Lemma 3.4.6. *We have* $\dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 = m_\infty$.

Proof. Let $L \cong L_1 \times \cdots \times L_m$ as before. Let r be the sum of the numbers of real embeddings of all the number fields L_i in L and s the sum of the numbers of pairs of complex embeddings of L_i in L. We begin by observing that $m_\infty = r + s$. To see this, factorise f into its irreducible factors in $\mathbb{R}[x]$:

$$f(x) = f_1 \dots f_r f_{r+1} \dots f_{m_\infty},$$

where f_i are of degree 1 for $i = 1, \dots, r$ and are of degree 2 for $i = r+1, \dots, m_\infty$. Hence, $\deg f = r + 2(m_\infty - r)$. Since $\deg(f) = r + 2s$, this gives that $m_\infty - r = s$.

Note that Dirichlet's Unit Theorem (see [12, Chapter 1, §7]) is applicable to the algebra L as

$$\mathcal{O}_L^\times \cong \prod_{i=1}^{m} \mathcal{O}_{L_i}^\times.$$

Thus, we obtain

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cong \mathcal{O}_L^\times[2] \times (\mathbb{Z}/2\mathbb{Z})^{r+s-1},$$

where $r+s-1$ is called the rank of $\mathcal{O}_L^\times$. Since $\mathcal{O}_L^\times[2] = \mu_2(L) = \{\pm 1\}$, we obtain

$$\begin{aligned}\dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 &= \dim \mathcal{O}_L^\times[2] + \operatorname{rank} \mathcal{O}_L^\times \\ &= 1 + r + s - 1 \\ &= r + s,\end{aligned}$$

from which the result follows. □

The following is the main theorem of this section:

Theorem 3.4.7 (Stoll)**.** *One has*

$$\dim \mathrm{Sel}^2(\mathbb{Q}, J) \leq m_\infty - 1 + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)).$$

Proof. By Lemma 3.4.4 and Lemma 3.4.6, we get

$$\dim W_0 = \dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 + \dim \mathrm{Cl}(L)[2] = m_\infty + \dim \mathrm{Cl}(L)[2].$$

Hence, using Lemma 3.4.3 and Lemma 3.4.5, we get

$$\begin{aligned}\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq \dim \widetilde{\mathrm{Sel}} - 1 \\ &= \dim W_0 + \dim W - 1 \\ &= m_\infty - 1 + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)),\end{aligned}$$

as desired. □

Corollary 3.4.8. *Let $C : y^2 = f(x)$ be a hyperelliptic curve with $f(x) \in \mathbb{Q}[x]$ monic, squarefree and of odd degree. One has the following bound on* $\operatorname{rank} J(\mathbb{Q})$*:*

$$\operatorname{rank} J(\mathbb{Q}) \leq m_\infty - m + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)),$$

where m is the number of irreducible factors of $f(x)$ in $\mathbb{Q}[x]$.

Proof. This directly follows from Theorem 2.3.1 and Theorem 3.4.7. □

Chapter 4

A refined estimation

We describe the idea in the article [4] of Harris B. Daniels, Àlvaro Lozano-Robledo and Erik Wallace. They obtain stronger bounds on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ for certain special classes of hyperelliptic curves.

4.1 Adding a condition at infinity

Similarly to the previous chapter, we approximate $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ by a larger subgroup of $L^\times/(L^\times)^2$, whose dimension is easier to estimate.

Recall that we have defined for all $p \in S \setminus \{\infty\}$, $J_p = \delta_p(J(\mathbb{Q}_p))$. For the place at infinity, we define in a similar way:

$$J_\infty = \delta_\infty(J(\mathbb{R})).$$

Recall also the maps

$$\mathrm{res}_\infty : H \to H_\infty \text{ and } \mathrm{val} : H \to I(L)/I(L)^2$$

we have defined in the previous chapter. Finally, for $S = \{\infty, 2\} \cup \{p \mid p^2 \text{ divides } \mathrm{disc}(f)\}$, recall that we have defined $G_p = \mathrm{val}_p(J_p)$ and put

$$G = \prod_{p \in S \setminus \{\infty\}} G_p \subseteq I(L)/I(L)^2.$$

With the notations as above, we now put

$$\widehat{\mathrm{Sel}} = \{\xi \in L^\times/(L^\times)^2 \mid \mathrm{val}(\xi) \in G,\ \ \mathrm{res}_\infty(\xi) \in J_\infty\}.$$

Clearly, one has

$$\widehat{\mathrm{Sel}} = \widetilde{\mathrm{Sel}} \cap \mathrm{res}_\infty^{-1}(J_\infty).$$

Being the intersection of the finite subgroup $\widetilde{\mathrm{Sel}}$ of exponent 2 with the subgroup $\mathrm{res}_\infty^{-1}(J_\infty)$ of $L^\times/(L^\times)^2$, the above equality shows that $\widehat{\mathrm{Sel}}$ is itself a finite group of exponent 2 and hence has the structure of a finite-dimensional $\mathbb{F}_2$-vector space. Moreover, we have

Lemma 4.1.1. *One has the following containments:*

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widehat{\mathrm{Sel}} \subseteq \widetilde{\mathrm{Sel}}.$$

Proof. As we noted above, $\widehat{\mathrm{Sel}} = \widetilde{\mathrm{Sel}} \cap \mathrm{res}_\infty^{-1}(J_\infty)$. So the second containment is clear. Also, having already proved in Lemma 3.4.2 that $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widetilde{\mathrm{Sel}}$, to prove the first containment, it is enough to prove that $\mathrm{res}_\infty(\xi) \in J_\infty$ whenever $\xi \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. But this obviously follows from the definiton of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ in Theorem 3.2.4. □

Since $\widehat{\mathrm{Sel}}$ consists of elements in $\widetilde{\mathrm{Sel}}$ satisfying an extra condition at infinity, we can rightfully expect the upper bound on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ obtained by approximating by $\dim \widehat{\mathrm{Sel}}$ to be more precise.

4.2 Restriction map at infinity

In this section, we will look more closely at the map res_∞ and see that it actually agrees with the signature map sgntr.

We restrict ourselves to the case where $f(x)$ has $n \geq 3$ real roots and is of degree n. In this case, the algebra L defined by $f(x)$ is said to be *totally real*. So if we write

$$L \cong L_1 \times \cdots \times L_m,$$

then L_i is a totally real number field for each $i = 1, \ldots, m$. We define

$$\tau_i : L \hookrightarrow \mathbb{R},\ i = 1, \ldots, n,$$

an embeddings of the algebra L, via

$$\tau_i(\alpha) = \tau_i(\alpha_1, \alpha_2, \ldots, \alpha_m) := \tau_i(\alpha_j),$$

where $(\alpha_1, \ldots, \alpha_m) \in L$, and $\tau_i : L_j \hookrightarrow \mathbb{R}$ is an embedding of the real number field L_j with $\alpha_j \in L_j$. Note that given $\alpha = (\alpha_1, \ldots, \alpha_m) \in L$, for each $i = 1, \ldots, n$, there exists a unique $\alpha_j \in L_j$ such that τ_i is an embedding of L_j. So the map is well-defined. In particular, for each $i = 1, \ldots, m$, there are $[L_i : \mathbb{Q}]$-many real embeddings of L_i among all the embeddings $\tau_1, \ldots, \tau_n$ so that

$$\sum_{i=1}^{m} [L_i : \mathbb{Q}] = \deg(f) = n,$$

the number of all embeddings $\tau_1, \ldots, \tau_n$ of the algebra L. Finally, we can, and do, order the embeddings $\tau_1, \ldots, \tau_n$ in accordance with the ordering of the number fields $L_1, \ldots, L_m$.

Since f has all real roots and is of degree n, we have

$$L_\infty = \mathbb{R}[T]/(f(T)) \cong \mathbb{R}^n$$

as $\mathbb{R}$-algebras. Also,

$$\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{\pm 1\}.$$

Hence, by definition,

$$\mathrm{res}_\infty : H = \ker(N : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \to H_\infty = \ker(N_\infty : (\mathbb{R}^n)^\times/((\mathbb{R}^n)^\times)^2 \to \{\pm 1\}),$$

where N_∞ is induced by the norm map

$$(\alpha_i, \ldots, \alpha_n) \mapsto \prod_i \alpha_i \in \mathbb{R}^\times.$$

Suppose $\alpha = (\alpha_1, \ldots, \alpha_m) \in H$, then $N(\alpha) = \prod_i \tau_i(\alpha) = 1$. We notice that

$$\mathrm{res}_\infty(\alpha) = (\tau_1(\alpha), \ldots, \tau_n(\alpha)),$$

so that

$$N_\infty(\mathrm{res}_\infty(\alpha)) = \prod_i \tau_i(\alpha) = 1,$$

as required. We extend the domain of res_∞ to $L^\times/(L^\times)^2$ and still call the resulting map res_∞. That is, we have defined

$$\mathrm{res}_\infty : L^\times/(L^\times)^2 \to \{\pm 1\}^n, \qquad \alpha \longmapsto (\tau_1(\alpha), \ldots, \tau_n(\alpha)).$$

Consider now the signature homomorphism

$$\mathrm{sgntr} : L^\times \to \{\pm 1\}^n,$$

given by

$$\alpha \mapsto \left(\frac{\tau_i(\alpha)}{|\tau_i(\alpha)|} \right)_{i=1,\ldots,n}.$$

We obtain

Proposition 4.2.1. *It follows that* res_∞ *agrees with* sgntr *in the sense that for any* $\alpha \in L^\times/(L^\times)^2$, *if* $\tilde{\alpha} \in L^\times$ *denotes its lift to* $L^\times$, *then*

$$\mathrm{res}_\infty(\alpha) = \mathrm{sgntr}(\tilde{\alpha}).$$

Proof. Let $\alpha \in L^\times/(L^\times)^2$ be arbitrary. Note first that if $\bar{\alpha}$ and $\tilde{\alpha}$ are two different lifts of α to $L^\times$, then $\mathrm{sgntr}(\bar{\alpha}) = \mathrm{sgntr}(\tilde{\alpha})$. So, if $i \in \{1, \ldots, n\}$ is arbitrary, then we want to show that

$$\left(\frac{\tau_i(\tilde{\alpha})}{|\tau_i(\tilde{\alpha})|}\right) = \tau_i(\alpha) \mod (\mathbb{R}^\times)^2.$$

But $\tau_i(\alpha) \mod (\mathbb{R}^\times)^2 \in \{\pm 1\}$. Hence this is obvious by a sign analysis. □

Now, let $\mathcal{O}_L^{\times,+} \subseteq \mathcal{O}_L^\times$ be the subgroup of totally positive units of $\mathcal{O}_L$. These are by definition the elements $\alpha \in \mathcal{O}_L^\times$ such that $\tau_i(\alpha) > 0$ for all $i = 1, \ldots, n$. From Proposition 4.2.1, it follows that

$$\ker\left(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}\right) = \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2.$$

Definition 4.2.2. *We put*

$$\rho_\infty = \dim\left(\mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2\right),$$

and

$$j_\infty = \dim\left(\mathrm{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cap J_\infty\right).$$

In particular, if every totally positive unit of L *is a square in* L, *then we have* $\rho_\infty = 0$.

Proposition 4.2.3. *We have*

$$\dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) = j_\infty + \rho_\infty.$$

Proof. Considering the surjective group homomorphism

$$\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2} : \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty) \to \mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \cap J_\infty,$$

it clearly follows from above that

$$\begin{aligned}\dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) &= \dim\left(\mathrm{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cap J_\infty\right) + \dim\ker\left(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}\right)\\ &= \dim\left(\mathrm{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cap J_\infty\right) + \dim\left(\mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2\right)\\ &= j_\infty + \rho_\infty.\end{aligned}$$

□

Remark 4.2.4. *In [4], the above proposition and construction is only done for number fields. Hence, we have generalised this to algebras. This will allow us to generalise the refinement of the bound on the rank they obtained in [4, Proposition 2.25] to algebras as well. See Theorem 4.5.1.*

4.3 A new bound on the dimension of the 2- Selmer group

As a piece of notation, we begin by putting $L_{J_\infty} = \mathrm{res}_\infty^{-1}(J_\infty)$ to have

$$\widehat{\mathrm{Sel}} = \{\xi \in L_{J_\infty} \mid \mathrm{val}(\xi) \in G\}.$$

As in §3.4, we will define certain subspaces $\widehat{W_0} \subseteq L_{J_\infty}$ and $\widehat{W} \subseteq I(L)/I(L)^2$ and compute the dimension of $\widehat{\mathrm{Sel}}$ with the help of these subspaces.

Indeed, we put

$$\widehat{W_0} = \ker(\mathrm{val} : L_{J_\infty} \to I(L)/I(L)^2) \subseteq L_{J_\infty}.$$

and

$$\widehat{W} = G \cap \mathrm{val}(L_{J_\infty}) \subseteq I(L)/I(L)^2.$$

Observe that the subspaces $\widehat{W_0}$ and $\widehat{W}$ are analogues of the ones we have defined in §3.4. Observe also that

$$\dim(\widehat{W_0}) = \dim(W_0 \cap L_{J_\infty}) \leq \dim(W_0),$$

and

$$\dim(\widehat{W}) = \dim(W \cap \mathrm{val}(L_{J_\infty})) \leq \dim(W).$$

The following two lemmas should therefore look familiar:

Lemma 4.3.1. *Let the subspaces $\widehat{W_0}$ and $\widehat{W}$ be defined as above. We have*

$$\dim \widehat{\mathrm{Sel}} = \dim \widehat{W_0} + \dim \widehat{W}.$$

Proof. Consider the group homomorphism

$$\widehat{\mathrm{Sel}} \xrightarrow{\widehat{\varphi}} G \cap \mathrm{val}(L_{J_\infty}), \qquad \xi \mapsto \mathrm{val}(\xi).$$

We claim that $W_0 = \ker(\widehat{\varphi})$. First observe that $\widehat{\varphi}$ is surjective by construction. Moreover, the containment $\ker(\widehat{\varphi}) \subseteq W_0$ is a triviality.

Conversely, if $\xi \in \widehat{W_0}$, to show that $\xi \in \ker(\widehat{\varphi})$, we only need to show $\mathrm{val}(\xi) \in G$. But we have already showed this in Lemma 3.4.5. Thus, we conclude that $\ker(\widehat{\varphi}) = W_0$. □

Before we state the next lemma, we need to introduce some notation. Let

$$U = (\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \cap L_{J_\infty} \text{ and } \mathrm{Cl}(L_{J_\infty}) = I(L)/P(L_{J_\infty}),$$

where $P(L_{J_\infty})$ is the group of principal fractional ideals $\mathfrak{A} = (\alpha)$ with a generator $\alpha \in L$ such that $\mathrm{res}_\infty(\alpha) \in J_\infty$. Moreover, we put

$$\mathrm{Cl}(L_{J_\infty})[2] = \{[\mathfrak{A}] \in \mathrm{Cl}(L_{J_\infty}) \mid \mathfrak{A}^2 = (\alpha) \text{ for some } \alpha \in L_{J_\infty}\}.$$

Note that then we have an exact sequence

$$0 \to \mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) \to L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) \to I(L) \to \mathrm{Cl}(L_{J_\infty}) \to 0.$$

We obtain

Lemma 4.3.2. *There exists a short exact sequence*

$$0 \to U \to \widehat{W_0} \to \mathrm{Cl}(L_{J_\infty})[2] \to 0.$$

In particular,

$$\dim \widehat{W_0} = \dim U + \dim \mathrm{Cl}(L_{J_\infty})[2].$$

Proof. Similarly to Lemma 3.4.4, one applies the Snake Lemma to the diagram

$$\begin{array}{ccccccccc}
 & & L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) & \xrightarrow{2} & L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) & \longrightarrow & L_{J_\infty} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{val}} & & \\
0 & \longrightarrow & I(L) & \xrightarrow{2} & I(L) & \longrightarrow & I(L)/I(L)^2 & \longrightarrow & 0
\end{array}$$

to get an exact sequence

$$\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) \xrightarrow{2} \mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) \to \widehat{W_0} \to \mathrm{Cl}(L_{J_\infty}) \xrightarrow{2} \mathrm{Cl}(L_{J_\infty}),$$

which induces a short exact sequence

$$0 \to \mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty)/(\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty))^2 \to \widehat{W_0} \to \mathrm{Cl}(L_{J_\infty})[2] \to 0.$$

Therefore, it remains to see that

$$\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty)/(\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty))^2 \cong \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty).$$

To this end, consider the map

$$\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) \to \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty),\ u \mapsto \overline{u}.$$

Note that if $u \in \mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty)$, then we have $u \in \mathcal{O}_L^\times$ and $\mathrm{res}_\infty^{-1}(\overline{u}) \in J_\infty$. So the map is well-defined and is also clearly surjective. Moreover, it is also clear that the kernel of the map is $(\mathcal{O}_L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty))^2$.

Therefore, we obtain the desired isomorphism and hence the exact sequence in the theorem. The claim on dimensions is immediate from the exact sequence. □

Let $P(L) \subseteq I(L)$ be the subgroup of *principal ideals* of L, $P^+(L) \subseteq P(L)$ be the subgroup of $P(L)$ consisting of principal ideals generated by totally positive elements and $P(L_{J_\infty})$ be as above. We then have

Lemma 4.3.3. *One has $P^+(L) \subseteq P(L_{J_\infty}) \subseteq P(L)$. In particular,*

$$\mathrm{Cl}(L)[2] \subseteq \mathrm{Cl}(L_{J_\infty})[2] \subseteq \mathrm{Cl}^+(L)[2],$$

where $\mathrm{Cl}^+(L)$ denotes the narrow class group of L.

Proof. Note that the second containment follows from the definition. So we only prove the first containment that $P^+(L) \subseteq P(L_{J_\infty})$.

To this end, assume that $\alpha \in L^\times$ is a totally positive element. Let $\overline{\alpha}$ be its class in $L^\times/(L^\times)^2$. We then have $\mathrm{res}_\infty(\overline{\alpha}) = (1, \ldots, 1)$. This implies that

$$\overline{\alpha} \in \ker(\mathrm{res}_\infty) \subseteq \mathrm{res}_\infty^{-1}(J_\infty).$$

Thus, $\mathrm{res}(\overline{\alpha}) \in J_\infty$ and the principal ideal (α) generated by the totally positive element $\alpha \in L^\times$ is in $P(L_{J_\infty})$. Thus, $P^+(L) \subseteq P(L_{J_\infty})$.

Finally, the containments $P^+(L) \subseteq P(L_{J_\infty}) \subseteq P(L)$ clearly imply the desired containments of 2-torsion subgroups of the class groups. □

The following theorem is in some sense the analogue of Theorem 3.4.7 from the previous chapter.

Theorem 4.3.4. *We have*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) + \dim \mathrm{Cl}^+(L)[2] + \dim G \cap \mathrm{val}(L_{J_\infty}),$$

Proof. The results we have obtained in this section clearly imply

$$\begin{aligned}
\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq \dim \widehat{\mathrm{Sel}} \\
&= \dim \widehat{W_0} + \dim \widehat{W} \\
&= \dim U + \dim \mathrm{Cl}(L_{J_\infty})[2] + \dim \widehat{W} \\
&= \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) + \dim \mathrm{Cl}(L_{J_\infty})[2] + \dim G \cap \mathrm{val}(L_{J_\infty}) \\
&\leq \dim(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)) + \dim \mathrm{Cl}^+(L)[2] + \dim G \cap \mathrm{val}(L_{J_\infty}).
\end{aligned}$$

□

Remark 4.3.5. *The bound in the above theorem is not immediately comparable with Stoll's bound (Theorem 3.4.7). However, we observe, for example, that*

$$\dim(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)) \leq m_\infty - 1.$$

To see this, it is enough to find an element in $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ which does not belong to the intersection $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)$. But $\mathrm{res}_\infty(-1)$ does the job. Indeed, since J_∞ is contained in the kernel of the norm map $N_\infty : L_\infty^\times/(L_\infty^\times)^2 \to \mathbb{R}^\times/(\mathbb{R}^\times)^2$, we have $N_\infty(j) = 1$ for any $j \in J_\infty$. However,

$$N(\mathrm{res}_\infty(-1)) = N(-1) = -1,$$

as $\deg(f)$ is odd. Thus, $\mathrm{res}_\infty(-1) \notin \mathrm{res}_\infty(J_\infty)$ and the result follows.

4.4 Totally positive units

In this section, we study totally positive units in number fields as a preliminary to the next section, where we will obtain some refinements of the bound we obtained in Theorem 4.3.4. In particular, we will be able to get the term $\mathrm{Cl}^+(L)$ in the bound under control.

Lemma 4.4.1. *Let L be a totally real number field of odd degree $n \geq 3$. Define*

$$\rho = \dim_{\mathbb{F}_2} \mathrm{Cl}(L)/2\,\mathrm{Cl}(L),\ \rho^+ = \dim_{\mathbb{F}_2} \mathrm{Cl}^+(L)/2\,\mathrm{Cl}^+(L),\ \textit{and}\ \rho_\infty = \dim_{\mathbb{F}_2}(\mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2).$$

Then there exists an exact sequence

$$0 \to \{\pm 1\}^n/\operatorname{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \to \mathrm{Cl}^+(L) \to \mathrm{Cl}(L) \to 0.$$

In particular, $\rho^+ \leq \rho_\infty + \rho$.

Proof. Recall that $P(L)$ denotes the group of principal ideals in L and $P^+(L)$ the group of principal ideals generated by totally positive elements. We then have the isomorphisms:

$$\mathrm{Cl}(L) \cong I(L)/P(L) \cong (I(L)/P^+(L))/(P(L)/P^+(L)) \cong \mathrm{Cl}^+(L)/(P(L)/P^+(L)),$$

yielding the following exact sequence relating the narrow and usual class groups:

$$0 \to P(L)/P^+(L) \to \mathrm{Cl}^+(L) \to \mathrm{Cl}(L) \to 0. \tag{*}$$

Also, the map $\alpha \mapsto (\alpha)$ that sends $\alpha \in L^\times$ to the principal ideal (α) it generates yields the exact sequence

$$1 \to \mathcal{O}_L^\times \to L^\times \to P(L) \to 0.$$

Let $L^{\times,+} \subseteq L^\times$ be the subgroup of totally positive elements. By definition, $P^+(L)$ is the image of $L^{\times,+}$ in $P(L)$. This gives an isomorphism

$$P(L)/P^+(L) \cong L^\times/\mathcal{O}_L^\times L^{\times,+}.$$

So the exact sequence (*) can be wrtitten as

$$0 \to L^\times/\mathcal{O}_L^\times L^{\times,+} \to \mathrm{Cl}^+(L) \to \mathrm{Cl}(L) \to 0. \tag{**}$$

Now, consider the surjective homomorphism

$$\{\pm 1\}^n \to L^\times/\mathcal{O}_L^\times L^{\times,+},$$

mapping an n-tuple $(\varepsilon_i)_{i=1,\dots,n} \in \{\pm 1\}^n$ to the class of an element $\alpha \in L^\times$ that satisfies

$$\mathrm{sgntr}(\alpha) = (\varepsilon)_{i=1,\dots,n}.$$

Note that if $\alpha, \beta \in L^\times$ such that $\mathrm{sgntr}(\alpha) = \mathrm{sgntr}(\beta)$, then since sgntr is a group homomorphism, we have

$$\mathrm{sgntr}(\alpha\beta^{-1}) = \mathrm{sgntr}(\alpha)\,\mathrm{sgntr}(\beta)^{-1} = 1$$

so that $\alpha\beta^{-1} \in \mathcal{O}_L^\times L^{\times,+}$. Hence the map is well-defined. Moreover, the kernel of this homomorphism is $\operatorname{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right)$. Hence we get an isomorphism

$$\{\pm 1\}^n/\operatorname{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cong L^\times/\mathcal{O}_L^\times L^{\times,+}$$

and the exact sequence (**) can be written as

$$0 \to \{\pm 1\}^n/\operatorname{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \to \mathrm{Cl}^+(L) \to \mathrm{Cl}(L) \to 0, \tag{***}$$

as needed.

Finally, to see that $\rho^+ \leq \rho_\infty + \rho$, first observe that

$$\dim\{\pm 1\}^n/\operatorname{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) = n - \dim \operatorname{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right).$$

Considering now the surjective homomorphism

$$\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}:\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\to\mathrm{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right),$$

since $\dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right)=n$ and $\rho_\infty=\dim\left(\mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)\right)^2$ is the dimension of $\ker\left(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}\right)$, it follows that

$$\dim\{\pm1\}^n/\mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2)=n-(n-\rho_\infty)=\rho_\infty.$$

Thus, $\rho^+\leq\rho_\infty+\rho$ by exactness of the sequence (***). Proof is complete. □

The proof of the following theorem is technical. So we only give a reference for it. The corollary following it will prove important in subsequent sections.

Theorem 4.4.2. *Let $L/\mathbb{Q}$ be a finite Abelian extension with Galois group of odd exponent n, and suppose that -1 is congruent to a power of 2 modulo n. Then, in the notation of the above theorem, we have $\rho=\rho^+$.*

Proof. See [14]. □

Corollary 4.4.3. *Let L be a cyclic number field of odd prime degree p, and suppose that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even. Then, $\rho=\rho^+$. In particular,* $\dim\mathrm{Cl}(L)[2]=\dim\mathrm{Cl}^+(L)[2]$.

Proof. By assumption $\mathrm{Gal}(L/\mathbb{Q})\cong\mathbb{Z}/n\mathbb{Z}$ for $n\geq2$. Suppose that the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$ is even. This is equivalent to -1 being congruent to a power of 2 modulo n. Thus result follows from the previous theorem. □

We finally state the following proposition with its proof omitted. We restrict to the case where L is a cyclic number field of odd prime $p\geq3$ degree and we let $\mathcal{O}_L^{\times,1}$ denote the units of norm 1.

Proposition 4.4.4. *Let L be as above. Suppose that the polynomial*

$$\phi_p(x)=(x^p-1)/(x-1)$$

is irreducible over $\mathbb{F}_2$. Then, either $\rho_\infty=0$, or $\rho_\infty=p-1$, in which case every unit in $\mathcal{O}_L^{\times,1}$ is totally positive.

Proof. See [4, Proposition 2.22]. □

4.5 Improvement of the rank bound

Remember that an algebra $L=\mathbb{Q}[x]/(f(x))$ defined by $f(x)\in\mathbb{Q}[x]$ is totally real if and only if $f(x)$ has $\deg(f)$-many real roots. Recall also that in §4.2, we have introduced the following notations:

$$\rho_\infty=\dim\left(\mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2\right)\text{ and }j_\infty=\dim(\mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2)\cap J_\infty).$$

With notations as above, we obtain

Theorem 4.5.1. *Let n be an odd number and let $C:y^2=f(x)$ be a hyperelliptic curve with $f(x)$ of degree n (and hence of genus $g=(n-1)/2$) such that L, the algebra defined by $f(x)$, is totally real of degree n. Then we have*

$$\dim\mathrm{Sel}^{(2)}(\mathbb{Q},J)\leq j_\infty+\rho_\infty+\dim\mathrm{Cl}^+(L)[2]+\dim G\cap\mathrm{val}(L_{J_\infty}).$$

Moreover,

(i) $\rho_\infty+j_\infty\leq n-1$.

(ii) $j_\infty\leq g$.

(iii) One has

$$\dim\mathrm{Sel}^{(2)}(\mathbb{Q},J)\leq j_\infty+2\rho_\infty+\dim\mathrm{Cl}(L)[2]+\dim G\cap\mathrm{val}(L_{J_\infty}).$$

(iv) If $G \cap \mathrm{val}(L_{J_\infty})$ is trivial, then

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}^+(L)[2] \leq j_\infty + 2\rho_\infty + \dim \mathrm{Cl}(L)[2].$$

Proof. We have shown in Proposition 4.2.3 that

$$\dim \left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) = j_\infty + \rho_\infty.$$

Therefore, the first bound is basically the same as the one we obtained in Theorem 4.3.4. We prove the rest one by one:

(i) Since

$$\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) \subseteq \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2,$$

Lemma 3.4.6 implies that

$$\rho_\infty + j_\infty \leq \dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 = m_\infty = n,$$

where the last equality follows from the asumption that L is totally real. Moreover, $\mathrm{res}_\infty(-1) \notin J_\infty$ as shown before in Remark 4.3.5. Hence, the result follows.

(ii) Recall that we have defined $J_\infty = \delta_\infty(J(\mathbb{R})/2J(\mathbb{R}))$ and we know that δ_∞ is injective by Theorem 3.2.2. This yields by Theorem 1.3.5 that

$$\dim(J_\infty) = \dim J(\mathbb{R})/2J(\mathbb{R}) = m_\infty - 1 - g.$$

Hence the containment $\mathrm{res}_\infty\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cap J_\infty \subseteq J_\infty$ implies

$$j_\infty \leq \dim(J_\infty) = m_\infty - 1 - g = n - 1 - \frac{n-1}{2} = \frac{n-1}{2} = g,$$

as desired.

(iii) By Lemma 4.4.1, we have $\dim \mathrm{Cl}^+(L)[2] \leq \rho_\infty + \dim \mathrm{Cl}(L)[2]$. Thus the result follows.

(iv) Clear from the previous part.

□

In the following, we finally obtain a neat bound on $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ under the assumption that L is a cyclic number field.

Theorem 4.5.2. *Suppose that L is a cyclic number field of odd degree $n \geq 3$, such that the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$ is even. Then we have*

$$\dim \mathrm{Sel}^2(\mathbb{Q}, J) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)).$$

Hence, if $\rho_\infty = 0$, then

$$\dim \mathrm{Sel}^2(\mathbb{Q}, J) \leq g + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)).$$

Proof. Clear from Corollary 4.4.3 and Theorem 4.5.1. □

Corollary 4.5.3. *Let $C : y^2 = f(x)$ be a hyperelliptic curve such that the algebra L defined by $f(x)$ is a cyclic number field of odd degree $n \geq 3$. Then we have the following bound on* $\mathrm{rank}\, J(\mathbb{Q})$*:*

$$\mathrm{rank}\, J(\mathbb{Q}) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)).$$

Proof. Clear from Theorem 4.5.2 above. Note in particular that L being a number field means that $f(x)$ is irreducible over $\mathbb{Q}$ so that $\dim J(\mathbb{Q})[2] = 0$ by Theorem 1.3.1. So the above bound cannot be made any better using Theorem 2.3.1. □

Chapter 5

Some hyperelliptic Jacobians

We aim to compute the rank bounds of some families of hyperelliptic curves explicitely. We shall make use of the improvements on the bounds we obtained in the previous chapter. We will also obtain a lower bound for the rank of certain hyperelliptic Jacobians whenever the curve has sufficiently many rational points. We will finally include a very short discussion about the bounds on the 2-torsion of class groups and obtain some rank bounds involving discriminants.

5.1 A family of elliptic curves

Let $n \geq 1$ be an integer such that $D = 3n^2 + 3n + 1$ is squareefree. We consider the following family of elliptic curves:

$$E_n : y^2 = f_n(x) = x^3 + (9n+6)x^2 + (9n+3)x - 1,$$

which is due to F. Thaine, see [25]. In this section, we will prove that $\operatorname{rank} E_n(\mathbb{Q})$ can be bounded only in terms of $\dim \mathrm{Cl}(L_n)[2]$ by using Theorem 4.5.2. We remark that by a result of T. Nagel, see [11], there are infinitely many $n \geq 1$ such that $D = 3n^2 + 3n + 1$ is squarefree; *i.e.*, the above family E_n is infinite.

Since E_n is an elliptic curve, it can be identified with its Jacobian J. We have $\operatorname{disc}(f_n(x)) = (27D)^2$. Also, $f_n(x)$ is irreducible over $\mathbb{Q}$ for any n. So the algebra L_n defined by $f_n(x)$ is a cubic field. Since $\operatorname{disc}(f_n(x)) > 0$, we conclude that L_n is a cyclic cubic field. Moreover, the order of 2 in $(\mathbb{Z}/3\mathbb{Z})^\times$ is 2, which is even. Hence, we can use the bound in Theorem 4.5.2.

Lemma 5.1.1. *In the above set-up, we have $\rho_\infty = 0$.*

Proof. Note that $f_n(x)$ has two negative roots and one positive root and roots are all units. Therefore, for any root α of $f_n(x)$, we must have $N(\alpha) = 1$. However, α is not totally positive. Hence, we have found an element in $\mathcal{O}_L^{\times,1}$ which is not totally positive. Moreover the polynomial

$$\phi_3(x) = (x^3 - 1)/(x - 1) = x^2 + x + 1$$

is clearly irreducible in $\mathbb{F}_2$. Thus, the result follows by Proposition 4.4.4. □

With the following lemma, we find the images $G_v = \mathrm{val}_v(J_v) \subseteq I_v$ to be trivial for almost all places $v \in S = \{\infty, 2\} \cup \{v \mid v^2 \text{ divides } \operatorname{disc}(f_n)\}$. More precisely, we have

Lemma 5.1.2. *In the above set-up, for any $p \in S \setminus \{\infty, 3\}$, $f_n(x)$ is irreducible over $\mathbb{Q}_p$.*

Proof. Let $p = 2$. Then, reducing the polynomial $f_n(x)$ in $\mathbb{F}_2[x]$, we have

$$f_n(x) = \begin{cases} x^3 + x + 1 & n \equiv 0 \mod 2 \\ x^3 + x^2 + 1 & n \equiv 1 \mod 2 \end{cases}.$$

In both cases, we see that $f_n(x)$ is irreducible over $\mathbb{F}_2$, hence it is irreducible over $\mathbb{Q}_2$.

Now, let $p > 3$ be a prime such that p^2 divides $\operatorname{disc}(f_n(x))$; *that is*, p divides D. We compute that

$$f_n(x-(3n+2)) = x^3 - 9Dx + 9D(2n+1).$$

Moreover, we have

$$4D - 3(2n+1)^2 = 1,$$

which implies $\gcd(D, 2n+1) = 1$. Since D is squarefree by assumption, we see that $f_n(x-(3n+2))$ is irreducible over $\mathbb{Z}_p$ by Eisenstein criterion applied with prime p. Hence, it follows that $f_n(x)$ is irreducible over $\mathbb{Q}_p$, as claimed. □

We obtain the following theorem on $\operatorname{rank} E_n(\mathbb{Q})$:

Theorem 5.1.3. *Let E_n, $n \geq 1$, be the family of elliptic curves defined above. We have*

$$\operatorname{rank} E_n(\mathbb{Q}) \leq 3 + \dim \operatorname{Cl}(L_n)[2].$$

Proof. Fix an $n \geq 1$ and consider

$$G_n = \prod_{p \in S \setminus \{\infty\}} G_{n,p} \subseteq \prod_{p \in S \setminus \{\infty\}} I_{n,p}.$$

By Lemma 3.3.4,

$$\dim I_{n,p} = m_{n,p} - 1,$$

where $m_{n,p}$ is the number of irreducible factors of $f_n(x)$ in $\mathbb{Q}_p$. From Lemma 5.1.2, it follows that when $p > 3$, $\dim I_{n,p} = 1 - 1 = 0$ and hence, $G_{n,p}$ is trivial. On the other hand, when $p = 3$, we have

$$f_n(x) \equiv x^3 - 1 = (x-1)^3 \mod 3,$$

which implies that $\dim I_{n,3} = 3 - 1 = 2$. Therefore,

$$\dim \ker(G_n \to \operatorname{Cl}(L_n)/2\operatorname{Cl}(L_n) \leq \dim G_n = 2.$$

Moreover, since $f_n(x)$ is irreducible over $\mathbb{Q}$ and E_n identifies with its Jacobian, we have

$$\dim E_n(\mathbb{Q})[2] = 1 - 1 = 0,$$

by Theorem 1.3.1. Note finally that the genus g of $E_n(\mathbb{Q})$ is 1. Therefore, Theorem 2.3.1 and Theorem 4.5.2 imply

$$\begin{aligned}
\operatorname{rank} E_n(\mathbb{Q}) &\leq \dim \operatorname{Sel}^2(\mathbb{Q}, J) - \dim E_n(\mathbb{Q})[2] \\
&= g + \dim \operatorname{Cl}(L_n)[2] + \dim \ker(G_n \to \operatorname{Cl}(L_n)/2\operatorname{Cl}(L_n)) - \dim E_n(\mathbb{Q})[2] \\
&\leq 3 + \dim \operatorname{Cl}(L_n)[2],
\end{aligned}$$

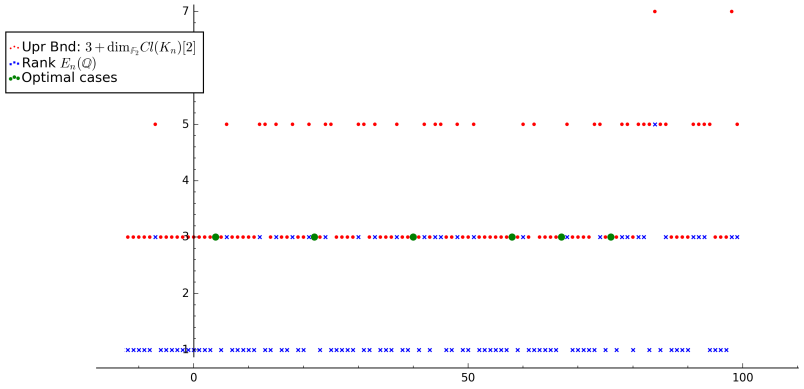
as claimed. □

Remark 5.1.4. *Since $f_n(x)$ has all real roots, it follows that $m_\infty = 3$. Therefore, if we used the bound in Theorem 3.4.7 for the above family of elliptic curves, we would obtain the bound*

$$\operatorname{rank} E_n(\mathbb{Q}) \leq 4 + \dim \operatorname{Cl}(L_n)[2],$$

which is weaker than the bound we found in the above theorem. The family $E_n : y^2 = f_n(x)$ is therefore an explicit example illustrating how Stoll's bound in Theorem 3.4.7 can be made stronger with the "refined estimation".

Remark 5.1.5. *We finally remark that the bound we found above is optimal, meaning that there are curves E_n from this family satisfying that $\operatorname{rank} E_n(\mathbb{Q}) = 3 + \dim \operatorname{Cl}(L_n)[2]$. Below picture created using Sage shows the optimal cases for varying n in the horizontal axis. Note that by assumption, we must only consider $n \geq 1$ such that $D = 3n^2 + 3n + 1$ is squarefree. Indeed, it turns out that among such $n \in [1, 100]$, when $n = 4, 40, 58, 67, 76$, the bound is optimal.*



5.2 Joshi-Tzermias family of hyperelliptic curves

Let $p \geq 5$ be a prime. In this section, we will consider the following family of hyperelliptic curves:

$$C : y^2 = f(x) = \prod_{i=0}^{p-1}(x - a_i) + p^2 d^2,$$

where $d \geq 1$ is an integer and a_i are distinct modulo p. This family is special in the sense that it has *many* rational points. This will allow us to have a bound on its Jacobian rank from below.

Following theorem is key to this section. We state its contrapositive as a corollary to emphasise that it yields a lower bound on the rank of a Jacobian.

Theorem 5.2.1 (Coleman's Effective Chabauty)**.** *Let $C/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 2$ and let J be the Jacobian associated with C. Let r denote the rank of the Jacobian J. Suppose that $r \leq g - 1$. Then, for any prime $p \geq 2g + 1$ for which C has good reduction, which is to be denoted by $\widetilde{C}$, we have*

$$\#C(\mathbb{Q}) \leq \#\widetilde{C}(\mathbb{F}_p) + 2g - 2.$$

Proof. See [2]. □

Corollary 5.2.2. *Let $C/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 2$ and let J be the Jacobian associated with C. Let r denote the rank of the Jacobian J. Suppose that, for any prime $p \geq 2g+1$ for which C has good reduction, which is to be denoted by $\widetilde{C}$, we have $\#\widetilde{C}(\mathbb{F}_p) + 2g - 2 \leq \#C(\mathbb{Q})$. Then we have the following lower bound on the rank r:*

$$g - 1 \leq r.$$

Lemma 5.2.3. *Let*

$$C : y^2 = f(x) = \prod_{i=0}^{p-1}(x - a_i) + p^2 d^2$$

be a curve from the Joshi-Tzermias family and let $J/\mathbb{Q}$ denote its Jacobian. Let $g = (p-1)/2$ be its genus. Then

(i) $\operatorname{rank} J(\mathbb{Q}) \geq g$,

(ii) If $f(x)$ is irreducible over $\mathbb{Q}$, then $\operatorname{rank} J(\mathbb{Q}) \geq 2g$.

Proof. (i) Since for all $i = 0, \ldots, p-1$, a_i's are distinct modulo p, the reduction $\widetilde{C}$ of C modulo p is given by

$$\widetilde{C} : y^2 = x^p - x,$$

which can be easily checked to be non-singular. Note that every affine $\mathbb{F}_p$-rational point of $\widetilde{C}$ is of the form $(a, 0)$, where $a \in \mathbb{F}_p$. Adding the point at infinity, we get

$$\#\widetilde{C}(\mathbb{F}_p) = p + 1 = 2g + 2.$$

On the other hand, the points $P_i = (a_i, \pm pd)$ is in $C(\mathbb{Q})$ for all $i = 0, \ldots, p-1$. Again, with the point at infinity counted, we have

$$\#C(\mathbb{Q}) \geq 2p + 1 = 4g + 3.$$

But then we get

$$4g + 3 \geq 2g + 2 + 2g - 2 = 4g.$$

Thus, result follows by Corollary 5.2.2.

(ii) See [7, Theorem 1.1]. □

We have

Lemma 5.2.4. *For a fixed prime $p \geq 5$ and an integer $d \geq 1$, write*

$$f_{a_0}(x) = (x - a_0) \prod_{i=1}^{p-1} (x - a_i) + p^2 d^2,$$

with a_i all distinct modulo p. Then, if a_0 is large enough, then $f_{a_0}(x)$ has p distinct real roots.

Proof. Fix $j \geq 1$. We have

$$f_{a_0}\Big(a_j \pm \frac{1}{2}\Big) = \Big(a_j - a_0 \pm \frac{1}{2}\Big)\Big(\pm \frac{1}{2}\Big) \prod_{i \neq j} \Big(a_j - a_i \pm \frac{1}{2}\Big) + p^2 d^2.$$

If we choose a_0 so large that

$$\Big|\Big(a_j - a_0 \pm \frac{1}{2}\Big) \prod_{i \neq j} \Big(a_j - a_i \pm \frac{1}{2}\Big)\Big| > 2p^2 d^2,$$

then we see that $f_{a_0}(a_j + 1/2)$ and $f_{a_0}(a_j - 1/2)$ have distinct signs for $j = 1, \ldots, p-1$. This implies that $f_{a_0}(x)$ has p distinct real roots by the Intermediate Value Theorem. □

Therefore, fixing a prime $p \geq 5$ and an integer $d \geq 1$, we have obtained an infinite family of Joshi-Tzermias hyperelliptic curves $f(x) \in \mathbb{Q}[x]$ such that $f(x)$ is of degree p and has p distinct real roots so that the algebra L defined by $f(x)$ is totally real. Therefore, Theorem 4.5.1 is applicable. Thus, we obtain

Theorem 5.2.5. *Let $C : y^2 = f(x)$ be a hyperelliptic curve from the family described above so that it has genus $g = (p-1)/2$. Let j_∞, ρ_∞ and L_{J_∞} be as defined before (see §4.1 and §4.2). Then we obtain*

$$g \leq \operatorname{rank} J(\mathbb{Q}) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}^+(L)[2] + \dim G \cap \mathrm{val}(L_{J_\infty}).$$

Moreover, the results of Theorem 4.5.1 hold true in this case.

Proof. Trivial from Lemma 5.2.3. □

5.3 Obtaining bounds that involve the discriminants

Let $C : y^2 = f(x)$ be a hyperelliptic curve with $f(x) \in \mathbb{Q}[x]$ monic, squarefree and of odd degree such that $f(x)$ defines the algebra L. We will see that $\operatorname{rank} J(\mathbb{Q})$ can be bounded only in terms of $\operatorname{disc}(f)$ as $f(x) \in \mathbb{Q}[x]$ runs through monic and squarefree polynomials of fixed odd degree n.

When L is a number field, an improvement of the Brauer-Siegel Theorem on the size of $\mathrm{Cl}(L)[2]$ has been made in the article [1]. Namely, if L is a number field of degree n, then one has

$$|\mathrm{Cl}(L)[2]| = \mathcal{O}_\epsilon(|\operatorname{disc}(L)|^{1/2-\delta_n+\epsilon}),$$

for some $\delta_n > 0$. Since $\operatorname{disc}(L) \leq \operatorname{disc}(f)$, this implies that

$$\dim \mathrm{Cl}(L)[2] \ll_{n,\epsilon} (1/2 - \delta_n + \epsilon) \log(\operatorname{disc}(f)). \tag{*}$$

Recall that when $L = L_1 \times \cdots \times L_m$ is an algebra with L_i's number fields for $i = 1, \ldots, m$, we have defined $\mathrm{Cl}(L) = \mathrm{Cl}(L_1) \times \cdots \times \mathrm{Cl}(L_m)$ so that $\dim \mathrm{Cl}(L)[2] = \dim \mathrm{Cl}(L_1)[2] + \cdots + \dim \mathrm{Cl}(L_m)[2]$. This implies that (*) holds when L is an algebra as well.

On the other hand, we can put a "trivial" bound on $\dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L))$ in terms of $\operatorname{disc}(f)$ without having to assume L to be a number field. Indeed,

$$\begin{aligned}\dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) \leq \dim G &= \sum_{p \in S \setminus \{\infty\}} \dim G_p \\ &\leq \sum_{p \in S \setminus \{\infty\}} \dim I_p \\ &\leq (|S| - 1)(n-1),\end{aligned}$$

where we have used the definition of G and the fact $\dim I_p = m_p - 1 \leq n - 1$ (see Lemma 3.3.4). By definition, S contains ∞, 2 and odd primes p such that p^2 divides $\operatorname{disc}(f)$. But $p^2 | \operatorname{disc}(f)$ implies $p \leq \sqrt{|\operatorname{disc}(f)|}$. We note that the Prime Number Theorem implies

$$|\{p : \text{ prime} \mid p \leq \sqrt{|\operatorname{disc}(f)|}\}| = \pi(\sqrt{|\operatorname{disc}(f)|}) \ll \frac{\sqrt{|\operatorname{disc}(f)|}}{\log \sqrt{|\operatorname{disc}(f)|}}.$$

Since $n - 1$ is considered as a constant, we obtain

$$\dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) \ll_n \frac{\sqrt{\operatorname{disc}(f)}}{\log \sqrt{\operatorname{disc}(f)}}.$$

We have the following proposition:

Proposition 5.3.1. *Let $n \geq 1$ be an odd integer, and let $C : y^2 = f(x)$ be a hyperelliptic curve with $f(x) \in \mathbb{Q}[x]$ monic, squarefree and of degree n. Then we have*

$$\operatorname{rank} J(\mathbb{Q}) \ll_n \frac{\sqrt{|\operatorname{disc}(f)|}}{\log \sqrt{|\operatorname{disc}(f)|}}.$$

Proof. Corollary 3.4.8 and the results we have obtained above above yield

$$\begin{aligned}\operatorname{rank} J(\mathbb{Q}) &\leq m_\infty - m + \dim \mathrm{Cl}(L)[2] + \dim \ker(G \to \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) \\ &\ll_{n,\epsilon} 1 + (1/2 - \delta_n + \epsilon) \log(\operatorname{disc}(f)) + \frac{\sqrt{\operatorname{disc}(f)}}{\log \sqrt{\operatorname{disc}(f)}} \\ &\ll_n \log(\operatorname{disc}(f)) + \frac{\sqrt{\operatorname{disc}(f)}}{\log \sqrt{\operatorname{disc}(f)}} << _n \frac{\sqrt{\operatorname{disc}(f)}}{\log \sqrt{\operatorname{disc}(f)}},\end{aligned}$$

as desired. □

References

[1] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, Yongqiang Zhao. *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves.* https://arxiv.org/abs/1701.02458, [v1], Tue, 10 Jan 2017.

[2] Robert F. Coleman. *Effective Chabauty.* Duke Math J. 52 (3) 765-770, 1985.

[3] Gary Cornell, Joseph H. Silverman. *Arithmetic Geometry.* Springer-Verlag New York, 1986.

[4] Harris B. Daniels, Álvaro Lozano-Robledo, Erik Wallace. *Bounds of the Rank of the Mordell-Weil Group of Jacobians of Hyperelliptic Curves.* https://arxiv.org/abs/1708.07896, [v4], Thu, 11 Jan 2018.

[5] Robin Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics, Springer-Verlag New York, 1977.

[6] Marc Hindry, Joseph H. Silverman. *Diophantine Geometry, An Introduction.* Graduate Texts in Mathematics, Springer-Verlag New York, 2000.

[7] Kirti Joshi, Pavlos Tzermias. *On the Coleman-Chabauty Bound.* Théorie des nombres, Série I, 459-463, 1999.

[8] Arthur Mattuck. *Abelian varieties over p-adic ground fields.* Annals of Mathematics 62, 92-119, 1955.

[9] James Milne. *Abelian Varieties.* http://www.jmilne.org/math/CourseNotes/AV.pdf, unpıblished course notes.

[10] David Mumford. *Tata Lectures on Theta II.* Birkhäuser Basel, 2007.

[11] Trygve Nagel. *Zur Arithmetik der Polynome.* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, Vol. 1, 179-194, 1992.

[12] Jürgen Neukirch. *Algebraic Number Theory.* A Series of Comprehensive Studies in Mathematics, Springer-Verlag Berlin Heidelberg, 1999.

[13] Jürgen Neukirch. *Class Field Theory, The Bonn Lectures.* Edited by Alexander Schmidt. https://www.mathi.uni-heidelberg.de/ schmidt/Neukirch-en/, electronic version.

[14] Bernard Oriat. *Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint des certains corps de nombres.* Bulletin de la S. M. F., tome 104, p. 301-307, 1976.

[15] Bjorn Poonen. *The Selmer Group, the Shafarevich-Tate Group, and the Weak Mordell-Weil Group.* http://math.univ-lyon1.fr/ roblot/ihp/weakmw.pdf, unpublished notes.

[16] Edward F. Schaefer. *Computing a Selmer group of a Jacobian using functions on the curve.* Mathematische Annalen, 310, 447-471, 1998.

[17] Edward F. Schaefer. *2-Descent on the Jacobians of Hyperelliptic Curves.* Journal of Number Theory, Vol. 51, Issue 2, 219-232, 1995.

[18] Edward F. Schaefer. *Class Groups and Selmer Groups.* Journal of Number Theory, 56, 79-114, 1996.

[19] Jean-Pierre Serre. *Local Fields.* Springer-Verlag New York, 1979.

[20] Jean-Pierre Serre. *A Course in Arithmetic.* Springer-Verlag New York, 1973.

[21] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Springer-Verlag New York, 2009.

[22] Peter Stevenhagen. *Number Rings.* http://websites.math.leidenuniv.nl/algebra/ant.pdf, unpublished notes.

[23] Michael Stoll. *Implementing 2-descent for Jacobians of hyperelliptic curves.* Acta Arithmetica 98.(3) - 2001.

[24] Richard Taylor. *Galois Representations.* Annales de la Faculté des Sciences de Toulouse 13, 73-119, 2004.

[25] Francisco Thaine. *On the Construction of Families of Cyclic Polynomials Whose Roots Are Units.* Experimental Mathematics 17:3, 315, 2011.