Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Matematica

2-Selmer groups of twists of elliptic curves over quadratic field extensions

Relatore
Prof. Remke Kloosterman

Laureando
Doniyor Yazdonov
2070795

11 July 2024

Acknowledgements

I would like to express my heartfelt gratitude to my supervisor, Prof. Remke Kloosterman, for their unwavering support, guidance, and valuable insights throughout this project. Their expertise and encouragement have been instrumental in shaping this thesis.

Moreover, I am grateful to Prof. Matteo Longo for supporting me a lot during my master's studies.

I am also deeply thankful to my family members for their love, patience, and understanding during this challenging academic pursuit. Their encouragement and belief in me have been my driving force.

Lastly, I extend my appreciation to all those who contributed to this work, directly or indirectly. Your support has made this achievement possible.

Contents

Introduction

For an elliptic curve over a number field K, written E/K, given by a Weierstrass equation

$$y^2 = x^3 + ax + b, \qquad a, b \in K$$

the quadratic twist of E/K is an elliptic curve over K, written E_d/K, with the Weierstrass equation of the form

$$dy^2 = x^3 + ax + b, \qquad a, b \in K$$

for a squarefree integer d.

The 2-Selmer group of E/K is the subgroup of $H^1(G_{\bar{K}/K}, E[2])$ defined by

$$S^{(2)}(E/K) = \ker(H^1(G_{\bar{K}/K}, E[2]) \longrightarrow \prod_{v \in M_K} \mathrm{WC}(E/K_v))$$

where $\mathrm{WC}(E/K_v)$ is the Weil-Châtelet group for the elliptic curve E over K_v, the completion of K at a valuation v.

Let $E/\mathbb{Q}$ be an elliptic curve with full rational 2-torsion. The aim of the thesis is to study the 2-Selmer groups $S^{(2)}(E_d/K)$ of E_d over a fixed quadratic number field K when d varies over squarefree integers.

The thesis consists of three chapters and two appendices. In the first chapter, we review the basic theory of elliptic curves E/K over a perfect field K and the maps between elliptic curves by following the book The Arithmetic of Elliptic Curves by J. H. Silverman [16].

The next chapter is about the Selmer groups and Selmer structures. In the first section of the chapter, we discuss the $\bar{K}$-isomorphisms of elliptic curves over a number field K. Next, we review the Selmer and Shafarevich-Tate groups and their properties. Lastly, we discuss the Selmer structures and 2-Selmer group groups over quadratic extension, mostly based on K. Kramer's article, Arithmetic of elliptic curves upon quadratic extension [6]. From this chapter, we conclude the importance of two-isogenies, particularly, 2-Selmer groups.

In the last chapter, we give the recently obtained results based on the article of Adam Morgan and Ross Peterson, with the title, On the 2-Selmer groups of twists after quadratic extension [12]. The brief description of the main result is the following: as d

varies over squarefree integers, we discuss the behavior of the quadratic twists E_d over some fixed quadratic number field. We show that for 100% twists the dimension of the 2-Selmer group over K is given by a formula. Consequently, using the results from the work of P. Shiu, A Brun-Titchmarsh theorem for multiplicative functions [15], we prove that for 100% of twists E_d, the action of $\mathrm{Gal}(K/\mathbb{Q})$ on 2-Selmer group of E_d over K is trivial. At the end, we construct an example of families of quadratic twists in which a positive proportion of 2-Selmer groups over K have non-trivial $\mathrm{Gal}(K/\mathbb{Q})$-action, which shows that previous results are just statistical phenomena.

As a prerequisite, we present two appendices at the end of the thesis. In appendix A, we discuss the main properties of group cohomology which we use throughout the thesis.

Lastly, in appendix B, we discuss the theory of valuations and completions, and the places of a number field mainly following the book Cohomology of number fields by A. Schmidt J. Neukirch and K. Wingberg [5, Chapter 2].

Chapter 1

Elliptic Curves

1.1 Definition of an elliptic curve

In this section, we discuss the basic theory of elliptic curves, particularly we impose an abelian group structure on elliptic curves. Let K be a perfect field and $\bar{K}$ be an algebraic closure of K.

Definition 1.1.1. *An elliptic curve over K is defined by a smooth projective curve E of genus 1 together with a point $O \in E(K)$, and written E/K.*

Let us now define a certain form of homogeneous equations such that every elliptic curve can be written as that form due to the Riemann-Roch theorem.

Definition 1.1.2. *The curve given by the equation of the form*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

is called Weierstrass equation, where $a_1, ..., a_6 \in K$. Furthermore, define O to be the point $[0, 1, 0]$.

We usually write the Weiestrass equation by nonhomogeneous coordinates $x = X/Z$ and $y = Y/Z$, and we will have

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

If the characteristic of $\bar{K}$ is different from 2 and 3, then the curve can be described as a plane algebraic curve which consists of solutions (x, y) for:

$$y^2 = x^3 + ax + b$$

for some $a, b \in K$.
The first fundamental result of Section 1.1 is the following.

Proposition 1.1.3. *Let E be an elliptic curve over K. Then there exists a morphism*

$$\phi : E \to \mathbb{P}^2,$$

that gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

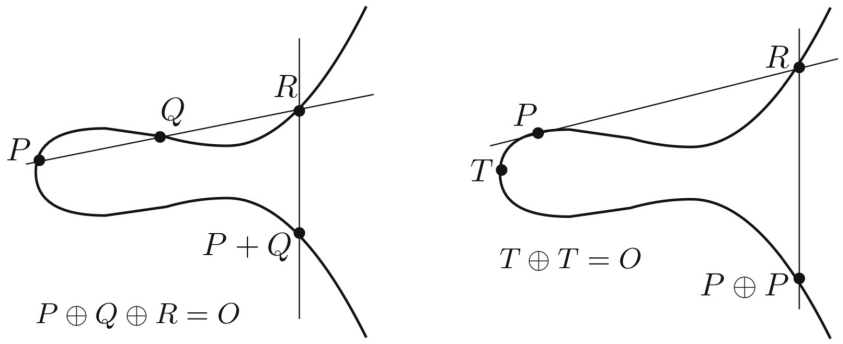
where $a_1, ..., a_6 \in K$ and $\phi(O) = [0, 1, 0]$. Conversely, every smooth cubic curve C given by a Weierstrass equation above is an elliptic curve over K with $O = [0, 1, 0]$.

Proof. See [16, p.59]. □

Due to this significant result, we can always think of an elliptic curve as a smooth cubic curve given by a Weierstrass equation with a base point $O = [0, 1, 0]$.

Let E/K be an elliptic curve given by a Weierstrass equation. Thus we have that E/K describes the points in $\bar{K}^2$ satisfies the Weierstrass equation together with the point $O = [0, 1, 0]$ at infinity. We now impose a group structure on E/K giving a group operation as follows:

Let $P, Q \in E/K$ and l be the line passing through P and Q (in the case of $P = Q$, let l be the tangent to E/K at P), let R be the intersection of l and E/K (such a point always exist and unique due to the Bézout's theorem, see [4, p.54]), and let l' be the line through R and O. Then again, l' intersects E/K at R, O and a third point. Let us define $P \oplus Q$ (or just $P + Q$) to be the third point.



Proposition 1.1.4. *Let E/K be an elliptic curve given by a Weierstrass equation. The binary operation defined above imposes an abelian group structure on $E(\bar{K})$ with identity element $O = [0, 1, 0]$. Moreover,*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of $E(\bar{K})$.

Proof. See [16, p.52]. □

Let $m \in \mathbb{Z}$ and $P, Q \in E/K$. We write if $P + Q = O$, then $Q := -P$ and also

$$[m]P = \underbrace{P + P + ... + P}_{m \text{ times if } m \geq 1}, \qquad [m]P = \underbrace{-P - P - ... - P}_{|m| \text{ times if } m \leq -1}, \qquad [0]P = O.$$

The second fundamental result of the Section 1.1 is the following which states that the addition law on an elliptic curve defined above is a morphism.

Theorem 1.1.5. *Let E/K be an elliptic curve. Then the binary operations*

$$\begin{aligned} \pm : E \times E &\longrightarrow E \\ (P_1, P_2) &\longmapsto P_1 \pm P_2 \end{aligned}$$

defined above define morphisms.

Proof. [16, p.64]. □

1.2 Isogenies

In this section, we review the basic properties of maps between elliptic curves.

Definition 1.2.1. *Let $E_1/K, E_2/K$ be two elliptic curves. An isogeny from E_1/K to E_2/K is a morphism*

$$\phi : E_1 \longrightarrow E_2$$

such that $\phi(O) = O$. Two elliptic curves $E_1/K, E_2/K$ are called isogenous if there is an isogeny from E_1 to E_2 and $\phi(E_1) \neq \{O\}$.

From the following theorem, we can deduce that an isogeny satisfies either

$$\phi(E_1) = \{O\} \text{ or } \phi(E_1) = E_2.$$

Theorem 1.2.2. *Let $\phi : C_1 \to C_2$ be a morphism between curves (projective varieties of dimension one). Then ϕ is either constant or surjective.*

Proof. See, for example [4, II.6.8] or [14, 1.5, Theorem 4]. □

Let $E_1/K, E_2/K$ be two elliptic curves. We denote the set of isogenies from E_1 to E_2 by

$$\mathrm{Hom}_K(E_1, E_2) := \{\text{isogenies } E_1 \to E_2\}.$$

If we impose an addition law to it as

$$(\phi + \psi)(P) = \phi(P) + \psi(P),$$

then $\mathrm{Hom}(E_1, E_2)$ becomes an abelian group with respect to this addition law, because by Theorem 1.1.5 $\psi + \phi$ is a morphism and $(\phi + \psi)(O) = \phi(O) + \psi(O) = O$, thus it is an isogeny.

In the case of $E_1 = E_2 = E$, we can compose isogenies that make $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$ a ring (called the *endomorphism ring of* E) whose addition law is $+$ defined above and multiplication is just composition.

Example 1.2.3. For any $m \in \mathbb{Z}$ we define the multiplication-by-m isogeny

$$[m] : E \longrightarrow E$$

in the following way; if $m \geq 1$, then

$$[m](P) := [m]P = \underbrace{P + P + \ldots + P}_{m \text{ times}}$$

For $m \leq -1$, we put $[m](P) := [-m](-P)$, and finally for the case $m = 0$ we put $[0](P) = O$.

Using the induction and Theorem 1.1.5 we can easily show that $[m]$ is a morphsim and since $[m](O) = O$ for any integer m, we can deduce that $[m]$ is an isogeny.

Definition 1.2.4. *Let E/K be an elliptic curve and let $m \in \mathbb{N}$. Then m-torsion subgroup of E/K, written $E(\bar{K})[m]$ or $E[m]$, is the set points of E/K of order m,*

$$E[m] = \{P \in E : [m]P = O\}.$$

And torsion subgroup of E/K, written $E(\bar{K})_{tors}$ or E_{tors} , is the set of points of finite order,

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

Here we give another example of an isogeny using so-called *translation map*.

Example 1.2.5. Let E/K be an elliptic curve and $Q \in E$. We define a map called translation-by-Q map

$$\tau_Q : E \longrightarrow E, \qquad P \longmapsto P + Q$$

Here the map τ_Q is an isomorphism with inverse map τ_{-Q}. Note this τ_Q is not an isogeny except the case $Q = O$. Now for any morphism

$$F : E_1 \longrightarrow E$$

of elliptic curves, the composition

$$\phi := \tau_{-F(O)} \circ F$$

is an isogeny, because we have that $\phi(O) = \tau_{-F(O)}(F(O)) = F(O) - F(O) = O$.

We know that an elliptic curve is an abelian group and an isogeny is a map between elliptic curves sanding O to O. The following theorem states that, in fact, any isogeny is a group homomorphsim.

Theorem 1.2.6. *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. Then ϕ is a group homomorphism, namely*

$$\phi(P + Q) = \phi(P) + \phi(Q) \qquad \textit{for all} \quad P, Q \in E.$$

Proof. See [16, p.71]. □

Corollary 1.2.7. *Let $\phi : E_1 \longrightarrow E_2$ be a nonzero isogeny. Then*

$$ker(\phi) = \phi^{-1}(O)$$

is a finite subgroup.

Proof. That is clearly a subgroup of E_1/K since ϕ is a group homomorphism by Theorem 1.2.6. From [16, Proposition 2.6] $\ker(\phi)$ is finite. □

Let $E_1/K, E_2/K$ be two elliptic curves and let $\phi : E_1 \longrightarrow E_2$ be a nonconstant isogeny. Then we induce an injective map of function fields as follows:

$$\phi^* : K(E_2) \longrightarrow K(E_1), \qquad \phi^* f = f \circ \phi.$$

Using that we define the *degree* of an isogeny and then define specific isogenies so-called the *dual isogenies* to show our fundamental result of Section 1.2.

Because of [16, Theorem 2.4] we have that $K(E_1)$ is a finite extension of $\phi^*(K(E_2))$ which validates our following definition.

Definition 1.2.8. *Let $\phi : E_1/K \longrightarrow E_2/K$ be an isogeny. Then if ϕ is constant, we define the degree of ϕ to be 0, otherwise its degree to be*

$$deg(\phi) = [K(E_1) : \phi^*(K(E_2))]$$

Theorem 1.2.9. *Let $\phi : E_1/K \longrightarrow E_2/K$ be an isogeny of degree m. Then there exists a unique isogeny (called dual isogeny to ϕ)*

$$\hat{\phi} : E_2 \longrightarrow E_1 \qquad \text{such that} \qquad \hat{\phi} \circ \phi = [m].$$

Proof. For the uniqueness, suppose that $\hat{\phi}, \hat{\phi}'$ be two isogenies such that $\hat{\phi}, \hat{\phi}' : E_2 \longrightarrow E_1$ and $\hat{\phi} \circ \phi = \hat{\phi}' \circ \phi = [m]$. Then

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0].$$

From Theorem 1.2.2 and since ϕ is nonconstant we have that $\hat{\phi} - \hat{\phi}'$ is a constant (note that $\hat{\phi}'(\phi(O)) = \hat{\phi}(\phi(O)) = [m](O) = O$, implies that $\hat{\phi} - \hat{\phi}' = O$), thus $\hat{\phi} = \hat{\phi}'$. For the proof of existence, see [16, p.81]. □

We now give the properties of the dual isogeny which leads us to another very useful description of $E[m]$.

Theorem 1.2.10. *Let $\phi : E_1/K \longrightarrow E_2/K$ be an isogeny and $m \in \mathbb{Z}$.*
(a) Let $deg(\phi) = m$. Then we have

$$\phi \circ \hat{\phi} = [m] \quad \text{on} \quad E_2.$$

(b) Let $\lambda : E_2/K \longrightarrow E_3/K$ be another isogeny. Then we have

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(c) Let $\psi : E_1/K \longrightarrow E_2/K$ be another isogeny. Then we have

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

(d) Far all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \qquad \text{and} \qquad deg[m] = m^2.$$

(e) $deg(\hat{\phi}) = deg(\phi)$.
(f) $\hat{\hat{\phi}} = \phi$.

Proof. The case when ϕ is constant is trivial, therefore here we prove the theorem (except (c), for the (c) see [16, p.83]) for the nonconstant case.
(a) Consider

$$((\phi \circ \hat{\phi} - [m]) \circ \phi = \phi \circ [m] - [m] \circ \phi = O$$

That is because for all $P \in E_1/K$ we have that $\phi([m]P) - [m](\phi(P)) = [m]\phi(P) - [m]\phi(P) = O$ (remember that ϕ was a group homomorphism). So since ϕ is not constant, Theorem 1.2.2 implies that $\phi \circ \hat{\phi} = [m]$.
(b) Let $n = \deg(\lambda)$, then we have that

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [mn].$$

Then by the uniqueness statement of Theorem 1.2.9 we get

$$\hat{\phi} \circ \hat{\lambda} = \widehat{\lambda \circ \phi}.$$

(d) For $m = 0$ it is true by definition and the case $m = 1$ is trivial. Using (c) by putting $\phi = [m]$ and $\psi = [1]$ yields

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]},$$

By induction on m we get that $\widehat{[m]} = [m]$ for all $m \in \mathbb{Z}$. Now let $d = \deg([m])$. Then by the definition of dual isogeny, we get

$$[d] = \widehat{[m]} \circ [m] = [m^2]$$

[16, Proposition 4.2] tells us that $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module, using this we get that $d = m^2$.
(e) Let $m = \deg[m]$. Then using (a) and (d), we get

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = \deg(\phi)\deg(\hat{\phi}) = m\deg(\hat{\phi}) \implies m = \deg(\hat{\phi}).$$

(f) Using (a),(b) and (d) we get

$$\phi \circ \hat{\phi} = [m] = \widehat{[m]} = \widehat{\phi \circ \hat{\phi}} = \hat{\hat{\phi}} \circ \hat{\phi}$$

Then again by the Theorem 1.2.2 we get $\phi = \hat{\hat{\phi}}$. □

Finally, here we give a good description of $E[m]$ as a result which we will use later.

Corollary 1.2.11. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}/\{0\}$*
(a) If $m \neq 0$ in K, which is either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ and $p \nmid m$, then

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) If $\mathrm{char}(K) = p \neq 0$, then one of the following holds.

1. *$E[p^n] = \{O\}$ for all $n \in \mathbb{N}$.*
2. *$E[p^n] = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ for all $n \in \mathbb{N}$.*

Proof. See [16, Corollary 6.4]. □

1.3 Reduction of an elliptic curve

In this section, we work on elliptic curves over a complete field K with respect to a discrete valuation v, with the finite residue field k. Let $O_v = \{x \in K : v(x) \geq 0\}$ be the ring of integers of K with respect to v. For more details of completions and valuations, see Appendix B. Let E/K be an elliptic curve with a Weierstrass equation

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

After the substitution $(x, y) \to (u^{-2}x, u^{-3}y)$ we get

$$E/K : y^2 + ua_1xy + u^3a_3y = x^3 + u^2a_2x^2 + u^4a_4x + u^6a_6,$$

By choosing u properly we obtain a Weierstrass equation with all coefficients in O_v. Consequently, the discriminant Δ of the Weierstrass equation satisfies $v(\Delta) \geq 0$ (For more information about the discriminant, see [16, p.42]). Now we are ready to define the minimal Weierstrass equation.

Definition 1.3.1. *Let E/K be an elliptic curve. A Weierstrass equation for E/K with coefficients in O_K is called the minimal Weierstrass equation at v if $v(\Delta)$ is minimal.*

Proposition 1.3.2. *Every elliptic curve E/K has a minimal Weierstrass equation.*

Proof. Existness just follows from the fact that v is the discrete valued map, more precisely v maps surjectively from K to $\mathbb{Z} \cup \{\infty\}$. □

Let π be uniformizer of O_v i.e. $v(\pi) = 1$ and let $k = O_v/\pi O_v$ be the residue field.

Definition 1.3.3. *Let E/K be an elliptic curve given by a minimal Weierstrass equation (1.1). Then the curve given by the equation*

$$\tilde{E}/k : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6. \tag{1.2}$$

with $\tilde{a}_i$ the image of a_i in k is called the reduction of E/K modulo π.

Here the curve $\tilde{E}/k$ might be singular or nonsingular which leads us to the following definition.

Definition 1.3.4. *Let E/K be an elliptic curve, and let $\tilde{E}/k$ be the reduction modulo π of a minimal Weierstrass equation for E/K.*
(a) E/K has good reduction if $\tilde{E}/k$ is smooth.
(b) E/K has multiplicative reduction if $\tilde{E}/k$ has a node.
(c) E/K has additive reduction if $\tilde{E}/k$ has a cusp.
In both cases (b) and (c) we say E/K has bad reduction.

In fact, these are the only possibilities for the Weierstrass equations, (see [16, Section 3.1] for details).

Example 1.3.5. Let $p \geq 5$ be a prime number. Then the elliptic curve

$$E_1/\mathbb{Q}_p : y^2 = x^3 + p^2x^2 + 1$$

has good reduction, however,

$$E_2/\mathbb{Q}_p : y^2 = x^3 + x^2 + p^2$$

has multiplicative reduction and

$$E_3/\mathbb{Q}_p : y^2 = x^3 + p$$

has additive reduction over $\mathbb{Q}_p$.

Our main interest is in the case of an elliptic curve over $\mathbb{Q}$ (we can think of $\mathbb{Q}$ as a subfield of its completion with respect to a discrete valuation). In this case, we conclude the following result which we will use in later chapters.

Since the characteristic of $\mathbb{Q}$ is 0, an elliptic curve over $\mathbb{Q}$ has a Weierstrass equation of the form

$$y^2 = x^3 + ax + b$$

with coefficients in $\mathbb{Z}$ and the discriminant $\Delta = -16(4a^3 + 27b^2)$. Let p be a prime number. The reduction modulo p induces the curve over $\mathbb{F}_p$ given by

$$y^2 = x^3 + \tilde{a}x + \tilde{b}$$

The curve given by a Weierstrass equation is singular if and only if its discriminant is equal to 0 (see, [16, Propostion 1.4]). From that, we can deduce that if $E/\mathbb{Q}$ has bad reduction at p, then $p \mid \Delta$, because if $E/\mathbb{Q}$ has bad reduction then by definition its reduction curve is singular, which is equivalent to say $4\tilde{a}^3 + 27\tilde{b}^2{=}0$ in $\mathbb{F}_p$ implies that p divides the discriminant of $y^2 = x^3 + ax + b$.

1.4 The Weil pairing

In this section, we first give the theory of divisors and then define the Weil pairing which we will use in later chapters. Let us begin by defining the divisors of an elliptic curve over a perfect field K.

Definition 1.4.1. *Let E/K be an elliptic curve. The divisor group of E/K is the free abelian group generated by the points of E/K and written $Div(E)$. Then a divisor D is a formal sum*

$$D = \sum_{P \in E} n_P(P)$$

where $n_P \in \mathbb{Z}$ and $n_P \neq 0$ for finitely many $P \in E$. The degree of D is defined by

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

The divisors of degree 0, denoted by $\mathrm{Div}^0(E)$, form a subgroup of $\mathrm{Div}(E)$.

Let $P \in E/K$ be a point and $\bar{K}[E]_P$ be the local ring of E/K at P and M_P be its maximal ideal. Then we have that $\bar{K}[E]_P$ is a discrete valuation ring which allows us to give the following definition (for the proof, see [16, Proposition 1.1]).

Definition 1.4.2. *Let E/K be an elliptic curve with a point $P \in E/K$. Then the valuation on $\bar{K}[E]_P$ is given by*

$$ord_P : \bar{K}[E]_P \longrightarrow \{0, 1, 2, ...\} \cup \{\infty\} \qquad ord_P(f) = sup\{n \in \mathbb{Z} : f \in M_P^n\}.$$

We can extend ord_P to $\bar{K}(E)$ by using $\mathrm{ord}_P(f/g) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.
Let $f \in \bar{K}(E)^*$. Then for f we define the divisor, written $\mathrm{div}(f)$, as follows

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P).$$

This is a divisor by [16, Proposition 1.2]. We now define an equivalent relation on $\mathrm{Div}(E)$ as follows: Two divisors D_1, D_2 are *linearly equivalent*, written $D_1 \sim D_2$, if there exists $f \in \bar{K}(E)^*$ such that $D_1 - D_2 = \mathrm{div}(f)$. The set of principal divisors form a subgroup of $\mathrm{Div}(E)$ and we write the quotient of $\mathrm{Div}(E)$ by that subgroup as $\mathrm{Pic}(E)$. Finally, we write the quotient of $\mathrm{Div}^0(E)$ by the subgroup of principal divisors as $\mathrm{Pic}^0(E)$.

Here we give some basic properties of divisors.

Proposition 1.4.3. *Let E/K be an elliptic curve and let $f \in \bar{K}(E)^*$.*
(a) $deg(div(f)) = 0$, namely $div(f) \in Div^0(E)$.
(b) For every $D \in Div^0(E)$ of degree 0 there exists a unique point $P \in E$ such that

$$D \sim (P) - (O).$$

Define

$$\sigma : Div^0(E) \longrightarrow E$$

to be the map that send D to its associated point P.
(c) The map σ is surjective.
(d) Let $D_1, D_2 \in Div^0(E)$. Then

$$\sigma(D_1) = \sigma(D_2) \iff D_1 \sim D_2.$$

Consequently, σ induces a bijection map of sets which we denote by the same σ.

$$\sigma : Pic^0(E) \longrightarrow E.$$

(e) The geometric group law on E/K constructed in (1.1) and the algebraic group law induced from $Pic^0(E)$ using σ are the same.

Proof. For (a), see [4, II.6.10] and for the rest of the theorem, see [16, Proposition 3.4]. □

Corollary 1.4.4. *Let E/K be an elliptic curve and let $D = \sum_{P \in E} n_P(P)$ be a divisor of degree 0. Then D is a principal if and only if*

$$\sum_{P\in E}[n_P]P = O.$$

holds in E.

Proof. From the Proposition 1.4.3 we conclude that

$$D \sim 0 \Longleftrightarrow \sigma(D) = 0 \Longleftrightarrow \sum_{P\in E}[n_P]\sigma((P)-(O)) = \sum_{P\in E}[n_P]P = O.$$

□

Now we are ready to define the Weil pairing. Let $m \geq 2$ be an integer and $p = \mathrm{char}(K)$. If $p \neq 0$ then we assume that $(p, m) = 1$. Let $T \in E[m]$. Then from the Corollary 1.4.4 there is a function $f \in \bar{K}(E)$ with the equality

$$\mathrm{div}(f) = m(T) - m(O).$$

and there is another function $g \in \bar{K}(E)$ with the equality (see, [16, p.93])

$$f \circ [m] = g^m.$$

Let $S \in E[m]$, then for any point $X \in E$, we have that

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

From the above equality we get that for all X, $g(X+S)/g(X)$ is a m^{th} root of unity. Specifically, we get the morphism

$$E \longrightarrow \mathbb{P}^1 \qquad X \longmapsto [g(X+S)/g(X), 1].$$

which is not surjective, Theorem 1.2.2 implies that it is constant.

Definition 1.4.5. *Let μ_m be the group of m^{th} roots of unity. The Weil e_m-pairing is a pairing*

$$e_m : E[m] \times E[m] \longrightarrow \mu_m \qquad \textit{by putting} \qquad e_m(S,T) = g(X+S)/g(X).$$

Note that in the definition, point X is chosen such that both functions $g(X+S)$ and $g(X)$ are defined and nonzero and we may see that $e_m(S,T)$ does not depend on the choice of g.

Here we give some basic properties of the Weil e_m-pairing.

Proposition 1.4.6. *The e_m-Weil pairing has the following properties:*
(a) It is bilinear:

$$e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T), \qquad e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2).$$

(b) It is alternating:

$$e_m(T,T) = 1.$$

(c) It is nondegenerate:

$$\textit{If } e_m(S,T) = 1 \textit{ for all } S \in E[m], \textit{ then } T = O.$$

(d) It is Galois invariant:

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) \text{ for all } \sigma \in G_{\bar{K}/K}.$$

(Note that here $G_{\bar{K}/K}$ is the Galois group of $\bar{K}/K$.)
(e) It is compatible:

$$e_{mn}(S,T) = e_m([n]S,T) \text{ for all } S \in E[mn] \text{ and } T \in E[m].$$

Proof. See, [16, Proposition 8.1]. □

From the properties of the Weil pairing, we can conclude the following result which we give as a corollary.

Corollary 1.4.7. *The e_m-Weil pairing is surjective, in other words, there exist points $S,T \in E[m]$ such that $e_m(S,T)$ is a primitive m^{th} root of unity. Moreover, if $E[m] \subset E(K)$, then $\mu_m \subset K^*$.*

Proof. The image of $e_m(S,T)$ is a subgroup of μ_m, assuming its order is n $(m \geq n)$. Then for all $S,T \in E[m]$, we have that

$$e_m([n]S,T) = e_m(S,T)^n = 1$$

by the nondegeneracy of the e_m we get that $[n]S = O$, for all $S \in E[m]$. Thus we have that $E[m] \subset E[n]$, from Corollary 1.2.11 we get that $m^2 \leq n^2$ which implies that $m = n$. If $E[m] \subset E(K)$, then by the Galois invariance of e_m-pairing we get that $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T)$, which means that $e_m(S,T) \in K$. Since the image of e_m-pairing is μ_m, we get the desired result $\mu_m \subset K^*$. □

Chapter 2

The Selmer Groups and Selmer Structures

2.1 Twisting-Elliptic curves

Let K be a number field and E be an elliptic curve over K. In this section, we study the elliptic curves over K which are isomorphic to E over $\bar{K}$.

Definition 2.1.1. *Let E/K be an elliptic curve. A twist of E/K is an elliptic curve E'/K that is isomorphic to E over $\bar{K}$.*

Remark 2.1.2. When we talk about the isomorphisms of elliptic curves here, we mean isomorphisms of smooth projective curves, namely, it is not necessary to send O to O.

We define an equivalent relation on the set of twists of E/K as follows: two twists are equivalent if they are isomorphic over K and denote the resulting class set as $\mathrm{Twist}(E/K)$.

The *isomorphism group* of E/K is the group of $\bar{K}$-isomorphisms from E to itself and we denote it by $\mathrm{Isom}(E)$.

Let E'/K be a twist of E/K with $\bar{K}$-isomorphism $\phi = [f_0, f_1, f_2] : E \longrightarrow E'$. Then Galois group $G_{\bar{K}/K}$ acts on ϕ in the natural way,

$$\phi^\sigma(P) = [f_0^\sigma(P), f_1^\sigma(P), f_2^\sigma(P)]$$

Now consider the map

$$\xi : G_{\bar{K}/K} \longrightarrow \mathrm{Isom}(E), \qquad \xi_\sigma = \phi^\sigma \phi^{-1}.$$

(Note that ϕ is defined over K if and only if $\xi_\sigma = \mathrm{Id}_E$ for all σ.) We claim that this map is 1-cocycle (see Appendix A for details of group cohomology), because

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1} = (\phi^\sigma)^\tau \phi^{-1} = (\phi^\sigma \phi^{-1} \phi)^\tau \phi^{-1} = (\xi_\sigma \phi)^\tau \phi^{-1} = \xi_\sigma^\tau \xi_\tau.$$

Denote the associated cohomology class of ξ in $H^1(G_{\bar{K}/K}, \mathrm{Isom}(E))$ by $\{\xi\}$. We now construct a bijection between $\mathrm{Twist}(E/K)$ and a certain cohomology set.

Theorem 2.1.3. *Let E/K be an elliptic curve and E'/K be a twist of E/K with a $\bar{K}$-isomorphism $\phi : E \longrightarrow E'$. Then the cohomology class $\{\xi\}$ is uniquely determined by the K-isomorphism class of E' and is independent of the choice of ϕ. Consequently, we obtain a natural map*

$$Twist(E/K) \longrightarrow H^1(G_{\bar{K}/K}, Isom(E))$$

Moreover, the map is a bijection.

Proof. See, [16, Theorem 2.2]. □

Here we give an important example of a twist of an elliptic curve on which the thesis is based.

Example 2.1.4. Let E/K be an elliptic curve and $K(\sqrt{d})/K$ be a quadratic extension. Using the following quadratic character

$$\chi : G_{\bar{K}/K} \longrightarrow \{\pm 1\} \qquad \chi(\sigma) = \sqrt{d}^{\sigma}/\sqrt{d}$$

we define a 1-cocycle as follows:

$$\xi : G_{\bar{K}/K} \longrightarrow \mathrm{Isom}(E) \qquad \xi_\sigma = [\chi(\sigma)].$$

Let E'/K be the corresponding twist of E/K. Since the characteristic of K is 0, E/K has a Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in K$. After the easy calculation using the formulas

$$[\chi(\sigma)](x, y) = (x, \chi(\sigma)y), \quad \sqrt{d}^{\sigma} = \chi(\sigma)\sqrt{d}, \quad x^\sigma = x, \quad y^\sigma = \chi(\sigma)(y).$$

we find that

$$dy'^2 = x'^3 + ax' + b$$

is the equation of twist E'/K. This curve E'/K is called the *quadratic twist* of E/K and we denote it by E_d/K.

We now define certain twists of elliptic curves called *principal homogeneous spaces.*

Definition 2.1.5. *Let E/K be an elliptic curve. A principal homogeneous space for E/K is a smooth curve C/K together with an algebraic group action*

$$\mu : C \times E \longrightarrow C$$

such that the following three properties hold:

1) $\mu(p, O) = p$ for all $p \in C$.

2) $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$.

3) For all $p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$.

From the definition, it is not obvious that a principal homogeneous space C/K for E/K is a twist of E/K, here we prove it.

Proposition 2.1.6. *Let E/K be an elliptic curve and C/K be a homogeneous space for E/K. Define the map*

$$\theta : E \longrightarrow C, \qquad \theta(P) = \mu(p_0, P)$$

for a fixed point $p_0 \in C$. Then the map θ is an isomorphism defined over $K(p_0)$, particularly, C/K is a twist of E/K.

Proof. Since the action of E on C defined over K, we have that for all $\sigma \in G_{\bar{K}/K}$, $p_0^\sigma = p_0$. Using this we get

$$\theta(P)^\sigma = \mu(p_0, P)^\sigma = \mu(p_0^\sigma, P^\sigma) = \mu(p_0, P^\sigma) = \theta(P^\sigma).$$

which tells us that θ is defined over $K(p_0)$. Moreover, we know that for all $p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$ implies θ has degree one and then from [16, II.2.4] we conclude that θ is an isomorphism. □

Now we define an equivalent relation on the set of principal homogeneous spaces as follows: two homogeneous spaces C/K, C'/K for a given elliptic curve E/K are *equivalent* if there is an isomorphism $\theta : C \longrightarrow C'$ defined over K such that

$$\theta(\mu(p, P)) = \mu(\theta(p), P)$$

for all $p \in C, P \in E$. The equivalence class containing E/K is called *trivial class*. The set of equivalence classes of homogeneous spaces for E/K is called the *Weil-Châtelet group* for E/K and written $\mathrm{WC}(E/K)$. (We will explain later why this is a group through Theorem 2.1.8).

The following proposition clarifies which principal homogeneous spaces are trivial.

Proposition 2.1.7. *Let C/K be a homogeneous space for E/K. Then C/K is an element of the trivial class if and only if $C(K) \neq \emptyset$.*

Proof. Assume that C/K is in the trivial class. Then by the definition, there exists a K-isomorphism $\theta : E \longrightarrow C$ which is compatible with the action of E on E, C. Thus, $\theta(O) \in C(K)$ implies that $C(K) \neq \emptyset$.

Conversely, assume that $p_0 \in C(K)$. Then from Proposition 2.1.6 we have that the map

$$\theta : E \longrightarrow C, \qquad \theta(P) = \mu(p_0, P)$$

is an isomorphism defined over $K(p_0) = K$ and compatibility on θ is

$$\mu(p_0, P + Q) = \mu(\mu(p_0, P), Q)$$

which follows from the definition of principal homogeneous spaces. □

Theorem 2.1.8. *Let E/K be an elliptic curve. Then there is a natural bijection*

$$WC(E/K) \longrightarrow H^1(G_{\bar{K}/K}, E)$$

defined as follows: Let C/K be a homogeneous space for E/K and $p_0 \in C$ be any point. Then

$$\{C/K\} \longmapsto \{\sigma \mapsto p_0^\sigma - p_0\}.$$

Proof. See [16, Theorem 3.6]. □

Remark 2.1.9. Since $H^1(G_{\bar{K}/K}, E)$ is a group, we can define a group structure on $\mathrm{WC}(E/K)$ through the bijection between them as defined above. Without using the cohomology, we can also construct a group structure on $\mathrm{WC}(E/K)$. See [16, Exercise 10.2] and [19].

2.2 Selmer and Shafaravich-Tate groups

In this section, we review the Selmer and Shafaravich-Tate groups and their properties. The Selmer and Shafaravich-Tate groups are essential in understanding the arithmetic properties of elliptic curves, particularly they provide valuable information about the structure of the *Mordell-Weil groups*. First, let us discuss briefly the Mordell-Weil groups.

Let E/K be an elliptic curve over a number field K. We have seen in Proposition 1.1.4 that $E(K)$ is a subgroup of $E(\bar{K})$ and we call it *Mordell-Weil group*. Here we state its main property.

Theorem 2.2.1 (Mordell-Weil)**.** *The group $E(K)$ is finitely generated.*

Proof. The proof is based on two different theorems, the first is called *weak Mordell-Weil theorem* states that for any integer $m \geq 2$, the quotient group $E(K)/mE(K)$ is a finite group, and the second is called the *infinite descent theorem* uses height functions. For the proof of the former, see [16, VIII.1.1] and for the latter, see [16, VIII.3.1] □

After the Mordell-Weil theorem, the natural question arises, can we find the generators for $E(K)$?

[16, VIII.3.2] says that once we have generators for $E(K)/mE(K)$ for some integer $m \geq 2$, a finite amount of computation yields generators for $E(K)$. However, there is no certain method so far to find generators for $E(K)/mE(K)$. So computing the $E(K)/mE(K)$ leads us to the following theory.

Let $E/K, E'/K$ be two elliptic curves and $\phi : E \longrightarrow E'$ be a nonzero isogeny defined over K. We can take, for example, $E = E'$ and $\phi = [m]$. Then we have an exact sequence of $G_{\bar{K}/K}$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

where $E[\phi]$ is the kernel of ϕ. Then by taking Galois cohomology, we get a long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[\phi] & \longrightarrow & E(K) & \xrightarrow{\phi} & E'(K) \\ & & & & & \overset{\delta}{\swarrow} & \\ & & H^1(G_{\bar{K}/K}, E[\phi]) & \longrightarrow & H^1(G_{\bar{K}/K}, E) & \longrightarrow & H^1(G_{\bar{K}/K}, E') \end{array} \tag{2.1}$$

from this, we form the following short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, E[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, E)[\phi] \longrightarrow 0. \tag{2.2}$$

Note that from the bijection in the Theorem 2.1.8 we can replace the last term in (2.2) by the ϕ-torsion in $\mathrm{WC}(E/K)$. Now for any $v \in M_K$ we fix an extension of v to $\bar{K}$ which fixes an embedding $\bar{K} \subset \bar{K}_v$ and a decomposition group $G_v \subset G_{\bar{K}/K}$. Thus G_v acts on $E(\bar{K}_v), E'(\bar{K}_v)$ and repeating the above procedure we get the following exact sequences

$$0 \longrightarrow E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E)[\phi] \longrightarrow 0. \tag{2.3}$$

Our main interest is in the case of $E = E'$ and $\phi = [2]$. In this case the resulting short exact sequence

$$0 \longrightarrow E(K_v)/2E(K_v) \xrightarrow{\delta} H^1(G_v, E[2]) \longrightarrow H^1(G_v, E)[2] \longrightarrow 0. \tag{2.4}$$

is called the *Kummer sequence for* E/K and we denote the image of δ by $\mathcal{K}(E/K_v)$ and we call it *Kummer image for* E/K.

Now from the inclusions $G_v \subset G_{\bar{K}/K}$ and $E(\bar{K}) \subset E(\bar{K}_v)$ we get the restriction maps on cohomology and thus we get the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_{\bar{K}/K}, E[\phi]) & \longrightarrow & \mathrm{WC}(E/K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_v H^1(G_v, E[\phi]) & \longrightarrow & \prod_v \mathrm{WC}(E/K_v)[\phi] & \longrightarrow & 0 \end{array} \tag{2.5}$$

Our goal is to compute the image of δ, or equivalently, to compute the kernel of the map

$$H^1(G_{\bar{K}/K}, E[\phi]) \longrightarrow \mathrm{WC}(E/K).$$

Definition 2.2.2. *Let $\phi : E/K \longrightarrow E'/K$ be an isogeny. Then the ϕ-Selmer group of E/K is the subgroup of $H^1(G_{\bar{K}/K}, E[\phi])$ defined by*

$$S^{(\phi)}(E/K) = \ker(H^1(G_{\bar{K}/K}, E[\phi]) \longrightarrow \prod_{v \in M_K} WC(E/K_v)).$$

The Shafarevich-Tate group for E/K is the subgroup of $WC(E/K)$ defined by

$$Ш(E/K) = \ker(WC(E/K) \longrightarrow \prod_{v \in M_K} WC(E/K_v)).$$

Theorem 2.2.3. *Let $E/K \longrightarrow E'/K$ be an isogeny defined over K. Then we have the following*
(a) There is an exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \longrightarrow S^{(\phi)}(E/K) \longrightarrow Ш(E/K)][\phi] \longrightarrow 0.$$

(b) The Selmer group $S^{(\phi)}(E/K)$ is finite.

Proof. See, [16, Theorem 4.2]. □

The weak Mordell-Weil theorem is the special case of this theorem. If we put $E = E'$ and $\phi = [m]$, then we get the finiteness of $E(K)/mE(K)$.

Here we develop the method to compute the $E(K)/2E(K)$ for special types of elliptic curves.

Lemma 2.2.4. *Let M be a finite $G_{\bar{K}/K}$-module and $S \subset M_K$ be a finite set of places and define*

$$H^1(G_{\bar{K}/K}, M, S) := \{\xi \in H^1(G_{\bar{K}/K}, M) : \xi \text{ is unramified outside } S\}.$$

Then $H^1(G_{\bar{K}/K}, M, S)$ is finite.

Proof. See, [16, Lemma 4.3] □

Using the fact that if two elliptic curves $E_1/K, E_2/K$ are isogenous over K, then E_1 has bad reduction over K if and only if E_2 has bad reduction over K (see, [16, VII.7.2]), we deduce the following corollary:

Corollary 2.2.5. *Let $E/K \longrightarrow E'/K$ be an isogeny defined over K, and $S \subset M_K$ be a finite set of places containing*

$$M_K^\infty \cup \{v \in M_K^0 : E \text{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(\deg \phi) > 0\}.$$

Then we have $S^{(\phi)}(E/K) \subset H^1(G_{\bar{K}/K}, M, S)$.

Since $H^1(G_{\bar{K}/K}, M, S)$ is finite and computable, theoretically we can compute the Selmer group. To determine whether a given element $\xi \in H^1(G_{\bar{K}/K}, M, S)$ is in $S^{(\phi)}(E/K)$, we take the corresponding homogeneous spaces $\{C/K\} \in \mathrm{WC}(E/K)$ and check that for any places $v \in S$ whether $C(K_v) \neq \emptyset$.

Let E/K be an elliptic curve and $m \geq 2$ be an integer, and we assume that $E[m] \subset E(K)$. Let S be as defined in Corollary 2.2.5. From Corollary 1.4.7 our assumption $E[m] \subset E(K)$ implies that $\mu_m \subset K^*$ and by Hilbert's theorem 90 (see, [11, p.71]) we get that every homomorphism $G_{\bar{K}/K} \longrightarrow \mu_m$ has the form

$$\sigma \longmapsto \tfrac{\beta^\sigma}{\beta} \quad \text{for some } \beta \in \bar{K}^* \quad \text{satisfying} \quad \beta^m \in K^*.$$

Namely, there is an isomorphism

$$\delta_K : K^*/(K^*)^m \longrightarrow \mathrm{Hom}(G_{\bar{K}/K}, \mu_m) \text{ such that } \delta_K(b)(\sigma) = \frac{\beta^\sigma}{\beta}$$

where $\beta \in \bar{K}^*$ is chosen such that $\beta^m = b$.
Now let $K(S, m)$ be a subgroup of $K^*/(K^*)^m$ such that

$$K(S, m) := \{b \in K^*/(K^*)^m : \mathrm{ord}_v(b) \equiv 0 (\mathrm{mod}\ m) \text{ for all } v \notin S\}.$$

We can identify $E[m]$ with $\mu_m \times \mu_m$ as $G_{\bar{K}/K}$-modules and using the fact that $K^*/(K^*)^m \cong H^1(G_{\bar{K}/K}, \mu_m)$ (see, [16, B.2.5]) we get the following isomorphism

$$H^1(G_{\bar{K}/K}, E[m], S) \cong K(S, m) \times K(S, m).$$

So far we have been working with arbitrary isogenies $\phi : E \longrightarrow E'$, so to compute $E'(K)$, we have to find generators for $E'(K)/mE'(K)$ for some integer $m \geq 2$ as we discussed before. However, simply computing $E'(K)/\phi(E(K))$ is not enough. Therefore, here we also work with the dual isogeny $\hat{\phi}$ in order to solve this problem. After working with $\hat{\phi}$ we find the generators for $E(K)/\hat{\phi}(E'(K))$ and using the following elementary exact sequence

$$0 \longrightarrow \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[m])} \longrightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{mE(K)} \longrightarrow \frac{E(K)}{\hat{\phi}(E'(K))} \longrightarrow 0. \tag{2.6}$$

we can compute the generators for $E(K)/mE(K)$.

Here we give an example for two-isogenies.

Proposition 2.2.6. *Let E/K and E'/K be elliptic curves given by the Weierstrass equations*

$$E : y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$$

and let

$$\phi : E \longrightarrow E', \qquad \phi(x, y) = (\tfrac{y^2}{x^2}, \tfrac{y(b-x^2)}{x^2})$$

be the isogeny of degree 2 with kernel $E[\phi] = \{O, (0, 0)\}$. Let

$$S = M_K^{\infty} \cup \{v \in M_K^0 : v(2) \neq 0 \text{ or } v(b) \neq 0 \text{ or } v(a^2 - 4b) \neq 0\}.$$

For any $d \in K^*$, let C_d/K be the principal homogeneous space for E/K given by the Weierstrass equation

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Then there is an exact sequence

$$\begin{aligned} 0 \longrightarrow E'(K)/\phi(E(K) \xrightarrow{\delta} K(S, 2) &\longrightarrow WC(E/K) \\ d &\longmapsto \{C_d/K\} \end{aligned}$$

where δ is such that $\delta(X, Y) = X$, $\delta(O) = 1$ and $\delta(0, 0) = a^2 - 4b$. The ϕ-Selmer groups is

$$S^{(\phi)}(E/K) \cong \{d \in K(S, 2) : C_d(K_v) \neq \emptyset \text{ for all } v \in S\}.$$

Finally, the map

$$\psi : C_d \longrightarrow E' \qquad \psi(z, w) = (\frac{d}{z^2}, -\frac{dw}{z^3})$$

has the property that if $P \in C_d(K)$, then

$$\delta(\psi(P)) \equiv d (mod\ (K^*)^2.$$

Proof. See, [16, p.337]. □

Since the elliptic curve E' in Proposition 2.2.6 has the same form as E, we can apply everything in Proposition 2.2.6 to the dual isogeny $\hat{\phi} : E' \longrightarrow E$ and using the exact sequence (2.6) we can compute $E(K)/2E(K)$. Here we give an example from [16, Chapter 10].

Example 2.2.7. We compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for the elliptic curve

$$E/\mathbb{Q} : y^2 = x^3 - 6x^2 + 17x.$$

using the Proposition 2.2.6. Since the discriminant of the equation is $-2^9 17^2$, we have that $S = \{\infty, 2, 17\}$ and consequently, we can take $\mathbb{Q}(S, 2)$ as $\{\pm 1, \pm 2, \pm 17, \pm 34\}$. From the proposition we easily find that the curve E' which is 2-isogenous to E has the following equation

$$E'/\mathbb{Q} : Y^2 = X^3 + 12X^2 - 32X,$$

We have that $(0, 0) \in E'(\mathbb{Q})$ and using the Proposition 2.2.6 we get

$$\delta(0, 0) = -32 \equiv -2 (\text{mod } (\mathbb{Q}^*)^2)$$

It means that $-2 \in S^{(\phi)}(E/\mathbb{Q})$. Now, we check the other values of $d \in \mathbb{Q}(S, 2)$.
Case: d=2. In this case, the principal homogeneous space $C_2/\mathbb{Q}$ given by the equation

$$C_2 : 2w^2 = 4 + 24z^2 - 32z^4.$$

We may easily notice that $(z, w) = (\frac{1}{2}, 2) \in C_2(\mathbb{Q})$ is a rational solution of the equation. Then by Proposition 2.2.6 we have that $\psi(\frac{1}{2}, 2) = (8, -32) \in E'(\mathbb{Q})$ and $\delta(8, -32) = 8 \equiv 2 (\text{mod } (\mathbb{Q}^*)^2)$.
Case: d=17. In this case, the principal homogeneous space $C_{17}/\mathbb{Q}$ given by the equation

$$C_{17} : 17w^2 = 17^2 + 12 \cdot 17z^2 - 32z^4.$$

Assume that $C_{17}(\mathbb{Q}_{17}) \neq \emptyset$ and then there is a solution to the equation in $z, w \in \mathbb{Z}_{17}$. From the equation, we have that $z \equiv 0 (\text{mod } 17)$ and therefore, after the putting $z = 17Z$ we get

$$w^2 = 17 + 12 \cdot 17^2 Z^2 - 32 \cdot 17^3 Z^4,$$

From this, we get $w^2 \equiv 17 (\text{mod } 17^2)$ which contradicts to our assumption and hence $17 \notin S^{(\phi)}(E/\mathbb{Q})$.
So far, we know that $1, 2, -2 \in S^{(\phi)}(E/\mathbb{Q})$ and $17 \notin S^{(\phi)}(E/\mathbb{Q})$. Since $S^{(\phi)}(E/\mathbb{Q})$ is a subgroup of $\mathbb{Q}(S, 2)$, we have $S^{(\phi)}(E/\mathbb{Q}) = \{\pm 1, \pm 2\}$.
Similarly, repeating the above calculation with changing the roles of E and E' we get that $S^{(\hat{\phi})}(E'/\mathbb{Q}) = \{1, 17\}$. Thus, we have that

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \cong (\mathbb{Z}/2\mathbb{Z})^2 \qquad \text{and} \qquad E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \cong \mathbb{Z}/2\mathbb{Z}$$

The exact sequence (2.6) yields that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \qquad \text{and} \qquad E'(\mathbb{Q})/2E'(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$$

and finally

$$E(\mathbb{Q}) \cong E'(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

2.3 Selmer structures

This section discusses the properties of Selmer structures and their associated Selmer groups. For more details, see, for example, [8, 9, 10].

Let F be a number field, M be a finite $G_{\bar{F}/F}$-module annihilated by 2, so M is a finite-dimensional $\mathbb{F}_2$-vector space and let $M^* := \mathrm{Hom}(M, \mu)$ be the dual of M. Then M^* is a $G_{\bar{F}/F}$-module by the action: $(\sigma, \phi)(m) = \sigma\phi(\sigma^{-1}m)$ for $\sigma \in G_{\bar{F}/F}$ and $\phi \in M^*$.

For each place v of F, we define the *local Tate pairng*

$$(\cdot,\cdot)_v : H^1(G_{\bar{F}_v/F_v}, M) \times H^1(G_{\bar{F}_v/F_v}, M^*) \longrightarrow H^2(G_{\bar{F}_v/F_v}, \mu_2) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

which is the composition of cup-product and the local invariant map. (For details, see [5].)

Theorem 2.3.1 (Tate duality)**.** *$(\cdot,\cdot)_v$ is non-degenerate for all places v of F. Moreover, $H^1_{nr}(G_{\bar{F}_v/F_v}, M)$ and $H^1_{nr}(G_{\bar{F}_v/F_v}, M^*)$ are orthogonal complements under this pairing for each non-archimedean place $v \nmid 2$ such that inertia group I_{F_v} acts trivially on M.*

Proof. See [5, Corollary 7.2.6] for the non-archimedean case, [5, Corollary 7.2.17] for the Archimedian case and [5, Theorem 7.2.15] for the claim concerning the unramified subspaces. □

Definition 2.3.2. *A Selmer structure $\mathcal{L} = \{\mathcal{L}_v\}_v$ for M is a collection of subspaces*

$$\mathcal{L}_v \subseteq H^1(G_{\bar{F}_v/F_v}, M)$$

for each place v of F satisfying $\mathcal{L}_v = H^1_{nr}(G_{\bar{F}_v/F_v}, M)$ for all but finitely many places. The Selmer group $Sel_{\mathcal{L}}(F, M)$ associated to this structure $\mathcal{L}$ is defined by

$$Sel_{\mathcal{L}}(F, M) = \ker(H^1(G_{\bar{F}/F}, M) \longrightarrow \prod_{v \in M_F} H^1(G_{\bar{F}_v/F_v}, M)/\mathcal{L}_v.)$$

We denote $\mathcal{L}_v^*$ by the orthogonal complement of $\mathcal{L}_v$ under the local Tate pairing, so we have that $\mathcal{L}_v^* \subseteq H^1(G_{\bar{F}_v/F_v}, M^*)$. Now we define the *dual Selmer structure* $\mathcal{L}^*$ for M^* by announcing that $\mathcal{L}^* = \{\mathcal{L}_v^*\}_v$ and we call the associated Selmer group $\mathrm{Sel}_{\mathcal{L}^*}(F, M)$ as *dual Selmer group*.

Note that both the Selmer group and its dual are finite-dimensional $\mathbb{F}_2$-vector spaces. The following theorem describes the difference in their dimensions (dimensions are taken over $\mathbb{F}_2$).

Theorem 2.3.3. *Let $\mathcal{L} = \{\mathcal{L}_v\}_v$ be a Selmer structure for M. Then*

$$\dim\, Sel_{\mathcal{L}}(F, M) - \dim\, Sel_{\mathcal{L}^*}(F, M^*) =$$

$$= \dim\, H^0(G_{\bar{F}/F}, M) - \dim\, H^0(G_{\bar{F}/F}, M^*) + \sum_{v \in M_F} (\dim\, \mathcal{L}_v - \dim\, H^0(G_{\bar{F}_v/F_v}, M))$$

Proof. See [20, Proposition 1.6] and [17, Theorem 2]. □

Example 2.3.4. Let E/F be an elliptic curve. For any place v of F we have the Kummer image

$$\mathcal{K}(E, F_v) \subseteq H^1(G_{\bar{F}_v/F_v}, E[2])$$

defined in Section 2.2. Then the collection $\mathcal{K} = \{\mathcal{K}(E/F_v)\}_v$ defines a Selmer structure because of the fact that for a non-archimedean place $v \nmid 2$ of F at which E has good reduction, we have that

$$\mathcal{K}(E/F_v) = H^1_{\mathrm{nr}}(G_{\bar{F}_v/F_v}, E[2]).$$

Using the fact that the Selmer structure for $E[2]$ is self-dual (see, for example, [13, Proposition 4.10]) and using the Theorem 2.3.3 we get that

$$\sum_{v \in M_F} (\dim\ E(F_v)/2E(F_v) - \dim\ E(F_v)[2]) = 0. \tag{2.7}$$

This is because we have the following equalities for all places v

$$\dim\ (\mathcal{L}_v) = \dim\ \mathcal{K}(E/F_v) = \dim\ E(F_v)/2E(F_v)$$

and

$$H^0(G_{\bar{F}_v/F_v}, E[2]) = E(F_v)[2].$$

2.4 2-Selmer groups over quadratic extensions

We fix a quadratic extension $K/\mathbb{Q}$ and an elliptic curve $E/\mathbb{Q}$. We write $K = \mathbb{Q}(\sqrt{\theta})$ for a squarefree integer θ, and $G = \mathrm{Gal}(K/\mathbb{Q})$. In this section, we discuss the Selmer structures associated to E/K and their properties. Moreover, using their properties we study the 2-Selmer group of E/K. (For more information about the structure of the 2-Selmer group $S^{(2)}(E/K)$, see [6].)

First, we define two Selmer structures for $E[2]$ over $\mathbb{Q}$.

Definition 2.4.1. *Define the Selmer structure $\mathcal{F}$ for $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$-module $E[2]$ by putting, for any place v of $\mathbb{Q}$*

$$\mathcal{F}_v = \mathcal{F}(E/\mathbb{Q}_v) := \mathrm{res}^{-1}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w)) \leq H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2])$$

where w is a place of K extending v and $\mathrm{res}^{-1}_{K_w/\mathbb{Q}_v}$ is the inverse of the restriction map $\mathrm{res}_{K_w/\mathbb{Q}_v} : H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2]) \longrightarrow H^1(G_{\bar{K}_w/K_w}, E[2])$ (the definition of $\mathcal{F}_v$ does not depend on the choice of w). Denote by $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) \leq H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2])$ the resulting Selmer group. Finally, define the Selmer structure $\mathcal{C}$ for $E[2]$ as the dual of $\mathcal{F}$ and denote the resulting Selmer group by $\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$.

Lemma 2.4.2. *We have the equality*

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) = \mathrm{res}^{-1}_{K/\mathbb{Q}}(S^{(2)}(E/K)).$$

Proof. This follows from the compatibility of local and global restriction maps. □

Lemma 2.4.3. *The Selmer structure $\mathcal{C}$ has the following properties.*

(a) For each place v of $\mathbb{Q}$, we have that

$$\mathcal{C}(E/\mathbb{Q}_v) = \mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w)) \leq H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2])$$

where w is any place of K extending v and $\mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w))$ is the image of corestriction map (see Appendix A).

(b) For each place v of $\mathbb{Q}$, we also have that

$$\mathcal{C}(E/\mathbb{Q}_v) = \delta_v(N_{K_w/\mathbb{Q}_v}E(K_w)) = \mathcal{K}(E/\mathbb{Q}_v) \cap \mathcal{K}(E_\theta/\mathbb{Q}_v)$$

where $\delta_v : E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \hookrightarrow H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2])$ is the local Kummer map defined in the Section 2.2 and $N_{K_w/\mathbb{Q}_v} : E(K_w) \longrightarrow E(\mathbb{Q}_v)$ is local norm map defined by $N_{K_w/\mathbb{Q}_v}(P) = \sum_{\sigma \in Gal(K_w/\mathbb{Q}_v)} \sigma(P)$.

(c) Globally, we have

$$\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = S^{(2)}(E/\mathbb{Q}) \cap S^{(2)}(E_\theta/\mathbb{Q}).$$

Moreover, we have that

$$\mathrm{cor}_{K/\mathbb{Q}}(S^{(2)}(E/K)) \subseteq \mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]).$$

Proof. (a) [6, Equation (10)] states that $\mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w))$ and $\mathrm{res}^{-1}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w))$ are orthogonal complements under the local Tate pairing and moreover, [1, Proposition 9], [5, Corollary 7.1.4] imply that $\mathrm{cor}_{K_w/\mathbb{Q}_v}$ and $\mathrm{res}_{K_w/\mathbb{Q}_v}$ are adjoints with respect to the local Tate pairing. Thus we have that

$$\mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w)) \subseteq \mathcal{F}_v^*$$

and

$$\mathrm{res}_{K_w/\mathbb{Q}_v}(\mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathcal{K}(E/K_w))) \subseteq \mathcal{K}(E/K_w)^*.$$

The result follows from the fact that $\mathcal{K}(E/K_w)$ is its own orthogonal complement.
(b) The first equality comes from the fact that the local Kummer maps arising from Kummer sequences over K_w and $\mathbb{Q}_v$ commute with corestriction. For the second equality, see [6, Proposition 7].
(c) The equality

$$\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = S^{(2)}(E/\mathbb{Q}) \cap S^{(2)}(E_\theta/\mathbb{Q})$$

is natural consequence of (b) and the inclusion

$$\mathrm{cor}_{K/\mathbb{Q}}(S^{(2)}(E/K)) \subseteq \mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$$

comes from (a) and compatibility of the local and global corestriction maps. □

Remark 2.4.4. *Let v be a place of $\mathbb{Q}$. Since $\mathcal{K}(E/\mathbb{Q}_v)$ is its own orthogonal complement and the Selmer structure $\mathcal{F}$ is dual to $\mathcal{C}$, it follows from Lemma 2.4.3 that*

$$\mathcal{F}(E/\mathbb{Q}_v) = \mathcal{K}(E/\mathbb{Q}_v) + \mathcal{K}(E_\theta/\mathbb{Q}_v)$$

where the sum is taken inside $H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2])$.

In the following Lemma, we determine the difference between the dimensions of the Selmer groups $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])$ and $\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$ using Theorem 2.3.3.

Lemma 2.4.5. *We have the following equality*

$$\dim\, \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) - \dim\, \mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \sum_{v \in M_{\mathbb{Q}}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

Proof. For each place v of $\mathbb{Q}$ we have that the groups $\mathcal{C}(E/\mathbb{Q}_v)$ and $\mathcal{F}(E/\mathbb{Q}_v)$ are orthogonal complements under the local Tate pairing. Hence, we have that

$$\dim\, \mathcal{F}(E/\mathbb{Q}_v) = \dim\, H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2]) - \dim\, \mathcal{C}(E/\mathbb{Q}_v).$$

Similarly, since $\mathcal{K}(E/\mathbb{Q}_v)$ is its own orthogonal complement (see, [13, Proposition 4,10]) we have that

$$\dim\, H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2]) = 2\dim\, E(\mathbb{Q}_v)/2E(\mathbb{Q}_v).$$

Using part (b) of Lemma 2.4.3 we get

$$\dim\, \mathcal{F}_v = 2\dim\, E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) - \dim\, N_{K_w/\mathbb{Q}_v} E(K_w)/2E(\mathbb{Q}_v) =$$

$$= \dim\, E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) + \dim\, E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

Now from the Theorem 2.3.3 and the equation (2.7) we get that

$$\dim\, \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) - \dim\, \mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \sum_{v \in M_{\mathbb{Q}}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w)$$

$$+ \sum_{v \in M_{\mathbb{Q}}} (\dim\, E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) - \dim\, E(\mathbb{Q}_v)[2]) =$$

$$\sum_{v \in M_{\mathbb{Q}}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

□

We now review the properties of the 2-Selmer Group of E/K.

Lemma 2.4.6. *We have*

$$0 \longrightarrow H^1(G_{K/\mathbb{Q}}, E(K)[2]) \xrightarrow{\inf} \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) \xrightarrow{\mathrm{res}_{K/\mathbb{Q}}} S^{(2)}(E/K) \xrightarrow{\mathrm{cor}_{K/\mathbb{Q}}} \mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]). \tag{2.8}$$

Proof. Consider the short exact sequence of $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$-modules

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{F}_2[G] \xrightarrow{\epsilon} \mathbb{F}_2 \longrightarrow 0,$$

where ϵ is the map such that $\epsilon(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g$ and $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ acts on G via the quotient map $G_{\bar{\mathbb{Q}}/\mathbb{Q}} \twoheadrightarrow G$. By taking the tensor product over $\mathbb{F}_2$ with $E[2]$, and then taking Galois cohomology over $\mathbb{Q}$, we get an exact sequence of $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$-modules

$$H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2]) \longrightarrow H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2] \otimes_{\mathbb{F}_2} \mathbb{F}_2[G]) \longrightarrow H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2])$$

Using Shapiro's Lemma (see, [18, p.172]) we replace $H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2] \otimes_{\mathbb{F}_2} \mathbb{F}_2[G])$ by $H^1(G_{\bar{K}/K}, E[2])$ and get the following exact sequence

$$H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2]) \xrightarrow{\text{res}} H^1(G_{\bar{K}/K}, E[2]) \xrightarrow{\text{cor}} H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2])$$

The result now comes from combining the inflation-restriction exact sequence with Lemmas 2.4.2 and 2.4.3(c). □

Corollary 2.4.7. *If* $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = 0$*, then we have the following properties.*
(a) There is a short exact sequence

$$0 \longrightarrow H^1(G_{K/\mathbb{Q}}, E(K)[2]) \xrightarrow{\text{inf}} \text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) \xrightarrow{\text{res}_{K/\mathbb{Q}}} S^{(2)}(E/K) \longrightarrow 0$$

(b) We have that

$$\dim\, S^{(2)}(E/K) = -\dim\, \left(\frac{E(\mathbb{Q})[2]}{N_{K/\mathbb{Q}}(E(K)[2])}\right) + \sum_{v \in M_{\mathbb{Q}}} \dim\, E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

(c) The G-action on $S^{(2)}(E/K)$ is trivial.

Proof. (a) It follows easily from Lemma 2.4.6.
(b) It follows from Lemma 2.4.5 and (a), moreover, since G is cyclic, we have that

$$H^1(G_{K/\mathbb{Q}}, E(K)[2]) \cong \frac{E(\mathbb{Q})[2]}{N_{K/\mathbb{Q}}(E(K)[2])}.$$

(See [1, Section 8] for details of the isomorphism above).
(c) It follows from (a) and the fact that the image of the map

$$H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2]) \xrightarrow{\text{res}} H^1(G_{\bar{K}/K}, E[2])$$

is contained $H^1(G_{\bar{K}/K}, E[2])^G$. □

We nevertheless obtain a lower bound for the dim $S^{(2)}(E/K)$ even in the case where $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$ is not always trivial.

Lemma 2.4.8. *We have the following equality*

$$\dim\, S^{(2)}(E/K) \geq -2 + \sum_{v \in M_{\mathbb{Q}}} \dim\, E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

Proof. From Lemma 2.4.6 we get that

$$\dim\, S^{(2)}(E_d/K) \geq \dim\, \text{Sel}_{\mathcal{F}_d}(\mathbb{Q}, E_d[2]) - \dim\, \text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) - \dim\, H^1(G_{K/\mathbb{Q}}, E(K)[2]).$$

Now using the Lemma 2.4.5 and the equality

$$\dim\, H^1(G_{K/\mathbb{Q}}, E(K)[2]) \leq 2$$

which is a consequence of the description of the cohomology of cyclic groups, we get the desired result. □

2.5 A distributional result

In this section, we study the results after replacing $E/\mathbb{Q}$ with its quadratic twist $E_d/\mathbb{Q}$, particularly, the analytic properties of the function $g(d)$ of Notation 2.5.1. We denote by $\mathcal{F}_d$ and $\mathcal{C}_d$ the Selmer structures associated to E_d/K as in the Definition 2.4.1. Let us start with some notations:

Notation 2.5.1. Denote by Σ a finite set of places of $\mathbb{Q}$ which contains the real place, 2, all places ramifying in $K/\mathbb{Q}$ and all primes at which E has bad reduction. Next, for a squarefree integer d we write

$$g(d) := \sum_{v \in M_{\mathbb{Q}}} \dim\ E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w)$$

and write

$$w_{E,K}(d) := \#\{\, p \mid d : p \notin \Sigma, p \text{ inert in } K/\mathbb{Q},\ \dim\ E(\mathbb{Q}_p)[2] = 2\}$$

Now we are ready to state the following results.

Lemma 2.5.2. *Let p be a prime divisor of d such that $p \notin \Sigma$. Then $E_d(\mathbb{Q}_p^{\mathrm{nr}})$ has no points of exact order 4, particularly, it is also true for $E_d(\mathbb{Q}_d)$.*

Proof. We claim that $E[4]$ is unramified at p, because E has good reduction at p by assumption and so, the inertia group I_p at p acts trivially on $E[4]$. Hence, any $\sigma \in I_p$ acts on $E_d[4]$ as multiplication by quadratic character $\chi_d(\sigma)$. The restriction of χ_d to I_p is nontrivial since χ_d is ramified at p and so we get that

$$E_d[4]^{I_p} = \{P \in E_d[4] : P = -P\} = E_d[2]$$

□

Lemma 2.5.3. *Let $p \notin \Sigma$, d be squarefree integer and let $\mathfrak{p}$ be a prime of K lying over p. Then we have that*

$$\dim\ E_d(\mathbb{Q}_p)/N_{K_{\mathfrak{p}}/\mathbb{Q}_p} E_d(K_{\mathfrak{p}}) = \begin{cases} 2 & \text{if } p \mid d,\ p \text{ inert in } K/\mathbb{Q},\ \dim\ E_d(\mathbb{Q}_p)[2] = 2 \\ 0 & \text{otherwise} \end{cases}$$

Proof. See [12, p.1129]. □

Proposition 2.5.4. *As d varies in squarefree integers, we have that*

$$g(d) = 2w_{E,K}(d) + O(1)$$

Proof. We may ignore the places in Σ since the Σ is finite. Now the result follows from Lemma 2.5.3. □

We now study the distribution of $g(d)$ through the following notation.

Notation 2.5.5. Let $\delta_{E,K}$ be the natural density of primes p with $w_{E,K} = 1$.

Using the Chebotarev density theorem to the extension $K(E[2])/\mathbb{Q}$ we can compute the possible values of $\delta_{E,K}$. So we have the following table:

$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$	$\{1\}$	$\mathbb{Z}/2\mathbb{Z}$ $K\neq\mathbb{Q}(E[2])$	$\mathbb{Z}/2\mathbb{Z}$ $K=\mathbb{Q}(E[2])$	$\mathbb{Z}/3\mathbb{Z}$	S_3 $K\not\subseteq\mathbb{Q}(E[2])$	S_3 $K\subseteq\mathbb{Q}(E[2])$
$\delta_{E,K}$	$1/2$	$1/4$	0	$1/6$	$1/12$	0

The next Proposition gives us a distributional result for the function $g(d)$.

Proposition 2.5.6. *Suppose that $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$. Then for all $z \in \mathbb{R}$ we have that*

$$\lim_{X\to\infty} \frac{\#\{|d| \leq X \text{ squarefree } : \frac{g(d)-2\delta_{E,K}\log\log|d|}{\sqrt{4\delta_{E,K}\log\log|d|}} \leq z\}}{\#\{|d| \leq X \text{ squarefree }\}} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-t^2/2}dt.$$

Proof. See [12, p.1131]. □

In the case of $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$, we have the following basic result which states that for 100% of d, $\dim S^{(2)}(E_d/K)$ is larger than any fixed positive integer.

Corollary 2.5.7. *Suppose that $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$. Then for all $z \in \mathbb{R}$ we have that*

$$\lim_{X\to\infty} \frac{\#\{|d| \leq X \text{ squarefree } : \dim(S^{(2)}(E_d/K)) \leq z\}}{\#\{|d| \leq X \text{ squarefree}\}} = 0.$$

Proof. The result follows from Proposition 2.5.6 together with Lemma 2.4.8 which says that $\dim S^{(2)}(E_d/K) \geq g(d) - 2$. □

Chapter 3

Main Results

3.1 Statements of the main results

This section states our main technical theorem with three immediate consequences. Recall that $K = \mathbb{Q}(\sqrt{\theta})$ is a quadratic number field, $G = \mathrm{Gal}(K/\mathbb{Q})$ and $E/\mathbb{Q}$ is an elliptic curve with quadratic twist $E_d/\mathbb{Q}$ for a squarefree integer d. From now on, we assume that $E[2] \subseteq E(\mathbb{Q})$ and under this assumption we will prove that the Selmer group $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is trivial for 100% of d.

Theorem 3.1.1. *We have that*

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree } : |d| < X,\ \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree } : |d| < X\}} = 1.$$

Remark 3.1.2. *We will show stronger result in the Section 3.3, namely*

$$\#\{d \text{ squarefree } : |d| < X,\ \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E[2]) \neq 0\} \ll X\log(X)^{-0.0394}.$$

We now use the results from the previous sections to state some consequences of the theorem.

Corollary 3.1.3. *The G-action on $S^{(2)}(E_d/K)$ is trivial for 100% of squarefree integer d ordered by absolute value, and we have that*

$$\dim\ S^{(2)}(E_d/K) = -2 + \sum_{v\in M_{\mathbb{Q}}} \dim\ E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v}E(K_w). \tag{3.1}$$

Proof. This immediately follows from the Theorem 3.1.1 and Corollary 2.4.7. □

Corollary 3.1.4. *The distribution of the quantity*

$$\frac{\dim\ S^{(2)}(E_d/K) - \log\log|d|}{\sqrt{2\ \log\log|d|}}$$

is a standard normal, i.e. for every $z \in \mathbb{R}$ we have

$$\lim_{X\to\infty} \frac{\#\{|d| \leq X \text{ squarefree } : \frac{\dim\ S^{(2)}(E_d/K) - \log\log|d|}{\sqrt{2\ \log\log|d|}} \leq z\}}{\#\{|d| \leq X \text{ squarefree }\}} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-t^2/2}dt.$$

Proof. By the Corollary 3.1.3 we have that for 100% of d

$$\dim S^{(2)}(E/K) = -2 + \sum_{v \in M_{\mathbb{Q}}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w) = g(d) - 2.$$

By assumption, we have $E[2] \subseteq E(\mathbb{Q})$ which implies that $\delta_{E,K} = 1/2$ from the table. Now the result comes from the Proposition 2.5.6. □

As a third consequence of the main theorem, we give some results for the Mordell-Weil groups of the E_d/K.

Notation 3.1.5. We write

$$\Lambda(E_d/K) := E_d(K)/E_d(K)_{\text{tors}}$$

We call this the Mordell-Weil lattice. Note that the action of G on $E_d(K)$ makes $\Lambda(E_d/K)$ into a G-module.

Let M be a G-module. Then we denote by $M(-1)$ the G-module which is isomorphic to M as an abelian group with the new G-action of the generator σ of G is given by

$$m \mapsto -\sigma(m).$$

Lemma 3.1.6. *If* $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0$ *then we have the following isomorphism of* $\mathbb{Z}[G]$*-modules*

$$\Lambda(E_d/K) \cong \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{\theta d}/\mathbb{Q})(-1).$$

Proof. On the one hand, we have that by [2, Theorem 34.31], there exist unique $a, b, c \in \mathbb{N} \cup \{0\}$ such that

$$\Lambda(E_d/K) \cong \mathbb{Z}^a \oplus \mathbb{Z}(-1)^b \oplus \mathbb{Z}[G]^c,$$

On the other hand, we have an inclusion of G-modules

$$\Lambda(E_d/K)/2\Lambda(E_d/K) \subseteq S^{(2)}(E_d/K)/\delta(E_d[2]).$$

$S^{(2)}(E_d/K)/\delta(E_d[2])$ has trivial G-action which comes from Corollary 2.4.7, consequently $\Lambda(E_d/K)/2\Lambda(E_d/K)$ has trivial G-action too. Hence, we get that $c = 0$. Via the natural K-isomorphism $E_d \cong E_{\theta d}$, we can identify the points of $E_d(K)$ on which the generator of G acts as multiplication by -1 with $E_{\theta d}(\mathbb{Q})$. Thus, the result follows. □

Proposition 3.1.7. *If we have* $E_d(K)_{\text{tors}} = E_d[2]$ *and* $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0$*, then we have the following isomorphism of* $\mathbb{Z}[G]$*-modules*

$$E_d(K) \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{\theta d}/\mathbb{Q})(-1).$$

Proof. In fact, in this case we have that

$$E_d(K) \cong E_d[2] \oplus \Lambda(E_d/K) \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/K)$$

(See [12, p.1137] for more details). So by Lemma 3.1 we get the desired result. □

Corollary 3.1.8. *For* 100% *of* d*, there is an isomorphism of* $\mathbb{Z}[G]$*-modules*

$$E_d[K] \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{\theta d}/\mathbb{Q})(-1) \tag{3.2}$$

In other words, we have that

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree } : |d| < X, \ (3.2) \text{ holds } \}}{\#\{d \text{ squarefree } : |d| < X\}} = 1.$$

Proof. For any prime integer $p \geq 3$, at most two quadratic twists of E have rational p-torsion, because, otherwise E would have at least 3-dimensional p-torsion over a multi-quadratic extension, which is impossible. Particularly, for any prime integer $p \geq 3$, only finitely many twists of E can have p-torsion over K. As a result, by Mazur's theorem [7, Theorem 8], outside of a finite set of d we have that $E_d(K)_{\text{tors}} \subseteq E[2^\infty]$. On top of that, only finitely many quadratic twists have a point of order 4 by the Lemma 2.5.2. So the result now follows from Theorem 3.1.1 together with Proposition 3.1.7. □

3.2 Explicit local conditions for full 2-torsion

In this section, we give some algebraic preliminaries for the proof of the main theorem. We fix an elliptic curve $E/\mathbb{Q}$ with $E[2] \subseteq E[\mathbb{Q}]$ and a Weiestrass equation

$$E/\mathbb{Q} : y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{3.3}$$

for $E/\mathbb{Q}$, without loss of generality say $a_1, a_2, a_3 \in \mathbb{Z}$. We set $\alpha = a_1 - a_2$, $\beta = a_1 - a_3$, and $\gamma = a_2 - a_3$.

We now fix Σ a finite set of places of $\mathbb{Q}$ as Notation 2.5.1. Since Σ contains primes at which E has bad reduction, we conclude from Section 1.3 that Σ contains all primes dividing $2\alpha\beta\gamma$.

For the elliptic curve with equation (3.3) we have that $E[2] = \{O, P_1, P_2, P_3\}$, where $P_i = (a_i, 0)$. Its quadratic twist $E_d/\mathbb{Q}$ for a given squarefree integer d has a Weierstrass equation of the form

$$E_d/\mathbb{Q} : y^2 = (x - da_1)(x - da_2)(x - da_3)$$

with $E_d[2] = \{O, P_{1,d}, P_{2,d}, P_{3,d}\}$, where $P_{1,d} = (da_i, 0)$.

The following lemma describes the local conditions $\mathcal{C}(E_d/\mathbb{Q}_v)$ of Definition 2.4.1 at primes $p \notin \Sigma$.

Lemma 3.2.1. *Let* p *be a prime such that* $p \notin \Sigma$*. Then*
(a) if $p \nmid d$*, we have that*

$$\mathcal{C}(E_d/\mathbb{Q}_p) = \mathcal{K}(E_d/\mathbb{Q}_p) = H^1_{\text{nr}}(G_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p}, E_d[2])$$

(b) if $p \mid d$ *is split in* $K/\mathbb{Q}$*, we have that*

$$\mathcal{C}(E_d/\mathbb{Q}_p) = \mathcal{K}(E_d/\mathbb{Q}_p) = \delta_{d,p}(E_d[2])$$

where $\delta_{d,p} : E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \hookrightarrow H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E_d[2])$ *is the local Kummer map.*
(c) if $p \mid d$ *is inert in* $K/\mathbb{Q}$ *we have that*

$$\mathcal{C}(E_d/\mathbb{Q}_p) = 0.$$

Proof. (a) By Lemma 2.5.3, we have that dim $E_d(\mathbb{Q}_p)/N_{K_\mathfrak{p}/\mathbb{Q}_p}E_d(K_\mathfrak{p}) = 0$ which tells us $E_d(\mathbb{Q}_p) = N_{K_\mathfrak{p}/\mathbb{Q}_p}E_d(K_\mathfrak{p})$. By Lemma 2.4.3, we have that

$$\mathcal{C}(E_d/\mathbb{Q}_p) = \delta_p(N_{K_\mathfrak{p}/\mathbb{Q}_p}E_d(K_\mathfrak{p})) = \delta_p(E_d(\mathbb{Q}_p)) = \mathcal{K}(E_d/\mathbb{Q}_p).$$

The equality

$$\mathcal{K}(E_d/\mathbb{Q}_p) = H^1_{\mathrm{nr}}(G_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p}, E_d[2])$$

follows from the fact that for a non-archimedean place $v \nmid 2$ of a field F at which E has good reduction, we have that

$$\mathcal{K}(E/F_v) = H^1_{\mathrm{nr}}(G_{\bar{F}_v/F_v}, E[2]).$$

In our case, indeed, p is odd and E_d has good reduction since $p \notin \Sigma$. For (b) and (c) see [12, Lemma 7.2].

□

We now define a new Selmer structure, whose associated Selmer group contains $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a subgroup that admits an explicit description.

Definition 3.2.2. *Define the Selmer structure $\tilde{\mathcal{C}}_d$ for $E_d[2]$ via the local condition*

$$\tilde{\mathcal{C}}(E_d/\mathbb{Q}_v) = \begin{cases} \mathcal{C}(E_d/\mathbb{Q}_v) & \text{if } v \notin \Sigma \\ H^1(G_{\bar{\mathbb{Q}}_v/\mathbb{Q}_v}, E[2]) & \text{if } v \in \Sigma. \end{cases}$$

Write by $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ the associated Selmer group.

Note that if $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ is trivial, then $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is also trivial, since by construction, $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is a subgroup of $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$.

Notation 3.2.3. Write N for the product of all primes in Σ and write $d = ad'd''$, where d' is the product of all primes $p \mid d$ such that $p \notin \Sigma$ and p splits in $K/\mathbb{Q}$, and d'' is product of all primes $p \mid d$ such that $p \notin \Sigma$ and p inert in $K/\mathbb{Q}$.

We identify $H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E_d[2])$ as a subgroup of $(\mathbb{Q}^*/\mathbb{Q}^{*2})^2$ as in Section 2.2 and identify $(\mathbb{Q}^*/\mathbb{Q}^{*2})^2$ as the set of pairs of squarefree integers (note that there is a natural bijection between $\mathbb{Q}^*/\mathbb{Q}^{*2}$ and the set of squarefree integers.).

In the following Proposition, we describe $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ as a set of pairs of squarefree integers.

Proposition 3.2.4. *The Selmer group $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ consist of pairs (x_1, x_2) of squarefree integers satisfying the following conditions:*
(a) $x_i \mid Nd'$ for $i = 1, 2$.
(b) $(\frac{x_i}{p}) = 1$ for all $p \mid d''$ and $i = 1, 2$ (where $(\frac{n}{p})$ is the Legendre symbol.)
(c) for all $p \mid d'$ implies that $(x_1, d\alpha)_p(x_2, \alpha\beta)_p = (x_1, -\alpha\gamma)_p(x_2, -d\alpha)_p = 1$.

Proof. See [12, p.1141]. □

3.3 Proof of the main theorem

The aim of this section is to prove our main technical theorem using two external results. As stated early in Remark 3.1.2, we prove the following strictly stronger result.

Theorem 3.3.1. *We have that*

$$\#\{d \text{ squarefree } : |d| < X,\ \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E[2]) \neq 0\} \ll X\log(X)^{-0.0394} \tag{3.4}$$

In particular, we get

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree } : |d| < X,\ \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree } : |d| < X\}} = 1. \tag{3.5}$$

Remark 3.3.2. If we have (3.4), then using the fact

$$\#\{d \text{ squarefree } : |d| < X\} \approx \frac{12X}{\pi^2}$$

we get that

$$\frac{\#\{d \text{ squarefree } : |d| < X,\ \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) \neq 0\}}{\#\{d \text{ squarefree } : |d| < X\}} \ll \frac{X\log(X)^{-0.0394}}{\frac{12X}{\pi^2}} = \frac{\pi^2}{12\log(X)^{0.0394}}$$

which goes to 0 as $X \to \infty$. As a result, we get (3.5).

To prove Theorem 3.3.1, it suffices to prove the same result just for $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$, since $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is a subgroup of $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ by construction.

Notation 3.3.3. We define the following sets of prime integers:

$$P_0 := \{p \notin \Sigma,\ p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ non-split in } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$P_1 := \{p \notin \Sigma,\ p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ split in } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$P_2 := \{p \notin \Sigma,\ p \text{ inert } K/\mathbb{Q}\}.$$

Now for $i = 0, 1, 2$, we define F_i as the set of positive squarefree integers n such that all of the prime factors of n lie in P_i.

Note that the sets P_0, P_1, P_2 and Σ are pairwise disjoint and their union gives the set of all primes. Consequently, the sets F_i are also pairwise disjoint.

Definition 3.3.4. *Let d be a squarefree integer. Write $d = ad_0d_1d_2$ where $a \mid N, d_i \in F_i$ for $i = 0, 1, 2$. Then define*

$$S_d := \{x \text{ squarefree } : x \mid Nd_0d_1, (\frac{x}{p}) = 1 \text{ for all } p \mid d_2,\ (x, d\alpha)_p = 1 \text{ for all } p \mid d_1\}$$

Lemma 3.3.5. *If a pair of squarefree integers (x_1, x_2) is in $\mathrm{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$, then $x_1 \in S_d$.*

Proof. This immediately follows from Proposition 3.2.4 and the definition of S_d. □

Assuming the following Theorem we prove the Theorem 3.3.1.

Theorem 3.3.6. *We have that*

$$\#\{d \text{ squarefree } : |d| < X, S_d \neq 0\} \ll X\log\,(X)^{-0.0394}.$$

Proof of Theorem 3.3.1 assuming Theorem 3.3.6: By Lemma 3.3.5 and Theorem 3.3.6 we have that x_1-coordinate of any element of $\mathrm{Sel}_{\tilde{C}_d}(\mathbb{Q}, E_d[2])$ is trivial for 100% of squarefree integer d. Then the same is true for the x_2-coordinate by symmetry (to change the roles of x_1 and x_2 we can relabel a_1 and a_2 in Equation (3.2) for our elliptic curve). This demonstrates the limit statement of the Theorem 3.3.1, and executing the same argument while monitoring the error terms shows the overall result. □

We now state some important results to prove Theorem 3.3.6.

Let n be a positive integer, we denote by $w(n)$ the number of distinct prime factors of n, and for $i = 1, 2, 3$ we denote by $w_i(n)$ the number of distinct prime factors of n lie in P_i.

Theorem 3.3.7 (Brun-Titchmarsh Theorem for Multiplicative Functions)**.** *Let* $0 < \lambda_1 < \frac{1}{2}$ *and* $0 < \lambda_2 < \frac{1}{2}$, *and let* Y *be such that* $q < Y^{1-\lambda_1}$ *and* $X^{\lambda_2} < Y \leq X$. *Moreover, let* $(b, q) = 1$, *and let* $f(n)$ *be a non-negative multiplicative function. Then*

$$\sum_{\substack{X-Y<n\leq X \\ n\equiv b \pmod q}} f(n) \ll \frac{Y}{q\,\log X}\exp\,(\sum_{p\leq X}\frac{f(p)}{p}).$$

Proof. See the result of P. Shiu [15]. □

Using this result we prove the following Lemma which we will use later to prove the Theorem 3.3.6.

Lemma 3.3.8. *Let* a_0, a_1 *and* a_2 *be non-negative real numbers. Then we have that*

$$\sum_{\substack{X-Y<n\leq X \\ n \text{ squarefree}}} a_0^{w_0(n)}a_1^{w_1(n)}a_2^{w_2(n)} \ll \begin{cases} Y\log(X)^{\frac{a_0}{4}+\frac{a_1}{4}+\frac{a_2}{2}-1} & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \nsubseteq K, \\ Y\log(X)^{\frac{a_1}{2}+\frac{a_2}{2}-1} & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K. \end{cases}$$

uniformly for $2 \leq X\exp(-\sqrt{\log(X)}) \leq Y \leq X$.

Proof. Define the multiplicative function $f : \mathbb{Z} \longrightarrow \mathbb{R}_{\geq 0}$ such that for all $k \geq 1$, $f(p^k) = a_i$ for $p \in P_i$ $(i = 1, 2, 3)$, and $f(p) = 1$ for all $p \in \Sigma$. Note that if $\mathbb{Q}(\sqrt{\alpha\beta}) \nsubseteq K$, then P_0 and P_1 have Dirichlet density $\frac{1}{4}$, and P_2 has density $\frac{1}{2}$ and if $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ then $P_0 = \emptyset$ and P_1, P_2 both have density $\frac{1}{2}$. Using this we get that

$$\sum_{p\leq X}\frac{f(p)}{p} \sim \begin{cases} (\frac{a_0}{4}+\frac{a_1}{4}+\frac{a_2}{2})\log\,\log(X) & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \nsubseteq K, \\ (\frac{a_1}{2}+\frac{a_2}{2})\log\,\log(X) & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K. \end{cases}$$

Note that by the definition of $f(n)$, we have

$$\sum_{X-Y<n\leq X} f(n) \geq \sum_{\substack{X-Y<n\leq X \\ n \text{ squarefree}}} f(n) = \sum_{\substack{X-Y<n\leq X \\ n \text{ squarefree}}} a_0^{w_0(n)} a_1^{w_1(n)} a_2^{w_2(n)}$$

The result now follows from the Theorem 3.3.7 for $q = 1$, and λ_1, λ_2 are formed from the $2 \leq X\exp(-\sqrt{\log(X)}) \leq Y \leq X$. □

We now state the next important result to prove Theorem 3.3.6.

Proposition 3.3.9. *For any* $1 < \lambda < \frac{7}{8} + \frac{\sqrt{17}}{8} = 1.3903...$, *we have that*

$$\sum_{\substack{|d|<X \\ d \text{ squarefree}}} \lambda^{w_2(d)-w_0(d)}(\#S_d - 1) = o(X)$$

Moreover, for $\lambda = \frac{1}{4} + \frac{\sqrt{17}}{4}$ *we have that*

$$\sum_{\substack{|d|<X \\ d \text{ squarefree}}} \lambda^{w_2(d)-w_0(d)}(\#S_d - 1) \ll X\log(X)^{-0.0394}.$$

Proof. First step is to express the sum

$$\sum_{\substack{|d|<X \\ d \text{ squarefree}}} \lambda^{w_2(d)-w_0(d)}(\#S_d - 1)$$

as a sum of Jacobi symbols using the idea of [3, Lemma 8]. We then determine the bound to this sum using the techniques by Fouvry-Klüners in their work [3]. Further see, [12, pp.1145-1156]. □

Proof of Theorem 3.3.6. We first claim that

$$\#\{d \text{ squarefree } : |d| < X,\ w_0(d) \geq w_2(d)\} \ll X\log(X)^{-0.042}$$

Fix a real number $\lambda > 1$, then using the weak inequality we get that

$$\#\{d \text{ squarefree } : |d| < X,\ w_0(d) \geq w_2(d)\} \leq \sum_{|d|<X \text{ squarefree}} \lambda^{w_0(d)-w_2(d)} \leq$$

$$\leq 2 \sum_{0<d\leq X} \lambda^{w_0(d)-w_2(d)}.$$

Using the Lemma 3.3.8 for $X = Y$, and $a_0 = \lambda, a_1 = 1, a_2 = \frac{1}{\lambda}$ we get that

$$\sum_{0<d\leq X} \lambda^{w_0(d)-w_2(d)} \ll X\log(X)^{\frac{\lambda}{4}+\frac{1}{2\lambda}-\frac{3}{4}}$$

The exponent $\frac{\lambda}{4} + \frac{1}{2\lambda} - \frac{3}{4}$ reaches its maximal when $\lambda = \sqrt{2}$, so the exponent always less than $\frac{\sqrt{2}}{2} - \frac{3}{4} < -0.042$ which gives the claim.
Now fix $1 < \lambda < \frac{7}{8} + \frac{\sqrt{17}}{8}$. Then we have that

$$\#\{|d| < X : S_d \neq 0\} =$$
$$= \#\{|d| < X : \ S_d \neq 0, \ w_0(d) \geq w_2(d)\} + \#\{|d| < X : S_d \neq 0, \ w_2(d) > w_0(d)\}$$
$$\leq \#\{|d| < X : \ w_0(d) \geq w_2(d)\} + \#\{|d| < X : S_d \neq 0, \ w_2(d) > w_0(d)\}$$
$$\ll X\log(X)^{-0.042} + \sum_{|d|<X} \lambda^{w_2(d)-w_0(d)}(\#S_d - 1),$$

where d varies through squarefree integers. The result now follows from Proposition 3.3.9.

□

3.4 An example

In this section, we present an example of a subfamily of quadratic twists for which the 2-Selmer groups' statistical behavior differs from the family of all twists'. Particularly, $\mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is non-trivial for a positive proportion of d in our subfamily.

Take $K = \mathbb{Q}(\sqrt{\theta})$ to be an imaginary quadratic number field in which 2 is inert and has class number 1. Thus, $\theta \in \{-3, -11, -19, -43, -67, -163\}$.

Further, take

$$E : y^2 = x^3 - x$$

to be the congruent number curve.

Due to [12, Proposition 9.3], we have the following description of $S^2(E_p/K)$: For every prime number p there exist non-negative integers $e_1(E_p/K)$ and $e_2(E_p/K)$ such that we have a $G = \mathrm{Gal}(K/\mathbb{Q})$-module isomorphism

$$S^2(E_p/K) \cong \mathbb{F}_2^{e_1(E_p/K)} \oplus \mathbb{F}_2[G]^{e_2(E_p/K)}.$$

Example 3.4.1. The density of primes p for which $e_1(E_p/K) = e_1$ and $e_2(E_p/K) = e_2$ is as follows:

$$\lim_{X\to\infty} \frac{\#\{p \leq X \text{ prime } : e_1(E_p/K) = e_1 \text{ and } e_2(E_p/K) = e_2\}}{\#\{p \leq X \text{ prime }\}} = \begin{cases} \frac{9}{16} & (e_1, e_2) = (4, 0) \\ \frac{1}{16} & (e_1, e_2) = (2, 2) \\ \frac{1}{4} & (e_1, e_2) = (2, 1) \\ \frac{1}{8} & (e_1, e_2) = (2, 0). \end{cases}$$

In particular, the proportion of prime twists for which the G-action on $S^2(E_p/K)$ is non-trivial is equal to $\frac{5}{16}$. To see why it is correct refer to [12, Section 9].

Appendix A

Group Gohomology

In this appendix, we discuss the main properties of group cohomology (H^0 and H^1) that are used in Chapters 2 and 3.

A.1 Cohomology of finite groups

Let G be a finite group, and let M be an abelian group. An *action* of G on M is a map $G \times M \longrightarrow M$, $(\sigma, m) \mapsto m^\sigma$ such that

$$m^1 = m, \qquad (m + m')^\sigma = m^\sigma + m'^\sigma, \qquad (m^\sigma)^\tau = m^{\sigma\tau}.$$

for all $\sigma, \tau \in G$ and all $m, m' \in M$. A *G-module* is an abelian group together with an action of G.
Let M and N be G-modules. A *G-module homomorphism* is a homomorphism

$$\phi : M \longrightarrow N$$

such that

$$\phi(m^\sigma) = \phi(m)^\sigma$$

for all $m \in M, \sigma \in G$.

Definition A.1.1. *The 0^{th} cohomology group of the G-module M, denoted by $H^0(G, M)$, is the set*

$$H^0(G, M) = \{m \in M : m^\sigma = m \text{ for all } \sigma \in G\}.$$

$H^0(G, M)$ is the submodule of M consisting of all elements that are fixed by G.
Let

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0 \tag{A.1}$$

be an exact sequence of G-modules, namely, the maps ϕ and ψ are G-module homomorphisms such that ϕ is injective, ψ is surjective, and $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$. We claim that the following is also an exact sequence

$$0 \longrightarrow H^0(G, P) \xrightarrow{\phi} H^0(G, M) \xrightarrow{\psi} H^0(G, N) \tag{A.2}$$

We first show that $\phi(H^0(G, P)) \subseteq H^0(G, M)$. We take any element $p \in H^0(P, G)$, then $\phi(p)^\sigma = \phi(p^\sigma) = \phi(p)$ for all $\sigma \in G$, which implies that $\phi(p) \in H^0(M, G)$,

since p is arbitrary we get that $\phi(H^0(G,P)) \subseteq H^0(G,M)$. Similarly, we have that $\psi(H^0(G,M)) \subseteq H^0(G,N)$. Injectivity of ϕ in (A.2) follows from the injectivity of ϕ in (A.1). Now we have to check the equality $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$ in (A.2). We have that $\psi(\phi(p)) = 0$ for all $p \in P$, particularly, $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(\psi)$ in (A.2). Now take any element $m \in \mathrm{Ker}(\phi)$, then by the exactness of (A.1), there exists an element $p \in P$ such that $\phi(p) = m$, so $\phi(p^\sigma) = \phi(p)^\sigma = m^\sigma = m = \phi(p)$, now by the injectivity of ϕ, we get that $p \in H^0(G,P)$. Finally, we get $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$ in (A.2).

We now define the 1^{st} cohomology group of the G-module M.

Definition A.1.2. *Let M be a G-module. The group of 1-cochains from G to M is defined by*

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

The group of 1-cocycles from G to M is defined by

$$Z^1(G,M) = \{\xi \in C^1(G,M) : \xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau) \text{ for all } \sigma,\tau \in G\}.$$

The group of 1-coboundaries from G to M is defined by

$$B^1(G,M) = \{\xi \in C^1(G,M) : \text{ there exists } m \in M \text{ such that } \xi(\sigma) = m^\sigma - m \text{ for all } \sigma \in G\}$$

Now we claim that $B^1(G,M) \subset Z^1(G,M)$. Take 1-coboundary $\xi \in B^1(G,M)$, then for some $m \in M$ we have that $\xi(\sigma\tau) = m^{\sigma\tau} - m = (m^\sigma)^\tau - m = (m^\sigma)^\tau - m^\tau + m^\tau - m = \xi(\sigma)^\tau + \xi(\tau)$ for all $\sigma,\tau \in G$. Hence we get that $B^1(G,M) \subset Z^1(G,M)$.

Definition A.1.3. *The 1^{st} cohomology group of the G-module M is the quotient group*

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

Example A.1.4. When G acts trivially on M, i.e., $m^\sigma = m$ for all $\sigma \in G$ and $m \in M$, a 1-cocycle is simply a homomorphism of groups and every 1-coboundary is zero. Hence $H^1(G,M) = \mathrm{Hom}(G,M)$.

Proposition A.1.5. *Let*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

be an exact sequence of G-modules. Then there is a long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(G,P) & \longrightarrow & H^0(G,M) & \xrightarrow{\phi} & H^0(G,N) \\ & & & \overset{\delta}{\swarrow} & & & \\ & & H^1(G,P) & \longrightarrow & H^1(G,M) & \longrightarrow & H^1(G,N) \end{array}$$

where δ is defined as follows:
Let $n \in H^0(G,N)$. Then there exists an $m \in M$ such that $\psi(m) = n$, and $m^\sigma - m \in P$ for all $\sigma \in G$, the map $\sigma \mapsto m^\sigma - m : G \longrightarrow P$ is a 1-cocycle, whose class we define to be $\delta(n)$.

Proof. We already proved the exactness of the sequence

$$0 \longrightarrow H^0(G,P) \xrightarrow{\phi} H^0(G,M) \xrightarrow{\psi} H^0(G,N)$$

The map δ is defined such that the sequence is exact at $H^1(G,P)$. The remaining part is also straightforward (see [16, p.417], for details). □

Let H be a subgroup of G. Then any G-module becomes H-module. Moreover, if $\xi : G \longrightarrow M$ is a 1-cochain, then we obtain the restricted 1-cochain from H to M. This process takes cocycles to cocycles, coboundaries to coboundaries, in this way, we obtain a *restriction homomorphism*

$$\mathrm{Res} : H^1(G,M) \longrightarrow H^1(H,M).$$

Remark A.1.6. Let H be a normal subgroup of a group G, and let M be a G-module. Then the submodule $H^0(H,M)$ has a natural structure as G/H-module. Let $\xi : G/H \longrightarrow H^0(H,M)$ be a 1-cochain, then composing with the projection $G \longrightarrow G/H$ and with the inclusion $H^0(H,M) \subset M$ gives a cochain from G to M

$$G \longrightarrow G/H \xrightarrow{\xi} H^0(H,M) \xhookrightarrow{i} M.$$

In this way, we obtain an *inflation homomorphism*

$$\mathrm{Inf} \ : H^1(G/H, H^0(H,M)) \longrightarrow H^1(G,M)$$

Proposition A.1.7. *Let M be a G-module and let H be a normal subgroup of G. Then the following sequence is exact:*

$$0 \longrightarrow H^1(G/H, H^0(H,M)) \xrightarrow{\mathrm{Inf}} H^1(G,M) \xrightarrow{\mathrm{Res}} H^1(H,M).$$

Proof. Let $\xi : G/H \longrightarrow M^H$ be a 1-cocycle, then ξ induces

$$\bar{\xi} : G \to G/H \to H^0(G,M) \to M$$

which is 1-cocycle, and class $\bar{\xi}$ is the inflation of class of ξ. Then if $\bar{\xi}$ is a coboundary, there exists $m \in M$ such that $\bar{\xi}(\sigma) = m^\sigma - m$ for all $\sigma \in G$. But $\bar{\xi}$ is constant on the cosets of H, hence

$$m^\sigma - m = m^{\sigma\tau} - m \text{ for all } \sigma \in H$$

i.e. $m^\sigma = m$ for all $\sigma \in H$. So $m \in H^0(M,G)$ and therefore ξ is a boundary.
From the definition it is clear that

$$\mathrm{Res} \circ \mathrm{Inf} = 0.$$

Lastly, we prove the exactness at $H^1(G,M)$. Let $\xi : G \longrightarrow M$ be a 1-cocycle whose restriction to H is a coboundary; then there exists $m \in M$ such that $\xi(\tau) = m^\tau - m$ for all $\tau \in H$. Subtracting from ξ to the coboundary $\sigma \mapsto m^\sigma - m$, we are reduced to the case where $\xi|_H = 0$. The formula

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)$$

then shows that ξ is constant on the cosets of H, and then that the image of ξ is contained in $H^0(M,H)$. Thus ξ is the inflation of a 1-cocycle $G/H \longrightarrow H^0(M,G)$, and the proof is complete. □

A.2 Galois Cohomology

Let K be a perfect field, and let $\bar{K}$ be an algebraic closure of K. The group $G_{\bar{K}/K}$ of automorphisms of $\bar{K}$ fixing the elements of K has a natural topology, called the *Krull topology*, for which a subgroup is open if and only if it is the subgroup fixing a finite extension of K. When $G_{\bar{K}/K}$ endowed with its Krull topology, then $G_{\bar{K}/K}$ is called the Galois group of $\bar{K}$ over K.

Definition A.2.1. *A $G_{\bar{K}/K}$-module M is said to be discrete if the map $G_{\bar{K}/K} \times M \longrightarrow M$ is continuous relative to the discrete topology on M and the Krull topology on G. This is equivalent to requiring that for all $m \in M$, the stabilizer of m,*

$$\{\sigma \in G_{\bar{K}/K} : m^\sigma = m\},$$

is a subgroup of finite index in $G_{\bar{K}/K}$.

Example A.2.2. $M = \bar{K}$ and $M = \bar{K}^*$ are $G_{\bar{K}/K}$-modules under the natural action of Galois group $G_{\bar{K}/K}$. It is because for any $x \in \bar{K}$, the extension $K(x)/K$ is finite, so the stabilizer of x has a finite index in $G_{\bar{K}/K}$.

We now define 0^{th} and 1^{st} cohomology groups of a $G_{\bar{K}/K}$-module in the same way as in the case of finite groups.

Definition A.2.3. *The 0^{th} cohomology group of the $G_{\bar{K}/K}$-module M is the set*

$$H^0(G_{\bar{K}/K}, M) = \{m \in M : m^\sigma = m \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Let M be a $G_{\bar{K}/K}$-module, then we say that a map $\xi : G_{\bar{K}/K} \longrightarrow M$ is *continuous* if is is again continuous for the Krull topology on $G_{\bar{K}/K}$ and the discrete topology on M. The *group of continuous 1-cocycles from $G_{\bar{K}/K}$ to M* is the group of continuous maps $\xi : G_{\bar{K}/K} \longrightarrow M$ such that

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau).$$

and we denote it by $Z^1_{\text{cont}}(G_{\bar{K}/K}, M)$. As an example, we can give the following (coboundary) maps

$$\sigma \mapsto m^\sigma - m$$

which are continuous since M has the discrete topology.

Definition A.2.4. *The 1^{st} cohomology group of the $G_{\bar{K}/K}$-module M is the quotient group*

$$H^1(G_{\bar{K}/K}, M) = \frac{Z^1_{\text{cont}}(G_{\bar{K}/K}, M)}{B^1(G_{\bar{K}/K}, M)}.$$

where $B^1(G_{\bar{K}/K}, M)$ is the group of 1-coboundaries.

Example A.2.5. When $G_{\bar{K}/K}$ acts trivially on M, i.e., $m^\sigma = m$ for all $\sigma \in G_{\bar{K}/K}$ and $m \in M$, we have that $H^0(G_{\bar{K}/K}, M) = M$ and $H^1(G_{\bar{K}/K}, M)$ is just the group of continuous homomorphisms from $G_{\bar{K}/K}$ to M.

The fundamental exact sequences in the Propositions A.1.5 and A.1.7 carry over word by word from finite groups to groups $G_{\bar{K}/K}$ with Krull topology.

Proposition A.2.6. *Let*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

be an exact sequence of $G_{\bar{K}/K}$-modules. Then there is a long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G_{\bar{K}/K}, P) \longrightarrow H^0(G_{\bar{K}/K}, M) \xrightarrow{\phi} H^0(G_{\bar{K}/K}, N) \\ \xrightarrow{\delta} H^1(G_{\bar{K}/K}, P) \longrightarrow H^1(G_{\bar{K}/K}, M) \longrightarrow H^1(G_{\bar{K}/K}, N) \end{aligned}$$

where δ is defined as in the Proposition A.1.5.

As usual, we define the restriction and inflation maps for M a discrete $G_{\bar{K}/K}$-module. Let L/K be a finite Galois extension. Then $G_{\bar{K}/L}$ is a subgroup of finite index in $G_{\bar{K}/K}$, so that M is naturally a discrete $G_{\bar{K}/L}$-module, and this allows us to define the *restriction map* from $H^1(G_{\bar{K}/K}, M)$ to $H^1(G_{\bar{K}/L}, M)$,

$$\mathrm{Res} : H^1(G_{\bar{K}/K}, M) \longrightarrow H^1(G_{\bar{K}/L}, M).$$

$G_{\bar{K}/L}$ is a normal subgroup of $G_{\bar{K}/K}$, and the quotient $G_{\bar{K}/K}/G_{\bar{K}/L}$ is finite group $G_{L/K}$. Then the submodule $H^0(G_{\bar{K}/L}, M)$ has a natural stucture as a $G_{L/K}$-module. Let $\xi : G_{L/K} \longrightarrow H^0(G_{\bar{K}/L}, M)$ be a 1-cocycle, then composing with the projection $G_{\bar{K}/K} \longrightarrow G_{L/K}$ and with the inclusion $H^0(G_{\bar{K}/L}, M) \subset M$ gives a 1-cocycle from $G_{\bar{K}/K}$ to M

$$G_{\bar{K}/K} \longrightarrow G_{L/K} \xrightarrow{\xi} H^0(G_{\bar{K}/L}, M) \xhookrightarrow{i} M.$$

This gives an *inflation map*

$$\mathrm{Inf} \ : H^1(G_{L/K}, H^0(G_{\bar{K}/L}, M)) \longrightarrow H^1(G_{\bar{K}/K}, M).$$

Proposition A.2.7. *Let M be a $G_{\bar{K}/K}$-module. Then the following sequence is exact:*

$$0 \longrightarrow H^1(G_{L/K}, H^0(G_{\bar{K}/L}, M)) \xrightarrow{\mathrm{Inf}} H^1(G_{\bar{K}/K}, M) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L}, M).$$

Proof. The proof is identically the same with the proof of Proposition A.1.7. □

We finish the section with the following useful facts about the cohomology of the additive and multiplicative groups of a field K.

Proposition A.2.8. *Let K be a field and m be an integer. Then we have*
(a) $H^1(G_{\bar{K}/K}, \bar{K}) = 0$.
(b) $H^1(G_{\bar{K}/K}, \bar{K}^*) = 0$.
(c) Assume that either $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K)$ *does not divide m. Then*

$$H^1(G_{\bar{K}/K}, \mu_m) \cong K^*/(K^*)^m$$

Proof. For the (a) and (b), see [16, p.420].
(c) Consider the following exact sequence of $G_{\bar{K}/K}$-modules

$$1 \longrightarrow \mu_m \longrightarrow \bar{K}^* \xrightarrow{z \to z^m} \bar{K}^* \longrightarrow 1.$$

Then from Proposition A.2.6 we have the long exact sequence

$$\longrightarrow K^* \xrightarrow{z \to z^m} K^* \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mu_m) \longrightarrow H^1(G_{\bar{K}/K}, \bar{K}^*) \longrightarrow$$

From (b) we have that $H^1(G_{\bar{K}/K}, \bar{K}^*) = 0$, thus we get the desired result. □

Appendix B

Valuations and Completions

In this appendix, we discuss the theory of valuations and completions, and the places of a number field mainly following the [5, Chapter 2].

B.1 Valuations and completions

Definition B.1.1. *Let K be a field. A valuation or an absolute value on K is a function*

$$|\ |: K \longrightarrow \mathbb{R}$$

satisfying the properties:
(i) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
(ii) $|xy| = |x||y|$ for all $x, y \in K$,
(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Two absolute values $|\ |_1$ and $|\ |_2$ are called *equivalent* if there is a positive real number c such that $|\ |_1 = |\ |_2^c$.

Definition B.1.2. *The absolute value $|\ |$ is called non-archimedean if $|n| \leq 1$ for all $n \in \mathbb{Z}$. Otherwise, it is called Archimedean.*

The following Proposition gives us another equivalent definition of non-archimedean absolute values.

Proposition B.1.3. *The absolute value $|\ |$ is non-archimedean if and only if it satisfies the strong triangle inequality*

$$|x + y| \leq \max\{|x|, |y|\}.$$

Proof. Assume that the strong triangle inequality holds, then we have that

$$|n| = |1 + 1 + ... + 1| \leq |1| = 1$$

for all natural number n. Using the equality $|n| = |-n|$ for all $n \in \mathbb{Z}$, we get $|n| \leq 1$ for all $n \in \mathbb{Z}$. Conversely, let $|n| \leq 1$ for all $n \in \mathbb{Z}$. Let $x, y \in K$ and $n \in \mathbb{Z}$, then

$$|x + y|^n = |\sum_{k=0}^{n} C_n^k x^{n-k} y^k| \leq \sum_{k=0}^{n} |x|^{n-k}|y|^k \leq (n + 1)\ \max\{|x|^n, |y|^n\}.$$

So, for any $n \in \mathbb{N}$ we get

$$|x+y| \leq \sqrt[n]{n+1}\, \max\{|x|, |y|\}$$

and hence $|x+y| \leq \max\{|x|, |y|\}$ by letting $n \to \infty$. □

Example B.1.4. In $\mathbb{Q}$ we have the following absolute values:
1) The standard Archimedean absolute value $|\ |$ (also denoted by $|\ |_\infty$), which is defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

2) p-adic absolute value $|\ |_p$, for each prime number p, defined by

$$|x|_p = p^{-\mathrm{ord}(x)}$$

$\mathrm{ord}(x)$ is an integer r such that $x = p^r a/b$, where a and b are integers relatively prime to p. p-adic absolute value satisfies (i) and (ii) of the Definition B.1.2, and the strong triangle inequality, implies that $|\ |_p$ is a non-archimedean absolute value.

We now discuss the completion of a field with respect to an absolute value.

Definition B.1.5. *Let K be a field and $|\ |$ be an absolute value on K. Then K is called complete with respect to the absolute value $|\ |$ if every Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ in K converges to an element $a \in K$, namely*

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Recall that a sequence $\{a_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence if for every $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that

$$|a_n - a_m| < \epsilon \text{ for all } n, m \geq N.$$

From any valued field $(K, |\ |)$ we can get a complete valued field $(\hat{K}, |\ |)$ by the process of completion, in the same way as $\mathbb{R}$ is constructed from $\mathbb{Q}$ with respect to the usual absolute value.

Let R be the ring of all Cauchy sequences of $(K, |\ |)$, consider the maximal ideal $\mathfrak{m}$ of all nullsequences with respect $|\ |$, and define

$$\hat{K} := R/\mathfrak{m}.$$

We can embed the field K into $\hat{K}$ by sending every $a \in K$ to the class of the constant Cauchy sequence $(a, a, a, ...)$. The absolute value $|\ |$ is extended from K to $\hat{K}$ by giving the element $a \in \hat{K}$ which is represented by Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ the value

$$|a| := \lim_{n\to\infty} |a_n|.$$

Note that the limit exists since $||a_n| - |a_m|| \leq |a_n - a_m|$ which implies that $|a_n|$ is a Cauchy sequence in $\mathbb{R}$. One easily proves that $\hat{K}$ is complete with respect to the extended $|\ |$.

We denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to p-adic absolute value. Due to A. Ostrowski, we have the following important theorem about the classification of absolute values on $\mathbb{Q}$.

Theorem B.1.6 (A. Ostrowski)**.** *Any absolute value on $\mathbb{Q}$ is equivalent to one of the following: a p-adic absolute value for some prime number p, standard Archimedean absolute value $|\ |_\infty$, or the trivial absolute value $|\ |_0$ which is defined by $|x|_0 = 1$ for all $x \neq 0$.*

Proof. See [5, Chapter 2]. □

B.2 Places of a number field

Fix a number field K. In this section, we extend the absolute values on $\mathbb{Q}$ to absolute values on the number field K and classify these extended absolute values.

Definition B.2.1. *A place of a number field K is an equivalent class of absolute values on K. We denote by M_K the set of all places, by M_K^∞ the set of Archimedean places, and by M_K^0 the set of non-archimedean places.*

The absolute values on K are divided into Archimedeans and non-archimedeans. The Archimedean absolute values arise in the following way: Let $n = [K : \mathbb{Q}]$, then K admits exactly n distinct embeddings $\sigma : K \hookrightarrow \mathbb{C}$. Each such embedding is used to define an absolute value on K according to the setting

$$|x|_\sigma = |\sigma(x)|_\infty$$

where $|\ |_\infty$ is the usual absolute value on $\mathbb{C}$. Note that two conjugate embeddings define the same absolute value.

The non-archimedean absolute values on K arise in much the same way as they do on $\mathbb{Q}$. However, one may not be able to uniquely factor elements of K into primes. The idea is to work with the prime ideals of the ring of integer O_K instead since we know that every ideal in O_K admits a unique (up to reordering) prime factorization. Let $\mathfrak{p}$ be a prime ideal of O_K, then there exists a unique prime number p such that the prime ideal $\mathfrak{p}$ lies above p. Now for every element $x \in O_K$, we define

$$|x|_\mathfrak{p} = p^{-\mathrm{ord}_\mathfrak{p} x / \mathrm{ord}_\mathfrak{p} p}.$$

where $\mathrm{ord}_\mathfrak{p} x$ is the order of $\mathfrak{p}$ in the prime factorization of the ideal (x). One can check that it is indeed an absolute value on K and we call it as $\mathfrak{p}$-adic absolute value.

Interestingly, thanks to the extended A. Ostrowki's theorem, these are the only absolute values on a number field up to equivalence.

Theorem B.2.2 (A. Ostrowski)**.** *Let K be a number field. Then any nontrivial absolute value on K is equivalent to one of the following: the Archimedean absolute values which come from the embeddings $\sigma : K \hookrightarrow \mathbb{C}$ defined above or the non-archimedean absolute value $|\ |_\mathfrak{p}$ for a prime ideal of O_K defined above.*

Proof. See, [5, Chapter 2]. □

We refer to the real embedding $\sigma : K \longrightarrow \mathbb{R}$, the complex conjugate pairs $\{\sigma, \bar{\sigma}\}$ of the complex embeddings $\sigma : K \longrightarrow \mathbb{C}$, and the nonzero prime ideals in the ring O_K as *real places, complex places* and *non-archimedean places*, respectively (we skip the trivial absolute value since it is mostly irrelevant).

Remark B.2.3. Let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals in O_K. Then $\mathfrak{p}$-adic absolute value and $\mathfrak{q}$-adic absolute value are inequivalent because, by the Chinese remainder theorem, there exists an element $x \in O_K$ such that $x \equiv 0 (\text{mod } \mathfrak{p})$ and $x \equiv 1 (\text{mod } \mathfrak{q})$, so the $\mathfrak{p}$-adic absolute value of x is less than 1 and the $\mathfrak{q}$-adic absolute value of x equals 1, and so these two absolute values are inequivalent by the definition.

Example B.2.4. For $K = \mathbb{Q}$, by the Theorem B.1.6, the following non-trivial absolute values occur: the usual absolute value, denoted by $|\ |_\infty$, the p-adic absolute value for any prime number p. If we consider the fact that any two p-adic and q-adic absolute values are inequivalent by the Remark B.2.3, then we could conclude that

$$M_{\mathbb{Q}} = \{p : p \text{ prime number}\} \cup \{\infty\}.$$

Bibliography

[1] M. F. Atiyah and C. T. C. Wall. *Cohomology of groups, Algebraic number theory.* Thompson, Washington, DC, 1967.

[2] C. W. Curtis and I. Reiner. *Methods of representation theory*, volume 1. John Wiley & Sons, New York, 1990.

[3] F. Étienne and K. Jürgen. On the 4-rank of class groups of quadratic number fields. *Inventiones mathematicae*, 167(3), 2007.

[4] R. Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977.

[5] A. Schmidt J. Neukirch and K. Wingberg. *Cohomology of number fields.* Springer, Berlin, 2 edition, 2008.

[6] K. Kramer. Arithmetic of elliptic curves upon quadratic extension. *Transactions of the American Mathematical Society*, 264(1):121–135, 1981.

[7] B. Mazur. Modular curves and the Eisenstein ideal. *Publications mathématiques de l'IHÉS*, 47:33–186, 1977.

[8] B. Mazur and K. Rubin. Kolyvagin systems. *Memoirs of the American Mathematical Society*, 168, 2004.

[9] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics*, 166(2):579–612, 2007.

[10] J. S. Milne. On the arithmetics of abelian varieties. *Inventiones Mathamaticae*, 17:177–190, 1972.

[11] J. S. Milne. *Fields and Galois theory.* 2022.

[12] A. Morgan and R. Paterson. On 2-Selmer groups of twists after quadratic extension. *London Mathematical Society*, 105:1110–1166, 2022.

[13] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *American Mathematical Society*, 25(1):245–269, 2012.

[14] I. R. Shafarevich. *Basic algebraic geometry.* Springer-Verlag, Berlin, 1977.

[15] P. Shiu. A Brun-Ritchmarch theorem for multiplicative functions. *Journal for Pure and Applied Mathematics*, 313:161–170, 1980.

[16] J. H. Silverman. *The arithmetic of elliptic curves.* Springer, New York, 2 edition, 2016.

[17] L. C. Washington. *Galois cohomology, modular forms and Fermat's last theorem.* Springer, New York, 1997.

[18] Ch. A. Weibel. *An introduction to homological algebra.* Cambridge University Press, Cambridge, 1994.

[19] A. Weil. On algebraic groups and homogeneous spaces. *American Journal of Mathematics*, 77(2):493–512, 1995.

[20] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, 141:443–551, 1995.