UNIVERSITY OF CALIFORNIA,
IRVINE

Selmer ranks of twists of algebraic curves

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Myungjun Yu

Dissertation Committee:
Professor Karl Rubin, Chair
Professor Alice Silverberg
Professor Daqing Wan

2016

Dedication

To my parents, for their unconditional support in the pursuit of my dreams.

Table of Contents

Acknowledgements

First of all, I would like to express my everlasting gratitude to Professor Karl Rubin for his advice and support throughout my graduate years at University of California, Irvine. He has been always willing to help me and share his ideas with me, which has been very crucial to my understanding of mathematics. I am also very grateful to him for careful reading of my thesis work. His comments and ideas to improve this thesis have been extremely helpful. Without his guidance, the completion of my thesis would not have been possible.

I would also like to thank Professor Alice Silverberg and Professor Daqing Wan for their interest in my research and their advice on my career as a mathematician. I also thank Liang Xiao for many inspiring mathematical conversations. His knowledge over many subjects was always surprising and gave me motivation to study; I was very fortunate to share some time with him here in Irvine. I would like to extend my thanks to Professor Barry Mazur for his interest in my work and support.

I would like to express my gratitude to Professor Haseo Ki for his support and encouragement whenever I visit him. Moreover he always shows his passion for mathematics, which is very motivating. Additionally I would like to thank my reference in Korea: Professor Hyoung June Ko, Professor June Bok Lee, Professor Yongnam Lee, Professor Soogil Seo, and Professor Jaebum Sohn.

I would like to express my special thanks to Hayan Nam. She was always there whenever I was stressed out by research and anxiety. I would not have survived without her continuous care and encouragement. I would like to extend my thanks to my academic brother Heng Su, who has been always trying to be helpful both mentally and mathematically. It is him who enabled me to find examples in Section 3.4. I am extremely grateful to Dennis Eichhorn for proofreading and advice. I would also like to thank Rufei Ren for showing me his smart ideas for our project.

I am very thankful to Wan Lee. He showed me the beauty of the class field theory, which made me want to study algebraic number theory further. In 2008, when I was not sure to pursue my dreams in mathematics, I clearly remember the moment that he came to me and convinced me I should do mathematics. I would also like to express my gratitude to Chan-Ho Kim for being a fantastic mentor. His advice has been extremely helpful to establish my attitude toward mathematics.

Last but not least, I would like to express my sincere gratitude to my family for their emotional support and love. Without them, I would not be able to complete my Ph.D. study.

Curriculum Vitae

Myungjun Yu

B.S. in Mathematics, Yonsei University, 2010

Ph.D. in Mathematics, University of California, Irvine, 2016

Abstract of the Dissertation

Selmer ranks of twists of algebraic curves

By

Myungjun Yu

Doctor of Philosophy in Mathematics
University of California, Irvine, 2016
Professor Karl Rubin, Chair

Inspired by recent papers of Mazur-Rubin [8] and Klagsbrun-Mazur-Rubin [6], this thesis investigates Selmer ranks of twists of Jacobians of various algebraic curves over number fields. For example, we find sufficient conditions on hyperelliptic curves $C_{2,f}$ over a number field such that for any nonnegative integer r, there exist infinitely many quadratic twists of $C_{2,f}$ whose Jacobians have 2-Selmer ranks equal to r. This theorem is even more generalized to the superelliptic curve case in this dissertation. We also present some results on 2-Selmer ranks of elliptic curves. In particular, we prove if the set of 2-Selmer ranks of quadratic twists of an elliptic curve over a number field contains an integer c, it contains all integers larger than c having the same parity as c.

Chapter 1

Introduction and Preliminaries

1.1 Introduction

We investigate Selmer ranks of elliptic curves, hyperelliptic curves and superelliptic curves in the families of twists. For example, we find sufficient conditions for such curves to have infinitely many twists whose Jacobians have Selmer ranks equal to r, for any given nonnegative integer r.

1.1.1 Selmer ranks of twists of hyperelliptic curves and superelliptic curves

Let E be an elliptic curve over a number field K. For the family of quadratic twists of E, Mazur and Rubin [8] proved the following theorem.

Theorem 1.1.1 (Mazur and Rubin). *Suppose that K is a number field, and E is an elliptic curve over K such that $\mathrm{Gal}(K(E[2])/K) \cong S_3$. Let Δ_E be the discriminant of some model of E, and suppose further that K has a place v_0 satisfying one of the following conditions:*

- *v_0 is real and $(\Delta_E)_{v_0} < 0$, or*
- *$v_0 \nmid 2\infty$, E has multiplicative reduction at v_0, and $\mathrm{ord}_{v_0}(\Delta_E)$ is odd.*

Then for every $r \geq 0$, there are infinitely many quadratic twists E'/K of E such that $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E'/K)) = r$.

We study the generalization of Theorem 1.1.1 to Jacobians of hyperelliptic and superelliptic curves. Let p be a prime.

Definition 1.1.2. A superelliptic curve $C_{p,f}$ over a field L is a smooth projective curve in the projective space $\mathbb{P}^2$ whose affine model is

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

where f is a separable polynomial (not necessarily monic) defined over L such that $p \nmid \deg(f)$. The curve $C_{p,f}$ has a point at infinity, which is denoted by ∞. When $p = 2$ (so $\pi = 2$), we call $C_{2,f}$ a hyperelliptic curve. We denote the Jacobian of $C_{p,f}$ by $J_{p,f}$.

Remark 1.1.3. More standard definition of superelliptic curves $C_{p,f}$ includes the case when p divides $\deg(f)$, in which case $C_{p,f}$ has p points at infinity.

In the following theorems, see Definition 1.2.10 for the definition of a π-Selmer group.

Theorem 1.1.4. *Suppose that K is a number field and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $n \equiv 3 \pmod 4$ and $\mathrm{Gal}(f) \cong S_n$ or A_n. Suppose further that K has a real embedding. Then for every $r \geqq 0$, the Jacobian $J_{2,f}$ has infinitely many quadratic twists $J_{2,df}$ where $d \in K^\times/(K^\times)^2$ such that $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J_{2,df}/K)) = r$.*

Theorem 1.1.5. *Suppose that K is a number field containing ζ_p, and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\mathrm{Gal}(f) \cong S_n$. Then for every $r \geqq 0$, the Jacobian $J_{p,f}$ has infinitely many twists $J_{p,df}$ where $d \in K^\times/(K^\times)^p$ such that $\dim_{\mathbf{F}_p}(\mathrm{Sel}_\pi(J_{p,df}/K)) = r$.*

Corollary 1.1.6. *Under the assumptions of Theorem 1.1.5 (resp. Theorem 1.1.4), there are infinitely many twists $J_{p,df}$ (resp. $J_{2,df}$) such that $J_{p,df}(K)$ (resp. $J_{2,df}(K)$) is finite.*

For a quadratic character $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$, let E^χ and $J_{2,f}^\chi$ denote the quadratic twists of E and $J_{2,f}$ by χ, respectively. In the elliptic curve case, Kramer showed that (see [7, Theorem 1] and [8, Theorem 2.8]) there is a (parity) relation between two Selmer groups $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^\chi/K)$ as follows.

Theorem 1.1.7 (Kramer)**.** *Let E be an elliptic curve over a number field K. Suppose $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$. Then*

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E/K)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^{\chi}/K)) \equiv \sum_v h_{E,v}(\chi_v)(mod\ 2),$$

where χ_v is the restriction of χ to G_{K_v}, and $h_{E,v}(\chi_v)$ is defined locally for every place v (Definition 1.2.8).

We generalize this result to the hyperelliptic curve case.

Theorem 1.1.8. *Let $C_{2,f}$ be a hyperellipitc curve over a number field K. Suppose that $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$. Then*

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J_{2,f}/K)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,f}/K)) \equiv \sum_v h_{J_{2,f},v}(\chi_v)(mod\ 2),$$

where χ_v is the restriction of χ to G_{K_v} and $h_{J_{2,f},v}$ is given in Definition 1.2.8.

Remark 1.1.9. The sum on the right hand side of the equation in Theorem 1.1.8 turns out to be a finite sum. See Lemma 2.1.14.

In fact, this generalization plays an important role in proving the following theorem, which is proved for elliptic curves by Klagsbrun, Mazur and Rubin [6, Theorem 7.6] first.

Theorem 1.1.10. *Let $C_{2,f}$ be a hyperelliptic curve defined over a number field K. For all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K,X) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,f}/K)) \text{ is even }\}|}{|\mathcal{C}^2(K,X)|} = \frac{1+\delta_{J_{2,f}}}{2},$$

where $\mathcal{C}^2(K,X)$ and $\delta_{J_{2,f}}$ are defined in Definition 3.3.2 and Definition 3.3.1, respectively.

Corollary 1.1.11. *If K has a real embedding and $\deg(f) \equiv 3(mod\ 4)$, then for all sufficiently large X,*

$$|\{\chi \in \mathcal{C}(K,X) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,f}/K)) \text{ is even }\}| = |\{\chi \in \mathcal{C}(K,X) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,f}/K)) \text{ is odd }\}|.$$

Remark 1.1.12. The condition $\deg(f) \equiv 3(\mathrm{mod}\ 4)$ can't be dropped in Corollary 1.1.11. When $\deg(f) \equiv 1$ modulo 4, $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,f}/K))$ may have constant parity for all quadratic twists $J^{\chi}_{2,f}$. See Proposition 3.4.1 and Proposition 3.4.4.

1.1.2 2-Selmer ranks of quadratic twists of elliptic curves

Let E be an elliptic curve over a number field K. In this section, we write $r_2(E)$ for $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E/K))$ for simplicity. For E, one may study the set

$$A_E := \{r_2(E^\chi) : E^\chi \text{ is a quadratic twist of } E\},$$

i.e., the set of (non-negative) integers r that appear as 2-Selmer ranks of some quadratic twists of E.

Definition 1.1.13. Let E be an elliptic curve over K. We say E satisfies the *constant 2-Selmer parity condition* if K has no real embedding and E acquires good reduction everywhere over an abelian extension of K.

The following theorem is due to Dokchitser and Dokchitser [2, Remark 4.9].

Theorem 1.1.14 (Dokchitser and Dokchitser)**.** *If E satisfies the constant 2-Selmer parity condition, all integers in A_E have the same parity.*

Theorem 1.1.15. *Let E be an elliptic curve over a number field K. Then there exist infinitely many quadratic characters χ such that $r_2(E^\chi) = r_2(E) + 2$.*

Let t_E denote the smallest integer in A_E. For an elliptic curve E, clearly

$$A_E \subset \mathbf{Z}_{\geq t_E}. \tag{1.1}$$

By applying Theorem 1.1.15 inductively, we can see

Theorem 1.1.16. *Let E be an elliptic curve over a number field K. Then $A_E \supset \{r \equiv t_E \pmod 2 : r \geq t_E\}$, (with equality if E satisfies the constant 2-Selmer parity condition).*

We find sufficient conditions on E so that equality holds in (1.1) (See Theorem 4.3.9, Theorem 4.3.10 and Theorem 4.2.2).

Theorem 1.1.17. *Suppose that $\mathrm{Gal}(K(E[2])/K)$ has order 1 or 2. Suppose that either*

1. *K has a real embedding, or*

2. $\mathrm{Gal}(K(E[2])/K)$ *has order* 2 *and* E *has multiplicative reduction at a place* $\mathfrak{q}$ *such that* $\mathfrak{q} \nmid 2$ *and* $v_{\mathfrak{q}}(\Delta_E)$ *is odd, where* Δ_E *is the discriminant of a model of* E *and* $v_{\mathfrak{q}}$ *is the normalized (additive) valuation of* $K_{\mathfrak{q}}$*.*

Then $A_E = \mathbf{Z}_{\geq t_E}$*.*

Let Σ be a finite set of places of K containing all primes above 2, all primes where E has bad reduction, and all infinite places. We suppose the elements (finite places) of Σ generate the ideal class group of K. For t_E, we have a trivial lower bound $\dim_{\mathbf{F}_2}(E(K)[2])$. However, this lower bound turns out not to be sharp in some cases. Klagsbrun [5] found examples of elliptic curves E such that t_E is at least s_2+1, where s_2 denotes the number of complex places of K (see Example 4.4.1 and Remark 4.4.2 for a discussion of this). In Section 4.4, when $E[2] \subset E(K)$, we give an upper bound for t_E as follows (see Theorem 4.4.6 and Theorem 4.4.8).

Theorem 1.1.18. *Suppose that* $E[2] \subset E(K)$*. We have* $t_E \leq |\Sigma| + 1$*. If moreover,* E *does not satisfy the constant* 2*-Selmer parity condition, then* $t_E \leq |\Sigma|$*.*

1.2 Preliminaries

1.2.1 Hyperelliptic curves and superelliptic curves

Let p be a prime and K be a number field containing ζ_p, where ζ_p is a primitive p-th root of unity Let $\pi = 1 - \zeta_p$.

Definition 1.2.1. Let L be a field of characteristic 0, and $\zeta_p \in L$. We write

$$\mathcal{C}^p(L) := \mathrm{Hom}(G_L, \boldsymbol{\mu}_p).$$

If L is a local field, we often identify $\mathcal{C}^p(L)$ with $\mathrm{Hom}(L^\times, \boldsymbol{\mu}_p)$ via the local reciprocity map, and let $\mathcal{C}^p_{\mathrm{ram}}(L) \subset \mathcal{C}^p(L)$ be the subset of ramified characters in $\mathcal{C}^p(L)$. Then $\chi \in \mathcal{C}^p_{\mathrm{ram}}(L)$ if and only if $\chi(\mathcal{O}_L^\times) \neq 1$, where $\mathcal{O}_L^\times$ is the unit group of the ring of integers of L, by local class field theory.

Remark 1.2.2. Let $C_{p,f}$ be a superelliptic curve defined over L of any characteristic other than p. Note that $J_{p,f}$ has a natural $\mathbf{Z}[\zeta_p]$-action induced by $\zeta_p(\alpha, \beta) = (\alpha, \zeta_p \beta)$, where (α, β) is a point of $y^p = f(x)$. In other words, there is a natural map

$$\boldsymbol{\mu}_p \to \mathrm{Aut}(J(C_{p,f})),$$

where $\boldsymbol{\mu}_p$ is the multiplicative group of p-th roots of unity.

Lemma 1.2.3. *Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $f(x)$. Let $J_{p,f}[\pi]$ denotes the $\mathbf{F}_p$-vector space of the π-torsion points of $J_{p,f}$. Then*

$$[(\alpha_1, 0) - \infty], [(\alpha_2, 0) - \infty], \cdots, [(\alpha_{n-1}, 0) - \infty]$$

form a basis of $J_{p,f}[\pi]$. Moreover,

$$[(\alpha_n, 0) - \infty] = -[(\alpha_1, 0) - \infty] - [(\alpha_2, 0) - \infty] - \cdots - [(\alpha_{n-1}, 0) - \infty].$$

Proof. For example, see [19, Proposition 3.2]. □

Remark 1.2.4. Let $C_{p,f}$ be a superelliptic curve defined over a field L of any characteristic other than p. Assume that $\boldsymbol{\mu}_p \subset L$. By a twist of $J_{p,f}/L$, we mean a pair (A', ϕ) such that A' is an algebraic group over L and $\phi : A' \to J_{p,f}$ is an isomorphism over $\overline{L}$. We denote the set of twists of $J_{p,f}/L$ by $\mathrm{Twist}(J_{p,f}/L)$. It is well-known (for example, see Proposition 5 in [20, Chapter3 §1]) that there is a bijection

$$\mathrm{Twist}(J_{p,f}/L) \to H^1(G_L, \mathrm{Aut}(J_{p,f})). \tag{1.2}$$

It maps $\phi : A' \cong J_{p,f}$ to the cocycle $\xi : G_L \to \mathrm{Aut}(J_{p,f})$, where $\xi_\sigma = \phi^\sigma \circ \phi^{-1}$.

Then we have a composition of maps

$$\mathrm{Hom}(G_L, \boldsymbol{\mu}_p) \to H^1(G_L, \mathrm{Aut}(J_{p,f})) \to \mathrm{Twist}(J_{p,f}/L), \tag{1.3}$$

where the first map is given by the map $\boldsymbol{\mu}_p \to \mathrm{Aut}(J_{p,f})$ in Remark 1.2.2. The last map is the bijection given above.

Definition 1.2.5. A p-twist of $J_{p,f}$ by $\chi \in \mathcal{C}^p(K)$ is the image of χ in (1.3) and is denoted by $J^{\chi}_{p,f}$.

Remark 1.2.6. We find an explicit superelliptic curve whose Jacobian is exactly $J_{p,f}^{\chi}$ here. Let $C_{p,f}$ be a superelliptic curve over a field L. Assume that $\boldsymbol{\mu}_p \subset L$. For $\chi \in \mathcal{C}^p(L)$, let d be the preimage of χ in the Kummer map

$$L^{\times}/(L^{\times})^p \cong \operatorname{Hom}(G_L, \boldsymbol{\mu}_p),$$

i.e., $\sigma(d^{1/p})/d^{1/p} = \chi(\sigma)$ for $\sigma \in G_L$, where $d^{1/p}$ is a choice of p-th root of d. There is an isomorphism

$$\phi : J_{p,d^{-1}f} \cong J_{p,f}$$

given by the isomorphism $C_{p,d^{-1}f} \cong C_{p,f}$ taking (a, b) to $(a, d^{1/p}b)$. Then the image of $(J_{p,d^{-1}f}, \phi)$ of the map (1.2) is represented by a cocycle ξ such that $\xi_\sigma : J_{p,f} \to J_{p,f}$ taking $[(a, b) - \infty]$ to $[(a, \chi(\sigma)b) - \infty]$. Therefore we conclude that $J_{p,f}^{\chi} = J_{p,d^{-1}f}$.

Remark 1.2.7. Let $C_{p,f}$ be a superelliptic curve defined over a number field K containing a p-th root of unity ζ_p. Then there is a canonical (Gal$(\overline{K}/K)$-module) isomorphism

$$J_{p,f}^{\chi}[\pi] \cong J_{p,f}[\pi],$$

which can be deduced directly from Lemma 1.2.3 and Remark 1.2.6.

1.2.2 Local conditions

In this section, we assume that K is a number field containing a p-th root of unity ζ_p and $C_{p,f}$ is a superelliptic curve over K. Recall that $\pi = 1 - \zeta_p$. From now on, we fix embeddings $\overline{K} \hookrightarrow \overline{K_v}$ for all places v so that $G_{K_v} \subset G_K$.

Definition 1.2.8. For $\chi \in \mathcal{C}^p(K_v)$, define

$$\alpha_{J_{p,f},v}(\chi) := \operatorname{Im}(J_{p,f}^{\chi}(K_v)/\pi J_{p,f}^{\chi}(K_v) \to H^1(K_v, J_{p,f}^{\chi}[\pi]) \cong H^1(K_v, J_{p,f}[\pi])),$$

where the first map is given by the Kummer map. Define

$$h_{J_{p,f},v}(\chi) := \dim_{\mathbf{F}_p}(\alpha_{J_{p,f},v}(1_v)/(\alpha_{J_{p,f},v}(1_v) \cap \alpha_{J_{p,f},v}(\chi))).$$

Remark 1.2.9. For $\chi \in \mathcal{C}^p(K_v)$, the constant $h_{J_{p,f},v}(\chi)$ quantifies the difference between two local conditions $\alpha_{J_{p,f},v}(1_v)$ and $\alpha_{J_{p,f},v}(\chi)$. For example, if $\alpha_{J_{p,f},v}(1_v) = \alpha_{J_{p,f},v}(\chi)$, then $h_{J_{p,f},v}(\chi) = 0$

Now we define the π-Selmer group of a superelliptic curve, which generalizes the 2-Selmer group of an elliptic curve.

Definition 1.2.10. For $\chi \in \mathcal{C}^p(K)$, define the π-Selmer group

$$\mathrm{Sel}_\pi(J^\chi_{p,f}/K) := \{x \in H^1(K, J_{p,f}[\pi]) : \mathrm{res}_v(x) \in \alpha_{J_{p,f},v}(\chi_v) \text{ for every } v\},$$

where res_v is the restriction map and χ_v is the restriction of χ to G_{K_v}.

1.3 Layout

Chapter 2 considers the superelliptic curve case. In section 2.1, we introduce various lemmas concerning local conditions of Selmer groups. In section 2.2, when a certain Galois group is large enough, we show that we can control the images of the localization maps (by choosing appropriate primes). Theorem 1.1.5 is proved at the end of section 2.3.

Chapter 3 discusses the hyperelliptic curve case. In section 3.1, we define Metabolic spaces and Lagrangian subspaces to be used to prove a parity relation (Theorem 1.1.8). Section 3.3 discusses the parity distribution of 2-Selmer ranks of Jacobians of hyperelliptic curves in the family of quadratic twists and proves Theorem 1.1.10. Applying results in section 3.2, Theorem 1.1.4 is proved in section 3.3. Section 3.4 exhibits certain examples such that all quadratic twists have even 2-Selmer ranks.

Chapter 4 concerns the elliptic curve case. In section 4.2, Theorem 1.1.15 is proved. Theorem 1.1.17 is proved in section 4.3. In section 4.4, when $\mathrm{Gal}(K(E[2])/K)$ has order 2, we find an upper bound for t_E as in Theorem 1.1.18.

Chapter 2

Superelliptic curves

In this chapter, fix a prime number p, a number field K containing a p-th root of unity ζ_p, and a separable polynomial $f(x) \in K[x]$ so that $p \nmid n(:= \deg(f))$ and $\mathrm{Gal}(f) \subset S_n$. Let $C_{p,f}$ denote a superelliptic curve defined over K. For the rest of the paper, a local field is either an archimedean field, or a finite extension of $\mathbf{Q}_\ell$ for some prime number ℓ. If K_v is an archimedean field, we write $v|\infty$, and if the residue characteristic of K_v is ℓ we write $v|\ell$. Let 1_v denote the trivial character in $\mathcal{C}^p(K_v)$. We denote the Jacobian $J_{p,f}$ of $C_{p,f}$ simply by J in this chapter. The main theorem (Theorem 1.1.5) is proved at the end of section 2.3.

2.1 Comparison of local conditions

Definition 2.1.1. Let V be a finite dimensional vector space over $\mathbf{F}_p$. We write $d_p(V)$ for the dimension of V over $\mathbf{F}_p$.

Recall that π denotes $1-\zeta_p$. Let $\lambda : J \to \hat{J}$ be the canonical principal polarization. Then $J[\pi]$ is self-dual; i.e., $\lambda^{-1}(\hat{J}[\hat{\pi}]) = J[\pi]$, where $\hat{\pi}$ is the dual isogeny of π(see [19, Proposition 3.1]). Let $\langle\ ,\ \rangle_\pi$ denote the Cartier pairing (for example, see Section 1 in [16]) for $\pi : J \to J$ (multiplication by π).

Definition 2.1.2. Define a pairing

$$e_\pi : J[\pi] \times J[\pi] \to \boldsymbol{\mu}_p$$

by sending (x, y) to $\langle x, \lambda(y)\rangle_\pi$.

Remark 2.1.3. By properties of the Cartier pairing, the pairing e_π is bilinear, nondegenerate, and G_K-equivariant. In fact, e_π can be defined more concretely as follows. If e_p is the Weil pairing of $J[p]$ associated to the canonical principal polarization λ,

$$e_\pi(a, b) := e_p(a, (\pi^{p-2})^{-1}(b)),$$

which can be proved by using functoriality in [16, Corollary 1.3(ii)]. Here $(\pi^{p-2})^{-1}(b)$ denote any inverse image of b of the map $\pi^{\mathfrak{p}-2} : J \to J$. If $p = 2$, then e_π is nothing but the Weil pairing of $J[2]$ associated to the canonical principal polarization.

The following theorem follows from Tate's local duality.

Theorem 2.1.4. *Tate's local duality and the paring e_π give a nondegenerate pairing*

$$\langle\ ,\ \rangle_v : H^1(K_v, J[\pi]) \times H^1(K_v, J[\pi]) \longrightarrow H^2(K_v, \zeta_p) = \mathbf{F}_p. \tag{2.1}$$

If $p = 2$, then the pairing is symmetric.

Proof. For example, see [15, Theorem 7.2.6]. The last assertion holds because the pairings given by cup product and the Weil pairings are alternating. □

Lemma 2.1.5. *The image of the Kummer map*

$$J(K_v)/\pi J(K_v) \to H^1(K_v, J[\pi])$$

is its own orthogonal complement under pairing (2.1)*.*

Proof. We prove it by applying the well-known fact that the image of the Kummer map

$$J(K_v)/pJ(K_v) \to H^1(K_v, J[p])$$

is its own orthogonal complement in Tate's local duality for $H^1(K_v, J[p])$ and diagram chasing. By applying long exact sequences to the following diagrams

$$\begin{tikzcd}
0 \arrow[r] & J[\pi] \arrow[r] \arrow[d, hook] & J \arrow[r, "\pi"] \arrow[d, equal] & J \arrow[r] \arrow[d, "p/\pi"] & 0 \\
0 \arrow[r] & J[p] \arrow[r] & J \arrow[r, "p"] & J \arrow[r] & 0
\end{tikzcd}
\qquad
\begin{tikzcd}
0 \arrow[r] & J[\pi] \arrow[r] & J \arrow[r, "\pi"] & J \arrow[r] & 0 \\
0 \arrow[r] & J[p] \arrow[r] \arrow[u, "\pi^{p-2}"'] & J \arrow[r, "p"] \arrow[u, "\pi^{p-2}"'] & J \arrow[r] \arrow[u, "u"'] & 0
\end{tikzcd}$$

we get the following commutative diagrams with exact rows

$$\begin{tikzcd}
0 \arrow[r] & J(K_v)/\pi J(K_v) \arrow[r, "\phi"] \arrow[d, "p/\pi"] & H^1(K_v, J[\pi]) \arrow[r, "\lambda"] \arrow[d, "s"] & H^1(K_v, J)[\pi] \arrow[r] \arrow[d, "s'"] & 0 \\
0 \arrow[r] & J(K_v)/pJ(K_v) \arrow[r, "\phi'"] & H^1(K_v, J[p]) \arrow[r, "\lambda'"] & H^1(K_v, J)[p] \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
J(K_v)/\pi J(K_v) \arrow[r, "\phi"] & H^1(K_v, J[\pi]) \\
J(K_v)/pJ(K_v) \arrow[r, "\phi'"] \arrow[u, "u"] & H^1(K_v, J[p]), \arrow[u, "\pi^{p-2}"]
\end{tikzcd}$$

where ϕ and ϕ' are the Kummer maps and s, s' are natural maps. Let $\mathrm{Im}(\phi)$ denote the set of the image of the map ϕ. We want to show that $\mathrm{Im}(\phi) = \mathrm{Im}(\phi)^{\perp}$. First we show that $\mathrm{Im}(\phi) \subset \mathrm{Im}(\phi)^{\perp}$; i.e., $\mathrm{Im}(\phi) \perp \mathrm{Im}(\phi)$. We have $\mathrm{Im}(s \circ \phi) \subset \mathrm{Im}(\phi')$ and $\mathrm{Im}(\pi^{p-2} \circ \phi') = \mathrm{Im}(\phi \circ u) = \mathrm{Im}(\phi)$ since the map u is surjective. By the fact that $\mathrm{Im}(\phi') \perp \mathrm{Im}(\phi')$, we obtain $s^{-1}(\mathrm{Im}(\phi')) \perp \mathrm{Im}(\pi^{p-2} \circ (\phi'))$ because the following diagram commutes

$$\begin{tikzcd}
H^1(K_v, J[\pi]) \arrow[d, "s"] & \times & H^1(K_v, J[\pi]) \arrow[r, "\cup"] & H^2(K_v, \boldsymbol{\mu}_p) \arrow[d, equal] \\
H^1(K_v, J[p]) & \times & H^1(K_v, J[p]) \arrow[r, "\cup"] \arrow[u, "\pi^{p-2}"] & H^2(K_v, \boldsymbol{\mu}_p).
\end{tikzcd}$$

Therefore $\mathrm{Im}(\phi) \perp \mathrm{Im}(\phi)$, or equivalently $\mathrm{Im}(\phi) \subset \mathrm{Im}(\phi)^{\perp}$. Next we show $\mathrm{Im}(\phi)^{\perp} \subset \mathrm{Im}(\phi)$. Let $b \in H^1(K_v, J[\pi])$ be an orthogonal element to $\mathrm{Im}(\phi)$. Then

$$\begin{aligned}
s(b) \perp (\pi^{p-2})^{-1}(\mathrm{Im}\phi) &\Rightarrow s(b) \perp \mathrm{Im}(\phi') \\
&\Rightarrow s(b) \in \mathrm{Im}(\phi') \\
&\Rightarrow s(b) \in \ker(\lambda') \\
&\Rightarrow 0 = \lambda' \circ s(b) = s' \circ \lambda(b) \\
&\Rightarrow \lambda(b) = 0 \\
&\Rightarrow b \in \ker(\lambda) = \mathrm{Im}(\phi).
\end{aligned}$$

Hence we are done. □

Remark 2.1.6. By Lemma 2.1.5 applied to J^{χ}, for $\chi \in \mathcal{C}^p(K_v)$, one can see that $\alpha_{J,v}(\chi)$ is its own orthogonal complement in (2.1). Since the pairing (2.1) is non-degenerate, we have

$$d_p(H^1(K_v, J[\pi])) = 2d_p(\alpha_{J,v}(\chi)).$$

Lemma 2.1.7. *Suppose that* $v \nmid p\infty$ *and* J/K_v *has good reduction. Then*

$$\alpha_{J,v}(1_v) \cong J[\pi]/(\mathrm{Frob}_v - 1)J[\pi],$$

where the isomorphism is given by evaluating cocycles at a Frobenius automorphism Frob_v.

Proof. Under the assumption, we have an exact sequence

$$0 \longrightarrow J[\pi] \longrightarrow J(K_v^{\mathrm{ur}}) \xrightarrow{\pi} J(K_v^{\mathrm{ur}}) \longrightarrow 0,$$

where K_v^{ur} is the maximal unramified extension of K_v. Taking the long exact sequence, we get an exact sequence

$$0 \longrightarrow J(K_v)/\pi J(K_v) \longrightarrow H^1(K_v^{\mathrm{ur}}/K_v, J[\pi]) \longrightarrow H^1(K_v^{\mathrm{ur}}/K_v, J(K_v^{\mathrm{ur}}))[\pi] \longrightarrow 0.$$

It is well-known that $H^1(K_v^{\mathrm{ur}}/K_v, J(K_v^{\mathrm{ur}})) = 0$ (e.g., see [12, proposition 1]). Hence

$$\alpha_{J,v}(1_v) \cong J(K_v)/\pi J(K_v) \cong H^1(K_v^{\mathrm{ur}}/K_v, J[\pi]) \cong J[\pi]/(\mathrm{Frob}_v - 1)J[\pi],$$

as wanted (for the last isomorphism, which is given by evaluating cocycles at Frob_v, see [18, Lemma B.2.8]). □

We identify $\alpha_{J,v}(1_v)$ with $J(K_v)/\pi J(K_v)$ in the proof of the Lemma below.

Lemma 2.1.8. *Suppose that* $\chi \in \mathcal{C}^p(K_v)$, *and* $F_v := \overline{K}_v^{\ker(\chi)}$. *Then we have*

$$\alpha_{J,v}(1_v) \cap \alpha_{J,v}(\chi) \supseteq (\mathbf{N}(J(F_v)) + \pi J(K_v))/\pi J(K_v), \tag{2.2}$$

where $\mathbf{N}(J(F_v))$ *is the image of the norm map* $J(F_v) \to J(K_v)$ *and the intersection is taken in* $H^1(K_v, J[\pi])$. *In particular, if* $\mathbf{N}(J(F_v)) = J(K_v)$, *then* $h_{J,v}(\chi) = 0$.

Proof. Consider the commutative diagrams

$$\begin{tikzcd}
J(F_v)/\pi J(F_v) \arrow[r] & H^1(F_v, J[\pi]) & & H^1(F_v, J[\pi]) \arrow[d, "\mathrm{cor}"] & J(F_v)/\pi J(F_v) \arrow[l] \arrow[d, "\mathbf{N}"] \\
J(K_v)/\pi J(K_v) \arrow[r] \arrow[u, "i"] & H^1(K_v, J[\pi]) \arrow[u, "\mathrm{res}"'] & & H^1(K_v, J[\pi]) & J(K_v)/\pi J(K_v) \arrow[l]
\end{tikzcd}$$

$$\begin{tikzcd}
H^1(F_v, J[\pi]) \arrow[d, "\mathrm{cor}"] & \times & H^1(F_v, J[\pi]) \arrow[r, "\cup"] & H^2(F_v, \boldsymbol{\mu}_p) \cong \mathbf{Z}/p\mathbf{Z} \arrow[d, "\mathrm{cor} = \mathrm{id}"] \\
H^1(K_v, J[\pi]) & \times & H^1(K_v, J[\pi]) \arrow[u, "\mathrm{res}"'] \arrow[r, "\cup"] & H^2(K_v, \boldsymbol{\mu}_p) \cong \mathbf{Z}/p\mathbf{Z},
\end{tikzcd}$$

where i is the natural map and $\mathbf{N}$ is induced by the norm map.

For convenience, let

$$\begin{aligned}
&A = \alpha_{J,v}(1_v), \\
&B = \alpha_{J,v}(\chi), \text{ and} \\
&D = J(F_v)/\pi J(F_v) \cong J^\chi(F_v)/\pi J^\chi(F_v).
\end{aligned}$$

By Lemma 2.1.5, we have $D = D^\perp \subseteq \mathrm{res}(A)^\perp = \mathrm{cor}^{-1}(A)$, and similarly, $D = D^\perp \subseteq \mathrm{res}(B)^\perp = \mathrm{cor}^{-1}(B)$. Therefore, $\mathbf{N}(D) = \mathrm{cor}(D) \subseteq A \cap B$. □

Lemma 2.1.9. *Let A be an abelian variety defined over K_v such that $\mathbf{Z}[\zeta_p] \subset \mathrm{End}_{G_{K_v}}(A)$. Suppose that $v \nmid p\infty$. Then*

$$A(K_v)/\pi A(K_v) \cong A(K_v)[p^\infty]/\pi(A(K_v)[p^\infty]).$$

Proof. Multiplication by π is surjective on the pro-(prime to p) part of $A(K_v)$, so only the pro-p part $A(K_v)[p^\infty]$ contributes to $A(K_v)/\pi A(K_v)$, whence the result follows. □

Lemma 2.1.10. *Suppose that $\chi \in \mathcal{C}^p(K_v)$, and $F_v = \overline{K}_v^{\ker(\chi)}$, where $v \nmid p\infty$. Then the following hold.*

1. *$d_p(\alpha_{J,v}(1_v)) = d_p(J(K_v)/\pi J(K_v)) = d_p(J(K_v)[\pi])$.*

2. *Suppose further that, the extension F_v/K_v is ramified and J has good reduction. Then $J(K_v)/\pi J(K_v) \cong J(F_v)/\pi J(F_v)$.*

Proof. We have an exact sequence

$$0 \longrightarrow J(K_v)[\pi] \longrightarrow J(K_v)[p^\infty] \xrightarrow{\pi} J(K_v)[p^\infty] \longrightarrow J(K_v)[p^\infty]/\pi J(K_v)[p^\infty] \longrightarrow 0.$$

Hence (i) follows from Lemma 2.1.9.

Now we prove (ii). Under the assumptions, $K_v(J[p^\infty])$ is an unramified extension over K_v. Therefore $K_v(J(F_v)[p^\infty]) = K_v$, so $J(K_v)[p^\infty] = J(F_v)[p^\infty]$. Assertion (ii) follows from passing through (Lemma 2.1.9)

$$\begin{aligned} J(K_v)/\pi J(K_v) &\cong J(K_v)[p^\infty]/\pi(J(K_v)[p^\infty]) \\ &\cong J(F_v)[p^\infty]/\pi(J(F_v)[p^\infty]) \\ &\cong J(F_v)/\pi J(F_v). \end{aligned}$$

□

Lemma 2.1.11. *Suppose that $\sigma \in \mathrm{Gal}(f) \subset S_n$ consists of b orbits. Let $J[\pi]^{\sigma=1}$ denote the subgroup of $J[\pi]$ which consists of the elements fixed by σ. Then*

$$d_p(J[\pi]^{\sigma=1}) = b - 1.$$

Proof. Let σ be $(\alpha_{11}\alpha_{12}\cdots\alpha_{1i_1})(\alpha_{21}\cdots\alpha_{2i_2})\cdots(\alpha_{b1}\cdots\alpha_{bi_b})$, where α_{xy} are the roots of f. We rearrange α_{xy} so that $p \nmid i_b$, which is always possible because $p \nmid n$. Let a_{xy} denote the divisor classes $[(\alpha_{xy}, 0) - \infty]$. Then with the equality $\sum a_{xy} = 0$ (Lemma 1.2.3), one can show that

$$a_{11} + a_{12} + \cdots + a_{1i_1}, a_{21} + \cdots + a_{2i_2}, \cdots\cdots, a_{(b-1)1} + \cdots + a_{b-1i_{b-1}}$$

form a basis of $J[\pi]^{\sigma=1}$. □

Remark 2.1.12. Suppose that $v \nmid p\infty$. Let K_v^{ur} be the maximal unramified extension of K_v. It is well-known that if J/K_v has good reduction, then $J[\pi] \subset J[p] \subset J(K_v^{\mathrm{ur}})$. Let Frob_v denote the Frobenius automorphism of K_v^{ur}. Restricting Frob_v to $K(J[\pi])$, one can regard Frob_v as an element in S_n (since S_n acts on the set of roots of f by permutation).

Lemma 2.1.13. *Suppose that $v \nmid p\infty$, and J has a good reduction. Let b be the number of orbits of $\mathrm{Frob}_v \in S_n$. Then*

$$d_p(\alpha_{J,v}(1_v)) = b - 1.$$

Proof. Note that $J(K_v)[\pi] = J[\pi]^{\mathrm{Frob}_v=1}$. Then the lemma follows from Lemma 2.1.11 and Lemma 2.1.10. □

Lemma 2.1.14. *Let $\chi \in \mathcal{C}^p(K_v)$. Suppose that J has good reduction, $v \nmid p\infty$, and χ is unramified. Then $h_{J,v}(\chi) = 0$ (equivalently, $\alpha_{J,v}(1_v) = \alpha_{J,v}(\chi)$).*

Proof. Let $F_v = \overline{K}_v^{\ker(\chi)}$. It follows from [9, Corollary 4.4] that $\mathbf{N}(J(F_v)) = J(K_v)$. Thus, by Lemma 2.1.8, $h_{J,v}(\chi) = 0$. □

Lemma 2.1.15. *Suppose that $\chi \in \mathcal{C}^p(K_v)$ is non-trivial, and $F_v := \overline{K}_v^{\ker(\chi)}$, where $v \nmid p\infty$. Suppose that $J(K_v)/\pi J(K_v) \cong J(F_v)/\pi J(F_v)$ (which is satisfied if the extension F_v/K_v is ramified and J has good reduction by Lemma 2.1.10). Then*

$$\alpha_{J,v}(1_v) \cap \alpha_{J,v}(\chi) = \{0\};$$

i.e., $h_{J,v}(\chi) = \dim_{\mathbf{F}_p}(J(K_v)[\pi])$.

Proof. Consider the following commutative diagrams

$$\begin{tikzcd}
J(F_v)/\pi J(F_v) \arrow[r] & H^1(F_v, J[\pi]) \\
J(K_v)/\pi J(K_v) \arrow[u, "\cong"', "i"] \arrow[r, "j"] & H^1(K_v, J[\pi]) \arrow[u, "\mathrm{res}"']
\end{tikzcd}
\qquad
\begin{tikzcd}
H^1(F_v, J[\pi]) \arrow[d, "\mathrm{cor}"] & J(F_v)/\pi J(F_v) \arrow[l] \arrow[d, "\mathbf{N}"] \\
H^1(K_v, J[\pi]) & J(K_v)/\pi J(K_v) \arrow[l, "j"']
\end{tikzcd}$$

as in the proof of Lemma 2.1.8. The map i in the diagrams is an isomorphism by assumptions. Let $a \in J(F_v)$. Then $a = \pi b + c$ where $b \in J(F_v)$ and $c \in J(K_v)$. Therefore

$$\mathbf{N}(a) = \pi\mathbf{N}(b) + pc \in \pi J(K_v).$$

This means the map $\mathbf{N}$ in the diagrams is actually the zero map. Let

$$\begin{aligned}
A &:= J(K_v)/\pi J(K_v), \\
B &:= J^\chi(K_v)/\pi J^\chi(K_v), \text{ and} \\
D &:= J(F_v)/\pi J(F_v) \cong J^\chi(F_v)/\pi J^\chi(F_v),
\end{aligned}$$

for simplicity. From now on, we identify A, B and D with their Kummer images. We need to show that $A \cap B = \{0\}$. In other words, we want to show that $A + B$ $(= (A \cap B)^\perp) = H^1(K_v, J[\pi])$. One inclusion is trivial. For the other inclusion, let x be an element in $H^1(K_v, J[\pi])$. According to third diagram in the proof of Lemma 2.1.8, we have $\mathrm{res}^{-1}(D) =$

$(\mathrm{cor}(D))^\perp = 0^\perp = H^1(K_v, J[\pi])$, so we can find $y \in A$ such that $\mathrm{res}(x - y) = 0$. Since $x - y \in \ker(\mathrm{res})$, it is enough to show that

$$\ker(\mathrm{res}) \subseteq A + B. \tag{2.3}$$

By the Inflation-Restriction Sequence,

$$\ker(\mathrm{res}) \cong H^1(F_v/K_v, J[\pi]^{G_{F_v}}).$$

But actually, $J[\pi]^{G_{F_v}} = J(F_v)[\pi] = J(K_v)[\pi]$ by Lemma 2.1.10(i). Hence we have

$$\ker(\mathrm{res}) \cong \mathrm{Hom}(\mathrm{Gal}(F_v/K_v), J(K_v)[\pi]). \tag{2.4}$$

Let $\psi : J \cong J^\chi$ be an isomorphism defined over F_v. We have the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & \\
 & \mathrm{Hom}(\mathrm{Gal}(F_v/K_v), J(K_v)[\pi]) \arrow[d] & \\
J(K_v)/\pi J(K_v) \arrow[r, hook, "j"] \arrow[d] & H^1(K_v, J[\pi]) \arrow[d] & J^\chi(K_v)/\pi J^\chi(K_v) \arrow[l, hook', "j^\chi"'] \arrow[d] \\
J(F_v)/\pi J(F_v) \arrow[r, hook] \arrow[rr, bend right, "\underset{\simeq}{\psi}"'] & H^1(F_v, J[\pi]) & J^\chi(F_v)/\pi J^\chi(F_v), \arrow[l, hook']
\end{tikzcd}$$

where the middle column is exact. Define a homomorphism

$$\phi : J(K_v)[\pi] \to \mathrm{Hom}(\mathrm{Gal}(F_v/K_v), J(K_v)[\pi])$$
$$P \mapsto j(\overline{P}) - j^\chi(\overline{\psi(P)}),$$

where $\overline{P}$ is the image of P in $J(K_v)/\pi J(K_v)$ and $\overline{\psi(P)}$ is the image of $\psi(P)$ in $J^\chi(K_v)/\pi J^\chi(K_v)$. That the map ϕ being well-defined can be shown by diagram chasing in the diagram above. We claim that the map ϕ is an isomorphism, which will imply (2.3). It is enough to show the map ϕ is injective since $J(K_v)[\pi]$ and $\mathrm{Hom}(F_v/K_v, J(K_v)[\pi])$ have the same dimension over $\mathbf{F}_p$. It can be easily checked that for $P \neq 0$,

$$(j(\overline{P}) - j^\chi(\overline{\psi(P)}))(\tau) \neq 0,$$

where τ is a nontrivial element in $\mathrm{Gal}(F_v/K_v)$, so we are done. □

Until the end of this section, assume that $p = 2$. We show that equality holds in (2.2) when $p = 2$. For the elliptic curve case, the following proposition is proved in [7, Proposition 7] and [11, Proposition 5.2].

Proposition 2.1.16. *Let $\chi \in \mathcal{C}^2(K_v)$. Then*

$$\alpha_{J,v}(1_v) \cap \alpha_{J,v}(\chi) = \mathbf{N}J(L_v)/2J(K_v), \tag{2.5}$$

where $L_v = \overline{K}_v^{\ker(\chi)}$, and $\mathbf{N}J(L_v)$ is the image of the norm map $\mathbf{N} : J(L_v) \to J(K_v)$.

The following two lemmas are used to prove the proposition.

Lemma 2.1.17. *Suppose that $\chi \in \mathcal{C}^2(K_v)$ is a nontrivial quadratic character, and $L_v := \overline{K}_v^{\ker(\chi)}$. Let*

$$\phi : H^1(K_v, J[2]) \to H^1(L_v, J[2])$$

be the restriction map. Then (i) $\ker(\phi) \subseteq \alpha_{J,v}(1_v) + \alpha_{J,v}(\chi)$, and (ii) $d_2(\ker(\phi)) = 2d_2(J(K_v)[2]) - d_2(J(L_v)[2])$.

Proof. Let

$$\begin{aligned} i :& J(K_v)/2J(K_v) \to H^1(K_v, J[2]), \text{ and} \\ i^\chi :& J^\chi(K_v)/2J^\chi(K_v) \to H^1(K_v, J^\chi[2]) \cong H^1(K_v, J[2]). \end{aligned}$$

By the Inflation-Restriction Sequence,

$$\ker(\phi) = H^1(L_v/K_v, J(L_v)[2]) = J(K_v)[2]/(\tau - 1)J(L_v)[2],$$

where $\mathrm{Gal}(L_v/K_v)$ is generated by τ. Then for any $P \in J(K_v)[2]$, its image c_P in $H^1(K_v, J[2])$ of the composition map

$$J(K_v)[2] \to J(K_v)[2]/(\tau - 1)J(L_v)[2] \subset H^1(K_v, J[2])$$

is given by $c_P(\sigma) = P$ if $\sigma|_{L_v} = \tau$, and $c_P(\sigma) = 0$ otherwise. With the isomorphism $J(\overline{K}_v) \cong J^\chi(\overline{K}_v)$, it is straightforward to check that $i(\overline{P}) + i^\chi(\overline{P^\chi}) = c_P$, where $\overline{P}$ and $\overline{P^\chi}$ represent the images of P in $J(K_v)/2J(K_v)$ and $J^\chi(K_v)/2J^\chi(K_v)$, respectively. This proves (i). The exact sequence

$$\begin{tikzcd} 0 \arrow[r] & J(K_v)[2] \arrow[r] & J(L_v)[2] \arrow[r, "\tau-1"] & J(K_v)[2] \arrow[r] & \ker(\phi) \arrow[r] & 0 \end{tikzcd}$$

shows (ii). □

Lemma 2.1.18. *Let L_v/K_v be a nontrivial quadratic extension. Then*

$$2d_2(J(K_v)[2]) - d_2(J(L_v)[2]) = 2d_2(J(K_v)/2J(K_v)) - d_2(J(L_v)/2J(L_v)).$$

Proof. Consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & J^{\chi}(K_v) \arrow[r] \arrow[d, "2"] & J(L_v) \arrow[r, "N"] \arrow[d, "2"] & J(K_v) \arrow[r] \arrow[d, "2"] & J(K_v)/N(J(L_v)) \arrow[r] \arrow[d, "2"] & 0 \\
0 \arrow[r] & J^{\chi}(K_v) \arrow[r] & J(L_v) \arrow[r, "N"] & J(K_v) \arrow[r] & J(K_v)/N(J(L_v)) \arrow[r] & 0.
\end{tikzcd}$$

Note that each row consists of two short exact sequences

$$\begin{aligned}
&0 \longrightarrow J^{\chi}(K_v) \longrightarrow J(L_v) \xrightarrow{\quad N \quad} NJ(L_v) \longrightarrow 0, \text{ and} \\
&0 \longrightarrow NJ(L_v) \longrightarrow J(K_v) \longrightarrow J(K_v)/N(J(L_v)) \longrightarrow 0.
\end{aligned}$$

Then applying the snake lemma for each short exact sequence and comparing the dimensions over $\mathbf{F}_2$ together with Remark 1.2.7 and Remark 2.1.6 show the result. □

Proof of Proposition 2.1.16. If L_v/K_v is trivial, then it is obvious. Thus assume L_v/K_v is a nontrivial quadratic extension. By Lemma 2.1.8, it is enough to show that

$$d_2(\alpha_{J,v}(1_v) \cap \alpha_{J,v}(\chi)) = d_2(\mathbf{N}J(L_v)/2J(K_v)). \tag{2.6}$$

Consider the following exact sequence ($M := J(K_v) + J^{\chi}(K_v) + 2J(L_v)$)

$$0 \longrightarrow M/2J(L_v) \longrightarrow J(L_v)/2J(L_v) \xrightarrow{\mathbf{N}} J(K_v)/2J(K_v) \longrightarrow J(K_v)/N(J(L_v)) \longrightarrow 0,$$

where the middle map $\mathbf{N}$ is induced by the norm map and $J^{\chi}(K_v)$ is regarded as a subgroup of $J(L_v)$. For simplicity, write X, Y, Z and W for the nontrivial terms in the exact sequence in order. Let $A = \alpha_{J,v}(1_v)$, and $B = \alpha_{J,v}(\chi)$. Then $d_2(A+B)+d_2(A\cap B) = d_2(H^1(K_v, J[2]))$ since $A \cap B$ is the orthogonal complement of $A + B$ in (2.1). Let

$$\phi : H^1(K_v, J[2]) \to H^1(L_v, J[2])$$

be the restriction map. We have $X = \phi(A + B)$, so by Remark 2.1.6, Lemma 2.1.17, and

Lemma 2.1.18,

$$\begin{aligned} d_2(X) &= d_2(A+B) - d_2(\ker(\phi)) \\ &= d_2(H^1(K_v, J[2])) - d_2(A \cap B) - d_2(\ker(\phi)) \\ &= d_2(H^1(K_v, J[2])) - d_2(A \cap B) - 2d_2(J(K_v)[2]) + d_2(J(L_v)[2]) \\ &= d_2(J(L_v)/2J(L_v)) - d_2(A \cap B). \end{aligned}$$

Then the equality $d_2(X) + d_2(Z) = d_2(Y) + d_2(W)$ shows (2.6), as desired. □

For the following lemma, we specify v_0 so that $K_{v_0} = \mathbf{R}$.

Lemma 2.1.19. *Let $C_{2,f}$ be a hyperelliptic curve over K_{v_0} ($\cong \mathbf{R}$). Let η be the sign character. Suppose that f has $2k_1 - 1$ real roots and $2k_2$ complex roots. Then*

1. $J(K_{v_0}) \cong (\mathbf{R}/\mathbf{Z})^{k_1+k_2-1} \oplus (\mathbf{Z}/2\mathbf{Z})^{k_1-1}$, *and*

2. $h_{J_{2,f},v_0}(\eta) = k_1 - 1$.

Proof. Complex conjugation corresponds to the element of S_n that consists of $2k_1 - 1$ cycles of length 1 and k_2 cycles of length 2. Hence [13, Remark I.3.7] and Lemma 2.1.11 show (i). Note that the image of the norm map $\mathbf{N} : J(\mathbf{C}) \to J(\mathbf{R})$ is the the connected component of 0 ($= (\mathbf{R}/\mathbf{Z})^{k_1+k_2-1}$) according to [13, Remark I.3.7]. Then (ii) follows from Proposition 2.1.16. □

2.2 Controlling the localization maps

We continue to assume K is a number field containing a primitive p-th root of unity ζ_p and $C_{p,f}$ is a superelliptic curve defined over K. Recall that the simple notation J stands for the Jacobian of $C_{p,f}$ and n denotes the degree of f. We write $\mathrm{Gal}(f)$ for the Galois group of the splitting field extension of $f \in K[x]$ over K. Note that there is an action of S_n on $J[\pi]$ induced by a permutation action of S_n on the roots of f by Lemma 1.2.3. In this way, we may view $\mathrm{Gal}(f)$ as a subgroup of S_n. Recall that $p \nmid n$.

Lemma 2.2.1. *We have $H^1(S_n, J[\pi]) = 0$.*

Proof. We regard S_n as the symmetric group on the set $\{1, 2, \cdots, n\}$. Let $H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1} \subset S_n$. We have an S_n-module isomorphism

$$\mathrm{Ind}_H^{S_n} \mathbf{F}_p \cong \mathbf{F}_p[S_n/H]$$

where $\mathrm{Ind}_H^{S_n} \mathbf{F}_p$ denotes the induced S_n-module of the H-module $\mathbf{F}_p$ (trivial action of H on $\mathbf{F}_p$). Let β_i be the image of the permutation $(i\ n)$ in $\mathbf{F}_p[S_n/H]$. Note that $\sigma(\beta_i) = \beta_{\sigma(i)}$ in S_n/H. We put

$$D = \{a(\beta_1 + \beta_2 + \cdots + \beta_n) \mid a \in \mathbf{F}_p\}.$$

Then

$$\mathrm{Ind}_H^{S_n} \mathbf{F}_p/D \cong \mathbf{F}_p[S_n/H]/D \cong J[\pi].$$

In the last isomorphism the map is defined by $\beta_i \mapsto \alpha_i$ where α_i are the roots of f. We have an (S_n-module) exact sequence

$$0 \longrightarrow D \xrightarrow{j} \mathrm{Ind}_H^{S_n} \mathbf{F}_p \longrightarrow \mathrm{Ind}_H^{S_n} \mathbf{F}_p/D \longrightarrow 0. \tag{2.7}$$

But since $p \nmid n$, we have a map

$$g : \mathrm{Ind}_H^{S_n} \mathbf{F}_p \longrightarrow D$$

defined by $a_1\beta_1 + \cdots + a_n\beta_n \mapsto n^{-1}(a_1 + \cdots + a_n)(\beta_1 + \cdots \beta_n)$ where n^{-1} is taken in $(\mathbf{Z}/p\mathbf{Z})^\times$. Clearly $g \circ j = \mathrm{id}_D$, so the exact sequence (2.7) splits. Hence

$$H^1(S_n, \mathrm{Ind}_H^{S_n} \mathbf{F}_p) \cong H^1(S_n, D) \oplus H^1(S_n, J[\pi]).$$

By Shapiro's lemma, $H^1(S_n, \mathrm{Ind}_H^{S_n} \mathbf{F}_p) \cong H^1(H, \mathbf{F}_p)$. If p is odd, $H^1(H, \mathbf{F}_p) = \mathrm{Hom}(H, \mathbf{F}_p) = 0$. If $p = 2$ (so $n \geq 3$), $H^1(H, \mathbf{F}_2) = \mathbf{Z}/2\mathbf{Z} = \mathrm{Hom}(S_n, D) = H^1(S_n, D)$. In either case, we have $H^1(S_n, J[\pi]) = 0$. □

Definition 2.2.2. We say that $C_{p,f}$ satisfies $(*)$ if one of the following holds.

- $p = 2$, $\mathrm{Gal}(f) \cong A_n$ or S_n, and $n \geq 5$.
- $p = 2, n = 3$, and $\mathrm{Gal}(f) \cong S_3$.
- p is an odd prime, and $\mathrm{Gal}(f) \cong S_n$.

If $c \in H^1(K, J[\pi])$ and $\sigma \in G_K$, let

$$c(\sigma) \in J[\pi]/(\sigma - 1)J[\pi]$$

denote the image of σ under any cocycle representing c.

Lemma 2.2.3. *Let N be a finite subgroup of $H^1(K, J[\pi])$ and $\sigma \in G_K$. Suppose that $\phi : N \longrightarrow J[\pi]/(\sigma - 1)J[\pi]$ is a homomorphism. Suppose that* $\mathrm{Gal}(K(J[\pi])/K) = \mathrm{Gal}(f) = \Omega$ *satisfies the following conditions.*

1. *$H^1(\Omega, J[\pi]) = 0$,*

2. *$J[\pi]$ is a simple Ω-module,*

3. *$\dim_{\mathbf{F}_p}(\mathrm{Hom}_\Omega(J[\pi], J[\pi])) = 1$, and*

4. *Ω does not act on $J[\pi]$ trivially.*

Then there exists an element $\rho \in G_K$ such that $\rho\ |_{K(J[\pi])K^{ab}} = \sigma\ |_{K(J[\pi])K^{ab}}$ and $c(\rho) = \phi(c)$ for all $c \in N$. In particular, if $C_{p,f}$ satisfies $(*)$, then there exists such an element $\rho \in G_K$.

Proof. The proof of Lemma 3.5 of [8] works here, too. For the last assertion, it is not difficult to check that (ii), (iii), and (iv) are satisfied when $C_{p,f}$ satisfies $(*)$. If $\mathrm{Gal}(f) \cong S_n$, the condition (i) is Lemma 2.2.1. If $p = 2$, and $\mathrm{Gal}(f) \cong A_n$, then $J[2]^{A_n = 1} = 0$. The Hochschild-Serre Spectral Sequence (for example, see [15, Proposition 1.6.7]) together with the fact that $H^1(S_n, J[2]) = 0$ shows that $H^1(A_n, J[2])^{S_n/A_n = 1} = 0$. Then $H^1(A_n, J[2]) = 0$ by the following fact that can be proved by a standard argument of group theory: If U, V are nontrivial 2-groups such that U acts on V, then V^U (:=the group of elements in V fixed by every element in U) is non-trivial. □

Remark 2.2.4. Note that if $C_{2,f}$ is an elliptic curve, and $\mathrm{Gal}(f) \cong A_3$, the condition (iii) in Lemma 2.2.3 does not hold.

Definition 2.2.5. For every place v of K, we write res_v for the restriction map (fixing an embedding $\overline{K} \hookrightarrow \overline{K}_v$)

$$\mathrm{res}_v : H^1(K, J[\pi]) \to H^1(K_v, J[\pi]).$$

Suppose that J has good reduction at $\mathfrak{q} \nmid p\infty$. Define the localization map

$$\mathrm{loc}_{\mathfrak{q}} : \mathrm{Sel}_{\pi}(J/K) \to \alpha_{J,\mathfrak{q}}(1_{\mathfrak{q}}) \cong J[\pi]/(\mathrm{Frob}_{\mathfrak{q}} - 1),$$

where the former map is $\mathrm{res}_{\mathfrak{q}}$ and the latter map given in Lemma 2.1.7. Note that $\mathrm{loc}_{\mathfrak{q}}$ is given by evaluating cocycles at a Frobenius automorphism $\mathrm{Frob}_{\mathfrak{q}}$.

We define various Selmer groups as follows.

Definition 2.2.6. Let $\mathfrak{q}$ be a prime of K and $\psi_{\mathfrak{q}} \in \mathcal{C}^p(K_{\mathfrak{q}})$. Define

$$\begin{aligned}\mathrm{Sel}_{\pi}(J, \psi_{\mathfrak{q}}) := \{x \in H^1(K, J[\pi]) | \mathrm{res}_v(x) \in \alpha_{J,v}(1_v) \text{ if } v \neq \mathfrak{q}, \text{ and} \\ \mathrm{res}_{\mathfrak{q}}(x) \in \alpha_{J,\mathfrak{q}}(\psi_{\mathfrak{q}})\}.\end{aligned}$$

Define

$$\begin{aligned}\mathrm{Sel}_{\pi,\mathfrak{q}}(J/K) := \{x \in H^1(K, J[\pi]) | \mathrm{res}_v(x) \in \alpha_{J,v}(1_v) \text{ if } v \neq \mathfrak{q}, \text{ and} \\ \mathrm{res}_{\mathfrak{q}}(x) = 0\}.\end{aligned}$$

Define

$$\mathrm{Sel}_{\pi}^{\mathfrak{q}}(J/K) := \ker(H^1(K, J[\pi]) \to \bigoplus_{v \neq \mathfrak{q}} H^1(K_v, J[\pi])/\alpha_{J,v}(1_v)).$$

Obviously, $\mathrm{Sel}_{\pi,\mathfrak{q}}(J/K) \subseteq \mathrm{Sel}_{\pi}(J/K) \subseteq \mathrm{Sel}_{\pi}^{\mathfrak{q}}(J/K)$.

Lemma 2.2.7. *The images of the right hand restriction maps of the following exact sequences are orthogonal complements under* (2.1)

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Sel}_{\pi}(J/K) \arrow[r] & \mathrm{Sel}_{\pi}^{\mathfrak{q}}(J/K) \arrow[r] & H^1(K_v, J[\pi])/\alpha_{J,\mathfrak{q}}(1_{\mathfrak{q}}), \\ 0 \arrow[r] & \mathrm{Sel}_{\pi,\mathfrak{q}}(J/K) \arrow[r] & \mathrm{Sel}_{\pi}(J/K) \arrow[r] & \alpha_{J,\mathfrak{q}}(1_{\mathfrak{q}}). \end{tikzcd}$$

In particular, $d_p(\mathrm{Sel}_{\pi}^{\mathfrak{q}}(J/K)) - d_p(\mathrm{Sel}_{\pi,\mathfrak{q}}(J/K)) = d_p(\alpha_{J,\mathfrak{q}}(1_{\mathfrak{q}})) = \frac{1}{2} d_p(H^1(K_{\mathfrak{q}}, J[\pi]))$.

Proof. The lemma follows from the Global Poitou-Tate Duality. For example, see [18, Theorem 1.7.3] or [10, Theorem 2.3.4]. □

2.3 π-Selmer ranks of Jacobians of superelliptic curves

We continue to assume that $C_{p,f}$ is a superelliptic curve over a number field K containing ζ_p. Let Σ denote a (finite) set of places which contains all places where J has bad reduction, all archimedean places, and all primes above p. We enlarge Σ, if necessary, so that $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0$. As before, we write J for the Jacobian of $C_{p,f}$. In this section, we prove that if p is an odd prime, there exist infinitely many p-twists of J whose Jacobians have π-Selmer ranks equal to any non-negative integer r.

Remark 2.3.1. Note that a p-twist (Definition 1.2.5) of a p-twist of $J_{p,f}$ is again a p-twist. This enables us to use an inductive argument. For example, if we have an algorithm to construct a p-twist of the Jacobian of a superelliptic curve having a strictly bigger π-Selmer group than the original π-Selmer group, we can make the π-Selmer group as big (the dimension over $\mathbf{F}_p$) as we want by taking p-twists.

Proposition 2.3.2. *Suppose that K is a number field containing ζ_p, and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\mathrm{Gal}(f) \cong S_n$. Let $J := J(C_{p,f})$. Suppose that $d_p(\mathrm{Sel}_\pi(J/K)) \geq 1$. Then there exist infinitely many p-twists J^χ such that $d_p(\mathrm{Sel}_\pi(J^\chi/K)) = d_p(\mathrm{Sel}_\pi(J/K)) - 1$.*

Proof. We prove this proposition by following the method of the proof of [8, Proposition 5.1]. Let Δ_f be the discriminant of the polynomial f. Let θ be the (formal) product of p^3, all primes where J has bad reduction and all archimedean places. Let $K(\theta)$ be its ray class field and $K[\theta]$ be the p-maximal subextension of $K(\theta)$. Then, $K[\theta]$ and $K(J[\pi])$ are linearly disjoint. Indeed, S_n has no normal subgroup of index p for an odd prime p. Therefore we can find an element $\sigma \in G_K$ such that $\sigma \mid_{J(K[\pi])}$ consists of 2 disjoint orbits ($\sigma|_{J(K[\pi])} \in \mathrm{Gal}(K(J[\pi])/K) = \mathrm{Gal}(f) = S_n$), and $\sigma \mid_{K[\theta]} = 1$.

Let

$$\phi : \mathrm{Sel}_\pi(J/K) \longrightarrow J[\pi]/(\sigma - 1)J[\pi]$$

be a homomorphism. By Lemma 2.2.3, we can find $\rho \in G_K$ such that

- $\rho \mid_{K[\theta]K(J[\pi])} = \sigma$

- $c(\rho) = \phi(c)$ for every $c \in \mathrm{Sel}_\pi(J/K)$.

Let N be a Galois extension of K containing $K(\theta)K(J[\pi])$, large enough so that the restriction of every element in $\mathrm{Sel}_\pi(J/K)$ to G_N is zero (Choosing such a G_N is possible because the Selmer group is finite).

By the Chebotarev density theorem, we can find a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \nmid p$, J has good reduction at $\mathfrak{q}$, the extension N/K is unramified at $\mathfrak{q}$ and $\mathrm{Frob}_\mathfrak{q} \in$ (the conjugacy class of ρ in $\mathrm{Gal}(N/K)$). Since $p \nmid [K(\theta) : K[\theta]]$, the restriction of ρ^k to $K(\theta)$ is trivial for some $p \nmid k$. Therefore $\mathfrak{q}^k$ is principal generated by $d \equiv 1 (\mathrm{mod}\ \theta)$. Let $F = K(\sqrt[p]{d})$. Then all places dividing θ split in F/K, the extension F/K is ramified at $\mathfrak{q}$, and nowhere else because its discriminant divides $p^p d^{p-1}$. Let χ denote the image of the Kummer map $K^\times/(K^\times)^p \cong \mathcal{C}^p(K)$. Therefore, by Lemma 2.1.14, $\alpha(1_v) = \alpha(\chi_v)$ for all places v except $\mathfrak{q}$, where χ_v is the restriction of χ to G_{K_v}.

Since J has good reduction at $\mathfrak{q}$,

$$\alpha_{J,\mathfrak{q}}(1_\mathfrak{q}) \cong J[\pi]/(\mathrm{Frob}_\mathfrak{q} - 1)J[\pi] \cong J[\pi]/(\rho - 1)J[\pi] = J[\pi]/(\sigma - 1)J[\pi].$$

The first isomorphism follows from Lemma 2.1.7. By Lemma 2.1.13 and our choice of σ, we have $d_p(\alpha_{J,\mathfrak{q}}(1_\mathfrak{q})) = 1$.

The localization map (Definition 2.2.5)

$$\mathrm{loc}_\mathfrak{q} : \mathrm{Sel}_\pi(J/K) \longrightarrow \alpha_{J,\mathfrak{q}}(1_\mathfrak{q}) \cong J[\pi]/(\rho - 1)J[\pi]$$

is given by evaluation of cocycles at $\mathrm{Frob}_\mathfrak{q} \sim \rho$. Therefore we have

$$\mathrm{loc}_\mathfrak{q}(\mathrm{Sel}_\pi(J/K)) = \phi(\mathrm{Sel}_\pi(J/K))$$

by Lemma 2.2.3. Note that $d_p(\mathrm{Sel}_\pi^\mathfrak{q}(J/K)) - d_p(\mathrm{Sel}_{\pi,\mathfrak{q}}(J/K)) = 1$ by Lemma 2.2.7. Choose ϕ so that $d_p(\mathrm{Im}(\phi)) = 1$. Then, $\mathrm{Sel}_\pi(J/K) = \mathrm{Sel}_\pi^\mathfrak{q}(J/K)$. Then Lemma 2.1.15 and Lemma 2.2.7 show that

$$d_p(\mathrm{Sel}_\pi(J^\chi/K)) = d_p(\mathrm{Sel}_\pi(J/K)) - 1.$$

□

Definition 2.3.3. Let θ be a (formal) product of primes of K. Define

$$\begin{aligned}\Sigma(\theta) &:= \Sigma \cup \{\mathfrak{q} : \mathfrak{q}|\theta\},\\ \mathcal{P}_{J,i} &:= \ \{\mathfrak{q} : \mathfrak{q} \notin \Sigma \text{ and } \dim_{\mathbf{F}_p}(J[\pi]^{G_{K_\mathfrak{q}}}) = i\} \quad \text{for } 0 \leq i \leq n-1, \text{ and}\\ \mathcal{P}_J &:= \ \mathcal{P}_{J,0} \coprod \mathcal{P}_{J,1} \coprod \mathcal{P}_{J,2} \coprod \cdots \coprod \mathcal{P}_{J,n-1} = \{\mathfrak{q} : \mathfrak{q} \notin \Sigma\}.\end{aligned}$$

Although $\mathcal{P}_{J,i}$ and $\mathcal{P}_J$ depend on the choice of Σ, we suppress it from the notation.

Remark 2.3.4. If $\mathfrak{q} \in \mathcal{P}_{J,i}$, then $d_p(\alpha_{J,\mathfrak{q}}(1_\mathfrak{q})) = i$ by Lemma 2.1.10.

Lemma 2.3.5. *Suppose that v is a prime of K such that $v \nmid p\infty$, and J has good reduction at v. If $\psi_v \in \mathcal{C}^p_{\text{ram}}(K_v)$, then*

$$J^{\psi_v}(K_v)[p^\infty] = J^{\psi_v}(K_v)[\pi] \ (\cong J(K_v)[\pi])$$

Proof. Let $L_v := \overline{K}_v^{\text{Ker}(\psi_v)}$ so that L_v is a (totally) ramified extension over K_v of degree p. Let $K_v^{\text{ur}}, L_v^{\text{ur}}$ denote the maximal unramified extensions over K_v, L_v, respectively. It is sufficient to prove that

$$J^{\psi_v}(K_v^{\text{ur}})[p^\infty] = J^{\psi_v}(K_v^{\text{ur}})[\pi]. \tag{2.8}$$

Let $\sigma \in \text{Gal}(L_v^{\text{ur}}/K_v^{\text{ur}})$ be non-trivial. Then

$$J^{\psi_v}(L_v^{\text{ur}})[p^\infty]^{\sigma=1} = J^{\psi_v}(K_v^{\text{ur}})[p^\infty].$$

It is well-known that the assumptions that $v \nmid p\infty$ and J has good reduction at v imply that $J[p^\infty] \subset J(K_v^{\text{ur}})$. Let

$$\lambda : J^{\psi_v} \cong J$$

be an isomorphism over L_v. Note that $\lambda^\sigma = \sigma\lambda\sigma^{-1} = \psi_v(\sigma)\lambda$. If $P \in J^{\psi_v}(K_v^{\text{ur}})[p^\infty]$, then

$$\lambda(P) = \lambda(P^\sigma) = \psi_v(\sigma)^{-1}\lambda^\sigma(P^\sigma) = \psi_v(\sigma)^{-1}(\lambda(P))^\sigma = \psi_v(\sigma)^{-1}\lambda(P), \tag{2.9}$$

whence $P = \zeta_p P$ if we take σ so that $\psi_v(\sigma) = \zeta_p^{-1}$. In the last equality in (2.9), we have used the fact that $J[p^\infty] \subset J(K_v^{\text{ur}})$. Now it is easy to see that (2.8) holds. □

Definition 2.3.6. Choose a nontrivial unramified character $\epsilon_\mathfrak{q} \in \mathcal{C}^p(K_\mathfrak{q})$ and a ramified character $\eta_\mathfrak{q} \in \mathcal{C}^p_{\text{ram}}(K_\mathfrak{q})$ for every prime $\mathfrak{q} \in \mathcal{P}_J$. Define

$$\eta_{\mathfrak{q},j} := \eta_\mathfrak{q} \epsilon_\mathfrak{q}^j$$

for every $0 \leq j \leq p-1$.

Obviously, all $\eta_{\mathfrak{q},j}$ are in $\mathcal{C}^p_{\text{ram}}(K_\mathfrak{q})$.

Lemma 2.3.7. *Suppose that p is an odd prime. Let $\mathfrak{q} \in \mathcal{P}_J$ be a prime such that every orbit of* $\mathrm{Frob}_\mathfrak{q} \in S_n$ *has length not divisible by p. Then for any a, b such that $0 \leqq a, b \leqq p-1$ and $a \neq b$,*

$$\alpha_{J,\mathfrak{q}}(\eta_{\mathfrak{q},a}) \cap \alpha_{J,\mathfrak{q}}(\eta_{\mathfrak{q},b}) = \{0\}.$$

Proof. Lemma 2.1.9 and Lemma 2.3.5 show that

$$\begin{aligned} J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})/\pi J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q}) &\cong J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[p^\infty]/\pi J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[p^\infty] \\ &\cong J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[\pi]/\pi J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[\pi] \\ &= J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[\pi]. \end{aligned}$$

Let $F_\mathfrak{q} := \overline{K}_\mathfrak{q}^{\mathrm{Ker}\ \epsilon_\mathfrak{q}^{b-a}}$, the degree p unramified extension over $K_\mathfrak{q}$. Since every orbit of $\mathrm{Frob}_\mathfrak{q}$ has length not divisible by p, the degree $[K_\mathfrak{q}(J[\pi]) : K_\mathfrak{q}]$ is not as well. In particular, $F_\mathfrak{q}$ and $K_\mathfrak{q}(J[\pi])$ are linearly disjoint over $K_\mathfrak{q}$. Then it follows that

$$J^{\eta_{\mathfrak{q},a}}(F_\mathfrak{q})[\pi] \cong J(F_\mathfrak{q})[\pi] = J(K_\mathfrak{q})[\pi] \cong J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[\pi].$$

Hence we have

$$J^{\eta_{\mathfrak{q},a}}(F_\mathfrak{q})/\pi J^{\eta_{\mathfrak{q},a}}(F_\mathfrak{q}) \cong J^{\eta_{\mathfrak{q},a}}(F_\mathfrak{q})[\pi] = J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})[\pi] \cong J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q})/\pi J^{\eta_{\mathfrak{q},a}}(K_\mathfrak{q}),$$

where the first isomorphism comes exactly as above. Finally, we apply Lemma 2.1.15 to get the conclusion. □

Lemma 2.3.8. *[6, Lemma 6.6] Suppose that G, H are abelian groups and $M \subset G \times H$ is a subgroup. Let π_G and π_H denote the projection maps from $G \times H$ to G and H, respectively. Let $M_0 := \ker(\pi_G : M \to G/G^p)$.*

1. *The image of the natural map* $\mathrm{Hom}((G \times H)/M, \boldsymbol{\mu}_p) \to \mathrm{Hom}(H, \boldsymbol{\mu}_p))$ *is exctly* $\{g \in \mathrm{Hom}(H, \boldsymbol{\mu}_p) : \pi_H(M_0) \subset \ker(g)\}$
2. *If* $M/M^p \to G/G^p$ *is injective, then* $\mathrm{Hom}((G \times H)/M, \boldsymbol{\mu}_p) \to \mathrm{Hom}(H, \boldsymbol{\mu}_p)$ *is surjective.*

Lemma 2.3.9. *Suppose that* $\mathcal{O}_{\mathfrak{q}}$ *is the ring of integers of* $K_{\mathfrak{q}}$ *for every prime ideal* $\mathfrak{q}$*. Then the natrual map*

$$\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^p \longrightarrow \prod_{\mathfrak{q} \in \mathcal{P}_{J,0}} \mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^p \tag{2.10}$$

is injective.

Proof. Let α be a nontrivial element of $\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^p$. We want to find a prime $\mathfrak{q}' \in \mathcal{P}_{J,0}$ such that $\alpha \notin (\mathcal{O}_{\mathfrak{q}'}^{\times})^p$. Two fields $K(\sqrt[p]{\alpha})$ and $K(J[\pi])$ are linearly disjoint over K because S_n doesn't have a normal subgroup of index p for an odd prime p. We choose an element $\tau \in G_K$ such that

- $\tau\mid_{K(\sqrt[p]{\alpha})} \neq 1$, and
- $\tau\mid_{K(J[\pi])} \in S_n$ is a n-cycle.

Let U be the conjugacy class of τ in $\mathrm{Gal}(K(\sqrt[p]{\alpha})K(J[\pi])/K)$. By the Chebotarev density theorem, there exist infinitely many $\mathfrak{q}'$ such that $\mathrm{Frob}_{\mathfrak{q}'} \in U$. Such a prime $\mathfrak{q}'$ satisfies both $\alpha \notin (\mathcal{O}_{\mathfrak{q}'}^{\times})^p$ and $\mathfrak{q}' \in \mathcal{P}_{J,0}$ if $\mathfrak{q}' \notin \Sigma$. □

Remark 2.3.10. One can check easily that Lemma 2.3.9 still holds if we replace Σ by a finite set containing Σ.

Proposition 2.3.11. *Suppose that* p *is an odd prime. Then there are infinitely many prime ideals* $\mathfrak{r} \in \mathcal{P}_{J,1}$ *and an integer* $0 \leq e \leq p-1$ *so that*

$$d_p(\mathrm{Sel}_\pi(J, \eta_{\mathfrak{r},e})) = d_p(\mathrm{Sel}_\pi(J/K)) + 1, \tag{2.11}$$

where $\eta_{\mathfrak{r},e}$ *is as in Definition 2.3.6.*

Proof. Since $\mathrm{Gal}(K(J[\pi]/K) \cong S_n$, we can find a prime $\mathfrak{r} \in \mathcal{P}_{J,1}$ (equivalently, $\mathrm{Frob}_{\mathfrak{r}}$ has 2 orbits) such that neither of the order of the orbits of $\mathrm{Frob}_{\mathfrak{r}} \in S_n$ is divisible by p (which is possible since p is an odd prime) and that the localization map (Definition 2.2.5)

$$\mathrm{loc}_{\mathfrak{r}} : \mathrm{Sel}_{\pi}(J/K) \longrightarrow \alpha_{J,\mathfrak{r}}(1_{\mathfrak{r}}) \cong J[\pi]/(\mathrm{Frob}_{\mathfrak{r}} - 1)J[\pi]$$

is trivial by Lemma 2.2.3 combined with the Cheboterev Density Theorem. In other words, $\mathrm{Sel}_{\pi}(J/K) = \mathrm{Sel}_{\pi,\mathfrak{r}}(J/K)$. By Lemma 2.2.7, $\dim_{\mathbf{F}_p}(\mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K)) = \dim_{\mathbf{F}_p}(\mathrm{Sel}_{\pi,\mathfrak{r}}(J/K)) + 1$. Denote the image of the restriction map

$$\mathrm{res}_{\mathfrak{r}} : \mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K)) \to H^1(K_{\mathfrak{r}}, J[\pi])$$

by $\mathrm{res}_{\mathfrak{r}}(\mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K))$. Then the set $\mathrm{res}_{\mathfrak{r}}(\mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K))$ is a 1-dimensional $\mathbf{F}_p$-vector subspace of $H^1(K_{\mathfrak{r}}, J[\pi])$. But Lemma 2.3.7, Lemma 2.1.15, and Lemma 2.1.14 together show that one can find a $\eta_{\mathfrak{r},e} \in \mathcal{C}^p_{\mathrm{ram}}(K_{\mathfrak{r}})$ such that

$$\mathrm{res}_{\mathfrak{r}}(\mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K)) = \alpha_{J,\mathfrak{r}}(\eta_{\mathfrak{r},e}),$$

since there are exactly $p+1$ pairwise distinct 1-dimensional subspaces of $H^1(K_{\mathfrak{r}}, J[\pi])$ because $\mathfrak{r} \in \mathcal{P}_{J,1}$ (so $d_2(H^1(K_{\mathfrak{r}}, J[\pi]) = 2)$. It follows that $\mathrm{Sel}_{\pi}^{\mathfrak{r}}(J/K) = \mathrm{Sel}_{\pi}(J, \eta_{\mathfrak{r},e})$, so we are done. □

Proposition 2.3.12. *Suppose that K is a number field containing ζ_p, and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\mathrm{Gal}(f) \cong S_n$. Let $J := J(C_{p,f})$. Then there exist infinitely many p-twists J^{χ} such that $d_p(\mathrm{Sel}_{\pi}(J^{\chi}/K)) = d_p(\mathrm{Sel}_{\pi}(J/K)) + 1$.*

Proof. The main technique in the proof is already used in that of [6, Proposition 6.8]. Suppose that $\mathfrak{r} \in \mathcal{P}_{J,1}$ is as in Proposition 2.3.11. As stated earlier in this section we can enlarge Σ, if necessary, so that $\mathrm{Pic}(\mathcal{O}_{K,\Sigma(\mathfrak{r})}) = 0$. Thus global class field theory gives

$$\mathcal{C}^p(K) = \mathrm{Hom}(\mathbf{A}_K^{\times}/K^{\times}, \boldsymbol{\mu}_p) = \mathrm{Hom}((\textstyle\prod_{v \in \Sigma(\mathfrak{r})} K_v^{\times} \times \prod_{\mathfrak{q} \notin \Sigma(\mathfrak{r})} \mathcal{O}_{\mathfrak{q}}^{\times})/\mathcal{O}_{K,\Sigma(\mathfrak{r})}^{\times}, \boldsymbol{\mu}_p).$$

Let $\psi_{\mathfrak{r},e} \in \mathcal{C}^p_{\mathrm{ram}}(K_{\mathfrak{r}})$ be the character such that (2.11) holds. Define

$$\begin{aligned} Q &:= \mathcal{P}_J - \{\mathcal{P}_{J,0} \cup \Sigma(\mathfrak{r})\}, \\ M &:= \mathcal{O}^{\times}_{K,\Sigma(\mathfrak{r})}, \\ G &:= \prod_{\mathfrak{q}\in\mathcal{P}_{J,0}} \mathcal{O}^{\times}_{\mathfrak{q}}, \text{ and} \\ H &:= \prod_{\mathfrak{q}\in Q} \mathcal{O}^{\times}_{\mathfrak{q}} \times \prod_{v\in\Sigma(\mathfrak{r})} K^{\times}_v. \end{aligned}$$

By Remark 2.3.10, the map $M/M^p \to G/G^p$ is injective. Therefore

$$\begin{aligned} \mathcal{C}^p(K) = \mathrm{Hom}((G\times H)/M, \boldsymbol{\mu}_p) &\longrightarrow \mathrm{Hom}(H, \boldsymbol{\mu}_p) \\ &\cong \prod_{\mathfrak{q}\in Q} \mathrm{Hom}(\mathcal{O}^{\times}_{\mathfrak{q}}, \boldsymbol{\mu}_p) \times \prod_{v\in\Sigma(\mathfrak{r})} \mathrm{Hom}(K^{\times}_v, \boldsymbol{\mu}_p) \end{aligned}$$

is surjective by Lemma 2.3.8. Since the map is surjective, there exists a $\chi \in \mathcal{C}^p(K)$ satisfying

- $\chi_{\mathfrak{r}} = \psi_{\mathfrak{r},e}$,
- $\chi_{\mathfrak{q}}|_{\mathcal{O}^{\times}_{\mathfrak{q}}} = 1_{\mathfrak{q}}$ for $q \in Q$, and
- $\chi_v = 1_v$ for $v \in \Sigma$,

where $\chi_{\mathfrak{r}}, \chi_{\mathfrak{q}}, \chi_v$ are the restrictions of χ to $G_{K_{\mathfrak{r}}}, G_{K_{\mathfrak{q}}}, G_{K_v}$, respectively. Then in particular, $\chi_{\mathfrak{q}}$ is an unramified character if $\mathfrak{q} \in Q$. Note that by Lemma 2.1.14 the local conditions of two Selmer groups $\mathrm{Sel}_\pi(J^\chi/K)$ and $\mathrm{Sel}_\pi(J/K)$ are the same except at $\mathfrak{r}$, namely, $\alpha_{\mathfrak{p}}(\chi_{\mathfrak{p}}) = \alpha_{\mathfrak{p}}(1_p)$ for $\mathfrak{p} \neq \mathfrak{r}$. Therefore, $\mathrm{Sel}_\pi(J^\chi/K) = \mathrm{Sel}_\pi(J, \eta_{\mathfrak{r},e})$, so by Proposition 2.3.11,

$$d_p(\mathrm{Sel}_\pi(J^\chi/K)) = d_p(\mathrm{Sel}_\pi(J/K)) + 1$$

□

Proof of Theorem 1.1.5. Proposition 2.3.2, Proposition 2.3.12, and induction complete the proof □

Chapter 3

Hyperelliptic curves

In this chapter, we keep the notation from the previous chapter except that J denotes the Jacobian of a hyperelliptic curve $C_{2,f}$. Theorem 1.1.8 is proved in section 3.2. Section 3.3 proves Theorem 1.1.10 and Theorem 1.1.4. Section 3.4 exhibits certain examples such that all quadratic twists have even 2-Selmer ranks.

3.1 Canonical quadratic forms

In this section, we give a proof of the fact that the two quadratic forms (defined below) on $J[2]$ and $J^{\chi}[2]$ induced from the Heisenberg groups coincide. This enables us to show a parity relation between two Selmer groups $\mathrm{Sel}_2(J/K)$ and $\mathrm{Sel}_2(J^{\chi}/K)$ (See Theorem 1.1.8).

Let V be a $\mathbf{F}_2$-vector space. Following [6], we define quadratic forms, metabolic spaces, and Lagrangian (maximal isotropic) subspaces.

Definition 3.1.1. A *quadratic form* on V is a function $q : V \to \mathbf{F}_2$ such that

- $q(0) = 0$, and
- the map $(v, w)_q := q(v + w) - q(v) - q(w)$ is a bilinear form.

We say that X is a *Lagrangian subspace* or *maximal isotropic subspace* of V if $q(X) = 0$ and $X = X^{\perp}$ in the induced bilinear form.

A *metabolic space* (V, q) is a vector space V with a quadratic form $(,)_q$ such that $(,)_q$ is nondegenerate and V contains a *Lagrangian subspace.*

Lemma 3.1.2. *Suppose that (V, q) is a metabolic space such that $d_2(V) = 2n$. Then for a given Lagrangian subspace X of V, there are exactly $2^{n(n-1)/2}$ Lagrangian subspaces that intersect X trivially; i.e.,*

$$|\{Y : Y \textit{ is a Lagrangian subspace such that } Y \cap X = \{0\}\}| = 2^{n(n-1)/2}.$$

Proof. This is immediate from Proposition 2.6 (b),(c), and (e) in [17]. □

The most interesting case for our purposes is when $V = H^1(K_v, J[2])$ for local fields K_v. In this case, there is a canonical way to construct a quadratic form $q_{\mathcal{H}}$ using the Heisenberg group defined below (for more general case, see [17, §4]). The associated bilinear form (Definition 3.1.1) given by such a quadratic form is the same as the pairing (2.1) (see [17, Corollary 4.7]). Then $\alpha_{J,v}(1_v)$ is a Lagrangian space by [17, Proposition 4.9], so $(H^1(K_v, J[2]), q_{\mathcal{H}})$ is a metabolic space. We explain the construction of $q_{\mathcal{H}}$ in more detail below. Following [3, Theorem A.8.1.1] we define a Theta (Weil) divisor.

Definition 3.1.3. Let C be a smooth projective curve of genus $g \geq 1$. If $j : C \to J(C)$ is an injection, define a Theta (Weil) divisor (depending on j) $\Theta_{J(C),j}$ by

$$\Theta_{J(C),j} := j(C) + \cdots + j(C) \ (g\text{-1 copies}).$$

Remark 3.1.4. Our main interest is when C is a hyperelliptic curve $C_{2,f}$. In such case, we fix an embedding $j : C_{2,f} \to J$ by sending (x, y) to $[(x, y) - \infty]$. Then the Theta divisor Θ_J satisfies

$$[-1]^*\Theta_J = \Theta_J,$$

since $-[(x, y) - \infty] = [(x, -y) - \infty]$ in $\mathrm{Pic}^0(C_{2,f})(\cong J)$.

Now we define the Heisenberg group for $[2] : J \to J$.

Definition 3.1.5. The Heisenberg group $\mathcal{H}_{J/K,\Theta}$ is defined by

$$\mathcal{H}_{J/K,\Theta_J} := \{(x, g) : x \in J[2], \text{ and } g \in K(J) \text{ such that } \mathrm{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J\}$$

where τ_x is translation by x, and $K(J)$ is the function field of J over K. The group operation is given by $(x, g)(x', g') = (x + x', \tau_{x'}^*(g)g')$.

Remark 3.1.6. By [17, Remark 4.5] and [3, Corollary A.8.2.3], we see that Definition 3.1.5 is a special case of the definition given in the paragraph just before [17, Proposition 4.6]. Let L be a field of characteristic 0, over which J is defined. There is an exact sequence

$$1 \to \overline{L}^{\times} \to \mathcal{H}_{J/L,\Theta_J} \to J[2] \to 0, \tag{3.1}$$

where the middle maps are given by sending t to $(0, t)$, and by projection. Then a quadratic form $\mathfrak{q}_{\mathcal{H}}$ is given by the connecting homomorphism

$$H^1(L, J[2]) \to H^2(L, \overline{L}^{\times}).$$

Note that the construction of $q_{\mathcal{H}}$ is functorial with respect to base extension.

Definition 3.1.7. Let $C_{2,f}$ be a hyperelliptic curve over a local field K_v. Define

$$\mathfrak{q}_{J,v} : H^1(K_v, J[2]) \to H^2(K_v, \overline{K}_v^{\times}) \cong \mathbf{Q}/\mathbf{Z}$$

given by the connecting homomrphism of the exact sequence

$$1 \to \overline{K}_v^{\times} \to \mathcal{H}_{J/K_v,\Theta_J} \to J[2] \to 0.$$

Lemma 3.1.8. *Let $C_{2,f}$ be a hyperelliptic curve over a number field K. Suppose that $x \in H^1(K, J[2])$. Then*

$$\sum_v \mathfrak{q}_{J,v}(\mathrm{res}_v(x)) = 0,$$

where res_v is the restriction map from $H^1(K, J[2])$ to $H^1(K_v, J[2])$.

Proof. We have an exact sequence (see [15, Theorem 8.1.17] for reference)

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Br}(K) \arrow[r] & \bigoplus_v \mathrm{Br}(K_v) \arrow[r, "\oplus \mathrm{inv}_v"] & \mathbf{Q}/\mathbf{Z} \arrow[r] & 0. \end{tikzcd}$$

The lemma follows from the functoriality mentioned in Remark 3.1.6. □

Lemma 3.1.9. *Let $K(J)$ be the function field of J over K. Suppose that $g \in K(J)$ satisfies $\mathrm{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J$ for some $x \in J[2]$. Then $g \circ [-1] = g$.*

Proof. Note that $\mathrm{div}([-1]^*(g)) = [-1]^*(2\tau_x^*(\Theta_J) - 2\Theta_J) = 2\tau_{-x}^*(\Theta_J) - 2\Theta_J = \mathrm{div}(g)$ since $[-1]^*\Theta_J = \Theta_J$. Hence $[-1]^*g = cg$ for some constant c, and c has to be either 1 or -1.

Let η be the generic point which corresponds to the divisor Θ_J. Write $\widehat{\mathcal{O}}_\eta$ for the completion of the local ring $\mathcal{O}_\eta$ (since Θ_J is an irreducible divior, $\mathcal{O}_\eta$ is a discrete valuation ring). Then there is an isomorphism

$$\widehat{\mathcal{O}}_\eta \cong k(\Theta)[[t]],$$

where $k(\Theta)$ is the residue field of $\mathcal{O}_\eta$, and t is a uniformizer. Then $[-1]^* \in \mathrm{Aut}(k(\Theta)[[t]])$ is induced by $[-1]$. Since $[-1]^*$ has order 2, $[-1]^*$ sends t to $(\pm t) + (\text{higher degree terms})$. By assumption, $v_\Theta(g) = -2$, where v_Θ denote the valuation along Θ_J. Hence if one views g as an element in $k(\Theta)((t))$, it is immediate that $[-1]^*g$ and g have the same leading term. Therefore $c = 1$, and this completes the proof. □

Let J' be the Jacobian of another hyperelliptic curve and $\lambda : J \to J'$ be an isomorphism over $\overline{K}_v$. By functoriality, the isomorphism λ induces an isomorphism $\lambda^* : \mathcal{H}_{J'/K_v,\Theta_{J'}} \to \mathcal{H}_{J/K_v,\Theta_J}$. It is easy to check that the map

$$\mathrm{Isom}(J, J') \to \mathrm{Isom}(\mathcal{H}_{J'/K_v,\Theta_{J'}}, \mathcal{H}_{J/K_v,\Theta_J})$$

given by $\lambda \mapsto \lambda^*$ is a G_{K_v}-equivariant homomorphism. Now we show that the induced quadratic forms above are indeed the same for all quadratic twists. The following theorem generalizes [6, Lemma 5.2].

Theorem 3.1.10. *Suppose that $\chi \in \mathcal{C}^2(K_v)$. The canonical isomorphism $J[2] \cong J^\chi[2]$ identifies $\mathfrak{q}_{J,v}$ and $\mathfrak{q}_{J^\chi,v}$ for every place v.*

Proof. Fix an isomorphism $\lambda : J \to J^\chi$ defined over the field $\overline{K}_v^{\mathrm{Ker}(\chi)}$. For every $\sigma \in G_{K_v}$, we have

$$\lambda^\sigma = \lambda \circ [\chi(\sigma)] = \lambda \circ [\pm 1].$$

Hence $(\lambda^*)^\sigma = (\lambda^\sigma)^* = [\pm 1]^* \circ \lambda^*$. For all g such that $\mathrm{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J$ for some $x \in J[2]$, we have $[-1]^*g = g$ by Lemma 3.1.9. Therefore $(\lambda^*)^\sigma = \lambda^*$ for all $\sigma \in G_{K_v}$, whence $\mathfrak{q}_{J,v} = \mathfrak{q}_{J^\chi,v}$ since the following diagram commutes.

$$\begin{tikzcd}
1 \arrow[r] & \overline{K}_v^\times \arrow[r] & \mathcal{H}_{J/K_v,\Theta_J} \arrow[r] & J[2] \arrow[r] & 0 \\
1 \arrow[r] & \overline{K}_v^\times \arrow[r] \arrow[u, equal] & \mathcal{H}_{J^\chi/K_v,\Theta_{J^\chi}} \arrow[r] \arrow[u, "\lambda^*"', "\simeq"] & J^\chi[2] \arrow[r] \arrow[u, "\simeq"] & 0.
\end{tikzcd}$$

□

Proof of Theorem 1.1.8. Combine Theorem 3.1.10 with [6, Theorem 3.9]. □

3.2 2-Selmer ranks of hyperelliptic curves

Let K be a number field and $f \in K[X]$ be a separable polynomial of odd degree (≥ 3) such that $\alpha_1, \alpha_2, \cdots \alpha_n$ are the roots of f. By an appropriate transformation of $C_{2,f}$, we may assume that α_i are algebraic integers. We are mainly interested in the case where $\mathrm{Gal}(f) \cong S_n$ or A_n.

Let Δ_f ($:= \prod_{i<j}(\alpha_i - \alpha_j)^2$) be the discriminant of the polynomial f. Let Σ be a set of primes containing all archimedean places, all primes above 2, and all primes that divide Δ_f (hence $C_{2,f}$, so $J(C_{2,f})$ also, has good reduction at all primes not in Σ). We enlarge Σ so that $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 1$, where $\mathcal{O}_{K,\Sigma}$ is the ring of Σ-integers, and fix it from now on. Note that

$$\sqrt{\Delta_f} \in \mathcal{O}_{K,\Sigma}^\times \text{ if } \mathrm{Gal}(f) = A_n, \text{ and}$$
$$\sqrt{\Delta_f} \notin \mathcal{O}_{K,\Sigma}^\times \text{ if } \mathrm{Gal}(f) = S_n.$$

Lemma 3.2.1. *1. If $\mathfrak{q} \in \mathcal{P}_{J,i}$ for some even i and $\chi_\mathfrak{q} \in \mathcal{C}^2(K_\mathfrak{q})$, then $\chi_\mathfrak{q}(\Delta_f) = 1$.*

2. If $\mathfrak{q} \in \mathcal{P}_{J,i}$ for some odd i and $\chi_\mathfrak{q} \in \mathcal{C}^2(K_\mathfrak{q})$, then $\chi_\mathfrak{q}(\Delta_f) = 1$ if and only if $\chi_\mathfrak{q}$ is unramified.

Proof. It is well-known that $\sqrt{\Delta_f}$ is fixed exactly by even permutations. The condition $\mathfrak{q} \in \mathcal{P}_{J,i}$ is equivalent to $\mathrm{Frob}_\mathfrak{q}|_{K(J[2])} \in S_n$ being a product of $i+1$ disjoint cycles by Lemma 2.1.13. Therefore if i is even, then $\mathrm{Frob}_\mathfrak{q}|_{K(J[2])}$ is an even permutation because n is odd, so $\sqrt{\Delta_f} \in K_\mathfrak{q}$. In other words, $\Delta_f \in (K_\mathfrak{q}^\times)^2$; i.e., $\chi_\mathfrak{q}(\Delta_f) = 1$ for all $\chi_\mathfrak{q} \in \mathcal{C}^2(K_\mathfrak{q})$. This shows (i). If i is odd, then $\mathrm{Frob}_\mathfrak{q}|_{K(J[2])}$ is an odd permutation, so it does not fix $\sqrt{\Delta_f}$. Hence $\Delta_f \notin (K_\mathfrak{q}^\times)^2$. Therefore by the definition of Σ and $\mathcal{P}_{J,i}$(not intersecting Σ), the discriminant Δ_f must generate $\mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^2 \cong \mathbf{Z}/2\mathbf{Z}$, from which (ii) follows. □

Lemma 3.2.2. *Define $\mathcal{A} \subset K^\times/(K^\times)^2$ by*

$$\mathcal{A} := \ker(\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2 \to \prod_{\mathfrak{q}\in\mathcal{P}_{J,0}} \mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^2).$$

Then $\mathcal{A}$ is generated by Δ_f if $\mathrm{Gal}(f) \cong S_n$*, and $\mathcal{A}$ is trivial if* $\mathrm{Gal}(f) \cong A_n$*.*

Proof. If $\mathrm{Gal}(f) \cong S_n$, there is only one intermediate field $K(\sqrt{\Delta_f})$ between K and $K(J[2])$ of degree 2 over K. Hence if $\alpha \in \mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$ is not equal to Δ_f, then $K(\sqrt{\alpha})$ and $K(J[2])$ are linearly disjoint over K. Then by the Chebotarev Density Theorem, there exists a prime $\mathfrak{q}$ and $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K(J[2])K(\sqrt{\alpha})/K)$ such that

- $\mathrm{Frob}_\mathfrak{q}(\sqrt{\alpha}) = -\sqrt{\alpha}$, and
- $\mathrm{Frob}_\mathfrak{q}|_{K(J[2])} \in \mathrm{Gal}(f) = S_n$ is an n-cycle.

By Lemma 2.1.11 and the conditions on $\mathrm{Frob}_\mathfrak{q}$, we have $\mathfrak{q} \in \mathcal{P}_{J,0}$ and $\sqrt{\alpha} \notin \mathcal{O}_\mathfrak{q}^\times$, so $\alpha \notin \mathcal{A}$. Lemma 3.2.1(i) with $i = 0$ shows that $\Delta_f \in \mathcal{A}$. If $\mathrm{Gal}(f) \cong A_n$, the same argument with $\Delta_f \in (\mathcal{O}_{K,\Sigma}^\times)^2$ shows that $\mathcal{A}$ is trivial. □

For a prime $\mathfrak{q}$, we write $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(J/K))$ for the image of $\mathrm{Sel}_2^\mathfrak{q}(J/K)$ of the map

$$\mathrm{res}_\mathfrak{q} : H^1(K, J[2]) \to H^1(K_\mathfrak{q}, J[2]).$$

Lemma 3.2.3. *The* $\mathbf{F}_2$*-vector space* $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(J/K))$ *is a Lagrangian subspace in the metabolic space* $(H^1(K_\mathfrak{q}, J[2]), q_{J,\mathfrak{q}})$*, where* $q_{J,\mathfrak{q}}$ *is the quadratic form arising from the Heisenberg group of* $J[2]$*.*

Proof. By Lemma 2.2.7,

$$d_2(\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(J/K))) = \frac{1}{2}d_2(H^1(K_\mathfrak{q}, J[2])).$$

Then [17, Proposition 4.9], [17, Corollary 4.7] and Lemma 3.1.8 show that $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(J/K))$ is a Lagrangian subspace. □

Let $\mathfrak{q}$ be a place where $\mathfrak{q} \nmid p\infty$ and J has good reduction. Recall that the localization map

$$\mathrm{loc}_\mathfrak{q} : \mathrm{Sel}_2(J/K) \to \alpha_{J,\mathfrak{q}}(1_\mathfrak{q}) \cong J[2]/(\mathrm{Frob}_\mathfrak{q} - 1)J[2]$$

is given by evaluating cocycles at $\mathrm{Frob}_\mathfrak{q}$. The following two Propositions are the main ingredient of Theorem 3.2.7.

Lemma 3.2.4. *Suppose that* $\mathrm{Gal}(f) \cong A_n$ *or* S_n. *For an even number* i, *suppose that* $\mathfrak{r} \in \mathcal{P}_{J,i}$ *and* $\psi_{\mathfrak{r}} \in \mathcal{C}^2(K_{\mathfrak{r}})$. *Then, there is a* $\chi \in \mathcal{C}^2(K)$ *such that*

$$\mathrm{Sel}_2(J^{\chi}/K) = \mathrm{Sel}_2(J, \psi_{\mathfrak{r}}).$$

Proof. Recall that $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0$, so $\mathrm{Pic}(\mathcal{O}_{K,\Sigma(\mathfrak{r})}) = 0$. Thus global class field theory shows that

$$\mathcal{C}^2(K) = \mathrm{Hom}(\mathbf{A}_K^{\times}/K^{\times}, \pm 1) = \mathrm{Hom}((\textstyle\prod_{v \in \Sigma(\mathfrak{r})} K_v^{\times} \times \prod_{\mathfrak{q} \notin \Sigma(\mathfrak{r})} \mathcal{O}_{\mathfrak{q}}^{\times})/\mathcal{O}_{K,\Sigma(\mathfrak{r})}^{\times}, \pm 1).$$

Let

$$\begin{aligned} Q &:= \mathcal{P}_J - \{\mathcal{P}_{J,0} \cup \Sigma(\mathfrak{r})\}, \\ M &:= \mathcal{O}_{K,\Sigma(\mathfrak{r})}^{\times}, \\ G &:= \prod_{\mathfrak{q} \in \mathcal{P}_{J,0}} \mathcal{O}_{\mathfrak{q}}^{\times}, \text{ and} \\ H &:= \prod_{\mathfrak{q} \in Q} \mathcal{O}_{\mathfrak{q}}^{\times} \times \prod_{v \in \Sigma(\mathfrak{r})} K_v^{\times}. \end{aligned}$$

Define a map ϕ

$$\begin{aligned} \phi : \mathcal{C}^2(K) = \mathrm{Hom}((G \times H)/M, \pm 1) \longrightarrow & \mathrm{Hom}(H, \pm 1) \\ & \cong \prod_{\mathfrak{q} \in Q} \mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^{\times}, \pm 1) \times \prod_{v \in \Sigma(\mathfrak{r})} \mathrm{Hom}(K_v^{\times}, \pm 1). \end{aligned}$$

Then by Lemma 3.2.2 and Lemma 2.3.8, ϕ is surjective if $\mathrm{Gal}(f) \cong A_n$, and $\mathrm{Im}(\phi)$ is exactly $\{g \in \mathrm{Hom}(H, \pm 1) : g(\Delta_f) = 1\}$ if $\mathrm{Gal}(f) \cong S_n$. In either case, for all local characters $\psi_{\mathfrak{r}} \in \mathcal{C}^2(K_{\mathfrak{r}})$, there is a global character $\chi \in \mathcal{C}^2(K)$ such that

- $\chi_{\mathfrak{r}} = \psi_{\mathfrak{r}}$,
- $\chi_{\mathfrak{q}}|_{\mathcal{O}_{\mathfrak{q}}^{\times}} = 1_{\mathfrak{q}}$ for $q \in Q$,
- $\chi_v = 1_v$ for $v \in \Sigma$

by Lemma 3.2.1, where $\chi_{\mathfrak{r}}, \chi_{\mathfrak{q}}, \chi_v$ are the restrictions of χ to $G_{K_{\mathfrak{r}}}, G_{K_{\mathfrak{q}}}, G_{K_v}$, respectively. For example, if $\mathrm{Gal}(f) \cong S_n$, the existence of such a χ can be seen by Lemma 3.2.1(i). Then by Lemma 2.1.14, $\alpha_{\mathfrak{p}}(1_{\mathfrak{p}}) = \alpha_{\mathfrak{p}}(\chi_{\mathfrak{p}})$ for all places $\mathfrak{p}$ except $\mathfrak{r}$. □

Proposition 3.2.5. *Suppose that* $\mathrm{Gal}(f) \cong A_n$ *or* S_n *and suppose that* $d_2(\mathrm{Sel}_2(J/K)) \geq 2$. *Then there exist infinitely many* $\chi \in \mathcal{C}^2(K)$ *such that*

$$d_2(\mathrm{Sel}_2(J^\chi/K)) = d_2(\mathrm{Sel}_2(J/K)) - 2.$$

Proof. Decreasing 2-Selmer rank by 2 by twisting when $n = 3$ and $\mathrm{Gal}(f) \cong A_3$ is done in [8, Proposition 5.2]. Thus, assume that $C_{2,f}$ satisfies $(*)$ (Definition 2.2.2). Choose $\mathfrak{r} \in \mathcal{P}_{J,2}$ so that $d_2(\mathrm{Im}(\mathrm{loc}_\mathfrak{r})) = 2$, which is poosible by Lemma 2.2.3 and the Chebotarev Density Theorem. Then $d_2(\mathrm{Sel}_{2,\mathfrak{r}}(J/K)) = d_2(\mathrm{Sel}_2(J/K)) - 2$. By Lemma 2.2.7,

$$d_2(\mathrm{Sel}_2^\mathfrak{r}(J/K)) = d_2(\mathrm{Sel}_{2,\mathfrak{r}}(J/K)) + 2,$$

whence $\mathrm{Sel}_2^\mathfrak{r}(J/K) = \mathrm{Sel}_2(J/K)$. Taking any ramified character $\psi_\mathfrak{r} \in \mathcal{C}^2_{\mathrm{ram}}(K_\mathfrak{r})$, we see that $d_2(\mathrm{Sel}_2(J, \psi_\mathfrak{r})) = d_2(\mathrm{Sel}_2(J/K)) - 2$. The rest follows from Lemma 3.2.4. □

Proposition 3.2.6. *Suppose that* $\mathrm{Gal}(f) \cong A_n$ *or* S_n. *Then there exist infinitely many* $\chi \in \mathcal{C}^2(K)$ *such that*

$$d_2(\mathrm{Sel}_2(J^\chi/K)) = d_2(\mathrm{Sel}_2(J/K)) + 2.$$

Proof. First assume that $C_{2,f}$ satisfies $(*)$. Choose $\mathfrak{r} \in \mathcal{P}_{J,2}$ so that $\mathrm{Im}(\mathrm{loc}_\mathfrak{r}) = 0$ and $\mathrm{Frob}_\mathfrak{r}|_{J(K[2])} \in \mathrm{Gal}(f) \subseteq S_n$ is a product of 3 disjoint cycles of odd lengths. Choosing such an $\mathfrak{r}$ is possible by Lemma 2.2.3 and the Chebotarev Density Theorem. If $n = 3$ and $\mathrm{Gal}(f) \cong A_3$, one can find a sufficiently big field N containing $K(J[2])$ that is Galois over K, and $c(\sigma) = 0$ for $\sigma \in G_N$ and $c \in \mathrm{Sel}_2(J/K)$. Then there are infinitely many primes $\mathfrak{r}(\in \mathcal{P}_{J,2})$ such that $\mathrm{Frob}_\mathfrak{r}|_{\mathrm{Gal}(N/K)} = 1$ by the Chebotarev density theorem.

In either case, we have $\mathrm{Sel}_2(J/K) = \mathrm{Sel}_{2,\mathfrak{r}}(J/K)$. By Lemma 2.2.7 and Lemma 3.2.3.

$$d_2(\mathrm{Sel}_2^\mathfrak{r}(J/K)) = d_2(\mathrm{Sel}_{2,\mathfrak{r}}(J/K)) + 2$$

and $\mathrm{res}_\mathfrak{r}(\mathrm{Sel}_2^\mathfrak{r}(J/K))$ is a Lagrangian subspace (Lemma 3.2.3) of the metabolic space $(H^1(K_\mathfrak{r}, J[2]), q_{J,\mathfrak{r}})$ that intersects $\alpha_{J,\mathfrak{r}}(1_\mathfrak{r})$ trivially. Let $\mathcal{C}^2_{\mathrm{ram}}(K_\mathfrak{r}) = \{\psi_1, \psi_2\}$. Then $\alpha_{J,\mathfrak{r}}(1_\mathfrak{r}) \cap \alpha_{J,\mathfrak{r}}(\psi_1) = \alpha_{J,\mathfrak{r}}(1_\mathfrak{r}) \cap \alpha_{J,\mathfrak{r}}(\psi_2) = \{0\}$ by Lemma 2.1.15, and $\alpha_{J,\mathfrak{r}}(\psi_1) \cap \alpha_{J,\mathfrak{r}}(\psi_2) = \{0\}$ by Lemma 2.3.7. By Lemma 3.1.2, there are exactly 2 Lagrangian subspaces that intersect $\alpha_{J,\mathfrak{r}}(1_\mathfrak{r})$ trivially, so there exists a $\psi_\mathfrak{r} \in \mathcal{C}^2_{\mathrm{ram}}(K_\mathfrak{r})$ such that $\alpha_{J,\mathfrak{r}}(\psi_\mathfrak{r}) = \mathrm{res}_\mathfrak{r}(\mathrm{Sel}_2^\mathfrak{r}(J/K))$. Hence it follows that $d_2(\mathrm{Sel}_2(J, \psi_\mathfrak{r})) = d_2(\mathrm{Sel}_2(J/K)) + 2$. Now Lemma 3.2.4 proves the proposition. □

Finally, Proposition 3.2.5 and Proposition 3.2.6 show the following by induction.

Theorem 3.2.7. *Suppose that $C_{2,f}$ is a hyperelliptic curve over a number field K such that $\mathrm{Gal}(f) \cong A_n$ or S_n. Then for all $r \equiv d_2(\mathrm{Sel}_2(J_{2,f}/K))$ (mod 2), there exist infinitely many quadratic characters $\chi \in \mathcal{C}^2(K)$ such that $d_2(\mathrm{Sel}_2(J^{\chi}_{2,f}/K)) = r$.*

3.3 Parity of 2-Selmer ranks of Jacobians of hyperelliptic curves

We continue to assume that J is the Jacobian of $C_{2,f}$, where $n = \deg(f)$ is odd.

Definition 3.3.1. For every $v \in \Sigma$ and $\chi_v \in \mathcal{C}^2(K_v)$, we define $\omega_v : \mathcal{C}^2(K_v) \to \{\pm 1\}$ by

$$\omega_v(\chi_v) := (-1)^{h_{J,v}(\chi_v)} \chi_v(\Delta_f).$$

Define

$$\delta_{J,v} := \frac{1}{|\mathcal{C}^2(K_v)|} \sum_{\chi \in \mathcal{C}^2(K_v)} \omega_v(\chi) \quad \text{and} \quad \delta_J := (-1)^{d_2(\mathrm{Sel}_2(J/K))} \prod_{v \in \Sigma} \delta_{J,v}.$$

Definition 3.3.2. Define a function $\mathcal{C}^2(K) \to \mathbf{Z}_{>0}$ by

$$\|\chi\| := \max\{\mathbf{N}(\mathfrak{q}) : \chi \text{ is ramified at } \mathfrak{q}\},$$

where $\mathbf{N}(\mathfrak{q})$ is the order of the residue field of $K_{\mathfrak{q}}$. If $X > 0$, let $\mathcal{C}^2(K, X) \subset \mathcal{C}^2(K)$ be the subgroup

$$\mathcal{C}^2(K, X) := \{\chi \in \mathcal{C}^2(K) : \|\chi\| < X\}.$$

The following proposition is in fact the same as [6, Proposition 7.2] in a slightly more general setting (hyperelliptic curves). For $\chi \in \mathcal{C}^2(K)$, let

$$r(\chi) := d_2(\mathrm{Sel}_2(J^{\chi}/K))$$

and χ_v be the restriction of χ to G_{K_v}.

Proposition 3.3.3. *Suppose that $\chi \in \mathcal{C}^2(K)$. Then*

$$r(\chi) \equiv r(1_K) \ (\mathit{mod}\ 2) \Longleftrightarrow \prod_{v \in \Sigma} \omega_v(\chi_v) = 1.$$

Proof. Let θ be a (formal) product of primes not in Σ such that χ is ramified exactly at the primes which divide θ. Then by Lemma 3.2.1,

$$\prod_{\mathfrak{q}\notin\Sigma} \chi_{\mathfrak{q}}(\Delta_f) = (-1)^{|\{\mathfrak{q}:\mathfrak{q}\in\mathcal{P}_{J,i} \text{ for odd } i \text{ and } \mathfrak{q}|\theta\}|}.$$

Note that for $\mathfrak{q}|\theta$, we have $(-1)^{h_{J,\mathfrak{q}}(\chi_{\mathfrak{q}})} = \chi_{\mathfrak{q}}(\Delta_f)$ by Lemma 2.1.15, Lemma 3.2.1, and Remark 2.3.4. Therefore Theorem 1.1.8 and Lemma 2.1.14 show that

$$\begin{aligned} r(\chi) \equiv r(1_K) \pmod 2 &\iff (-1)^{\Sigma_v h_{J,v}(\chi_v)} = 1 \\ &\iff \prod_{v\in\Sigma} \omega_v(\chi_v)\chi_v(\Delta_f) \prod_{v\notin\Sigma} \chi_v(\Delta_f) = 1. \end{aligned}$$

Clearly $\prod_v \chi_v(\Delta_f) = 1$, so this completes the proof. □

The following theorem is remarkable theorem due to Klagsbrun, Mazur, and Rubin ([6, Theorem 7.6]) (for the elliptic curve case).

Theorem 3.3.4. *For all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}^2(K,X) : d_2(\mathrm{Sel}_2(J^\chi/K)) \textit{ is even }\}|}{|\mathcal{C}^2(K,X)|} = \frac{1+\delta_J}{2}.$$

Proof. See the proof of Theorem 7.6 in [6]. Without difficulty, one can see [6, Theorem 7.6] can be extended to the hyperelliptic curve case. □

Proposition 3.3.5. *Suppose that K has a real embedding $K \hookrightarrow K_{v_0}$. Then*

$$\delta_{J,v_0} = \begin{cases} 1 \textit{ if } n \equiv 1 \ (\textit{mod } 4) \\ 0 \textit{ if } n \equiv 3 \ (\textit{mod } 4). \end{cases}$$

Proof. Let η be the sign character in $\mathcal{C}^2(K_{v_0}) = \mathrm{Hom}(K_{v_0}^\times, \pm 1)$ sending negative numbers to -1. Suppose that f has $2k_1 - 1$ real roots and $2k_2$ complex roots so that $2k_1 + 2k_2 - 1 = n$. Let $\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \cdots \beta_{k_2}, \overline{\beta_{k_2}}$ denote the complex roots of f, where $\overline{\beta_i}$ is the complex conjugate of β_i. Then by an appropriate rearrangement of the roots, we get

$$\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 = c\bar{c} \prod_{1\le i\le k_2} (\beta_i - \overline{\beta_i})^2$$

for some c. Hence $\eta(\Delta_f) = (-1)^{k_2}$. By Lemma 2.1.19, we deduce that

$$(-1)^{h_{J,v_0}(\eta)} = (-1)^{k_1-1}.$$

Therefore $\delta_{J,v_0} = 1/2(1+\omega_{v_0}(\eta)) = 1/2(1+(-1)^{k_1+k_2-1})$, so the proposition follows from the equality $2k_1 + 2k_2 - 1 = n$. □

As an easy application, we have

Corollary 3.3.6. *Suppose that $n \equiv 3 \ (mod\ 4)$, and K has a real embedding. Then for all sufficiently large X, we have*

$$|\{\chi \in \mathcal{C}^2(K,X) : r(\chi) \text{ is even } \}| = |\{\chi \in \mathcal{C}^2(K,X) : r(\chi) \text{ is odd } \}| = \frac{|\mathcal{C}^2(K,X)|}{2}.$$

Remark 3.3.7. If $n \equiv 1 \pmod 4$ or if K has no real embedding, we have to know values of $\delta_{J,v}$ other than δ_{J,v_0} to compute an accurate density. In fact, the "disparity constant" δ_J may not be zero. We display such examples in the next section.

Theorem 3.2.7 and Theorem 3.3.4 show the following.

Theorem 3.3.8. *Suppose that $C_{2,f}$ is a hyperelliptic curve defined over a number field K such that $n = \deg(f)$ is odd. Suppose that $\mathrm{Gal}(f) \cong S_n$ or A_n, and the disparity constant δ_J is neither -1 nor 1. Then for every $r \geqq 0$, the Jacobian J of $C_{2,f}$ has infinitely many quadratic twists J^χ such that $d_2(\mathrm{Sel}_2(J^\chi/K)) = r$.*

Proof of Theorem 1.1.4. It is a corollary of Theorem 3.3.8 by Proposition 3.3.5. □

Corollary 3.3.9. *Suppose that $C_{2,f}$ is a hyperelliptic curve defined over a number field K. Let $n = \deg(f)$, and suppose that $n \equiv 3 (mod\ 4)$ and $\mathrm{Gal}(f) \cong S_n$ or A_n. Suppose further that K has a real embedding. Then for every $r \geqq 0$, the Jacobian J of $C_{2,f}$ has infinitely many quadratic twists J^χ such that $d_2(\mathrm{Sel}_2(J^\chi/K)) = r$.*

3.4 Examples

In this section, we show that the condition $n \equiv 3 (\mathrm{mod}\ 4)$ in Theorem 1.1.4 cannot be dropped, by giving counterexamples when $n = 5$. In fact, we give an explicit example of a hyperelliptic curve $C_{2,h}/\mathbf{Q}$ such that $d_2(\mathrm{Sel}_2(J^{\chi}_{2,h}/\mathbf{Q}))$ has constant parity for all quadratic twists $J^{\chi}_{2,h}$. More precisely, the main result of this section is the following.

Proposition 3.4.1. *Suppose that $C_{2,h}$ is a hyperelliptic curve over $\mathbf{Q}$ whose affine model is*

$$y^2 = h(x) := -273(6x+1)(91x^2+54x+9)(100x^2+60x+1)$$

Then $d_2(\mathrm{Sel}_2(J^{\chi}_{2,h}/\mathbf{Q}))$ is even for any quadratic twist $J_{2,h}$.

Let E be an elliptic curve labelled 1440D1 in [1]:

$$y^2 = x^3 - 273x + 1672.$$

Then

$$E[2] = \{\infty, (-19,0), (8,0), (11,0)\}.$$

Define an isomorphism $\psi : E[2] \to E[2]$ by sending $(\alpha_i, 0)$ to $(\beta_i, 0)$, where

$$\alpha_1 = -19, \alpha_2 = 8, \alpha_3 = 11, \beta_1 = 8, \beta_2 = 11, \text{ and } \beta_3 = -19.$$

Clearly, ψ does not come from an isomorphism $E \to E$ since E does not have complex multiplication (the j-invariant of E is not an integer).

Proposition 4 in [4] shows that the Jacobian of the curve defined by $y^2 = h(x)$ where

$$h(x) = -(-810Ax^2 + 81B)(81Ax^2 - 90B)(-90Ax^2 - 810B)$$

is isomorphic to the quotient of $E \times E$ by the graph of ψ. The constant A and B are as in Proposition 4 in [4], and one can see $A = 1990170 = -B$ by simple algebra. Then by a rational transformation of $y^2 = h(x)$ by

$$x = \frac{3x'+1}{x'}, y = \frac{cy'}{x'^3},$$

where $c = 2^2 \times 3^{14} \times 5^2 \times 7 \times 13$, we get

$$y'^2 = -273(6x'+1)(91x'^2+54x'+9)(100x'^2+60x'+1).$$

By abuse of notation, let

$$h(x) := -273(6x+1)(91x^2+54x+9)(100x^2+60x+1).$$

Then the above observation shows that J is isogenous to $E \times E$ over $\mathbf{Q}$.

Definition 3.4.2. Let A be an abelian variety over a number field K. Define

$$\mathrm{Sel}_n(A/K) := \{x \in H^1(K, A[n]) : \mathrm{res}_v(x) \in \mathrm{Im}(i_v) \text{ for all places } v\},$$

where res_v is the restriction map

$$\mathrm{res}_v : H^1(K, A[n]) \to H^1(K_v, A[n])$$

and i_v is the Kummer map $i_v : A(K_v)/nA(K_v) \to H^1(K_v, A[n])$. If p is a prime, we define $\mathrm{Sel}_{p^\infty}(A/K)$ to be the direct limit of the Selmer groups $\mathrm{Sel}_{p^k}(A/K)$.

Lemma 3.4.3. *Suppose that $C_{2,h}$ and E are as above. Then for any $\chi \in \mathcal{C}^2(\mathbf{Q})$,*

$$d_2(\mathrm{Sel}_2(J^{\chi}_{2,h}/\mathbf{Q})) \equiv d_2(J_{2,h}(\mathbf{Q})[2]) \ (mod\ 2)$$

Proof. Since $J_{2,h}$ and $E \times E$ are isogenous over $\mathbf{Q}$, the induced map

$$\mathrm{Sel}_{2^\infty}(J_{2,h}/\mathbf{Q}) \to \mathrm{Sel}_{2^\infty}((E \times E)/\mathbf{Q})$$

has finite kernel and cokernel. Hence

$$\mathrm{corank}_{\mathbf{Z}_2}(J_{2,h}/\mathbf{Q}) = \mathrm{corank}_{\mathbf{Z}_2}((E \times E)/\mathbf{Q}),$$

so $\mathrm{corank}_{\mathbf{Z}_2}(J_{2,h}/\mathbf{Q})$ is even. In a similar way, one can see that $\mathrm{corank}_{\mathbf{Z}_2}(J^{\chi}_{2,h}/\mathbf{Q})$ is even for all quadratic twists $J^{\chi}_{2,h}$. We have the following two exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & J_{2,h}(\mathbf{Q}) \otimes \mathbf{Q}_2/\mathbf{Z}_2 \arrow[r] & \mathrm{Sel}_{2^\infty}(J_{2,h}/\mathbf{Q}) \arrow[r] & \text{Ш}[2^\infty] \arrow[r] & 0, \text{ and} \\
0 \arrow[r] & J_{2,h}(\mathbf{Q})/2J_{2,h}(\mathbf{Q}) \arrow[r] & \mathrm{Sel}_2(J_{2,h}/\mathbf{Q}) \arrow[r] & \text{Ш}[2] \arrow[r] & 0,
\end{tikzcd}$$

where the group Ш is the Shafarevich-Tate group of $J_{2,h}/\mathbf{Q}$. From the above exact sequences, we see that

$$\begin{aligned}
d_2(\mathrm{Sel}_2(J_{2,h}/\mathbf{Q})) &= \mathrm{rk}(J_{2,h}(\mathbf{Q})) + d_2(J_{2,h}(\mathbf{Q})[2]) + d_2(\text{Ш}_{\mathrm{div}}[2]) + d_2(\text{Ш}/\text{Ш}_{\mathrm{div}}[2]) \\
&= \mathrm{corank}_{\mathbf{Z}_2}(J_{2,h}/\mathbf{Q}) + d_2(\text{Ш}/\text{Ш}_{\mathrm{div}}[2]) + d_2(J_{2,h}(\mathbf{Q})[2]) \\
&\equiv d_2(J_{2,h}(\mathbf{Q})[2]) \ (\mathrm{mod}\ 2),
\end{aligned}$$

where the last congruence holds by the following. Note that $C_{2,h}$ has a rational point ∞, so the (K-rational) theta divisor given by $j : C_{2,h} \to J_{2,h}$ sending P to $[P - \infty]$ produces a principal polarization. See Section $A.8.2$ of [3] for more details. Then the congruence follows from the following two general facts.

1. If A is an abelian variety over a number field K that has a principal polarization coming from a K-rational (Weil) divisor, then there is a paring
$$Ш_{A/K} \times Ш_{A/K} \to \mathbf{Q}/\mathbf{Z},$$
that is alternating and nondegenerate after division by maximal divisible subgroup.

2. If there is a finite abelian group B with an alternating non-degenerate pairing
$$B \times B \to \mathbf{Q}/\mathbf{Z},$$
then $d_2(B[2])$ is even.

Similarly, one can see

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^{\chi}_{2,h}/\mathbf{Q})) \equiv \dim_{\mathbf{F}_2}(J^{\chi}_{2,h}(\mathbf{Q})[2]) \pmod 2$$

for all quadratic twists $J^{\chi}_{2,h}$. Then the lemma follows from Remark 1.2.7. □

Proof of Proposition 3.4.1. It is easy to see $d_2(J_{2,h}(\mathbf{Q})[2]) = 2$ by Lemma 2.1.11. Then Lemma 3.4.3 completes the proof. □

We show one more example in the following proposition.

Proposition 3.4.4. *Let $C_{2,g}$ be a hyperelliptic curve given by*

$$y^2 = g(x) = (2x+1)(3x^2+4x+2)(3x^2+2x+1).$$

Then $d_2(\mathrm{Sel}_2(J^{\chi}_{2,g}/\mathbf{Q})$ is even for all $\chi \in \mathcal{C}^2(K)$.

Proof. Let E' be the elliptic curve $y^2 = x^3 - x$. Let

$$\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = 0, \beta_1 = -1, \beta_2 = 0, \text{ and }, \beta_3 = 1.$$

Then one can proceed exactly in the same way as above to get a hyperelliptic curve $C_{2,g'}$ given by $y^2 = g'(x)$ for some $g' \in \mathbf{Q}[X]$, whose Jacobian is isogenous to $E' \times E'$ and is a quadratic twist of $J_{2,g}$. It is easy to see $d_2(J_{2,g}(\mathbf{Q})[2]) = 2$ by Lemma 2.1.11. Then the rest follows as in Lemma 3.4.3. □

Chapter 4

Elliptic curves

Let K be a number field and E be an elliptic curve defined over K. We drop K from the notation $\mathrm{Sel}_2(E/K)$ and write $\mathrm{Sel}_2(E)$ for simplicity. The 2-Selmer rank $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E))$ is denoted by $r_2(E)$ in this chapter.

4.1 Selmer groups and comparing local conditions

Definition 4.1.1. For every place v of K, we let

$$\mathrm{res}_v : H^1(K, E[2]) \to H^1(K_v, E[2])$$

denote the restriction map of group cohomology. Let T be a finite set of places. let

$$\mathrm{res}_T : H^1(K, E[2]) \to \bigoplus_{v \in T} H^1(K_v, E[2])$$

denote the sum of restriction maps.

We define various Selmer groups as follows.

Definition 4.1.2. Let T be a finite set of places of K. Let $S = \{v_1, \cdots, v_k\}$ be a (finite) set of places such that $S \cap T = \varnothing$. Let $\psi_{v_j} \in \mathcal{C}^2(K_{v_j})$. Define

$$\begin{aligned}\mathrm{Sel}_2(E, \psi_{v_1}, \cdots, \psi_{v_k}) := \{x \in H^1(K, E[2]) | \mathrm{res}_v(x) \in \alpha_{E,v}(1_v) \text{ if } v \notin S, \text{ and} \\ \mathrm{res}_{v_j}(x) \in \alpha_{E,v_j}(\psi_{v_j}) \text{ for } 1 \leq j \leq k\}.\end{aligned}$$

Define

$$\mathrm{Sel}_{2,T}(E, \psi_{v_1}, \cdots, \psi_{v_k}) := \{x \in \mathrm{Sel}_2(E, \psi_{v_1}, \cdots, \psi_{v_k}) | \mathrm{res}_T(x) = 0\}.$$

Define

$$\mathrm{Sel}_2^T(E, \psi_{v_1}, \cdots, \psi_{v_k}) := \{x \in H^1(K, E[2]) | \mathrm{res}_v(x) \in \alpha_{E,v(1_v)} \text{ if } v \notin S \cup T, \text{ and } \\ \mathrm{res}_{v_j}(x) \in \alpha_{E,v_j}(\psi_{v_j}) \text{ for } 1 \leq j \leq k\}.$$

For a place $v \notin S$, we simply write $\mathrm{Sel}_{2,v}(E, \psi_{v_1}, \cdots, \psi_{v_k})$, $\mathrm{Sel}_2^v(E, \psi_{v_1}, \cdots, \psi_{v_k})$ for $\mathrm{Sel}_{2,\{v\}}(E, \psi_{v_1}, \cdots, \psi_{v_k})$, $\mathrm{Sel}_2^{\{v\}}(E, \psi_{v_1}, \cdots, \psi_{v_k})$, respectively.

Definition 4.1.3. For convenience, we write $r_2(E^\chi), r_2(E, \psi_{v_1}, \cdots, \psi_{v_n})$ for $d_2(\mathrm{Sel}_2(E^\chi)), d_2(\mathrm{Sel}_2(E, \psi_{v_1}, \cdots, \psi_{v_n}))$, respectively.

The following theorem is due to [6, Theorem 3.9 and Lemma 5.2(ii)].

Theorem 4.1.4 (Kramer, Klagsbrun-Mazur-Rubin)**.** *Let $\chi \in \mathcal{C}^2(K)$. We have*

$$r_2(E) - r_2(E^\chi) \equiv \sum_v h_{E,v}(\chi_v) (mod\ 2),$$

where χ_v is the restriction of χ to G_{K_v} and $h_{E,v}$ is given in Definition 1.2.8. Let $S = \{v_1, \cdots, v_k\}$ be a (finite) set of places. Let $\psi_{v_i} \in \mathcal{C}^2(K_{v_i})$. We have

$$r_2(E, \psi_{v_1}, \cdots, \psi_{v_k}) - r_2(E) \equiv \sum_{i=1}^{k} h_{E,v_i}(\psi_{v_i}) (mod\ 2).$$

From now on, let Σ denote a finite set of places of K containing all primes above 2, all primes where E has bad reduction, and all infinite places. Recall the notation $\mathcal{P}_{E,i}$ and $\mathcal{P}_E$ (Definition 2.3.3). We recall the following Lemma here for the reader's convenience.

Lemma 4.1.5. *For $\mathfrak{q} \in \mathcal{P}_{E,i}$ and $\chi \in \mathcal{C}^2(K_\mathfrak{q})$,*

1. *$d_2(\alpha_{E,\mathfrak{q}}(\chi)) = d_2(E(K_\mathfrak{q})[2]) = i$ and*
2. *if $\chi \in \mathcal{C}^2_{\mathrm{ram}}(K_\mathfrak{q})$, then $\alpha_{E,\mathfrak{q}}(1_\mathfrak{q}) \cap \alpha_{E,\mathfrak{q}}(\chi) = \{0\}$, and $h_{E,\mathfrak{q}}(\chi) = i$.*

Proof. Lemma 2.1.10 and Lemma 2.1.15 prove the assertions. □

Theorem 4.1.6. *Let T be a finite set of places of K. Let $v_1, \cdots, v_k \notin T$ be places and $\psi_{v_j} \in \mathcal{C}^2(K_{v_j})$. The images of right hand restriction maps of the following exact sequences are orthogonal complements with respect to the pairing given by the sum of pairings* (2.1) *of the places $v \in T$*

$$\begin{aligned}
&0 \rightarrow \mathrm{Sel}_2(E, \psi_{v_1}, \cdots, \psi_{v_k}) \rightarrow \mathrm{Sel}_2^T(E, \psi_{v_1}, \cdots, \psi_{v_k}) \rightarrow \textstyle\bigoplus_{v\in T} H^1(K_v, E[2])/\alpha_{E,v}(1_v),\\
&0 \rightarrow \mathrm{Sel}_{2,T}(E, \psi_{v_1}, \cdots, \psi_{v_k}) \rightarrow \mathrm{Sel}_2(E, \psi_{v_1}, \cdots, \psi_{v_k}) \longrightarrow \textstyle\bigoplus_{v\in T} \alpha_{E,v}(1_v).
\end{aligned}$$

In particular,

$$\begin{aligned}
d_2(\mathrm{Sel}_2^T(E, \psi_{v_1}, \cdots, \psi_{v_k})) &- d_2(\mathrm{Sel}_{2,T}(E, \psi_{v_1}, \cdots, \psi_{v_k}))\\
&= \Sigma_{v\in T} d_2(\alpha_{E,v}(1_v)) = \Sigma_{v\in T}\frac{1}{2} d_2(H^1(K_v, E[2])).
\end{aligned}$$

Proof. The lemma follows from the Global Poitou-Tate Duality. For example, see [10, Theorem 2.3.4]. □

Corollary 4.1.7. *Suppose $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_n\}$, where $\mathfrak{q}_i \in \mathcal{P}_E$. Let $\psi_i \in \mathcal{C}^2_{\mathrm{ram}}(K_{\mathfrak{q}_i})$. Let $v_0 \notin T$ be a place and $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$. Suppose that the map $\mathrm{res}_T : \mathrm{Sel}_2(E, \psi_{v_0}) \to \bigoplus_{v\in T} \alpha_{E,v}(1_v)$ is surjective. Then we have*

1. $\mathrm{Sel}_2(E, \psi_{v_0}) = \mathrm{Sel}_2^T(E, \psi_{v_0})$, *and*
2. $\mathrm{Sel}_2(E, \psi_1, \cdots, \psi_n, \psi_{v_0}) = \mathrm{Sel}_{2,T}(E, \psi_{v_0})$.

Proof. The first assertion is clear because the orthogonality in Theorem 4.1.6 shows that the image of

$$\mathrm{res}_T : \mathrm{Sel}_2^T(E, \psi_{v_0}) \to \bigoplus_{v\in T} H^1(K_v, E[2])/\alpha_{E,v}(1_v)$$

is trivial. Lemma 4.1.5 shows that

$$\mathrm{Sel}_2(E, \psi_{v_0}) \cap \mathrm{Sel}_2(E, \psi_1, \cdots, \psi_n, \psi_{v_0}) = \mathrm{Sel}_{2,T}(E, \psi_{v_0}),$$

where the intersection is taken in $H^1(K, E[2])$. Now the second assertion is easy to see. □

Corollary 4.1.8. *Let $\mathfrak{q}$ be a place and let $v_1, \cdots, v_k$ be places of K not equal to $\mathfrak{q}$. Let $\psi_{v_j} \in \mathcal{C}^2(K_{v_j})$. For any $\phi_{\mathfrak{q}}, \eta_{\mathfrak{q}} \in \mathcal{C}^2(K_{\mathfrak{q}})$, we have*

$$|r_2(E, \psi_{v_1}, \cdots, \psi_{v_k}, \phi_{\mathfrak{q}}) - r_2(E, \psi_{v_1}, \cdots, \psi_{v_k}, \eta_{\mathfrak{q}})| \leq d_2(\alpha_{E,\mathfrak{q}}(1_{\mathfrak{q}})).$$

Proof. In Theorem 4.1.6, take $T = \{\mathfrak{q}\}$. Note that $\mathrm{Sel}_2(\psi_{v_1}, \cdots, \psi_{v_k}, \phi_{\mathfrak{q}})$ and $\mathrm{Sel}_2(\psi_{v_1}, \cdots, \psi_{v_k}, \eta_{\mathfrak{q}})$ contains $\mathrm{Sel}_{2,\mathfrak{q}}(\psi_{v_1}, \cdots, \psi_{v_k})$ and are contained in $\mathrm{Sel}_2^{\mathfrak{q}}(\psi_{v_1}, \cdots, \psi_{v_k})$, where the result easily follows from Theorem 4.1.6. □

4.2 Increasing 2-Selmer rank by twisting

Let E be an elliptic curve over a number field K and let Σ be as in previous section.

Lemma 4.2.1. *Let $\mathfrak{q}$ be a prime of K such that $\mathfrak{q} \nmid 2$. Then*

1. *if all the points of $E[4]$ are $K_{\mathfrak{q}}$-rational and χ is a nontrivial quadratic character, then $E^{\chi}(K_{\mathfrak{q}})[4] = E^{\chi}(K_{\mathfrak{q}})[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$;*

2. *if $E(K_{\mathfrak{q}})[4] = E(K_{\mathfrak{q}})[2]$, then the map $E(K_{\mathfrak{q}})[2] \to E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}})$ via the projection is an isomorphism.*

Proof. The first assertion (i) is obvious from the definition of quadratic twists. For (ii), multiplication by 2 is surjective on the pro-(prime to 2) part of $E(K_{\mathfrak{q}})$, so only the pro-2 part $E(K_{\mathfrak{q}})[2^{\infty}]$ contributes to $E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}})$, hence

$$E(K_{\mathfrak{q}})[2] = E(K_{\mathfrak{q}})[2^{\infty}]/2E(K_{\mathfrak{q}})[2^{\infty}] \cong E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}}).$$

□

The following generalizes methods that are used in the proof of Proposition 5.1 in [8].

Theorem 4.2.2. *Let E be an elliptic curve over a number field K. Then there exist infinitely many $\chi \in \mathcal{C}^2(K)$ such that $r_2(E^{\chi}) = r_2(E) + 2$.*

Proof. If $\mathrm{Gal}(K(E[2])/K) \cong S_3$ or A_3, the result follows from 3.2.6. Therefore, from now on, we assume that $\mathrm{Gal}(K(E[2])/K)$ has order 1 or 2, i.e., there exists a non-trivial rational 2-torsion point $P \in E(K)[2]$. Let θ be the formal product of 8, and all places in Σ not dividing 2. In particular, θ is divisible by primes where E has bad reduction. Let $K[\theta]$ be the maximal 2-subextension of $K(\theta)$, where $K(\theta)$ is the ray class field modulo θ.

Let L be a Galois extension containing $K(E[4])K[\theta]$ such that the image of the restriction map

$$\mathrm{Sel}_2(E) \subseteq H^1(K, E[2]) \to H^1(L, E[2]) = \mathrm{Hom}(G_L, E[2])$$

is trivial. Choose a prime (Chebotarev's density theorem) $\mathfrak{q} \notin \Sigma$ so that $\mathfrak{q}$ is unramified in L/K and $\mathrm{Frob}_{\mathfrak{q}}|_L = 1$. Note that the restriction map $H^1(K, E[2]) \to H^1(K_{\mathfrak{q}}, E[2])$ factors through the restriction $H^1(K, E[2]) \to H^1(L, E[2])$ because $\mathfrak{q}$ splits completely in L/K, so $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(E)) = 0$ and

$$\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E).$$

Moreover, there exists an odd integer k such that $\mathfrak{q}^k = (d)$ for some $d \in K^\times$ such that $d \equiv 1 \pmod{\theta}$. Note the following properties of the extension $K(\sqrt{d})/K$:

- $\mathfrak{q}$ is ramified in $K(\sqrt{d})/K$,
- If $v \notin \Sigma$ and $v \neq \mathfrak{q}$, then v is unramified in $K(\sqrt{d})/K$, and
- If $v \in \Sigma$, then v splits in $K(\sqrt{d})/K$.

Let E^d denote the quadratic twist of E by d. Then by Lemma 2.1.14, the local conditions of $\mathrm{Sel}_2(E)$ and $\mathrm{Sel}_2(E^d)$ are the same except at $\mathfrak{q}$, where two local conditions intersect trivially by Lemma 4.1.5. By Corollary 4.1.8 and the fact that $\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E)$, we have $0 \leq r_2(E^d) - r_2(E) \leq 2$. Moreover since $\mathfrak{q} \in \mathcal{P}_{E,2}$, Theorem 4.1.4 and Lemma 4.1.5 prove that

$$r_2(E^d) = r_2(E) \text{ or } r_2(E) + 2. \tag{4.1}$$

By our choice of a prime $\mathfrak{q}$, we have $E[4] \subset E(K_{\mathfrak{q}})$. By Lemma 4.2.1, P has a nonzero local Kummer image for E^d at $\mathfrak{q}$. Therefore $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(E^d)) \neq 0$, where $\mathrm{res}_{\mathfrak{q}} : \mathrm{Sel}_2(E^d) \to H^1(K_{\mathfrak{q}}, E[2])$ is the restriction map. Hence $\mathrm{Sel}(E^d)$ contains $\mathrm{Sel}_2(E)(= \mathrm{Sel}_{2,\mathfrak{q}}(E))$ properly, i.e., $r_2(E^d) \geq r_2(E) + 1$. Therefore by (4.1), we have $r_2(E^d) = r_2(E) + 2$. Since the only constraint on our choice of $\mathfrak{q}$ is $\mathrm{Frob}_{\mathfrak{q}}|_L = 1$ and there are infinitely many such primes (Chebotarev's density theorem), we have infinitely many quadratic twists with the desired property. □

Remark 4.2.3. A similar argument can show the following theorem: Let $C_{2,f}$ be a hyperelliptic curve over a number field K given by an affine model

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

where $n := \deg(f) > 1$ is odd. Let J be the Jacobian of $C_{2,f}$. If K contains a root of f, then for any given natural number r, there exist infinitely many quadratic twists J^χ such that $d_2(\mathrm{Sel}_2(J^\chi/K)) \geq r$.

4.3 Changing the parity of 2-Selmer rank by twisting

Recall that Σ is a finite set of places of K containing all places where E has bad reduction, all primes above 2, and all infinite places. We enlarge Σ, if necessary, so that $\mathrm{Pic}(O_{K,\Sigma}) = 1$, where $O_{K,\Sigma}$ denote the ring of Σ-integers. For the rest of the paper, we put $n := |\Sigma|$. Let Δ_E denote the discriminant of some model of the elliptic curve E.

Lemma 4.3.1. $d_2(O_{K,\Sigma}^\times/(O_{K,\Sigma}^\times)^2) = n$.

Proof. It is well-known that $O_{K,\Sigma}^\times \cong \mathbf{Z}^{n-1} \oplus \mathbf{Z}/m\mathbf{Z}$, where $m = \#\{\text{roots of unity in } K\}$ is divisible by 2 (for example, see [14, Proposition 6.1.1]). □

Lemma 4.3.2. *Let $\mathfrak{q} \notin \Sigma$ (so $\mathfrak{q} \nmid 2$) be a prime of K and suppose $g \in \mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^\times, \{\pm 1\})$ is non-trivial. Then $g(b) = \mathrm{Frob}_{\mathfrak{q}}(\sqrt{b})/\sqrt{b}$ for all $b \in \mathcal{O}_{K,\Sigma}^\times$. In particular, if $\psi \in \mathcal{C}_{\mathrm{ram}}^2(K_{\mathfrak{q}})$, then $\psi(b) = \mathrm{Frob}_{\mathfrak{q}}(\sqrt{b})/\sqrt{b}$ for all $b \in \mathcal{O}_{K,\Sigma}^\times$.*

Proof. We have

$$\mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^\times, \{\pm 1\}) = \mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^\times/(\mathcal{O}_{\mathfrak{q}}^\times)^2, \{\pm 1\}) \cong \mathbf{Z}/2\mathbf{Z}$$

because $\mathcal{O}_{\mathfrak{q}}^\times/(\mathcal{O}_{\mathfrak{q}}^\times)^2 \cong \mathbf{Z}/2\mathbf{Z}$. Note that $b \in (\mathcal{O}_{\mathfrak{q}}^\times)^2$ if and only if $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{b}) = \sqrt{b}$, where the assertion follows. □

.

Lemma 4.3.3. *The image of the restriction map*

$$\begin{aligned}\mathcal{C}^2(K) = \operatorname{Hom}(\mathbf{A}_K^\times/K^\times, \{\pm 1\}) &= \operatorname{Hom}((\textstyle\prod_{\mu\in\Sigma} K_\mu^\times \times \prod_{\nu\notin\Sigma} \mathcal{O}_\nu^\times)/\mathcal{O}_{K,\Sigma}^\times, \{\pm 1\}) \\ &\longrightarrow \textstyle\prod_{\mu\in\Sigma} \operatorname{Hom}(K_\mu^\times, \{\pm 1\}) \times \prod_{\nu\notin\Sigma} \operatorname{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})\end{aligned}$$

is the set of all $(((f_\mu)_{\mu\in\Sigma}), ((g_\nu)_{\nu\notin\Sigma}))$ *such that* $\prod_{\mu\in\Sigma} f_\mu(b) \prod_{\nu\notin\Sigma} g_\nu(b) = 1$ *for all* $b \in \mathcal{O}_{K,\Sigma}^\times$*, where* $f_\mu \in \operatorname{Hom}(K_\mu^\times, \{\pm 1\})$*,* $g_\nu \in \operatorname{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$*, and* g_ν *is trivial for all but finitely many* ν*.*

Proof. Global Class Field Theory and the condition $\operatorname{Pic}(\mathcal{O}_{K,\Sigma}) = 1$ show the equalities. It is clear that the image is as stated. □

Proposition 4.3.4. *Let* $v_0 \in \Sigma$ *and* $\psi_{v_0} \in \mathcal{C}^2(K_v)$*. Suppose that* $\psi_{v_0}(\mathcal{O}_{K,\Sigma}^\times) = 1$*. Then there exists* $\chi \in \mathcal{C}^2(K)$ *such that* $\operatorname{Sel}_2(E^\chi) = \operatorname{Sel}_2(E, \psi_{v_0})$

Proof. Put $f_\mu \in \operatorname{Hom}(K_\mu^\times, \{\pm 1\})$ for $\mu \in \Sigma$ and $g_\nu \in \operatorname{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$ for $\nu \notin \Sigma$ such that

- $f_{v_0} = \psi_{v_0}$,
- $f_v = 1_v$ for $v \in \Sigma\backslash\{v_0\}$, and
- $g_\mathfrak{p}$ is trivial for $\mathfrak{p} \notin \Sigma$.

By Lemma 4.3.3, there exists a character $\chi \in \mathcal{C}^2(K)$ such that for $\mu \in \Sigma$ and $\nu \notin \Sigma$, $\chi_\mu = f_\mu$ and $\chi_\nu|_{\mathcal{O}_\nu^\times} = g_\nu$, where χ_μ, χ_ν are restrictions of χ to $K_\mu^\times, K_\nu^\times$ via the local reciprocity maps, respectively. Now one can see the local conditions for $\operatorname{Sel}_2(E^\chi)$ and $\operatorname{Sel}_2(E, \psi_{v_0})$ are the same everywhere by Lemma 2.1.14. □

Lemma 4.3.5. *Let* v_0 *be a place in* Σ *and let* T *be a (finite) set of primes such that* $T \cap \Sigma = \varnothing$*. Suppose that* $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$*. Then there exist infinitely many primes* $\mathfrak{q} \notin \Sigma \cup T$ *for which there exists a character* $\chi \in \mathcal{C}^2(K)$ *satisfying the following conditions.*

1. $\chi_{v_0} = \psi_{v_0}$*,*
2. $\chi_v = 1_v$ *for* $v \in \Sigma\backslash\{v_0\}$*,*
3. χ_ω *is ramified for* $\omega \in T$*,*

4. *$\chi_{\mathfrak{p}}$ is unramified for $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$,*

5. *$\chi_{\mathfrak{q}}$ is ramified,*

where $\chi_{v_0}, \chi_v, \chi_\omega, \chi_{\mathfrak{p}}, \chi_{\mathfrak{q}}$ are restrictions of χ to $K_{v_0}^\times, K_v^\times, K_\omega^\times, K_{\mathfrak{p}}^\times, K_{\mathfrak{q}}^\times$ via the local reciprocity maps, respectively.

Proof. Let $\beta_1, \cdots, \beta_n$ be a basis of $O_{K,\Sigma}^\times/(O_{K,\Sigma}^\times)^2$. Choose a prime $\mathfrak{q}$ such that

$$\mathrm{Frob}_{\mathfrak{q}}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i) \cdot \prod_{\omega \in T} \mathrm{Frob}_\omega(\sqrt{\beta_i})/\sqrt{\beta_i} \tag{4.2}$$

for all i, where the existence is guaranteed by Chebotarev's density theorem. Put $f_\mu \in \mathrm{Hom}(K_\mu^\times, \{\pm 1\})$ for $\mu \in \Sigma$ and $g_\nu \in \mathrm{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$ for $\nu \notin \Sigma$ such that

- $f_{v_0} = \psi_{v_0}$,
- $f_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- g_ω is not trivial for $\omega \in T$,
- $g_{\mathfrak{p}}$ is trivial for $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $g_{\mathfrak{q}}$ is not trivial.

By Lemma 4.3.2, we have

$$g_{\mathfrak{q}}(\beta_i) = f_{v_0}(\beta_i) \cdot \prod_{v \in \Sigma \backslash \{v_0\}} f_v(\beta_i) \cdot \prod_{\omega \in T} g_\omega(\beta_i) \cdot \prod_{\mathfrak{p} \notin \Sigma \cup \{\mathfrak{q}\} \cup T} g_{\mathfrak{p}}(\beta_i).$$

By Lemma 4.3.3, this means that there exists a character $\chi \in \mathcal{C}^2(K)$ such that for $\mu \in \Sigma$ and $\nu \notin \Sigma$, $\chi_\mu = f_\mu$ and $\chi_\nu|_{\mathcal{O}_\nu^\times} = g_\nu$, where χ_μ, χ_ν are restrictions of χ to $K_\mu^\times, K_\nu^\times$ via the local reciprocity maps, respectively. It is easy to see χ satisfies the desired conditions. For example, for $\omega \in T$, $\chi_\omega|_{\mathcal{O}_\omega^\times} = g_\omega$, and this shows that χ_ω is ramified since $g_\omega(\mathcal{O}_\omega^\times) \neq 1$ by our construction. □

Proposition 4.3.6. *Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$.*

1. *If $\psi_{v_0}(\Delta_E) = -1$ and $\mathrm{Gal}(K(E[2])/K) \cong \mathbf{Z}/2\mathbf{Z}$, there exist infinitely many $\varphi \in \mathcal{C}^2(K)$ such that $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) + 1$.*

2. *If $\psi_{v_0}(\Delta_E) = 1$, there exist infinitely many $\varphi \in \mathcal{C}^2(K)$ such that $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) + 2$.*

3. *Suppose that $\psi_{v_0}(\Delta_E) = 1$ and there exists an element $c \in \mathrm{Sel}_2(E, \psi_{v_0})$. Let $T = \varnothing$ and choose $\mathfrak{q}$ and χ as in Lemma 4.3.5. Suppose that $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$. Then there exist infinitely many $\varphi \in \mathcal{C}^2(K)$ such that $r_2(E^\varphi/K) = r_2(E, \psi_{v_0})$.*

Proof. For (i) and (ii), let $T = \varnothing$ and we begin with choosing $\mathfrak{q}$ and χ as in Lemma 4.3.5. Note that the local conditions for $\mathrm{Sel}_2(E^\chi)$ and $\mathrm{Sel}_2(E, \psi_{v_0})$ are the same everywhere except possibly at $\mathfrak{q}$ by Lemma 2.1.14. Thus Corollary 4.1.8 shows that $|r_2(E^\chi) - r_2(E, \psi_{v_0})| \leq 2$. The conditions in (i) and the product formula imply $\chi_{\mathfrak{q}}(\Delta_E) = \psi_{v_0}(\Delta_E) = -1$, so $\Delta_E \notin (K_{\mathfrak{q}}^\times)^2$, which shows that $E(K_{\mathfrak{q}})[2] \cong \mathbf{Z}/2\mathbf{Z}$. Hence Theorem 4.1.4, Lemma 4.1.5 prove that $r_2(E^\chi)$ is $r_2(E, \psi_{v_0}) - 1$, or $r_2(E, \psi_{v_0}) + 1$. Then (i) follows from Theorem 4.2.2. For (ii), the condition $\psi_{v_0}(\Delta_E) = 1$ and the product formula imply $\chi_{\mathfrak{q}}(\Delta_E) = 1$, so $\Delta_E \in (K_{\mathfrak{q}}^\times)^2$, which shows that $E(K_{\mathfrak{q}})[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$ or $E(K_{\mathfrak{q}})[2] = 0$. Then Theorem 4.1.4, Lemma 4.1.5 show that $r_2(E^\chi)$ is $r_2(E, \psi_{v_0}) - 2$, or $r_2(E, \psi_{v_0})$ or $r_2(E, \psi_{v_0}) + 2$ and the rest follows from Theorem 4.2.2. To see (iii), note that the condition $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$ rules out the possibility for $r_2(E^\chi)$ to be $r_2(E, \psi_{v_0}) + 2$ in the proof of (ii) (for otherwise, $r_2(E^\chi) \geq d_2(\mathrm{Sel}_{2,\mathfrak{q}}(E^\chi)) + 3$ and this would mean $r_2(E^\chi) \geq d_2(\mathrm{Sel}_2^{\mathfrak{q}}(E^\chi)) + 1$, which is absurd). □

Lemma 4.3.7. *Suppose that K has a real place v_0, so $K_{v_0} \cong \mathbf{R}$. Let $\eta \in \mathcal{C}^2(K_{v_0})$ be the sign character. Then*

$$h_{v_0}(\eta) = \begin{cases} 0 & \text{if } d_2(E(K_{v_0})[2]) = 1, \\ 1 & \text{if } d_2(E(K_{v_0})[2]) = 2. \end{cases}$$

Proof. The image $\mathbf{N}(E(\mathbf{C}))$ of the norm map

$$\mathbf{N} : E(\mathbf{C}) \to E(\mathbf{R})$$

is the connected component of the identity of $E(\mathbf{R})$, i.e., $\mathbf{N}(E(\mathbf{C})) \cong \mathbf{R}/\mathbf{Z}$, where the result follows by Lemma 2.1.16. □

Lemma 4.3.8. *Let $M = K(E[2])$. The restriction map*

$$H^1(K, E[2]) \to H^1(M, E[2]) = \mathrm{Hom}(G_M, E[2]) \tag{4.3}$$

is an injection.

Proof. The Inflation-Restriction Sequence shows that the kernel of (4.3) is $H^1(M/K, E[2])$. It is well-known that $H^1(\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}), E[2]) = 1$ ($\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong S_3$). For the other cases, let σ be a generator of the cyclic group $\mathrm{Gal}(M/K)$. One can see $\mathrm{Ker}(\sigma+1) = \mathrm{Im}(\sigma-1)$, so the cohomology group vanishes. □

Theorem 4.3.9. *If K has a real embedding, there exist infinitely many $\chi \in \mathcal{C}^2(K)$ such that $r_2(E^\chi) = r_2(E) + 1$.*

Proof. Let $M = K(E[2])$. We assume $\mathrm{Gal}(M/K)$ has order 1 or 2, since otherwise we already know the result holds by [8, Theorem 1.5] and Theorem 4.2.2. We let v_0 be a real place, so that $K_{v_0} \cong \mathbf{R}$. Let $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$ denote the sign character, i.e., ψ_{v_0} sends negative numbers to -1.

Case 1: $E[2] \subset E(K)$. We have $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Therefore, there exists a point $P \in E(K)[2]$ that is not divisible by 2 in $E(K_{v_0})$. One can see $\mathrm{res}_{v_0}(\overline{P}) \neq 0$, where $\overline{P}$ is the image of P in the map $E(K) \to E(K)/2E(K) \to \mathrm{Sel}_2(E) \subset H^1(K, E[2])$, because the image of P in $E(K_{v_0})/2E(K_{v_0})$ is not trivial. The restriction map $\mathrm{Sel}_2(E)/\mathrm{Sel}_{2,v_0}(E) \to \alpha_{v_0}(1_{v_0})$ is an isomorphism (since $\mathrm{res}_{v_0}(\mathrm{Sel}_2(E)) \neq 0$) and the restriction map $\mathrm{Sel}_2(E, \psi_{v_0})/\mathrm{Sel}_{2,v_0}(E) \to \alpha_{v_0}(\psi_{v_0})$ is an injection. Therefore, Theorem 4.1.4 and Lemma 4.3.7 show that $r_2(E, \psi_{v_0}) = r_2(E) - 1$. Then the result follows from Proposition 4.3.6(ii).

Case 2: $\mathrm{Gal}(M/K) \cong \mathbf{Z}/2\mathbf{Z}$ and $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z}$ (i.e., $\psi_{v_0}(\Delta_E) = -1$). We have $\mathrm{Sel}_2(E) = \mathrm{Sel}_2(E, \psi_{v_0})$ since $\alpha_{v_0}(1_v), \alpha_{v_0}(\psi_{v_0}) \subset H^1(\mathbf{R}, E[2]) = 0$ in this case. The result follows form Proposition 4.3.6(i).

Case 3: $\mathrm{Gal}(M/K) \cong \mathbf{Z}/2\mathbf{Z}$ and $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ ($\Delta_E \notin (K^\times)^2$ and $\psi_{v_0}(\Delta_E) = 1$). Suppose that $\beta_1, \cdots, \beta_{n-1}, \Delta_E$ form a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$. By Corollary 4.1.8, we have $|r_2(E, \psi_{v_0}) - r_2(E)| \leq 1$. Then $r_2(E, \psi_{v_0}) = r_2(E) + 1$ or $r_2(E) - 1$ by Theorem 4.1.4 and Lemma 4.3.7. If $r_2(E, \psi_{v_0}) = r_2(E) - 1$, Proposition 4.3.6(ii) proves the result. Hence for the rest of the proof, we assume $r_2(E, \psi_{v_0}) = r_2(E) + 1$. Choose $c \in \mathrm{Sel}_2(E, \psi_{v_0}) \backslash \mathrm{Sel}_2(E)$. Then $\mathrm{res}_{v_0}(c) \neq 0$. Let $\tilde{c}$ denote the image of c in the map (4.3) in Lemma 4.3.8. Let $L := M(\sqrt{\beta_1}, \cdots, \sqrt{\beta_{n-1}})$ and $N := \overline{M}^{\ker(\tilde{c})}$ (we identify $\overline{K}$ and $\overline{M}$).

(i) First, suppose that $N \not\subset L$. Choose $\mathfrak{q} \in \mathcal{P}_{E,2}$ so that

- $\mathfrak{q}$ is unramified in NL/M
- $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i)$,
- $\mathrm{Frob}_{\mathfrak{q}}|_{\mathrm{Gal}(N/M)} \neq 1$, i.e., $N \not\subset K_{\mathfrak{q}}$.

It is possible because $N \not\subset L$. Note that $\mathfrak{q}$ is chosen as in Lemma 4.3.5 for $T = \varnothing$ (see (4.2)). Then $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$ since $N \not\subset K_{\mathfrak{q}}$. The result follows from Proposition 4.3.6(iii).

(ii) Now we assume that $N \subset L$. By choosing a basis again, we may assume that $\psi_{v_0}(\beta_1) = -1$ and $\psi_{v_0}(\beta_2) = \psi_{v_0}(\beta_3) = \cdots = \psi_{v_0}(\beta_{n-1}) = \psi_{v_0}(\Delta_E) = 1$. Since $\mathrm{res}_{v_0}(c) \neq 0$, we have $N \not\subset M(\sqrt{\beta_2}, \sqrt{\beta_3}, \cdots, \sqrt{\beta_{n-1}})(= L \cap K_{v_0})$. Choose $\mathfrak{q} \in \mathcal{P}_{E,2}$ so that

- $\mathfrak{q}$ is unramified in L/K
- $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i)$.

Clearly, $L \cap K_{\mathfrak{q}} = M(\sqrt{\beta_2}, \cdots, \sqrt{\beta_{n-1}})$. Note that $\mathfrak{q}$ is chosen as in Lemma 4.3.5 for $T = \varnothing$ (see (4.2)). Therefore $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$, since $N \subset K_{\mathfrak{q}}$ would mean $N \subset M(\sqrt{\beta_2}, \cdots, \sqrt{\beta_{n-1}})$, which is a contradiction. Then the theorem follows from Proposition 4.3.6(iii). □

Theorem 4.3.10. *Suppose that E has multiplicative reduction at a prime v_0, where $v_0 \nmid 2$. Then there exist (infinitely many) $\chi \in \mathcal{C}^2(K)$ such that $r_2(E^{\chi}) = r_2(E) + 3$. If moreover, $E(K)[2] \cong \mathbf{Z}/2\mathbf{Z}$ and $v_0(\Delta_E)$ is odd where v_0 denotes the normalized valuation of K_{v_0}, then there exist (infinitely many) $\chi \in \mathcal{C}^2(K)$ such that $r_2(E^{\chi}) = r_2(E) + 1$.*

Proof. If $E(K)[2] = 0$, [8, Theorem 1.5] and Theorem 4.2.2 prove the stronger statement that $A_E = \mathbf{Z}_{\geq 0}$. Suppose that $E(K)[2] \neq 0$. Choose the (non-trivial) quadratic unramified character $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$. By local class field theory, $\psi_{v_0}(\Delta_E) = 1$ if and only if $v_0(\Delta_E)$ is even. By Corollary 4.1.8, we have $|r_2(E) - r_2(E, \psi_{v_0})| \leq 2$. Therefore, [7, Proposition 1 and 2(a)] and Theorem 4.1.4 show that $r_2(E) - r_2(E, \psi_{v_0})$ is either -1 or 1. Let $T = \varnothing$ and choose $\mathfrak{q}$ and χ as in Lemma 4.3.5. If $\psi_{v_0}(\Delta_E) = 1$, [7, Proposition 1 and 2(a)] shows that $h_{v_0}(\psi_{v_0}) = 1$. Then Proposition 4.3.6(ii) and Theorem 4.2.2 prove the first assertion. If $\psi_{v_0}(\Delta_E) = -1$ (so $E(K)[2] \cong \mathbf{Z}/2\mathbf{Z}$), [7, Proposition 1 and 2(a)] shows that $h_{v_0}(\psi_{v_0}) = 0$, so $\mathrm{Sel}_2(E) = \mathrm{Sel}_2(E, \psi_{v_0})$. Therefore the second assertion follows from Proposition 4.3.6(i). □

4.4 An upper bound for t_E

We continue to assume that E is an elliptic curve over a number field K. Recall that t_E is the smallest number in the set $A_E = \{r_2(E^\chi) : \chi \in \mathcal{C}^2(K)\}$. In this section, we study t_E. Let s_2 be the number of complex places of K.

Example 4.4.1 (Klagsbrun [5]). *Let $E_{(m)}$ be the elliptic curve over K defined by the equation*

$$E_{(m)} : y^2 + xy = x^3 - 128m^2x^2 - 48m^2x - 4m^2. \tag{4.4}$$

Suppose that $1 + 256m^2 \notin (K^\times)^2$. Then $E_{(m)}$ has a single point $(-1/4, 1/8)$ of order 2 in $E_{(m)}(K)$. In [5], Klagsbrun shows that $t_{E_{(m)}} \geq s_2 + 1$. Note that in this paper $r_2(E)$ is defined (slightly) differently from that defined in [5] (In [5], the author subtracts the contribution of rational 2-torsion points from $d_2(\mathrm{Sel}_2(E))$ for the "2-Selmer rank"). As his example suggests, t_E can be a lot bigger than the trivial lower bound $d_2(E(K)[2])$.

Remark 4.4.2. If K contains $\sqrt{1 + 256m^2}$, then $E(K)$ contains all 2-torsion points. In this case, we still can prove $t_{E_{(m)}} \geq s_2$ using the argument in [5]. Note that all Lemmas and Propositions in Section 3 in *op. cit.* can be proved by the exactly same methods. However, in the proof of Proposition 4.1 in *op. cit.*, now the map from $\mathrm{Sel}_\phi(E)$ to $\mathrm{Sel}_2(E)$ is injective and $d_2(\mathrm{Sel}_{\hat{\phi}}(E'/K)) \geq 0$, so $r_2(E) \geq \mathrm{ord}_2(\mathcal{T}(E/E'))$ is the correct lower bound we can get from applying the argument of the proof of Proposition 4.1 in *op. cit.*.

For the rest of the paper, we let $|\Sigma| = n$ and $E[2] \subset E(K)$. Note that this means if $v \notin \Sigma$, then $v \in \mathcal{P}_{E,2}$. For a character $\chi \in \mathcal{C}^2(K)$ and a place v, we write $\chi_v \in \mathcal{C}^2(K_v)$ for the restriction of χ to $K_v^\times$ via the local reciprocity map. Let $L = K(\sqrt{\mathcal{O}_{K,\Sigma}^\times})$. Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$. We discuss an upper bound for t_E from now on.

Definition 4.4.3. If $\mathfrak{q} \notin \Sigma$, the composition map

$$\mathrm{Sel}_2(E, \psi_{v_0}) \xrightarrow{\mathrm{res}_\mathfrak{q}} \mathrm{Hom}_{ur}(G_{K_\mathfrak{q}}, E[2]) \cong E[2]$$

is given by sending $c \in \mathrm{Sel}_2(E, \psi_{v_0}) \subset \mathrm{Hom}(G_K, E[2])$ to $c(\mathrm{Frob}_\mathfrak{q})$, where $\mathrm{Frob}_\mathfrak{q}$ is a Frobenius automorphism at $\mathfrak{q}$ (note that $\mathrm{res}_\mathfrak{q}(c) \neq 0$ if and only if $c(\mathrm{Frob}_\mathfrak{q}) \neq 0$).

Lemma 4.4.4. *Suppose that $\phi_1, \cdots, \phi_n$ are homomorphisms from $\mathbf{F}_2^m$ to $\mathbf{F}_2^2$ where $m = n + k$ and $1 \leq k \leq n$ such that $\cap_{i=1}^n \ker(\phi_i) = \{0\}$. Then there exist $i_1, \cdots, i_k$ such that $\phi_{i_1} \times \cdots \times \phi_{i_k} : \mathbf{F}_2^m \to (\mathbf{F}_2^2)^k$ sending $v \in \mathbf{F}_2^m$ to $(\phi_{i_1}(v), \cdots, \phi_{i_k}(v))$ is surjective.*

Proof. Define $s_j = d_2(\mathrm{Im}(\phi_1 \times \cdots \times \phi_j))$. Then clearly $s_j = s_{j-1}$ or $s_j = s_{j-1} + 1$ or $s_j = s_{j-1} + 2$. Then there are at least k many j such that $s_j = s_{j-1} + 2$. Collect all j such that $s_j = s_{j-1} + 2$ and name them $i_1 < \cdots < i_k < \cdots$. Then it is easy to see $\phi_{i_1} \times \cdots \times \phi_{i_k}$ is surjective. □

Proposition 4.4.5. *Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$. Then*

1. $\mathrm{Sel}_2(E, \psi_{v_0}) \subseteq \mathrm{Hom}(\mathrm{Gal}(L/K), E[2])$, *and*

2. $r_2(E, \psi_{v_0}) \leq 2n$.

Proof. Clearly, we have $\mathrm{Sel}_2(E, \psi_{v_0}) \subseteq \mathrm{Hom}(G_K, E[2])$. For all nonzero $s \in \mathrm{Sel}_2(E, \psi_{v_0})$, we claim that $\overline{K}^{\ker(s)} \subseteq L = K(\sqrt{\mathcal{O}_{K,\Sigma}^\times})$. Indeed, for any quadratic extension $K(\sqrt{a})/K$, where all primes not in Σ are unramified, one can replace a with an element in $\mathcal{O}_{K,\Sigma}^\times$ because $\mathrm{Pic}(O_{K,\Sigma}) = 1$. Now the claim follows easily once we note that $\overline{K}^{\ker(s)}$ is a compositum of (possibly the same) quadratic extensions, where all primes not in Σ are unramified. Therefore, (i) follows from the Inflation-Restriction Sequence. By Lemma 4.3.1, $d_2(\mathrm{Gal}(L/K)) = n$, so (ii) is obvious. □

Theorem 4.4.6. *Suppose $E[2] \subset E(K)$. If $r_2(E, \psi_{v_0}) = n + k$ for $2 \leq k \leq n$, then there exist E^χ such that $r_2(E^\chi) = n - k + 2$. In particular $t_E \leq n + 1$.*

Proof. Let $\beta_1, \cdots, \beta_n$ be a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$. Let $L = K(\sqrt{\beta_1}, \cdots, \sqrt{\beta_n})$. Define $\sigma_i \in \mathrm{Gal}(L/K)$ so that $\sigma_i(\sqrt{\beta_i}) = -\sqrt{\beta_i}$ and $\sigma_i(\sqrt{\beta_j}) = \sqrt{\beta_j}$ for $j \neq i$. Note that an element $s \in \mathrm{Sel}_2(E, \psi_{v_0})$ is determined by $s(\sigma_1), \cdots, s(\sigma_n) \in E[2]$ by Proposition 4.4.5(i). Define $t_i \in \mathrm{Hom}(\mathrm{Sel}_2(E, \psi_{v_0}), E[2])$ sending $s \in \mathrm{Sel}_2(E, \psi_{v_0})$ to $s(\sigma_i)$. Applying Lemma 4.4.4, without loss of generality, we may assume $t_1 \times \cdots \times t_k$ is a surjection from $\mathrm{Sel}_2(E, \psi_{v_0})$ to $E[2]^k$. In other words, there exist s_{2i-1}, s_{2i} for $0 \leq i \leq k$ such that

- $s_{2i-1}(\sigma_i) = P_1$ and $s_{2i}(\sigma_i) = P_2$, where $P_1, P_2 \in E[2]$ is a basis of $E[2]$,

- $s_{2i-1}(\sigma_j) = s_{2i}(\sigma_j) = 0$ for $1 \leq j \neq i \leq k$.

For $1 \leq i \leq k$, let $\omega_i \in \mathcal{P}_{E,2}$ be a prime such that $\mathrm{Frob}_{\omega_i} = \sigma_i$ in $\mathrm{Gal}(L/K)$. Then by Definition 4.4.3 we have that

1. $\mathrm{res}_{\omega_i}(s_{2i-1})$ and $\mathrm{res}_{\omega_i}(s_{2i})$ generate $\alpha_{E,\omega_i}(1_{\omega_i}) = \mathrm{Hom}_{\mathrm{ur}}(G_{K_{\omega_i}}, E[2])$, and
2. $\mathrm{res}_{\omega_j}(s_{2i-1}) = \mathrm{res}_{\omega_j}(s_{2i}) = 0$ for $1 \leq j \neq i \leq k$.

Let $T = \{\omega_1, \cdots, \omega_k\}$. Let $\psi_i \in \mathcal{C}^2_{\mathrm{ram}}(K_{\omega_i})$. Then by Corollary 4.1.7 and Theorem 4.1.6, we have $\mathrm{Sel}_2(E, \psi_{v_0}) = \mathrm{Sel}_2^T(E, \psi_{v_0})$ and

$$r_2(E, \psi_1, \cdots, \psi_k, \psi_{v_0}) = r_2(E, \psi_{v_0}) - 2k. \tag{4.5}$$

By Lemma 4.3.5, there exist $\mathfrak{q} \in \mathcal{P}_{E,2} \backslash T$ and $\chi \in \mathcal{C}^2(K)$ so that

- $\chi_{v_0} = \psi_{v_0}$
- $\chi_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- χ_ω is ramified for $\omega \in T$,
- $\chi_\mathfrak{p}$ is unramified for $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $\chi_\mathfrak{q}$ is ramified.

Then $\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \chi_{\omega_1}, \cdots, \chi_{\omega_k}, \psi_{v_0}, \chi_\mathfrak{q})$. Theorem 4.1.4, Lemma 4.1.5, and Corollary 4.1.8 show

$$|r_2(E, \chi_{\omega_1}, \cdots, \chi_{\omega_k}, \psi_{v_0}, \chi_\mathfrak{q}) - r_2(E, \chi_{\omega_1}, \cdots, \chi_{\omega_k}, \psi_{v_0})|$$

is even and less than or equal to 2, so by (4.5), we have $r_2(E^\chi) = r_2(E, \psi_{v_0}) - 2k - 2$ or $r_2(E, \psi_{v_0}) - 2k$ or $r_2(E, \psi_{v_0}) - 2k + 2$. In any case, by Theorem 4.2.2, there exist infinitely many $\varphi \in \mathcal{C}^2(K)$ such that $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) - 2k + 2 = n + k - 2k + 2 < n + 1$. Proposition 4.4.5 with putting $\psi_{v_0} = 1_{v_0}$ shows that $t_E \leq n + 1$. □

Lemma 4.4.7. *Suppose that there exist* $c_1, c_2 \in \mathrm{Sel}_2(E, \psi_{v_0})$ *such that* $\mathrm{res}_\omega(c_1)$ *and* $\mathrm{res}_\omega(c_2)$ *generate* $\alpha_{E,\omega}(1_\omega) = \mathrm{Hom}_{\mathrm{ur}}(G_\omega, E[2])$ *for some prime* $\omega \notin \Sigma$. *Then there exist infinitely many* $\varphi \in \mathcal{C}^2(K)$ *such that* $r_2(E^\varphi/K) = r_2(E, \psi_{v_0})$.

Proof. Let $T = \{\omega\}$. By Lemma 4.3.5, there exist infinitely many $\mathfrak{q} \notin \Sigma \cup T$ for which there exists a character $\chi \in \mathcal{C}^2(K)$ such that

- $\chi_{v_0} = \psi_{v_0}$,
- $\chi_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- χ_ω is ramified,
- $\chi_\mathfrak{p}$ is unramified for all $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $\chi_\mathfrak{q}$ is ramified.

Note that $\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \psi_{v_0}, \chi_\omega, \chi_\mathfrak{q})$ by Lemma 2.1.14. Let $S = \{\omega, \mathfrak{q}\}$. Then $r_2(E, \psi_{v_0}) \geq d_2(\mathrm{Sel}_{2,S}(E^\chi)) + 2$, since by the condition on c_1, c_2, ω the following map is surjective

$$\mathrm{res}_\omega : \mathrm{Sel}_2(E, \psi_{v_0})/\mathrm{Sel}_{2,S}(E^\chi) \to \mathrm{Hom}_{\mathrm{ur}}(G_{K_\omega}, E[2]).$$

Note that $c_1, c_2, c_1 + c_2 \in \mathrm{Sel}_2^S(E^\chi) \backslash \mathrm{Sel}_2(E^\chi)$ since $\alpha_{E,\omega}(1_\omega) \cap \alpha_{E,\omega}(\chi_\omega) = \{0\}$ (Lemma 4.1.5). Therefore $d_2(\mathrm{Sel}_2^S(E^\chi)) \geq r_2(E^\chi) + 2$. Theorem 4.1.6 shows that $d_2(\mathrm{Sel}_2^S(E^\chi)) - d_2(\mathrm{Sel}_{2,S}(E^\chi)) = 4$. Then it follows that $r_2(E, \psi_{v_0}) \geq r_2(E^\chi)$ and $r_2(E, \psi_{v_0}) \equiv r_2(E^\chi) \pmod 2$ by Theorem 4.1.4. Then the assertion follows from Theorem 4.2.2. □

Theorem 4.4.8. *If E does not satisfy the constant 2-Selmer parity condition (Definition 1.1.13), then $t_E \leq n$.*

Proof. If $r_2(E) \equiv n \pmod 2$, the result follows from Theorem 4.4.6. From now on, we assume that $r_2(E) \not\equiv n \pmod 2$. Since E does not satisfy the constant 2-Selmer parity condition, there exist $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}^2(K_{v_0})$ such that $r_2(E, \psi_{v_0}) \equiv n \pmod 2$ by Theorem 4.1.4 (note that since $E[2] \subset E(K)$, all primes outside Σ are in $\mathcal{P}_{E,2}$, so twisting locally at primes not in Σ does not change the parity by Lemma 2.1.14 and Lemma 4.1.5). If $r_2(E, \psi_{v_0}) \leq n-2$ or $r_2(E, \psi_{v_0}) \geq n+2$, then the result follows from Proposition 4.3.6(ii), Theorem 4.4.6, respectively. Let $r_2(E, \psi_{v_0}) = n$. If $\psi_{v_0}(\mathcal{O}_{K,\Sigma}^\times) = 1$, Proposition 4.3.4 shows the result. Now let $\beta_1, \cdots, \beta_n$ be a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$ such that $\psi_{v_0}(\beta_1) = -1$ and $\psi_{v_0}(\beta_2) = \psi_{v_0}(\beta_3) = \cdots = \psi_{v_0}(\beta_n) = 1$.

Define $\sigma_1, \cdots, \sigma_n$ and $t_1, \cdots, t_n$ as in the proof of Theorem 4.4.6. If $d_2(\mathrm{Im}(t_1)) \geq 1$, let $c \in \mathrm{Sel}_2(E, \psi_{v_0})$ and $c(\sigma_1) \neq 0$. Choose $\mathfrak{q}$ ($T = \varnothing$) as in Lemma 4.3.5, i.e., $\mathrm{Frob}_\mathfrak{q} = \sigma_1$ in L/K (see (4.2)). Then $c(\mathrm{Frob}_\mathfrak{q}) = c(\sigma_1) \neq 0$, so Definition 4.4.3 shows $\mathrm{res}_\mathfrak{q}(c) \neq 0$. Then the result follows from Proposition 4.3.6(iii). Therefore for the rest of the proof, assume that $d_2(\mathrm{Im}(t_1)) = 0$. Then without loss of generality, we may assume $d_2(\mathrm{Im}(t_2)) = 2$. Choose $\omega \notin \Sigma$ so that $\mathrm{Frob}_\omega = \sigma_2$ in $\mathrm{Gal}(L/K)$. Then Definition 4.4.3 shows that there exist $c_1, c_2 \in \mathrm{Sel}_2(E, \psi_{v_0})$ such that $\mathrm{res}_\omega(c_1)$ and $\mathrm{res}_\omega(c_2)$ generate $\mathrm{Hom}_{\mathrm{ur}}(G_{K_\omega}, E[2])$. Now Lemma 4.4.7 completes the proof. $\square$

Bibliography

[1] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992.

[2] Tim Dokchitser and Vladimir Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658:39–64, 2011.

[3] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[4] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.

[5] Zev Klagsbrun. Elliptic curves with a lower bound on 2-Selmer ranks of quadratic twists. *Math. Res. Lett.*, 19(5):1137–1143, 2012.

[6] Zev Klagsbrun, Barry Mazur, and Karl Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)*, 178(1):287–320, 2013.

[7] Kenneth Kramer. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.*, 264(1):121–135, 1981.

[8] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[9] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[10] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[11] Barry Mazur and Karl Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Ann. of Math. (2)*, 166(2):579–612, 2007.

[12] William G. McCallum. Tate duality and wild ramification. *Math. Ann.*, 288(4):553–558, 1990.

[13] J. S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1986.

[14] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[15] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[16] Tadao Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)*, 2:63–135, 1969.

[17] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[18] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[19] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.

[20] Jean-Pierre Serre. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.