

**Università degli Studi di Padova**

---

**DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”**

**Corso di Laurea Magistrale in Mathematics**

**Kolyvagin's work  
on Elliptic Curves**

**Relatore:  
Prof. Matteo Longo**

**Candidato: Pietro Serafin  
Matricola: 2087939**

---

**Anno Accademico 2024/2025**

# Contents

<b>1</b>	<b>Elliptic Curves</b>	<b>1</b>
1.1	Elliptic curves over $\mathbb{C}$	4
1.1.1	Complex Multiplication	6
1.2	Elliptic curves and modular curves	7
1.2.1	Heegner Points	10
1.3	Elliptic curve as abelian variety	13
1.3.1	Galois cohomology	13
1.3.2	Selmer group and Šafarevič-Tate group	17
<b>2</b>	<b>Class Field Theory</b>	<b>20</b>
2.1	Orders of $K$	23
2.2	Ring class fields of conductor $c$	25
2.3	Hilbert class field	28
2.4	Idèlic formulation of class field theory	29
2.5	Application of the class field theory to the elliptic curves	31
<b>3</b>	<b>Duality Theorems</b>	<b>33</b>
3.1	Duality of local class field theory	33
3.2	Duality of global class field theory	35
<b>4</b>	<b>Euler System of Heegner Points</b>	<b>38</b>
4.1	Heegner points of the conductor $n$	38
4.2	Kolyvagin's cohomology classes	47
4.3	Localization of Kolyvagin's classes	51
<b>5</b>	<b>Kolyvagin's work on Modular Elliptic Curves</b>	<b>56</b>
5.1	Description of $Sel(E/K)_p$	56
5.2	Birch and Swinnerton-Dyer conjecture and Kolyvagin's theorem	64
5.2.1	L-series and the conjecture of Birch and Swinnerton-Dyer	64
5.2.2	Kolyvagin's theorem	69
	<b>Bibliography</b>	<b>75</b>

# Introduction

The aim of this Master Thesis is to discuss the nature of rational points of an elliptic curve over an imaginary quadratic field under certain hypotheses. In particular, we want to analyze Kolyvagin's results on Birch and Swinnerton-Dyer conjecture. To do so, we focus on the article [7] by Benedict H. Gross.

Let  $K$  be a number field and  $E$  be an elliptic curve. We define the *Mordell-Weil* group  $E(K)$  to be the group of rational points of  $E$  over  $K$ , i.e., the group

$$E(K) = \{(x, y) \in E : x \in K, y \in K\}.$$

At the beginning of the 20th century, the following theorem was stated and proved.

**Theorem 0.1.** (*Mordell-Weil*) *Let  $K$  be a number field and let  $E/K$  be an elliptic curve. Then the group  $E(K)$  is finitely generated.*

The Mordell-Weil theorem says that the group  $E(K)$  can be written in the form

$$E(K) = E_{tors}(K) \times \mathbb{Z}^r,$$

where the torsion group  $E_{tors}(K)$  is finite and  $r$ , defined to be the *rank* of the group  $E(K)$ , is a non-negative integer.

To simplify the study of  $E(K)$ , we may see the quotient group  $E(K)/mE(K)$ , with  $m \geq 2$  integer. Using the weak formulation of the Mordell-Weil theorem, we have that  $E(K)/mE(K)$  is a finite group (see [14, VIII, Th. 1.1]), and if we consider  $m$  coprime with  $\#E_{tors}(K)$ , we have that  $E(K)/mE(K) \cong (\mathbb{Z}/m\mathbb{Z})^r$ .

It is of particular interest to study the rank of  $E(K)$ ; in 1960 mathematicians Bryan Birch and Peter Swinnerton-Dyer enunciated a remarkable conjecture that relates the rank of  $E(K)$  with the analytical knowledge that provides the  $L$ -series of  $E$ . More precisely, this conjecture predicts that the integer  $r' = ord_{s=1} L(E/\mathbb{Q}, s)$  is equal to the rank  $r$  of  $E(\mathbb{Q})$ .

We are interested in verifying this conjecture for  $r' = 1$ , and then we restrict the study under the hypothesis that  $L(E/\mathbb{Q}, s)$  has a zero at  $s = 1$  of order 1. We assume that  $E$  is an elliptic curve of conductor  $N$  and  $K = \mathbb{Q}(\sqrt{-D})$  is an imaginary

quadratic field of discriminant  $-D < 0$ , where all prime factors of  $N$  are split. We define  $y_K$  as the basic Heegner point in  $E$  (see Chapter 4, p.40). From the work [6] of the mathematicians Benedict Gross and Don Bernard Zagier, we know that assuming the previous hypothesis is equivalent to requiring that the point  $y_K$  is of infinite order.

Our main purpose is to prove Kolyvagin's theorem, which states that if such a point  $y_K$  is non-torsion, then the rank of  $E(K)$  is equal to 1.

I hope, with this work, to highlight the fascinating way in which different mathematical arguments join together to converge in the proof of Kolyvagin's theorem.

In the first three chapters we give a general overview of the main results we will refer to later, which come from the study of elliptic curves, class field theory and duality theory. In particular, we focus on the definition of Heegner points, on complex multiplication theory and on its application to class field theory. By Galois cohomology, we also introduce the Selmer group  $Sel(E/K)_p$  and the Šafarevič-Tate group  $\text{III}(E/K)_p$ , which are subgroups, respectively, of the 1<sup>st</sup> cohomology groups  $H^1(K, E_p)$  and  $H^1(K, E)_p$ . They are in the exact sequence

$$0 \rightarrow E(K)/pE(K) \rightarrow Sel(E/K)_p \rightarrow \text{III}(E/K)_p \rightarrow 0,$$

and this suggests that they play a central role in the description of  $E(K)/pE(K)$ .

In Chapter 4, we actually begin to analyze analyzing the article of Gross. By theory of complex multiplication, we define the Heegner points  $y_n$  of conductor  $n$ , and by these we define certain cohomology classes  $c(n) \in H^1(K, E_p)$  and  $d(n) \in H^1(K, E)_p$ , analyzing their local and global properties. Following the idea of Kolyvagin, in Chapter 5 we see that all these classes  $c(n)$  are in  $Sel(E/K)_p$ , we use them to bound the order of  $Sel(E/K)_p$  and this fact allows us to prove Kolyvagin's theorem.

# 1 Elliptic Curves

As a first approach to the study of Kolyvagin's work, I would start with the central topic: elliptic curves. The main concept I would like to convey with this first chapter is the great versatility with which elliptic curves can be studied. We will see different ways in which an elliptic curve can be defined, and we will discover how the various aspects contribute to the proof of the main theorem, expressed in Chapter 5.

We will initially focus on the construction of an elliptic curve over the field of complex numbers and imaginary quadratic fields. This will allow us to introduce the theory of complex multiplication. Next, we will present elliptic curves as modular curves, which will allow us to define a special set of points on them, called Heegner points, and their properties. As a last step, using the structure of abelian variety of elliptic curves, we will introduce the Galois cohomology and, consequently, the Selmer group and the Šafarevič-Tate group.

Let us therefore begin by describing elliptic curves and highlighting their characteristics necessary to understand what follows. For further information, see [14]. Let  $K$  be a perfect field of characteristic different from 2 or 3,  $\bar{K}$  be a fixed algebraic enclosure of  $K$  and  $G_{\bar{K}/K}$  the Galois group of  $\bar{K}/K$ .

**Definition 1.1.** An *elliptic curve* is a pair  $(E, O)$ , where  $E$  is a non-singular curve of genus one and  $O \in E$ . The elliptic curve  $(E, O)$  is *defined* over  $K$ , written  $E/K$ , if  $E$  is defined over  $K$  as a curve, and  $O \in E(K)$ , the group of  $K$ -rational points on the elliptic curve  $E/K$ .

We denote elliptic curves by  $E$ , the point  $O$  being understood. In addition to the previous definition, we know that every elliptic curve can be written as the locus in  $\mathbb{P}^2$  of a cubic equation with only one point, the base point  $O$ , on the line at  $\infty$ . These particular equations, called *Weierstrass equations*, are of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \in \bar{K}[X, Y]$$

$O = [0, 1, 0]$  and  $a_1, \dots, a_6 \in \bar{K}$ . The following proposition shows that every elliptic curve can be written as a plane curve and, conversely, every smooth Weierstrass

plane cubic curve is an elliptic curve.

**Proposition 1.2.** [14, III, Prop. 3.1] *Let  $E$  be an elliptic curve over  $K$ . The following statements hold:*

(a) *There exist functions  $x, y \in K(E)$  such that the map*

$$\phi : E \longrightarrow \mathbb{P}^2, \phi = [x, y, 1]$$

*gives an isomorphism of  $E/K$  onto a curve determined by a Weierstrass equation*

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

*with coefficients  $a_1, \dots, a_6 \in K$  and satisfying  $\phi(O) = [0, 1, 0]$ . Functions  $x, y$  are called Weierstrass coordinates for the elliptic curve  $E$*

(b) *Conversely, every smooth cubic curve  $C$  given by a Weierstrass equation as in (a) is an elliptic curve defined over  $K$  with base point  $[0, 1, 0]$ .*

Studying these equations provides a more concrete algebraic understanding of elliptic curves, giving us valuable insight into the elliptic curve in question, like singularity and reductions. With the above notation, using the nonhomogeneous coordinates  $x = X/Z$  and  $y = Y/Z$ , we can simplify the equation by completing the square by the substitution  $y \rightarrow \frac{1}{2}(y - a_1x - a_3)$ . Thus we obtain the equation of the form:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where  $b_2 = a_1^2 + 4a_2$ ,  $b_4 = 2a_4 + a_1a_3$ ,  $b_6 = a_3^3 + 4a_6$ , and we can define the following quantities:

- The *discriminant* of the Weierstrass equation

$$(\Delta) = -b_2^2b_6 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

- The  $j$ -invariant of  $E$ :

$$j = \frac{(b_2^2 - 24b_4)^3}{\Delta}$$

- The *invariant differential* associated to Weierstrass equation

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

In particular, the  $j$ -invariant is invariant under isomorphisms of elliptic curves and under modular transformations that preserve the structure of the elliptic curve. Furthermore, for every  $j_0 \in \overline{K}$  there exists an elliptic curve defined over  $K(j_0)$  whose  $j$ -invariant is equal to  $j_0$ .

Thus,  $E \subset \mathbb{P}^2$  consists of the points  $P = (x, y)$  satisfying the Weierstrass equation, together with the point  $O = [0, 1, 0]$  at infinity. Now, using *composition law*, define the addition operation  $\hat{+} : E \times E \rightarrow E$ ,  $(P, Q) \rightarrow P \hat{+} Q$ , which associates to each pair of points  $P, Q \in E$  the intersection  $P \hat{+} Q$  between  $E$  and the line through  $O$  and  $R$ , where  $R$  is the intersection between  $E$  and the line through  $P$  and  $Q$ . With this notation, the set  $(E, \hat{+})$  of points of an elliptic curve with addition is an abelian group with identity  $O$ .

As the last element of the general theory of elliptic curves, we now define isogenies.

**Definition 1.3.** Let  $E_1, E_2$  be elliptic curves. An *isogeny* from  $E_1$  to  $E_2$  is a morphism  $\phi : E_1 \rightarrow E_2$  that satisfies  $\phi(O) = O$ .

Elliptic curves are an abelian group, and then maps between them form groups. The set of isogenies from  $E_1$  to  $E_2$  is denoted by  $Hom(E_1, E_2)$ , and then  $End(E)$  is the set of isogenies from  $E$  to itself. Specifically, they are torsion-free  $\mathbb{Z}$ -modules. Thanks to the abelian group structure defined above, we define a particular set of isogenies, called *multiplication-by- $m$  isogenies*. For each  $m \in \mathbb{Z}$ , we define the *multiplication-by- $m$  isogeny*

$$[m] : E \rightarrow E, \quad [m](P) = \underbrace{P \hat{+} P \hat{+} \dots \hat{+} P}_{m \text{ times}}$$

if  $m > 0$ . For  $m < 0$ , set  $[m](P) = [-m](-P)$ .

Then we can now define the torsion groups.

**Definition 1.4.** Let  $E$  be an elliptic curve and  $m \in \mathbb{Z}, m > 0$ . The  $m$ -torsion subgroup of  $E$ , denoted by  $E[m]$  or  $E_m$ , is the set of points of order  $m$ ,

$$E[m] = \{P \in E : [m](P) = 0\}$$

The torsion subgroup of  $E$ , denoted by  $E_{tors}$ , is the set of points of finite order:

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

Remark that, if  $E$  is defined over the field  $K$ , then  $E_{tors}(K)$  denotes the points of finite order in  $E(K)$ .

Now, let  $E/K$  be an elliptic curve and let  $m > 1$  be an integer, prime to  $\text{char}(K)$  if  $\text{char}(K) > 0$ . With the previous notation, we obtain following notions:

- a.  $\deg[m] = m^2$
- b.  $E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$
- c. each element  $\sigma \in G_{\bar{K}/K}$  acts on  $E[m]$ , since the fact  $[m](P) = 0$  implies that  $[m](P^\sigma) = ([m](P))^\sigma = O^\sigma = O$ , and then we obtain a representation

$$G_{\bar{K}/K} \rightarrow \text{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}).$$

See [14, III, Coroll. 6.4]

## 1.1 Elliptic curves over $\mathbb{C}$

To study Kolyvagin's work on modular elliptic curves, we now want to focus on an elliptic curve  $E/K$  with a cyclic  $N$ -isogeny, with  $K = \mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$  a quadratic imaginary field of discriminant  $-D$  where all prime factors of  $N$  are split. We also work with elliptic curves  $\mathbb{C}/\mathcal{O}_K$ , where  $\mathcal{O}_K$  is the ring of integers of  $K$ . In this section, we study elliptic curves on  $\mathbb{C}$  and introduce the theory of *complex*

*multiplication.* We shall see that an order of  $K$  is a lattice in  $\mathbb{C}$ , the main result of this section will be to see that  $E/\mathbb{C} \cong \mathbb{C}/\Lambda$ , where  $\Lambda$  is a lattice in  $\mathbb{C}$ , and conversely that  $\mathbb{C}/\Lambda$  is analytically isomorphic to  $E_\Lambda(\mathbb{C})$ , for a certain  $E_\Lambda/\mathbb{C}$  elliptic curve.

Let  $\Lambda \subset \mathbb{C}$  be a lattice, that is,  $\Lambda$  is a discrete subgroup of  $\mathbb{C}$  that contains an  $\mathbb{R}$ -basis for  $\mathbb{C}$ .

**Definition 1.5.** An *elliptic function* relative to a lattice  $\Lambda$  is a meromorphic function  $f(z)$  in  $\mathbb{C}$  that satisfies:  $f(z + \omega) = f(z), \forall z \in \mathbb{C}, \forall \omega \in \Lambda$ . The set of such functions is indicated by  $\mathbb{C}(\Lambda)$ .

Through the theory of elliptic functions, introducing a particular set of elliptic functions, called *Weierstrass*  $(\rho, \Lambda)$ -*function* associated to an elliptic curve  $E/\mathbb{C}$ , it is possible to obtain a complex analytical isomorphism of complex Lie groups  $\phi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ . Then, if  $\Lambda \subset \mathbb{C}$ ,  $\mathbb{C}/\Lambda$  is always complex analytically isomorphic to an elliptic curve. Let  $\Lambda_1, \Lambda_2$  be lattices in  $\mathbb{C}$ , and suppose  $\alpha \in \mathbb{C}$  has the property that  $\alpha\Lambda_1 \subset \Lambda_2$ . Then scalar multiplication by  $\alpha$  induces a well-defined holomorphic homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2, \quad \phi_\alpha(z) = \alpha z \pmod{\Lambda_2}.$$

Next theorem shows that these are essentially the only holomorphic maps from  $\mathbb{C}/\Lambda_1$  to  $\mathbb{C}/\Lambda_2$ .

**Theorem 1.6.** [14, VI, Th. 4.1] *Let lattices  $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ , let  $\alpha \in \mathbb{C}$  such that  $\alpha\Lambda_1 \subset \Lambda_2$ . Then:*

(a) *the association*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \rightarrow \{\text{holomorphic maps } \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\}$$

$$\alpha \rightarrow \phi_\alpha$$

*is a bijection*

(b) *let  $E_1, E_2$  elliptic curves corresponding to lattices  $\Lambda_1, \Lambda_2$  respectively, then the*

*natural inclusion*

$$\{\text{isogenies } \phi : E_1 \rightarrow E_2\} \rightarrow \{\text{holom. maps } \phi : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \text{ with } \phi(O) = O\}$$

*is a bijection.*

Then, exploiting the uniformization theorem (see [14, VI, §5]), we obtain the following.

**Theorem 1.7.** [14, VI, Th. 5.3] *The following categories are equivalent*

*A Objects: Elliptic curves over  $\mathbb{C}$*

*Maps: Isogenies*

*B Objects: Elliptic curves over  $\mathbb{C}$*

*Maps: Complex analytic maps taking  $O$  to  $O$*

*C Objects: Lattices  $\Lambda \subset \mathbb{C}$ , up to homothety*

*Maps:  $\text{Map}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$*

**Remark 1.8.** For every elliptic curve  $E/\mathbb{C}$ , there exists a lattice  $\Lambda \subset \mathbb{C}$ , unique up to homothety, such that  $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ .

### 1.1.1 Complex Multiplication

Next topic to discuss is *complex multiplication* of elliptic curves. We have seen above the definition of  $\text{End}(E)$ , and that if  $\text{char}(K) = 0$ , then  $[m] \in \text{End}(E) \forall m \in \mathbb{Z}$ . From the geometry of the elliptic curves we know that, for  $K \subset \mathbb{C}$  field of characteristic 0, the endomorphism ring of an elliptic curve  $E/K$  is either  $\mathbb{Z}$  or an order in an imaginary quadratic field (see [14, III, Corollary 9.4]. If  $\text{End}(E)$  is strictly larger than  $\mathbb{Z}$ , then we say that  $E$  has *complex multiplication*, or CM for short. Now, trying to combine what we have seen so far, let  $K/\mathbb{Q}$  be an imaginary quadratic field, let  $\mathcal{O}_K \subset K$  be the ring of integers of  $K$ , and let  $\text{Pic}(\mathcal{O}_K)$  be the ideal class group of  $\mathcal{O}_K$  (see Chapter 2). If we fix an embedding  $K \subset \mathbb{C}$ , then each ideal  $\Lambda$  of  $\mathcal{O}_K$  is a lattice  $\Lambda \subset \mathbb{C}$ , so we may consider the elliptic curve  $\mathbb{C}/\Lambda$ . From

(Theorem 1.6), we have:

$$\text{End}(\mathbb{C}/\Lambda) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$$

Further, the remark after (Theorem 1.7) says that up to isomorphism, the elliptic curve  $\mathbb{C}/\Lambda$  depends only on the ideal class  $\{\Lambda\} \in \text{Pic}(\mathcal{O}_K)$ . By Theorem 1.7 it also follows that the elliptic curves are isomorphic over  $\mathbb{C}$  if and only if the lattices to which they correspond are homothetic, and then we can say that, up to isomorphism,  $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$  for a unique ideal class  $\{\Lambda\} \in \text{Pic}(\mathcal{O}_K)$ .

The most important invariant of an isogeny is its degree  $\text{deg}(\alpha)$ , which is defined to be the order of its kernel. More precisely, if  $E$  corresponds to the lattice  $\Lambda$ , then it is easy to see that the kernel of  $\alpha : E(\mathbb{C}) \rightarrow E(\mathbb{C})$  is isomorphic to  $\Lambda/\alpha\Lambda$ . Thus, by properties of orders of  $\mathcal{O}_K$ , it follows that  $\text{deg}(\alpha) = |\Lambda/\alpha\Lambda| = N\alpha$ , where  $N(\alpha)$  is the norm of  $\alpha \in \mathcal{O} = \text{End}_{\mathbb{C}}(E)$ .

Lastly, as a corollary, we see that there are only finitely many isomorphism classes of elliptic curves  $E/\mathbb{C}$  with  $\text{End}(E/\mathbb{C}) \cong \mathcal{O}_K$ , and for them  $j(E)$  is algebraic over  $\mathbb{Q}$ .

## 1.2 Elliptic curves and modular curves

In 1993 Sir Andrew Wiles stated the *Modularity Theorem*, stating that every elliptic curve defined over  $\mathbb{Q}$  is modular. In this section, we want to present modular curves, the relation between modular and elliptic curves, and we want to see how they are constructed and the main properties of *Heegner points*.

In last section, we have seen that every elliptic curve is analytically isomorphic to a complex torus  $\mathbb{C}/\Lambda$ , where  $E$  is uniquely determined by the lattice  $\Lambda$ . Now we want to relate the lattice to a modular form, and observe how this lattice defines this. Define  $\mathbb{H} = \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}$ . Observe that every lattice  $\Lambda \in \mathbb{C}$  is homothetic to a lattice of the form  $\Lambda_{\tau} = \mathbb{Z} + \tau\mathbb{Z}$ , for certain  $\tau \in \mathbb{C}$ , and for homogeneity of functions defining  $\Lambda$ , it is enough to study them on space of lattices modulo homothety. Also note that  $SL_2(\mathbb{Z})$  acts on  $\mathbb{H}$  linear fractional transformations: for  $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ,

define  $\gamma_M : \mathbb{H} \rightarrow \mathbb{H}$ ,  $\gamma_M(\tau) = \frac{a\tau+b}{c\tau+d}$ .

**Definition 1.9.** A meromorphic function  $f$  on  $\mathbb{H}$  is called a *modular function of weight  $k$*  for  $SL_2(\mathbb{Z})$  if it satisfies:

- i.  $f(\tau) = (c\tau + d)^{-k} f(\gamma\tau), \forall M \in SL_2(\mathbb{Z})$
- ii. there is an integer  $n_0 = n_0(f)$  such that the Fourier expansion of  $f$  in the variable  $q = e^{2\pi i\tau}$  has the form:  $f(\tau) = \sum_{n=n_0}^{\infty} c(n)q^n$

We also say that  $f$  is a *modular form of weight  $k$*  if  $f$  is holomorphic in  $\mathbb{H}$  and  $n_0(f) = 0$ .

Observe that, for the  $E$  elliptic curve defined (uniquely) by the lattice  $\Lambda$ , the  $j$ -invariant function  $j(E) = j(\Lambda)$  is a modular function of weight 0 that is holomorphic in  $\mathbb{H}$ . Since  $j(\tau)$  is a modular function of weight 0, it defines a function on quotient space  $\mathbb{H}/SL_2(\mathbb{Z})$ , which has a natural structure as Riemann surface, and we obtain that the map  $j : \mathbb{H}/SL_2(\mathbb{Z}) \rightarrow \mathbb{C}$  is a complex analytic isomorphism of Riemann surfaces.

Now, define  $M_k =$  modular functions of weight  $2k$ , a  $\mathbb{C}$  vector space. To study spaces  $M_k$ , we use the *Hecke operator*  $T(n)$ , which sends modular forms of weight  $2k$  to modular forms of weight  $2k$ . in Chapter 4, we see that of particular interest are those modular forms that are simultaneous eigenfunctions for every Hecke operator  $T(n)$ , i.e., those modular forms such that  $T(n)f = \lambda(n)f, \forall n = 1, 2, \dots$

In our work, we are interested in elliptic curves with cyclic  $N$ -isogeny, and then we now focus on a specific subgroup of  $SL_2(\mathbb{Z})$ . Define the *Congruence* subgroup

$$\Gamma_0(N) = \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

There is a natural isomorphism between the space of weight-2 cusp forms for  $\Gamma_0(N)$  and the space of holomorphic 1-forms on the Riemann surface  $\mathbb{H}^*/\Gamma_0(N)$ , and Hecke operators defined above also act on the space of modular forms for  $\Gamma_0(N)$ . See [14, C.12, Prop 12.9]. Then we have seen that the points of the Riemann surface  $\mathbb{H}/\Gamma$  are in one-to-one correspondence with the isomorphism classes of elliptic

curves defined over  $\mathbb{C}$ . This correspondence associates to the point  $\tau \pmod{\Gamma_0(N)} \in \mathbb{H}/\Gamma_0(N)$  the elliptic curve  $E_\tau \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ .

**Remark 1.10.** If we consider  $\gamma \in \Gamma_0(N)$  and  $\tau \in \mathbb{H}/\Gamma_0(N)$ , then one easily checks that the subgroup  $\{1/N, 2/N, \dots, (N-1)/N\} \subset \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$  remains invariant under the action of  $\gamma$ . Thus  $\mathbb{H}/\Gamma_0(N)$  is a moduli space for the problem of determining equivalence classes of pairs  $(E, C)$ , where  $E$  is an elliptic curve and  $C \subset E$  is a cyclic subgroup of exact order  $N$ . Note that, from section 1, there is a one-to-one correspondence between finite subgroups  $C \subset E$  and isogenies  $\phi : E \rightarrow E'$  given by the association  $C \longleftrightarrow \ker\phi$ . Thus the points of  $\mathbb{H}/\Gamma_0(N)$  may also be viewed as classifying triples  $(E, E', \phi)$ , where  $\phi : E \rightarrow E'$  is an isogeny whose kernel is cyclic of order  $N$ .

For arithmetic applications, it is important to understand when an elliptic curve  $E/\mathbb{C}$ , or a point  $T \in E(\mathbb{C})$ , is defined over a number field. To illustrate, we note that although the Riemann surface  $\mathbb{H}/SL_2(\mathbb{C})$  classifies elliptic curves only over  $\mathbb{C}$ , we have a complex analytic isomorphism (Uniformization Theorem)

$$j : \mathbb{H}/SL_2(\mathbb{Z}) \rightarrow \mathbb{A}^1(\mathbb{C}),$$

where  $\mathbb{A}^1(\mathbb{C})$  is a variety defined over  $\mathbb{Q}$ . In addition, the elliptic curve  $E_\tau$  corresponding to  $\tau \in \mathbb{H}/SL_2(\mathbb{Z})$  is isomorphic, over  $\mathbb{C}$ , to an elliptic curve defined over  $\mathbb{Q}(j(\tau))$ . There is a general theory that deals with fields of definition for spaces  $\mathbb{H}/\Gamma_0(N)$  and their associated moduli problems, but we content ourselves with the following description for the quotient spaces associated to the family of the congruence subgroup  $\Gamma_0(N)$ .

**Theorem 1.11.** [14, C.13, Th. 13.1.a] *Let  $N > 0$  be an integer. Then there exists a smooth projective curve  $X_0(N)/\mathbb{Q}$  and a complex analytic isomorphism*

$$j_{N,0} : \mathbb{H}^*/\Gamma_0(N) \rightarrow X_0(N)(\mathbb{C})$$

*such that the following holds:*

*Let  $\tau \in \mathbb{H}/\Gamma_0(N)$ , then it defines the point  $j_{N,0}(\tau) \in X_0(N)$  and we consider*

the field  $K = \mathbb{Q}(j_{N,0}(\tau))$ . We have seen in remark 1.9 that  $\tau$  corresponds to an equivalence class of pairs  $(E, C)$ , where  $E$  is an elliptic curve and  $C \subset E$  is a cyclic subgroup of order  $N$ . Then this equivalence class contains a pair such that both  $E$  and  $C$  are defined over  $K$ , i.e.,  $E$  is an elliptic curve defined over  $K$  and  $C \subset E(\overline{K})$  is  $G_{\overline{K}/K}$ -invariant.

**Definition 1.12.** With previous notation, the curve  $X/\Gamma_0(N)$  is called a *modular curve*.

For an elliptic curve  $E/\mathbb{Q}$ , one might ask if there is a finite map  $\phi : X_0(N) \rightarrow E$  defined over  $\mathbb{Q}$  for some modular curve  $X_0(N)$ . If this happens, then we say that the elliptic curve is modular, and we call  $\phi$  a modular parametrization. Such elliptic curves have a very rich structure that can be used to study their arithmetic properties. Therefore, the Wiles' theorem mentioned above provides an extremely powerful tool for studying the arithmetic of the elliptic curves defined over  $\mathbb{Q}$ .

**Theorem 1.13.** (*Modularity Theorem, Wiles*) Every elliptic curve defined on  $\mathbb{Q}$  is modular, i.e. if  $E/\mathbb{Q}$  is an elliptic curve, then there exist an integer  $N$  and a surjective morphism  $\phi : X_0(N) \rightarrow E$  defined over  $\mathbb{Q}$ . More precisely, the integer  $N$  may be taken to be the conductor of  $E/\mathbb{Q}$ .

### 1.2.1 Heegner Points

Let  $K$  an imaginary quadratic field.

**Definition 1.14.** We say that  $\tilde{x} = (\phi : E \rightarrow E') \in X_0(N)(\mathbb{C})$  is a *Heegner point*, if both  $E$  and  $E'$  have complex multiplication by some order  $\mathcal{O} \subseteq K$ .

Referring to the modular structure, an elliptic curve  $E$  over  $\mathbb{C}$  is determined up to isomorphism by the homothety type of its period lattice  $\Lambda$ :  $E(\mathbb{C}) = \mathbb{C}/\Lambda$ . If  $x = (E \xrightarrow{\phi} E')$  is a point of  $X_0(N)$ , and we write  $E'(\mathbb{C}) = \mathbb{C}/\Lambda'$ , then we can modify by a homothety to obtain  $\Lambda \subset \Lambda'$ ,  $\phi = \text{identity}$ . Then  $\Lambda'/\Lambda \cong \mathbb{Z}/N\mathbb{Z}$ , so we can choose an oriented basis  $\langle \omega_1, \omega_2 \rangle$  of  $\Lambda$  over  $\mathbb{Z}$  such that  $\langle \omega_1, \frac{1}{N}\omega_2 \rangle$  is a basis for  $\Lambda'$ . The point  $z = \omega_1/\omega_2$  then lies in  $\mathbb{H}$ , the complex upper half-plane,

and the point  $x$  uniquely determines  $z$  up to the action of  $\Gamma_0(N)$ . Conversely, any  $z \in \Gamma_0(N)/\mathbb{H}$  determines a point  $x = (\mathbb{C}/\langle z, 1 \rangle) \xrightarrow{id} (\mathbb{C}/\langle z, \frac{1}{N} \rangle)$  of  $X_0(N)$ .

Recall that in last section we have seen that the map

$$Pic(\mathcal{O}) \rightarrow \{\text{elliptic curves with CM by } \mathcal{O}\}$$

given by  $\{\mathfrak{a}\} \rightarrow \mathbb{C}/\mathfrak{a}$  is a bijection.

**Proposition 1.15.** *The set of Heegner points is non-empty if and only if there exists an order  $\mathcal{O}$  and an ideal  $\mathcal{N} \subset \mathcal{O}$  such that  $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ .*

*Proof.* Suppose we have a Heegner point  $x_K = (\phi = E \rightarrow E') \in X_0(N)(\mathbb{C})$  with  $\ker \phi$  cyclic and  $E, E'$  have CM by  $\mathcal{O}$ . We can write  $E = \mathbb{C}/\mathfrak{a}, E' = \mathbb{C}/\mathfrak{b}$  for some invertible fractional ideals  $\mathfrak{a}, \mathfrak{b}$  of  $\mathcal{O}$ . Then there exists an  $\alpha \in K$  such  $\alpha\mathfrak{a} \subset \mathfrak{b}$  and  $\phi : \mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{b}, \phi((\text{mod}(\mathfrak{a}))) = \alpha x(\text{mod}(\mathfrak{b}))$ . Note that

$$\ker(\phi) = (\alpha^{-1}\mathfrak{b})/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}.$$

If we set  $\mathcal{N} = \alpha\mathfrak{a}\mathfrak{b}^{-1}$ , then  $\mathcal{O}\mathcal{N} = (\mathfrak{b}\mathfrak{b}^{-1})/\alpha\mathfrak{a}\mathfrak{b}^{-1} \cong \mathfrak{b}/\alpha\mathfrak{a} \cong (\alpha^{-1}\mathfrak{b})/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$ . Conversely, suppose that there is an ideal  $\mathcal{O}/\mathcal{N}$  such that  $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ . Choose an invertible fractional ideal  $\mathfrak{a}$  of  $\mathcal{O}$  and set  $E = \mathbb{C}/\mathfrak{a}$  and  $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$ . Both  $E$  and  $E'$  have CM by  $\mathcal{O}$ . Consider the isogeny

$$\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \quad \bar{x} \rightarrow \bar{x}$$

The kernel of this isogeny is  $\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a} \cong \mathfrak{a}/\mathcal{N}\mathfrak{a} \cong \mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ . □

**Proposition 1.16.** *(Heegner hypothesis) Suppose that every prime  $p$  dividing  $N$  splits in  $K$ . Then there exists an ideal  $\mathcal{N}$  of  $\mathcal{O}_K$  such that  $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ .*

*Proof.* Write  $N = p_1^{e_1} \dots p_r^{e_r}$ , and suppose  $p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \dots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}$ . Since  $\mathcal{O}/\mathfrak{p}_{i1} \cong \mathbb{Z}/p_i\mathbb{Z}, \dots, \mathcal{O}/\mathfrak{p}_{r1} \cong \mathbb{Z}/p_r\mathbb{Z}$  and since each  $\mathfrak{p}_{i1}$  is unramified, one can check that  $\mathcal{O}/\mathfrak{p}_{11}^{e_1} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}, \dots, \mathcal{O}/\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_r^{e_r}\mathbb{Z}$ . Set now  $\mathcal{N} = \mathfrak{p}_{11}^{e_1} \dots \mathfrak{p}_{r1}^{e_r}$ , then:

$$\mathcal{O}_K/\mathcal{N} \cong \mathcal{O}_K\mathfrak{p}_{11}^{e_1} \times \dots \times \mathcal{O}_K\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$$

□

**Theorem 1.17.** *For a given  $N$ , there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.*

*Proof.* First, recall Dirichlet's theorem on primes in arithmetic progressions, that states that there are infinitely many primes  $q$  such that  $q \equiv 1 \pmod{p}$ . Now, for simplicity, we assume that  $N = p$  and  $p \equiv 1 \pmod{p}$ . For each  $q \equiv 1 \pmod{p}$ ,  $\left(\frac{q}{p}\right) = 1$ ,  $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1$  and  $p$  splits completely in  $\mathbb{Q}(\sqrt{-q})$ . □

**Definition 1.18.** The *conductor* of  $E/K$  is the integral ideal of  $K$  defined by

$$N_{E/K} = \prod_{v \in M_K^0} \mathfrak{p}_v^{f_v}$$

where  $f_v$  is the *exponent of the conductor of  $E$  at  $v$*  defined by:

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has multiplicative reduction at } v \\ 2 + \delta_v & \text{if } E \text{ has additive reduction at } v \end{cases}$$

(for the definition of  $\delta_v$ , see [14, §C.16]).

By modularity theorem, we can define the Heegner point on an elliptic curve starting from the Heegner point defined on the modular curve.

**Definition 1.19.** Let  $E$  be an elliptic curve defined on  $\mathbb{Q}$  with conductor  $N$ , let  $K$  be an imaginary quadratic field satisfying the Heegner hypothesis and consider  $\phi : X_0(N) \rightarrow E$  the modular parameterization described above. Then the Heegner point relative to  $\tilde{x} \in X_0(N)$  is defined to be:  $\tilde{y} = \phi(\tilde{x})$

We describe the Heegner point by the data  $x = (\mathcal{O}, \mathcal{N}, \{\mathfrak{a}\})$ . In the next chapters, we study class field theory to analyze properties of the Heegner points, and to define the "Euler system of Heegner points".

### 1.3 Elliptic curve as abelian variety

In last sections, we have seen elliptic curves in connection with complex tori, to construct elliptic curves over  $\mathbb{C}$ , and with modular curves. In this section, now, we want to describe elliptic curves as abelian varieties.

An abelian variety over the field  $K$  is defined as a complete connected algebraic group over  $K$ , which is an algebraic variety over  $K$  together with regular maps of addition and inverse. An elliptic curve is an abelian variety over  $K$ , because it can be defined as the set of zeroes of an algebraic polynomial with coefficients in  $K$ , the Weierstrass equation, with the geometric structure compatible with the algebraic structure.

Furthermore,  $E$  is a module for the Galois group  $G_{\overline{K}/K}$ , because  $E$  has a structure that is compatible with the action of the Galois group on the algebraic closure of  $K$ .

These two conditions of  $E$  are equivalent, because the Galois group  $G_{\overline{K}/K}$  acts naturally on the solutions of the algebraic equation defined on  $K$ .

#### 1.3.1 Galois cohomology

We use Galois cohomology to study how  $G_{\overline{K}/K}$  acts on the  $G_{\overline{K}/K}$ -modules  $E$  and  $E[m]$ , defined in first section. Let  $G$  be a finite group, and let  $M$  and  $N$  be right  $G$ -modules. A  $G$ -module homomorphism  $\phi : M \rightarrow N$  is a homomorphism commuting with the action of  $G$ , i.e., we have  $\phi(m^\sigma) = \phi(m)^\sigma, \forall m \in M, \forall \sigma \in G$ . So, we now describe the largest submodule on  $M$  on which  $G$  acts trivially.

**Definition 1.20.** The  $0^{th}$  cohomology of the  $G$ -module  $M$ , denoted by  $M^G$  or  $H^0(G, M)$ , is the set:

$$H^0(G, M) = \{m \in M : m^\sigma = m, \forall \sigma \in G\}$$

i.e., the submodule of  $M$  consisting of all  $G$ -invariants elements.

Observe that, if

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

is an exact sequence of  $G$ -modules, we can check that taking  $G$ -invariants gives an exact sequence:

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

Note that the map on the right is not surjective in general.

**Definition 1.21.** let  $M$  be a  $G$ -module.

The *group of 1-cochains* from  $G$  to  $M$  is defined by:

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

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

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

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

$$B^1(G, M) = \{\xi \in C^1(G, M) : \exists m \in M \text{ s.t. } \xi_{\sigma} = m^{\sigma} - m, \forall \sigma \in G\} \subset Z^1(G, M)$$

The  $1^{\text{st}}$  *cohomology group* of the  $G$ -module  $M$  is the quotient group:

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

Then, with  $H^1(G, M)$  we study the group of 1-cocycles from  $G$  to  $M$  modulo the equivalence relation that two cocycles are identified if their difference has the form  $\sigma \rightarrow m^{\sigma} - m$  for some  $m \in M$ . Observe that if the action of  $G$  on  $M$  is trivial, then:  $H^0(G, M) = M$ ,  $H^1(G, M) = \text{Hom}(G, M)$ .

**Proposition 1.22.** [14, B.2, Prop.2.3] 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:

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

where  $\delta$  is the homomorphism defined as follows: let  $n \in H^0(G, N)$ , and choose  $m \in M$  such that  $\psi(m) = n$  and define a cochain  $\xi \in C^1(G, M)$  by  $\xi_\sigma = m^\sigma - m$ . Then the values of  $\xi$  are in  $P$ , and so  $\xi \in Z^1(G, P)$ , and we define  $\delta(n)$  to be the cohomology class of the 1-cocycle  $\xi$  in  $H^1(G, P)$ .

Let  $H$  be a subgroup of  $G$  and let  $\xi \in H^1(G, M)$  be a 1-cochain. Then, by restricting the domain of  $\xi$  to  $H$ , we obtain an  $H$ -to- $M$  cochain, and the process takes cocycles to cocycles and coboundaries to coboundaries. If instead we consider a normal subgroup  $H$  of  $G$ , then the submodule  $M^H$  of  $M$  consisting of elements of  $M$  fixed by  $H$  has a natural structure as a  $G/H$ -module. Hence composing with the projection  $G \xrightarrow{\pi} G/H$  and with the inclusion  $M^H \hookrightarrow M$  gives a  $G$ -to- $M$  cochain  $G \xrightarrow{\pi} G/H \xrightarrow{\xi} M^H \hookrightarrow M$ . As before, and the process takes cocycles to cocycles and coboundaries to coboundaries. We can now define the following two homomorphisms:

**Definition 1.23.**

(Restriction Homomorphism)  $Res : H^1(G, M) \rightarrow H^1(H, M)$

(Inflation Homomorphism)  $Inf : H^1(G/H, M^H) \rightarrow H^1(G, M)$

**Proposition 1.24.** (Inflation-Restriction Sequence) Let  $M$  be a  $G$ -module and let  $H$  be a normal subgroup of  $G$ . Then the following sequence is exact:

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

*Proof.* See [14, B.1, Prop. 1.3] □

Now we apply what we have already seen to the Galois group  $G_{\overline{K}/K}$ . We recall that  $G_{\overline{K}/K}$  is a profinite group, because it is the inverse limit of  $G_{L/K}$  as  $L$  varies

over all finite extensions of  $K$ , and then comes equipped with a topology in which a basis of open sets around identity consists of the collection of normal subgroups having a finite index in  $G_{\overline{K}/K}$ . These are the subgroups that are kernels of maps  $G_{\overline{K}/K} \rightarrow G_{L/K}$  for finite Galois extensions  $L/K$ .

**Definition 1.25.** A discrete  $G_{\overline{K}/K}$ -module is an abelian group on which  $G_{\overline{K}/K}$  acts such that the action is continuous for the profinite topology on  $G_{\overline{K}/K}$  and the discrete topology on  $M$ . Equivalently, the action of  $G_{\overline{K}/K}$  on  $M$  has the property that, for all  $m \in M$ , the stabilizer of  $m$  is a finite index subgroup in  $G_{\overline{K}/K}$ .

Now we adapt what was said before, using the fact that  $G_{\overline{K}/K}$  is profinite.

**Definition 1.26.** Let  $M$  be a  $G_{\overline{K}/K}$ -module. A map  $\xi : G_{\overline{K}/K} \rightarrow M$  is continuous if it is continuous for the profinite topology in  $G_{\overline{K}/K}$  and for the discrete topology in  $M$ .

Equivalently, for each  $m \in M$ , the set  $\xi^{-1}(m)$  is a union of cosets of subgroups of finite index in  $G_{\overline{K}/K}$ . The subgroup of  $G_{\overline{K}/K}$  of continuous 1-cocycles from  $G_{\overline{K}/K}$  to  $M$ , denoted by  $Z_{cont}^1(G_{\overline{K}/K}, M)$ , is the group of continuous maps  $\xi : G_{\overline{K}/K} \rightarrow M$  satisfying the cocycle condition:  $\xi_{\sigma\tau} = \xi_{\sigma}^{\tau} + \xi_{\tau}$ ,  $\sigma, \tau \in G$ .

After observing that every coboundary is continuous by definition, we can define 1<sup>st</sup> cohomology group of the  $G_{\overline{K}/K}$ -module  $M$  as the quotient group

$$H^1(G_{\overline{K}/K}, M) = \frac{Z_{cont}^1(G_{\overline{K}/K}, M)}{B^1(G_{\overline{K}/K}, M)}$$

With this notation, one has an analog for what is said in Proposition (1.19).

If  $L/K$  a finite Galois extension, then  $G_{\overline{K}/L}$  is a subgroup of finite index in  $G_{\overline{K}/K}$ , and  $M$  is naturally a  $G_{\overline{K}/L}$ -module. This leads to a restriction map on cohomology:

$$Res : H^1(G_{\overline{K}/K}, M) \rightarrow H^1(G_{\overline{K}/L}, M)$$

Further,  $G_{\overline{K}/L}$  is a normal subgroup of  $G_{\overline{K}/K}$ , and the quotient  $G_{\overline{K}/K}/G_{\overline{K}/L}$  is the finite group  $G_{L/K}$ . Then  $M^{G_{\overline{K}/L}}$  has a natural structure as  $G_{L/K}$ -module, and so any

1-cocycle  $\xi : G_{L/K} \rightarrow M^{G_{\bar{K}/L}}$  becomes a 1-cocycle for  $G_{\bar{K}/K}$  via the composition

$$G_{\bar{K}/K} \longrightarrow G_{L/K} \xrightarrow{\xi} M^{G_{\bar{K}/L}} \subset M$$

and this gives the inflation map

$$\text{Inf} : H^1(G_{L/K}, M^{G_{\bar{K}/L}}) \rightarrow H^1(G_{\bar{K}/K}, M)$$

Then we obtain the analog to the Proposition (1.21) about the exactness of Inflation-Restriction sequence for a  $G_{\bar{K}/K}$ -module. Now we state the following proposition, that gives us some fundamental facts about the cohomology of additive and multiplicative groups of a field.

**Proposition 1.27.** [14, B.2, Prop. 2.5] *Let  $K$  be a field. (a)  $H^1(G_{\bar{K}/K}, \bar{K}^+) = 0$  (b)  $H^1(G_{\bar{K}/K}, \bar{K}^*) = 0$  (c) Assume that either  $\text{Char}(K) = 0$  or that  $\text{Char}(K)$  does not divide  $m$ , and let  $\mu_m$  primitive  $m$ -root of unity. Then*

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

From now on, we say  $H^1(K, M)$  instead of  $H^1(G_{\bar{K}/K}, M)$ ,  $H^1(L, M)$  instead of  $H^1(G_{\bar{K}/L}, M)$ , and so on.

### 1.3.2 Selmer group and Šafarevič-Tate group

With notation used in definition (1.4), we obtain the short exact sequence of  $G_{\bar{K}/K}$ -modules  $0 \longrightarrow E[m] \longrightarrow E(\bar{K}) \xrightarrow{m} E(\bar{K}) \longrightarrow 0$ , and taking  $G_{\bar{K}/K}$ -cohomology, yields a long exact sequence that starts

$$\begin{array}{ccccccc} 0 & \longrightarrow & E[m] & \longrightarrow & E(\bar{K}) & \xrightarrow{m} & E(\bar{K}) \\ & & & & & \nearrow \delta & \\ H^1(K, E[m]) & \xleftarrow{\quad} & H^1(K, E(\bar{K})) & \xrightarrow{m} & H^1(K, E(\bar{K})) & & \end{array}$$

Then we can extract the short exact sequence

$$0 \longrightarrow E(K)/[m](E(K)) \xrightarrow{\delta} H^1(K, E[m]) \longrightarrow H^1(K, E)[m] \longrightarrow 0$$

which is called the *Kummer sequence* for  $E/K$ . In order to study  $E(K)$ , we now introduce the *Selmer group* and the *Šafarevič-Tate group*, which are subgroups of  $H^1(K, E[m])$  and  $H^1(K, E(\overline{K}))[m]$ , respectively.

Define  $M_K$  a complete set of inequivalent absolute values on  $K$ , and for each  $v \in M_K$  we fix an extension of  $v$  to  $\overline{K}$ , which serves to fix an embedding  $\overline{K} \subset \overline{K}_v$  and a decomposition group  $G_v \subset G_{\overline{K}/K}$ . Now,  $G_v$  acts on  $E(\overline{K}_v)$ , and repeating the above argument yields the exact sequences

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

The natural inclusions  $G_v \subset G_{\overline{K}/K}$  and  $E(\overline{K}) \subset E(\overline{K}_v)$  gives restriction maps on Galois cohomology, and following proposition in last section, we obtain the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(K)}{[m](E(K))} & \xrightarrow{\delta} & H^1(K, E[m]) & \longrightarrow & H^1(K, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigsqcup_{v \in M_K} \frac{E(K_v)}{[m](E(K_v))} & \xrightarrow{\delta} & \bigsqcup_{v \in M_K} H^1(G_v, E[m]) & \longrightarrow & \bigsqcup_{v \in M_K} H^1(K_v, E)[m] & \longrightarrow & 0 \end{array}$$

and this gives an idea of why we give the following two definitions.

**Definition 1.28.**

The *m-Selmer group* of  $E/K$  is the subgroup of  $H^1(K, E[m])$  defined by:

$$Sel_m(E/K) = \ker \left\{ H^1(K, E[m]) \rightarrow \bigsqcup_{v \in M_K} H^1(K_v, E(\overline{K}_v)) \right\}$$

The *Šafarevič-Tate group* is the subgroup of  $H^1(K, E)$  defined by:

$$\text{III}(E/K) = \ker \left\{ H^1(K, E(\overline{K})) \rightarrow \bigsqcup_{v \in M_K} H^1(K_v, E(\overline{K}_v)) \right\}$$

**Remark 1.29.**  $\text{III}(E/K)$  can be viewed as the subgroup of  $H^1(K, E)$  that has a  $K_v$ -rational point for every  $v \in M_K$ .

Observe also that one can check, working with cocycles, that the cohomological definitions of  $\text{Sel}_m(E/K)$  and  $\text{III}(E/K)$  do not depend on the extension of the place  $v \in M_K$  to  $\overline{K}$ , but only on  $E$  and  $K$ .

$\text{Sel}(E/K)_p$  is the largest subgroup of  $H^1(K, E_p)$  which maps to  $\text{III}(E/K)_p$ .

Then we immediately obtain the following theorem, observing the previous diagram.

**Theorem 1.30.** [14, X, Th. 4.2.a] *There is an exact sequence*

$$0 \longrightarrow E(K)/[m](E(K)) \longrightarrow \text{Sel}(E/K)_m \longrightarrow \text{III}(E/K)[m] \longrightarrow 0$$

## 2 Class Field Theory

Class field theory is the fundamental branch of algebraic number theory that describes the abelian Galois extensions of number fields. The theory of complex multiplication provides an analytic realization of class field theory for quadratic imaginary fields.

In this chapter, our main interest is to study the ring class field  $K_n$  of conductor  $n$  over  $K$ , for  $n$  a positive integer and  $K$  an imaginary quadratic field. This will allow us to construct the elements of the Euler System of Heegner Points.

After a brief review of imaginary quadratic fields and orders in imaginary quadratic fields, we shall state the basic facts from class field theory which will be used in the sequel. We will begin with the classical version, using ideals and ideal class group, and afterwards we will present the more modern idèlic version. For a more complete study of these arguments, see [13, pp. 115-120], [3, Chapter 2] and [16].

We define a number field  $K$  to be a subfield of the complex numbers  $\mathbb{C}$  which has finite degree over  $\mathbb{Q}$ , and let  $\mathcal{O}_K$  be the ring of integers of  $K$ . Recall that, for every non-zero ideal  $\mathfrak{a}$  of  $\mathcal{O}_K$ , the quotient ring  $\mathcal{O}_K/\mathfrak{a}$  is finite and the *norm* of  $\mathfrak{a}$  is defined to be  $N_{\mathbb{Q}}^K(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ . The ring of integers  $\mathcal{O}_K$  is a Dedekind domain, and then every nonzero ideal  $\mathfrak{a}$  in  $\mathcal{O}_K$  can be written as a product of prime ideals  $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ , where the decomposition is unique up to the order. Furthermore, the  $\mathfrak{p}_i$ 's are exactly the prime ideals of  $\mathcal{O}_K$  containing  $\mathfrak{a}$ . Notice that, if  $\mathfrak{p}$  is a non-zero prime, we define *residue field* of  $\mathfrak{p}$  the finite field  $\mathcal{O}_K/\mathfrak{p}$ .

We define *fractional ideals* to be the non-zero finitely generated  $\mathcal{O}_K$ -submodules of  $K$ , which can be written in the form  $\alpha\mathfrak{a}$ , where  $\alpha \in K$  and  $\mathfrak{a}$  is an ideal of  $\mathcal{O}_K$ .

**Proposition 2.1.** [3, II, Th. 5.7] *Let  $\mathfrak{a}$  be a fractional  $\mathcal{O}_K$ -ideal.*

(i)  *$\mathfrak{a}$  is invertible.*

(ii)  *$\mathfrak{a}$  can be written uniquely as a product  $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{r_i}$ , where  $r_i \in \mathbb{Z}$  and the  $\mathfrak{p}_i$ 's are distinct prime ideals of  $\mathcal{O}_K$ .*

Let  $I_K$  denote the group of all fractional ideals of  $K$  and let  $P_K \subset I_K$  be the subgroup of *principal fractional ideals*, i.e., those of the form  $\alpha\mathcal{O}_K$  for some  $\alpha \in K^*$ . The quotient  $\text{Pic}(\mathcal{O}_K) = I_K/P_K$  is the *ideal class group*, or *Picard*

group, and it is finite.

Let us now review some behavior of primes in finite extension, so let  $L$  be a finite extension of  $K$ . If  $\mathfrak{p}$  is a prime ideal of  $\mathcal{O}_K$ , then  $\mathfrak{p}\mathcal{O}_L$  is an ideal of  $\mathcal{O}_L$ , and hence has a prime factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_t^{e_t}$$

where  $\mathfrak{B}_i$ 's are distinct primes of  $L$  containing  $\mathfrak{p}$ . Let  $F_{\mathfrak{p}}$  be the residue field  $\mathcal{O}_K/\mathfrak{p}$  and  $F_{\mathfrak{B}}$  be its finite extension  $\mathcal{O}_L/\mathfrak{B}$  for each prime  $\mathfrak{B}_i$  containing  $\mathfrak{p}$ . Then we define the integer  $e_i$ , also written  $e_{\mathfrak{B}_i|\mathfrak{p}}$  as *ramification index* of  $\mathfrak{p}$  in  $\mathfrak{B}_i$ , and define  $f_i = f_{\mathfrak{B}_i|\mathfrak{p}} = |F_{\mathfrak{B}_i}/F_{\mathfrak{p}}|$  as the *inertial degree* of  $\mathfrak{p}$  in  $\mathfrak{B}_i$ . We say that  $\mathfrak{p}$  ramifies in  $L$  if any of the ramification indices  $e_i$  are greater than 1.

**Theorem 2.2.** [3, II, Th. 5.8, Th. 5.9] *Let  $K \subset L$  be number fields, and let  $\mathfrak{p}$  be a prime of  $K$ .*

(a) *If  $e_i$  (resp.  $f_i$ ),  $i = 1, \dots, t$ , are the ramification indices (resp. inertial degrees) defined above, then*

$$\sum_{i=1}^t e_i f_i = [L : K]$$

(b) *The Galois group  $\text{Gal}(L/K)$  acts transitively on the primes of  $L$  containing  $\mathfrak{p}$ , i.e., if  $\mathfrak{B}$  and  $\mathfrak{B}'$  are primes of  $L$  lying over  $\mathfrak{p}$ , then there exists  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma(\mathfrak{B}) = \mathfrak{B}'$ .*

(c) *The primes  $\mathfrak{B}_1, \dots, \mathfrak{B}_t$  of  $L$  lying over  $\mathfrak{p}$  have all the same ramification index  $e$  and the same inertial degree  $f$ , and then the formula in (i) becomes  $e \cdot f \cdot t = [L : K]$ .*

If  $\mathfrak{p}$  satisfies the stronger condition  $e = f = 1$ , we say that  $\mathfrak{p}$  *splits completely* in  $L$ . This prime is unramified and  $\mathfrak{p}\mathcal{O}_L$  is the product of  $[L : K]$  distinct primes.

Let  $K \subset L$  be Galois, and let  $\mathfrak{B}$  be a prime of  $L$ . Then the *decomposition group* and the *inertia group* of  $\mathfrak{B}$  are defined by

$$D_{\mathfrak{B}} = \{\sigma \in \text{Gal}(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$$

$$I_{\mathfrak{B}} = \{\sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{B}}, \forall \alpha \in \mathcal{O}_L\}$$

It is easy to see that  $I_{\mathfrak{B}} \subset D_{\mathfrak{B}}$  and that an element  $\sigma \in D_{\mathfrak{B}}$  induces an automorphism  $\tilde{\sigma}$  of  $F_{\mathfrak{B}}$  which is the identity on  $F_{\mathfrak{p}}$ , with  $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$ . If we define  $\tilde{G} = \text{Gal}(F_{\mathfrak{B}}/F_{\mathfrak{p}})$ , it follows that  $\tilde{\sigma} \in \tilde{G}$ . Thus, the map  $\sigma \rightarrow \tilde{\sigma}$  denotes a homomorphism  $D_{\mathfrak{B}} \rightarrow \tilde{G}$  whose kernel is the inertia group  $I_{\mathfrak{B}}$ .

The homomorphism  $D_{\mathfrak{B}} \rightarrow \tilde{G}$  is surjective, and then  $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \tilde{G}$ ,  $|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}$  and  $|D_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}} \cdot f_{\mathfrak{B}|\mathfrak{p}}$ .

Let  $K = \mathbb{Q}(\sqrt{-D})$  be an imaginary quadratic field of discriminant  $-D$ .

**Proposition 2.3.** [3, II, Prop. 5.16] *Let the nontrivial automorphism of  $K$  be denoted  $\alpha \rightarrow \alpha'$ . Let  $p$  be a prime in  $\mathbb{Z}$ . Let  $(-D/p)$  be the Kronecker symbol. (a) If  $(-D/p) = 0$  (i.e.,  $p \mid -D$ ), then  $p\mathcal{O}_K = \mathfrak{p}^2$  for some prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ . (b) If  $(-D/p) = 1$ , then  $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ , where  $\mathfrak{p} \neq \mathfrak{p}'$  are prime ideal in  $\mathcal{O}_K$ . (c) If  $(-D/p) = -1$ , then  $p\mathcal{O}_K$  is prime in  $\mathcal{O}_K$*

From the previous proposition, an integer prime  $p$  ramifies in  $K$  if and only if  $p$  divides  $-D$ , and  $p$  splits completely in  $K$  if and only if  $(-D/p) = 1$ .

Let us now restrict our interest to the case where  $L$  is a finite abelian extension of  $K$ . Then,  $L/K$  is a Galois extension and the Galois group  $\text{Gal}(L/K)$  is abelian. Let  $\mathcal{O}_L$  be the ring of integers of  $L$ , and let  $\mathfrak{p}$  be a prime in  $K$  which does not ramify in  $L$ . Let  $\mathfrak{B}$  be a prime of  $L$  lying over  $\mathfrak{p}$ .

By restriction, we get a homomorphism from the decomposition group of  $\mathfrak{B}$  to the Galois group of the residue fields,

$$\{\sigma \in \text{Gal}(L/K) : \mathfrak{B}^\sigma = \mathfrak{B}\} \longrightarrow \text{Gal}(F_{\mathfrak{B}}/F_{\mathfrak{p}}).$$

The Galois group  $\text{Gal}(F_{\mathfrak{B}}/F_{\mathfrak{p}})$  is cyclic and generated by the Frobenius automorphism

$$x \longrightarrow x^{N_{\mathbb{Q}}^{K\mathfrak{p}}}$$

Since  $\mathfrak{p}$  is an unramified prime in  $L$  and  $\text{Gal}(L/K)$  is abelian, there is a unique element  $\sigma \in \text{Gal}(L/K)$  which maps to the Frobenius automorphism and is determined by the condition

$$\sigma(x) \equiv x^{N_{\mathbb{Q}}^{K\mathfrak{p}}} \pmod{\mathfrak{B}} \quad \forall x \in \mathcal{O}_L.$$

Since  $L/K$  is an abelian extension and  $\mathfrak{p}$  is unramified,  $\sigma$  is uniquely determined by the prime  $\mathfrak{p}$ . This unique element of  $Gal(L/K)$  is called the *Artin symbol*, or *Frobenius element*, and is denoted  $((L/K)/\mathfrak{p})$ . See [3, Th. 5.19].

When  $K \subset L$  is an unramified abelian extension, notice that the Artin symbol  $((L/K)/\mathfrak{p})$  is defined for all primes  $\mathfrak{p}$  of  $\mathcal{O}_K$ . Let  $\mathfrak{a} \in I_K$  be a fractional ideal with prime factorization  $\mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i}$ ,  $r_i \in \mathbb{Z}$ , and then we can define the Artin symbol

$$((L/K)/\mathfrak{a}) = \prod_i ((L/K)/\mathfrak{p}_i)^{r_i}$$

and it defines a homomorphism, called the *Artin map*,

$$\psi_{L/K} : ((L/K)/\cdot) : I_K \rightarrow Gal(L/K).$$

## 2.1 Orders of $K$

**Definition 2.4.** Let  $K$  be an irrational quadratic field. We define an *order*  $\mathcal{O}$  of  $K$  to be a subset  $\mathcal{O} \subset K$  such that

- (a)  $\mathcal{O}$  is a subring of  $K$  containing 1.
- (b)  $\mathcal{O}$  is a finitely generated  $\mathbb{Z}$ -module.
- (c)  $\mathcal{O}$  contains a  $\mathbb{Q}$ -basis of  $K$ .

Note that  $\mathcal{O}_K$  is the maximal order of  $K$ , and exists an element  $\gamma \in \mathbb{C}$  such that  $\mathcal{O}_K = [1, \gamma]$ .

**Lemma 2.5.** [3, II, Lemma 7.2] Let  $\mathcal{O}$  be an order in the quadratic imaginary field  $K$ . Then  $\mathcal{O}$  has a finite index in  $\mathcal{O}_K$ , and if we set  $c = [\mathcal{O}_K : \mathcal{O}]$ , then

$$\mathcal{O} = \mathbb{Z} + c \cdot \mathcal{O}_K = [1, c\gamma].$$

The index  $c = [\mathcal{O}_K : \mathcal{O}]$  is called the *conductor* of the order. A fractional ideal of  $\mathcal{O}$  is a subset of  $K$ , which is a non-zero finitely generated  $\mathcal{O}$ -module, and it is invertible if and only if it is proper.

Define  $I(\mathcal{O})$  to be the the set of proper fractional  $\mathcal{O}$ -ideals,  $P(\mathcal{O}) \subset I(\mathcal{O})$  the subgroup of principal  $\mathcal{O}$ -ideals and  $Pic(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$  the *ideal class group*, or

Picard group, of the order  $\mathcal{O}$ . Let  $\mathfrak{a}$  be a proper  $\mathcal{O}$ -ideal, and define  $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$  to be the norm of  $\mathfrak{a}$ .

**Proposition 2.6.** *Let  $\mathcal{O}$  be an order in an imaginary quadratic field and  $\mathfrak{a}, \mathfrak{b}$  be proper  $\mathcal{O}$ -ideals. Then:*

- (i)  $N(\mathfrak{a}\mathcal{O}) = N(\mathfrak{a})$ .
- (ii)  $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ .
- (iii) *There exists a proper  $\mathcal{O}$ -ideal  $\bar{\mathfrak{a}}$ , called the inverse of  $\mathfrak{a}$ , such that  $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ .*

Observe that, given a non-zero integer  $M$ , then every ideal class in  $Pic(\mathcal{O})$  contains a proper  $\mathcal{O}$ -ideal whose norm is relatively prime to  $M$ .

An  $\mathcal{O}$ -ideal  $\mathfrak{a}$  is called *prime* to  $c$  provided that  $\mathfrak{a} + c\mathcal{O} = \mathcal{O}$ , and this happens if and only if its norm  $N(\mathfrak{a})$  is relatively prime to  $c$ . Note also that if  $\mathfrak{a}$  is prime to  $c$ , then it is proper. Let us denote  $I(\mathcal{O}, c)$  to be the subgroup of  $I(\mathcal{O})$  generated by  $\mathcal{O}$ -ideals prime to  $c$ , and  $P(\mathcal{O}, c)$  to be the subgroup of  $I(\mathcal{O}, c)$  generated by the principal ideals. Then we can describe  $Pic(\mathcal{O})$  in terms of  $I(\mathcal{O}, c)$  and  $P(\mathcal{O}, c)$  as follows.

**Proposition 2.7.** [3, II, Prop.7.19] *The inclusion  $I(\mathcal{O}, c) \subset I(\mathcal{O})$  induces the isomorphism*

$$Pic(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \cong I(\mathcal{O}, c)/P(\mathcal{O}, c)$$

Let  $m$  be a positive integer, and we define  $I_K(m)$  to be the subgroup of  $I_K$  generated by  $\mathcal{O}_K$ -ideals prime to  $m$ .

**Proposition 2.8.** [3, II, Prop. 7.20] *Let  $\mathcal{O}$  be the order of conductor  $c$  in an imaginary quadratic field  $K$ . Then:*

- (a) *If  $\mathfrak{a}$  is an  $\mathcal{O}_K$ -ideal prime to  $c$ , then  $\mathfrak{a} \cap \mathcal{O}$  is an  $\mathcal{O}$ -ideal prime to  $c$  of the same norm.*
- (b) *If  $\mathfrak{a}$  is an  $\mathcal{O}$ -ideal prime to  $c$ , then  $\mathfrak{a}\mathcal{O}_K$  is an  $\mathcal{O}_K$ -ideal prime to  $c$  of the same norm.*
- (c) *The map  $\mathfrak{a} \rightarrow \mathfrak{a} \cap \mathcal{O}$  induces an isomorphism  $I_K(c) \xrightarrow{\sim} I(\mathcal{O}, c)$ , and the inverse of this map is given by  $\mathfrak{a} \rightarrow \mathfrak{a} \cap \mathcal{O}_K$ .*

From this proposition, follows that there are natural isomorphisms:

$$\text{Pic}(\mathcal{O}) \cong I(\mathcal{O}, c)/P(\mathcal{O}, c) \cong I_K(c)/P_{K,\mathbb{Z}}(c),$$

where  $P_{K,\mathbb{Z}}(c)$  is the subgroup of  $I_K(c)$  generated by principal ideals.

## 2.2 Ring class fields of conductor $c$

Let  $K$  be an quadratic field. A *modulus* in  $K$  is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes  $\mathfrak{p}$  of  $K$ .

Notice that, since  $K$  is a purely imaginary field, a modulus may be regarded as an ideal of  $\mathcal{O}_K$ . Then, let  $I_K(\mathfrak{m})$  be the group of all fractional  $\mathcal{O}_K$ -ideals relatively prime to  $\mathfrak{m}$ , and let  $P_{K,1}(\mathfrak{m})$  be the subgroup of  $I_K(\mathfrak{m})$  generated by the principal ideals  $\alpha\mathcal{O}_K$ , where  $\alpha \in \mathcal{O}_K$  satisfies the condition  $\alpha \equiv 1 \pmod{\mathfrak{m}}$ . Note that  $P_{K,1}(\mathfrak{m})$  has finite index in  $I_K(\mathfrak{m})$ . A subgroup  $H \subset I_K(\mathfrak{m})$  is called a *congruence subgroup* for  $\mathfrak{m}$  if it contains  $P_{K,1}(\mathfrak{m})$ , and the quotient  $I_K(\mathfrak{m})/H$  is called a *generalized ideal class group* for  $\mathfrak{m}$ . Observe that, for  $\mathfrak{m} = 1$ ,  $P_{K,1}(1) = P_K$ .

Let  $\mathcal{O}_c$  be an order of conductor  $c$  in an imaginary quadratic field  $K$ . In the previous section, we have seen that  $\text{Pic}(\mathcal{O}_c) \cong I_K(c)/P_{K,\mathbb{Z}}(c)$ . If we use the prime ideal  $c\mathcal{O}_K$ , then:

$$P_{K,1}(c\mathcal{O}_K) \cong P_{K,\mathbb{Z}}(c) \subset I_K(c) = I_K(c\mathcal{O}_K),$$

and thus  $P_{K,\mathbb{Z}}(c)$  is a congruence subgroup of  $c\mathcal{O}_K$ .

The basic idea of class field theory is that the generalized ideal class groups are the Galois groups of all abelian extensions of  $K$ . To link a generalized ideal class group and the Galois groups of the relative abelian extension, we define the Artin map of an abelian extension of  $K$ .

Let  $K \subset L$  be an abelian extension, and let  $\mathfrak{m}$  be the prime ideal divisible by all

ramified primes of  $L$ . Given  $\mathfrak{p}$  a prime of  $L$  not dividing  $\mathfrak{m}$ , we have the Artin symbol  $((L/K)/\mathfrak{p}) \in \text{Gal}(L/K)$  from previous section, and it gives us a homomorphism

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \rightarrow \text{Gal}(L/K),$$

which is called the Artin map for  $K \subset L$  and  $\mathfrak{m}$ .

**Theorem 2.9.** (*Artin reciprocity theorem*) *Let  $K \subset L$  be an abelian extension, and let  $\mathfrak{m}$  be a modulus divisible by all primes of  $K$  that ramify in  $L$ . Then:*

(a) *The Artin map  $\Phi_{\mathfrak{m}}$  is surjective.*

(b) *If the exponents of the integral ideal  $\mathfrak{m}$  are sufficiently large, then  $\ker(\Phi_{\mathfrak{m}})$  is a congruence subgroup for  $\mathfrak{m}$ , and consequently the isomorphism*

$$I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \xrightarrow{\sim} \text{Gal}(L/K)$$

*shows that  $\text{Gal}(L/K)$  is a generalized ideal class group for the modulus  $\mathfrak{m}$ .*

*Proof.* See [3, II, Th. 8.5]. □

Since  $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$ , the Artin symbol depends only on  $\mathfrak{p}$  up to multiplication by an element  $\alpha$ , with  $\alpha \equiv 1 \pmod{\mathfrak{m}}$ .

With the following theorem, we see that there is one module that is better than the others.

**Theorem 2.10.** (*Conductor theorem*) *Let  $L$  be an Abelian extension of  $K$ . Then there is an integral ideal  $\mathfrak{c} = \mathfrak{c}_{L/K}$ , called the conductor of the extension  $L/K$ , such that:*

(i) *A prime of  $K$  ramifies in  $L$  if and only if it divides  $\mathfrak{c}$ .*

(ii) *For every modulus  $\mathfrak{m}$  divisible by all primes of  $K$  which ramifies in  $L$ ,  $\text{Ker}(\Phi_{\mathfrak{m}})$  is a congruence subgroup for  $\mathfrak{m}$  if and only if  $\mathfrak{c}|\mathfrak{m}$ .*

*Proof.* See [3, II, Th. 8.5] □

It follows by the previous theorem that for any modulus  $\mathfrak{m}$  there is a unique

abelian extension  $K_{\mathfrak{m}}$ , defined the *ray class field* for the modulus  $\mathfrak{m}$ , such that

$$P_{K,1}(\mathfrak{m}) = \ker(\Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}}).$$

In other words,

**Definition 2.11.** Let  $\mathfrak{c}$  be an integral ideal of  $K$ . A *ray class field* (modulo  $\mathfrak{c}$ ) is a finite abelian extension  $K_{\mathfrak{c}}/K$  with the property that, for any finite abelian extension  $L/K$ ,

$$\mathfrak{c}_{L/K} | \mathfrak{c} \Rightarrow L \subset K_{\mathfrak{c}}.$$

The ray class field  $K_{\mathfrak{c}}$  is characterized by the property that it is an abelian extension of  $K$  and satisfies

$$\{\text{primes of } K \text{ that split completely in } K_{\mathfrak{c}}\} = \{\text{prime ideals in } P(\mathfrak{c})\}$$

**Remark 2.12.** (1) Note that the conductor of the ray class field  $K_{\mathfrak{c}}$  may not be equal to  $\mathfrak{c}$ , but for this work we will adopt conditions whereby we will have that the ray class field of  $K$  (modulo  $\mathfrak{c}$ ) will be equal to the ring class field of  $K$  of conductor  $n$ .

(2) Observe that, when  $\mathfrak{m} = 1$ , this reduces to the Hilbert class field, which we will see in section 4.

We know that  $\text{Pic}(\mathcal{O}) = I_K(\mathcal{O}, \mathfrak{c})/P_K(\mathcal{O}, \mathfrak{c}) \cong I_K(\mathfrak{c})/P_{K,\mathbb{Z}}(\mathfrak{c})$ . Furthermore,  $P_{K,1}(\mathfrak{c}) \subset P_{K,\mathbb{Z}}(\mathfrak{c}) \subset I_K(\mathfrak{c})$ , so that  $\text{Pic}(\mathcal{O})$  is a generalized ideal class group of  $K$  for the modulus  $\mathfrak{c}\mathcal{O}_K$ . By the conductor theorem, this data determines a unique abelian extension  $L$  of  $K$ , called the *ring class field* of the order  $\mathcal{O}$ . The basic properties of  $L$  are, first, all primes of  $K$  ramified in  $L$  must divide  $\mathfrak{c}\mathcal{O}_K$ , and second, the Artin map gives us the isomorphisms:

$$\text{Pic}(\mathcal{O}) \cong I_K(\mathfrak{c})/P_{K,\mathbb{Z}}(\mathfrak{c}) \cong \text{Gal}(L/K),$$

and in particular,  $[L : K] = h(\mathcal{O})$ , where  $h(\mathcal{O})$  is the class number of  $\mathcal{O}$ .

**Lemma 2.13.** ([3, Lemma 9.3]) Let  $L$  be the ring class field of an order  $\mathcal{O}$  in an

imaginary quadratic field  $K$ . Then  $L$  is a Galois extension of  $\mathbb{Q}$ , and its Galois group can be written as a semidirect product

$$\text{Gal}(L/\mathbb{Q}) \cong \text{Gal}(L/K) \rtimes \mathbb{Z}/2\mathbb{Z},$$

where the nontrivial element of  $\mathbb{Z}/2\mathbb{Z}$  acts on  $\text{Gal}(L/K)$  by sending  $\sigma$  to  $\sigma^{-1}$ .

### 2.3 Hilbert class field

If we consider the case for the integral ideal  $\mathfrak{c} = (1)$ ,  $K_1$  is the maximal abelian extension of  $K$  which is unramified at all primes, called the *Hilbert class field* of  $K$ . Notice that

$$I_{K_1/K} = I((1)) = \{\text{all nonzero fractional ideals of } K\}$$

$$P_{K_1/K} = P((1)) = \{\text{all nonzero principal ideals of } K\}.$$

Then, the Artin Map induces an isomorphism between the ideal class group of  $K$  and the Galois group of the Hilbert class field of  $K$ .

**Theorem 2.14.** [3, II, Th. 5.23] *Let  $K_1$  be the Hilbert class field of a number field  $K$ , then the Artin map is surjective, and its kernel is exactly the subgroup  $P_K \subset I_K$ . Thus the Artin map induces an isomorphism*

$$(\cdot, K_1/K) : \text{Pic}(\mathcal{O}_K) = I_K/P_K \xrightarrow{\sim} \text{Gal}(K_1/K).$$

**Corollary 2.15.** [3, II, Coroll. 5.24] *Given a number field  $K$ , there is a one-to-one correspondence between the unramified abelian extensions  $M$  of  $K$  and the subgroups  $H$  of the ideal class group  $\text{Pic}(\mathcal{O}_K)$ . Furthermore, if the extension  $K \subset M$  corresponds to the subgroup  $H \subset \text{Pic}(\mathcal{O}_K)$ , then the Artin map induces an isomorphism*

$$\text{Pic}(\mathcal{O}_K)/H \xrightarrow{\sim} \text{Gal}(M/K).$$

**Corollary 2.16.** [3, II, Coroll. 5.25] *Let  $K_1$  be the Hilbert class field of a number field  $K$ , and let  $\mathfrak{p}$  be a prime ideal of  $K$ . Then  $\mathfrak{p}$  splits completely in  $K_1$  if and only*

if  $\mathfrak{p} \in P_K$ .

**Lemma 2.17.** [3, II, Lemma 5.28] Let  $K_1$  be the Hilbert class field of an imaginary quadratic field  $K$ , and let  $\tau$  denote the complex conjugation. Then  $\tau(K_1) = K_1$ , and hence  $K_1$  is Galois over  $\mathbb{Q}$ .

## 2.4 Idèlic formulation of class field theory

Let  $v$  be an absolute value of  $K$ , and let  $K_v$  be the completion of  $K$  at  $v$ . Further, let  $\mathcal{O}_v$  be the ring of integers of  $K_v$  if  $v$  is non-archimedean, and let  $\mathcal{O}_v = K_v$  otherwise. The Idèle group of  $K$  is the group

$$\mathcal{I}_K = \prod'_v K_v^*,$$

where  $\prod'$  indicates the the product is restricted relative to the  $\mathcal{O}_v$ 's. This means that an element  $s \in \prod_v K_v^*$  in the unrestricted product is in  $\mathcal{I}_K$  if and only if  $x_v \in \mathcal{O}_v^*$  for all but finitely many  $v$ . In particular, we can embed  $K^*$  into  $\mathcal{I}_K$  by using the natural diagonal embedding

$$K \hookrightarrow \mathcal{I}_K, \quad \alpha \rightarrow (\dots, \alpha, \alpha, \alpha, \dots),$$

since any  $\alpha \in K^*$  is in  $\mathcal{O}_v^*$  for all but finitely many  $K$ . Similarly, for any given  $v$  we embed  $K_v^*$  as a subgroup of  $\mathcal{I}_K$  via

$$K_v^* \hookrightarrow \mathcal{I}_K, \quad t \rightarrow (1, 1, \dots, 1, t, 1, \dots, 1)$$

where  $t$  is the  $v$ -component.

If  $v$  is a non archimedean absolute value corresponding to a prime ideal  $\mathfrak{p}$ , we will write  $K_{\mathfrak{p}}$  and  $\mathcal{O}_{\mathfrak{p}}$  in place of  $K_v$  and  $\mathcal{O}_v$ . We will also write  $ord_{\mathfrak{p}}$  for the corresponding normalized valuation.

Let  $s \in \mathcal{I}_K$  be an Idèle. We define the *ideal of  $s$*  as the fractional ideal of  $K$  given by

$$(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{ord_{\mathfrak{p}} s_{\mathfrak{p}}},$$

where the product is over all prime ideals of  $K$ . Note that  $(s)$  is well defined, since  $s_{\mathfrak{p}}$  is a  $\mathfrak{p}$ -adic unit for all but finitely many  $\mathfrak{p}$ . For any integral ideal  $\mathfrak{c}$  of  $K$ , let  $U_{\mathfrak{c}}$  be the subgroup of  $\mathcal{I}_K$  defined by

$$U_{\mathfrak{c}} = \{s \in \mathcal{I}_K : s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^*, s_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{c}\mathcal{O}_{\mathfrak{p}}} \text{ for all primes } \mathfrak{p}\}$$

Then  $U_{\mathfrak{c}}$  is an open subgroup of  $\mathcal{I}_K$ , and can be proven that  $K^*U_{\mathfrak{c}}$  is a subgroup of finite index in  $\mathcal{I}_K$ .

If  $L/K$  is a finite extension, then there is a natural norm map from  $\mathcal{I}_L$  to  $\mathcal{I}_K$ , and this is a continuous homomorphism

$$N_K^L : \mathcal{I}_L \rightarrow \mathcal{I}_K$$

defined by the prescription that the  $v$ -component of  $N_K^L x$  is

$$\prod_{w|v} N_{K_w}^{L_w} x_w$$

The idelic formulation of class field theory is given in terms of the reciprocity map described in the following theorem.

**Theorem 2.18.** [13, II, Th. 3.5] *Let  $K^{ab}$  be the maximal abelian extension of  $K$ . Then there exists a unique continuous homomorphism*

$$\mathcal{I}_K \rightarrow \text{Gal}(K^{ab}/K), \quad s \rightarrow [s, K]$$

*with the following property:*

*Let  $L/K$  be the a finite abelian extension, and let  $s \in \mathcal{I}_K$  be an Idèle whose ideal  $(s)$  is not divisible by any prime that ramifies in  $L$ . Then*

$$[s, K]|_L = ((s), L/K)$$

Here  $((s), L/K)$  is the Artin map, and  $\text{Gal}(K^{ab}/K)$  is given by the usual profinite topology. The homomorphism  $[\cdot, K]$  is called the *reciprocity map* for  $K$ .

The reciprocity map has the following additional properties:

- (i) The reciprocity map is surjective, and  $K^*$  is contained in its kernel. (ii) The reciprocity map is compatible with the norm map,

$$[x, L]|_{K^{ab}} = [N_K^L x, K], \quad \forall x \in \mathcal{I}_K$$

Let  $\mathfrak{p}$  be a prime ideal of  $K$ , let  $I_{\mathfrak{p}}^{ab} \subset \text{Gal}(K^{ab}/K)$  be the inertia group of  $\mathfrak{p}$  for the extension  $K^{ab}/K$ , let  $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$  be a uniformizer at  $\mathfrak{p}$ , and let  $L/K$  be any abelian extension that is unramified at  $\mathfrak{p}$ . Then

$$[\pi_{\mathfrak{p}}, K]|_L = (\mathfrak{p}, L/K) = \text{Frobenius for } L/K \text{ at } \mathfrak{p},$$

and

$$[\mathcal{O}_{\mathfrak{p}}^*, K] = I_{\mathfrak{p}}^{ab}$$

**Theorem 2.19.** [13, II, Th. 3.6] *Let  $\mathfrak{c}$  be an integral ideal of  $K$ , let  $K_{\mathfrak{c}}$  be the ray class field of  $K$  modulo  $\mathfrak{c}$  and let  $U_{\mathfrak{c}}$  be the subgroup of  $\mathcal{I}_K$  described above. Then the reciprocity map induces an isomorphism*

$$[\cdot, K] : \mathcal{I}_K / K^* U_{\mathfrak{c}} \xrightarrow{\sim} \text{Gal}(K_{\mathfrak{c}}/K).$$

Then  $[s, K]$  acts trivially on the ray class field  $K_{\mathfrak{c}}$  if and only if  $s$  can be written as  $s = \alpha u$  with  $\alpha \in K^*$  and  $u \in U_{\mathfrak{c}}$ .

## 2.5 Application of the class field theory to the elliptic curves

In this section, we use orders and class field theory to study the structure of an elliptic curve  $E$  having complex multiplication. In particular, we can learn more about the  $j$ -invariant of the elliptic curve.

Let  $\mathcal{O}_K$  be the ring of integers of the imaginary quadratic field  $K$ . For  $\Lambda \in \text{Pic}(\mathcal{O}_K)$ , consider the elliptic curve  $\mathbb{C}/\Lambda$  and denote the  $j$ -invariant of  $\mathbb{C}/\Lambda$  by  $j(\Lambda)$ .

**Theorem 2.20.** (Weber, Fueter) Let  $\{\Lambda\} \in \text{Pic}(\mathcal{O}_K)$ .

(a)  $j(\Lambda)$  is an algebraic integer.

(b) The field  $K(j(\Lambda))$  is the maximal unramified abelian extension, i.e.,  $K(j(\Lambda))$  is the Hilbert class field  $K_1$  of  $K$ .

(c)  $[K(j(\Lambda)) : K] = [\mathbb{Q}(j(\Lambda)) : \mathbb{Q}]$ .

*Proof.* See [14, C.11, Th. 11.2] □

Suppose that  $E/\mathbb{Q}$  is an elliptic curve with complex multiplication.

Suppose that  $\text{End}(E)$  is the full ring of integers  $\mathcal{O}_K$  in the imaginary quadratic field  $K = \text{End}(E) \otimes \mathbb{Q}$ . Since  $j(E) \in \mathbb{Q}$ , it follows by (c) that  $[K(j(E)) : K] = 1$ , and then  $K_1 = K$ .

Now, let us suppose that  $\text{End}(E)$  is not the full ring of integers  $\mathcal{O}_K$ , but an arbitrary order in  $K$ . Then there exists an integer  $n$  such that  $\text{End}(E)$  is of the form  $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ , the order of conductor  $n$ . We obtain  $[K(j(E)) : K] = |\text{Pic}(\mathcal{O}_n)|$ .

With notation in previous sections, we have the following theorem.

**Theorem 2.21.** [14, C.11, Ex. 11.3.2] If  $E$  is an elliptic curve with  $\text{End}(E) \cong \mathcal{O}_n$  where  $\mathcal{O}_n$  is the order of conductor  $n$  in a quadratic field  $K$ , then  $K_n = K(j(E))$ , where  $K_n$  is the ring class field of  $K$  of order  $n$ .

## 3 Duality Theorems

### 3.1 Duality of local class field theory

Let  $K_\lambda$  be a local field, with ring of integers  $\mathcal{O}_\lambda$  and finite residue field  $F_\lambda$  of characteristic  $l$ . Let  $E$  be an elliptic curve over  $K_\lambda$  with good reduction over  $\mathcal{O}_\lambda$ . If  $p \neq l$  be a prime, then  $E_p \cong \mathbb{Z}/p\mathbb{Z} \times_{\mathcal{O}_\lambda} \mathbb{Z}/p\mathbb{Z}$  is a finite étale group scheme of rank  $p^2$  over  $\mathcal{O}_\lambda$ . The Kummer sequence  $0 \rightarrow E_p \rightarrow E \xrightarrow{p} E \rightarrow 0$  induces an exact sequence

$$0 \longrightarrow E(K_\lambda)/pE(K_\lambda) \longrightarrow H^1(\mathcal{O}_\lambda, E_p) \longrightarrow H^1(\mathcal{O}_\lambda, E)_p \longrightarrow 0,$$

and since  $H^1(\mathcal{O}_\lambda, E) = 0$  we have the isomorphism

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} H^1(\mathcal{O}_\lambda, E_p).$$

Since  $E^1(K_\lambda)$ , the kernel of reduction, is  $l$ -divisible, the group  $E(K_\lambda)/pE(K_\lambda)$  is isomorphic to  $\tilde{E}(K_\lambda)/p\tilde{E}(F_\lambda)$ , so it has dimension  $\leq 2$  over  $\mathbb{Z}/p\mathbb{Z}$ , and the dimension is  $= 2$  if all the  $p$ -torsions on  $E$  are rational over  $K_\lambda$ .

Define

$$\{, \} : E_p \times E_p \longrightarrow \mu_p$$

to be the Weil pairing of finite group schemes over  $K_\lambda$ , where  $\mu_p$  is the group of  $p^{\text{th}}$ -roots of unity. By [14, Ch. III, Prop. 8.1], this pairing is bilinear, alternating, nondegenerate, and Galois invariant. The Weil pairing induces a cup-product pairing in Galois cohomology:

$$(*) \quad H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow H^2(K_\lambda, \mu_p),$$

see [15].

Let  $L$  be a finite unramified extension of  $K$ , and let  $G = \text{Gal}(L/K)$ . Define  $U_L$  to be the group of units of  $L$ . As  $H^2(G, U_L) = H^3(G, U_L) = 0$ , the cohomology sequence of the short exact sequence  $0 \rightarrow U_L \rightarrow L^\times \xrightarrow{\text{ord}_L} \mathbb{Z} \rightarrow 0$  gives an

isomorphism  $H^2(G, L^\times) \xrightarrow[\sim]{H^2(\text{ord}_L)} H^2(G, \mathbb{Z})$ . From the fact that  $H^r(G, \mathbb{Q})$  are torsion for all  $r > 0$  and by the exact sequence  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ , we have the isomorphism  $H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z})$ . Recall also that, by §1.3.1, we have  $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ , and  $G$  has a canonical topological generator, the Frobenius element  $\sigma = \text{Frob}_{L/K}$ . The composite of

$$H^2(L/K) \xrightarrow[\sim]{\text{ord}_L} H^2(G, \mathbb{Z}) \xleftarrow[\sim]{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

is called the *Invariant map*

$$\text{inv}_{L/K} : H^2(L/K) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

If we consider a tower of field extensions  $K \subset L \subset E$ , with both  $E$  and  $L$  unramified over  $K$ , then the diagram

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\text{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \text{Inf} \downarrow & & \downarrow \sim \\ H^2(E/K) & \xrightarrow{\text{inv}_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, because all the maps in the definition of  $\text{inv}$  are compatible with  $\text{Inf}$ , and as a consequence of this discussion get the following theorem.

**Theorem 3.1.** *There exists a unique isomorphism*

$$\text{inv}_K : H^2(K^{\text{un}}/K) \rightarrow \mathbb{Q}/\mathbb{Z}$$

with the property that, for every  $L \subset K^{\text{un}}$  of finite degree  $n$ ,  $\text{inv}_K$  induces the isomorphism

$$\text{inv}_{L/K} : H^2(L/K) \rightarrow \mathbb{Z}/n\mathbb{Z}$$

The invariant map of local class field theory gives a canonical isomorphism  $H^2(K_\lambda, \mu_p) = \text{Br}(K_\lambda) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$ , where we write  $\text{Br}(K_\lambda)$  for the Brauer group of  $K_\lambda$ , and Tate's local duality theorem states that the resulting pairing of  $\mathbb{Z}/p\mathbb{Z}$ -vector

spaces

$$\langle, \rangle_\lambda : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

is alternating and non-degenerate, by [10, Ch. 1, Coroll. 2.3]. The Kummer sequence gives a short exact sequence in Galois cohomology:

$$0 \longrightarrow E(K_\lambda)/pE(K_\lambda) \longrightarrow H^1(K_\lambda, E_p) \longrightarrow H^1(K_\lambda, E)_p \longrightarrow 0,$$

and by the cup-product (\*), the subspace  $E(K_\lambda)/pE(K_\lambda) \cong H^1(\mathcal{O}_\lambda, E_p)$  is isotropic for the pairing  $\langle, \rangle$ , since  $H^2(\mathcal{O}_\lambda, \mu_p) = 0$ .

**Proposition 3.2.** *The pairing  $\langle, \rangle$  induces a non-degenerate pairing of  $\mathbb{Z}/p\mathbb{Z}$ -vector spaces (of dimension  $\leq 2$ )*

$$\langle, \rangle_\lambda : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

*Proof.* It suffices to check that the subspace  $H^1(\mathcal{O}_\lambda, E_p)$  is maximal isotropic, or equivalently, that  $\dim H^1(K_\lambda, E_p) = \dim E(K_\lambda)_p$ . This is a general fact, due to [10, Ch. I, Thm. 2.6]. For more details, see [7, Prop. 7.5].  $\square$

## 3.2 Duality of global class field theory

We want to analyze the relation between local and global Artin maps. For each prime  $v$  of  $K$ , let  $K_v$  denote the completion of  $K$  at  $v$ . Let  $L/K$  be a finite abelian Galois extension and  $L_w$  with  $w$  lying over  $v$ , and define

$$G^v = \text{Gal}(L_w/K_v) \cong G(k(w)/k(v)),$$

where  $k(w)$  and  $k(v)$  are the residue fields respectively of  $L$  and  $K$ .

By Artin Reciprocity theorem stated in Chapter 2, there is an Artin map

$$\psi_{L/K} : \mathcal{I}_K \rightarrow \text{Gal}(L/K),$$

and for each prime  $v$  of  $K$  we have

$$K_v^* \xrightarrow{i_v} \mathcal{I}_K \xrightarrow{\psi_{L/K}} \text{Gal}(L/K)$$

where  $i_v$  is the map that sends an  $x \in K^*$  onto an element of  $\mathcal{I}_K$  whose  $v$ -component is  $x$  and other components are 1. Define  $\psi_v = \psi_{L/K} \circ i_v$ , and so we have

$$\psi_v : K_v^* \longrightarrow \text{Gal}(L/K).$$

This map is called the *local Artin map*.

If  $x = (x_v)_v \in \mathcal{I}_K$ , then with the previous notation we obtain

$$\psi_{L/K}(x) = \prod_v \psi_v(x_v).$$

This fact indicates that, through the study of idèles, the knowledge of all the local Artin maps  $\psi_v$  is equivalent to the knowledge of the global Artin map  $\psi_{L/K}$ . For a proof of these statements, see [16].

Studying the cohomology of idèles, we have the following proposition:

**Proposition 3.3.** [16, Prop. 7.3]

- (a)  $\mathcal{I}_K \cong \mathcal{I}_L^G$ , the group of idèles of  $L$  left fixed by all elements of  $G$ .
- (b)  $H^r(G, \mathcal{I}_L) \cong \coprod_v H^r(G_v, L_v^*)$ , where  $\coprod$  denotes the direct sum.

**Corollary 3.4.** (a)  $H^1(G, \mathcal{I}_L) = 0$ .

- (b)  $H^2(G, \mathcal{I}_L) = \coprod_v (\mathbb{Z}/n_v\mathbb{Z})$ , where  $n_v = [L_w : K_v]$ .

We write  $H^2(L/K)$  for  $H^2(\text{Gal}(L/K), L^*)$ . The cohomology group  $H^2(L_w/K_v)$  is cyclic of order  $n_v = [L_w : K_v]$ , and then

$$H^2(G, \mathcal{I}_K) = \prod_v H^2(L_w/K_v) \cong \prod_v \mathbb{Z}/n_v\mathbb{Z}.$$

With these statements, comparing with results from the last section, by the definition of Tate's local Tate duality  $\langle, \rangle_v : H^1(K_v, E_p) \times H^1(K_v, E_p) \longrightarrow H^2(K_v, \mu_p)$ , we

can define the Tate's global duality

$$\langle , \rangle = \sum_v \langle , \rangle_v : H^1(K, E_p) \times H^1(K, E_p) \longrightarrow H^2(K, E_p),$$

where, for every  $s, t \in H^1(K, E_p)$ , we have

$$\langle s, t \rangle = \sum_v \langle res_v(s), res_v(t) \rangle,$$

with  $res_v : H^1(K, E_p) \rightarrow H^1(K_v, E_p)$ .

Thus, we obtain the following commutative diagram.

$$\begin{array}{ccc} H^1(K, E_p) \times H^1(K, E_p) & \xrightarrow{\langle , \rangle} & H^2(K, E_p) \\ \downarrow \Pi_v & & \updownarrow \\ \prod H^1(K_v, E_p) \times \prod H^1(K_v, E_p) & \xrightarrow{\sum_v \langle , \rangle_v} & \prod H^2(K_v, E_p) \end{array}$$

For each prime  $v$  of  $K$ , let  $K_v$  denote the completion of  $K$  at  $v$ . Let  $L/K$  be a finite abelian Galois extension, with  $[L : K] = n$ . We have  $n = \sum_v n_v$ , where  $n_v = [L_w : K_v]$  for every  $w$  in  $L$  lying over  $v$ . Let us define

$$inv_v = inv_{L_w/K_v} : H^2(L_w/K_v) \rightarrow \mathbb{Z}/n_v\mathbb{Z},$$

and then we obtain:

$$inv_{L/K} = \prod_v inv_v$$

(see [16, §11]).

By class field theory, we obtain the following result on the invariant map.

**Theorem 3.5.** *If  $\alpha \in Br(K)$ , then*

$$\sum_v inv_v \alpha = 0$$

*Proof.* See [16, Th. B]. □

## 4 Euler System of Heegner Points

### 4.1 Heegner points of the conductor $n$

We continue the discussion started in 1.2 on Heegner points, and define Heegner points of conductor  $n$ .

Let  $n \geq 1$  be an integer prime to  $N$ , let  $K = \mathbb{Q}(\sqrt{-D})$  be an imaginary quadratic field with discriminant  $-D$  satisfying the Heegner hypothesis, i.e.,  $D$  is prime to  $N$  and all prime ideals  $l$  that divide  $N$  are split in  $K$ . By Proposition 1.15, we can define an ideal  $\mathcal{N}$  of  $\mathcal{O}_K$  such that  $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ .

Every order  $\mathcal{O}_n$  of  $\mathcal{O}_K$  is of the form  $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ , where  $n = [\mathcal{O}_n : \mathcal{O}_K]$  is the conductor of  $\mathcal{O}_n$  (see §2.1). Then, by Proposition 2.8, we can define the ideal  $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$  and, for each  $n$  relatively prime to  $D$  and to  $N$ , we obtain  $\mathcal{O}_n/\mathcal{N}_n \cong \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ . Consequently, the elliptic curve  $\mathbb{C}/\mathcal{O}_n$ , with its cyclic  $N$  isogeny to  $\mathbb{C}/\mathcal{N}^{-1}$ , defines a point in  $X_0(N)$ .

**Definition 4.1.** The Heegner point  $x_n = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\})$  described in §1.2 is defined to be a *Heegner point of conductor  $n$*  if  $\mathcal{O}_n$  is an order of  $\mathcal{O}_K$  of conductor  $n$ .

Note that  $\text{Gal}(K_n/K)$  acts on  $\text{Div}(X_0(N)(K_n))$ , and remember that from class field theory (§2.2) we have the isomorphism of groups

$$\text{Pic}(\mathcal{O}_n) \xrightarrow{\sim} \text{Gal}(K_n/K), \quad \{\mathfrak{a}\} \rightarrow \sigma_{\mathfrak{a}},$$

where  $\sigma_{\mathfrak{a}}$  is defined to be the Artin symbol of  $\mathfrak{a}$ .

We now see how  $\text{Gal}(K_n/K)$  acts on Heegner points. Let  $\mathfrak{b}$  an ideal of  $\mathcal{O}_n$  not dividing  $n$  and  $\sigma_{\mathfrak{b}}$  the Artin symbol of  $\{\mathfrak{a}\}$  in  $\mathcal{G}_n$ . If we define the Heegner point  $x_n = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\})$ , with  $\mathfrak{a}$  an ideal of  $\mathcal{O}_n$  and  $\mathcal{N}$  such that  $\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$ , then we have the formula  $\sigma_{\mathfrak{b}}(x_n) = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\})^{\sigma_{\mathfrak{b}}} = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\mathfrak{b}^{-1}\})$  (see [5, §0.4]).

**Proposition 4.2.** *The Heegner point  $x_n \in X_0(N)$  of conductor  $n$  lies in  $X_0(N)(K_n)$ , where  $K_n$  is the ring class field of  $\mathcal{O}_n$ .*

*Proof.* By Theorem 2.21,  $\mathbb{C}/\mathcal{O}_n$  is defined over  $K_n$ , and so by the moduli interpretation,  $x_n \in X_0(N)(K_n)$ . □

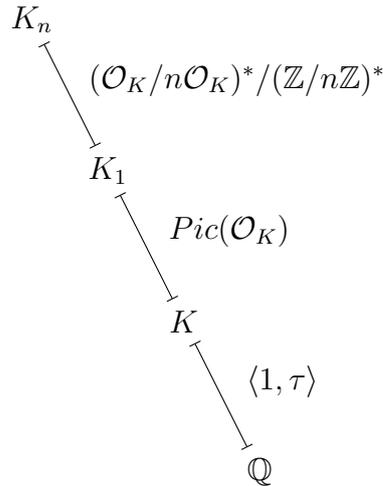
From §2.2, we know that  $Gal(K_n/K) \cong Pic(\mathcal{O}_n)$  and  $Gal(K_1/K) \cong Pic(\mathcal{O}_K)$ , now we want to define  $Gal(K_n/K_1) \cong Pic(\mathcal{O}_n)/Pic(\mathcal{O}_K)$ . Let  $I_K$  be the group of fractional ideals of  $\mathcal{O}_K$ ,  $P_K$  be the subgroup generated by principal ideals of  $I_K$ ,  $I_K(n) \subset I_K$  be the subgroup generated by  $\mathcal{O}_K$ -ideals prime to  $n$  and  $P_{K,\mathbb{Z}}(n)$  be the subgroup  $I_K(n)$  generated by principal ideals of the form  $\alpha\mathcal{O}_K$ , where  $\alpha \in \mathcal{O}_K$  satisfies  $\alpha \equiv a \pmod{n\mathcal{O}_K}$  for an integer  $a$  relatively prime to  $n$ . Then we get an exact sequence

$$\begin{array}{ccccccc} 0 & \rightarrow & (I_K(n) \cap P_K)/P_{K,\mathbb{Z}}(n) & \rightarrow & I_K(n)/P_{K,\mathbb{Z}}(n) & \rightarrow & I_K/P_K \\ & & & & \sim \downarrow & & \downarrow \sim \\ & & & & Pic(\mathcal{O}_n) & \longrightarrow & Pic(\mathcal{O}_K) \end{array}$$

and then  $Pic(\mathcal{O}_n)/Pic(\mathcal{O}_K) \cong (I_K(n) \cap P_K)/P_{K,\mathbb{Z}}(n)$ . We also know (see [3, Chapter 2, §7.27]) that there is an exact sequence

$$1 \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathcal{O}_K/n\mathcal{O}_K)^* \rightarrow (I_K(n) \cap P_K)/P_{K,\mathbb{Z}}(n) \rightarrow 1,$$

and then we obtain  $Gal(K_n/K_1) \cong (\mathcal{O}_K/n\mathcal{O}_K)^*/(\mathbb{Z}/n\mathbb{Z})^*$ . Finally, we define  $\tau$  to be the complex conjugation and we have the field diagram with Galois groups:



Note that  $\tau \in Gal(K/\mathbb{Q})$  lifts to an involution of  $K_n$  and acts on  $Gal(K_n/K)$  by  $\tau\sigma\tau^{-1} = \sigma^{-1}$ . Then  $Gal(K_n/K) = Pic(\mathcal{O}_n)$  is a normal subgroup in  $Gal(K_n/\mathbb{Q})$ ,

and since  $Gal(K/\mathbb{Q}) = \langle 1, \tau \rangle$  is of order 2, we find that  $Gal(K_n/\mathbb{Q})$  is the dihedral group  $Gal(K_n/\mathbb{Q}) = Pic(\mathcal{O}_n) \rtimes \langle 1, \tau \rangle$

Now, let  $Div(X_0(N)(K_n))$  be the group of divisors that are stable under the action of  $Gal(\overline{K}/K_n)$ . For  $q$  a prime not dividing  $N$ , define a Hecke correspondence:

$$T_q : Div(X_0(N)(K_n)) \rightarrow Div(X_0(N)(K_n))$$

$$T_q((\phi : E \rightarrow E')) \rightarrow \sum_{C \subset E[q], |C|=q} (E/C \rightarrow E'/\phi(C))$$

Let  $q$  be a prime not dividing  $nND$ . Define a trace map:

$$Tr_q : X_0(N)(K_{nq}) \rightarrow Div(X_0(N)(K_n), \quad z \rightarrow \sum_{\sigma \in Gal(K_{nq}/K_n)} \sigma(z)$$

Then we have the following

**Theorem 4.3.** *We have  $Tr_q(x_{nq}) = T_q(x_n)$ , it is an equality of divisors of degree  $l + 1$  on  $X_0(N)$  over  $K_m$ .*

*Proof.* See [5, §6] □

We introduced Heegner points on modular curves, now we want to define Heegner points on elliptic curves. Let  $E$  be an elliptic curve of conductor  $N$  over  $\mathbb{Q}$ . We know, by the Theorem 1.12 in §1.2, that every modular curve  $E$  over  $\mathbb{Q}$  is modular, and this means that if  $E/\mathbb{Q}$  has conductor  $N$ , there exists a parameterization, i.e., a surjective morphism  $\phi : X_0(N) \rightarrow E$  defined over  $\mathbb{Q}$ , which maps the cusp  $\infty$  of  $X_0(N)$  to the origin  $O$  of  $E$ .

**Definition 4.4.** Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with conductor  $N$  and let  $K$  be an imaginary quadratic field satisfying the Heegner hypothesis. Fix a modular parameterization  $\phi : X_0(N) \rightarrow E$ . Then the *Heegner point of conductor  $n$*  on the elliptic curve  $E$  is defined to be

$$y_n = \phi(x_n)$$

**Proposition 4.5.** *The point  $y_n \in E(\mathbb{C})$  lies in  $E(K_n)$*

*Proof.* We know that  $x_n$  lies in  $X_0(N)(K_n)$ , and since  $\phi$  is a morphism of algebraic curves defined over  $\mathbb{Q}$ , we conclude that  $y_n$  lies in  $E(K_n)$ .  $\square$

We will only consider  $y_n$  for  $n$  a square-free integer. Then we can define the trace map on Heegner points on  $E$ :

$$\text{Tr}_p : E(K_{np}) \rightarrow E(K_n), \quad z \rightarrow \sum_{\sigma \in \text{Gal}(K_{np}/K_n)} \sigma(z)$$

and the basic Heegner point:

$$y_K = \text{Tr}_{K_1/K}(y_1) = \sum_{\sigma \in \text{Gal}(K_1/K)} \sigma(y_1) \in E(K)$$

From now on, fix an odd prime  $p$  such that  $\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ , and assume  $p$  does not divide  $y_K$ , i.e., does not exist  $Q \in E(K)$  such that  $y_K = pQ$ . By Chapter 1,  $E_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ,  $\text{Aut}(E_p) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$  and we have obtained a representation  $\rho_q : G_{\overline{K}/K} \rightarrow \text{Aut}(E_q)$ . In all that follows, assume that  $E$  does not have complex multiplication over  $\mathbb{C}$ .

**Theorem 4.6.** (*Serre*) *Suppose that the elliptic curve  $E$  has no complex multiplication over  $\overline{K}$ . Then, for almost all prime numbers  $q$ , the homomorphism  $\rho_q : \text{Aut}(\overline{K}/K) \rightarrow \text{Aut}(E_q)$  is surjective.*

**Theorem 4.7.** (*Mazur*) *Let  $E/\mathbb{Q}$  be a semistable elliptic curve and  $N$  be a prime number. Then, with notation in the previous theorem, the image of  $\rho_N$  is  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  if  $N \geq 11$ .*

By previous two theorems, we see that the extension  $\mathbb{Q}(E_p)$  generated by the  $p$ -division points of  $E$  has Galois group isomorphic to  $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ . According to how we have defined the objects we are studying, we insist that every prime factor  $l$  of  $n$  does not divide  $N \cdot D \cdot p$  for all except a finite number of primes, and for all primes  $p \geq 1$ . Hence, the prime  $l$  is *unramified* in the extension  $K(E_p) = \mathbb{Q}(\sqrt{-D})(E_p)$ , and we define  $\text{Frob}(l)$  to be the conjugacy class in  $\text{Gal}(K(E_p)/\mathbb{Q})$  containing the Frobenius substitutions of the prime factors of  $l$  in  $K(E_p)$ .

Let  $Frob(\infty)$  be the conjugacy class of the complex conjugation  $\tau$ . We now state the Čebotarëv density theorem.

**Theorem 4.8.** (*Čebotarëv density theorem*) *Let  $L$  be a Galois extension of  $K$ , and let  $\langle \sigma \rangle$  be the conjugacy class of an element  $\sigma \in Gal(L/K)$ . Then the set*

$$\mathcal{S} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ in unramified in } L \text{ and } ((L/K)/\mathfrak{p}) = \langle \sigma \rangle\}$$

*has Dirichlet density*

$$\delta(\mathcal{S}) = \frac{|\langle \sigma \rangle|}{|Gal(L/K)|} = \frac{|\langle \sigma \rangle|}{[L : K]}.$$

*Proof.* See [3, Ch. 8, Thm. 8.17]. □

We consider  $K_n$  an abelian extension of  $K$ , and let  $n$  be a modulus divisible by all primes ramify in  $K_n$ . Then, given any element  $\sigma \in Gal(K_n/K)$ , the set of primes  $\mathfrak{p}$  not dividing  $n$  such that  $((K_n/K)/\mathfrak{p}) = \sigma$  has density  $\frac{1}{[K_n:K]}$ , and hence is infinite.

By Čebotarëv density theorem it follows that there are infinite primes  $l$  such that  $Frob(l) = Frob(\infty)$ , then consider an  $l$  satisfying this condition. A simple implication of the equality  $Frob(l) = Frob(\infty)$  is that  $\tau = Frob(\infty) = Frob(l)$  in  $Gal(K/\mathbb{Q})$ . Comparing the characteristic polynomial of  $Frob(l)$  acting on  $E_p$ , which is  $x^2 - a_l x + l$ , with the characteristic polynomial of  $\tau$ , that is  $x^2 - 1$ , we obtain:

$$a_l \equiv l + 1 \equiv 0 \pmod{p},$$

where  $l + 1 - a_l$  is the number of points on the reduction  $\tilde{E}$  in the finite field  $F_l = \mathbb{Z}/l\mathbb{Z}$ , and by hypothesis  $l$  is prime to  $p$ .

Consider  $\lambda$  be a prime factor of  $l$  lying over  $K$ . The fact that  $Frob(l) = \tau$  in  $Gal(K/\mathbb{Q})$  implies that the prime  $(l)$  remains inert in  $K$ , and then  $\lambda$  is unique. Let  $F_\lambda$  be the residue field of  $K$  at  $\lambda$ , which has  $l^2$  elements by previous observation. Since  $Frob(\infty) = Frob(l)$  as conjugacy classes in  $Gal(K(E_p)/\mathbb{Q})$ , the prime  $\lambda \in K$  splits completely in the extension  $K(E_p) = \mathbb{Q}(\sqrt{-D})(E_p)$ , since  $l$  is prime with  $N \cdot p \cdot D$ . Consider also that, if  $\pm$  denote the eigenspaces for the automorphism

group  $\langle 1, \tau \rangle$ , we find that  $\tilde{E}(F_\lambda)^+$  has order  $l + 1 - a_l$  and that  $\tilde{E}(F_\lambda)^-$  has order  $l + 1 + a_l$ . Since both orders of  $\tilde{E}(F_\lambda)^+$  and of  $\tilde{E}(F_\lambda)^-$  are congruent with 0 (mod  $p$ ), we have  $\tilde{E}(F_\lambda)_p^\pm \cong \mathbb{Z}/p\mathbb{Z}$ , and hence  $\tilde{E}(F_\lambda)_p \cong (\mathbb{Z}/p\mathbb{Z})^2$ , using the fact that  $\lambda$  splits completely in  $K(E_p)$ .

Our goal is to use Heegner points to study the Selmer group and the Šafarevič-Tate group.

Define  $\mathcal{G}_n = \text{Gal}(K_n/K)$  and  $G_n = \text{Gal}(K_n/K_1)$ . The exact sequence

$$0 \longrightarrow E_p \longrightarrow E \xrightarrow{p} E \longrightarrow 0$$

gives a commutative diagram:

$$\begin{array}{ccccccc}
 (**) & & & & & & 0 \\
 & & & & & & \downarrow \\
 & & & & & & H^1(K_n/K, E_p) \\
 & & & & & & \downarrow \text{Inf} \\
 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p \longrightarrow 0 \\
 & & \downarrow & & \sim \downarrow \text{Res} & & \downarrow \text{Res} \\
 0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & H^1(K_n, E)_p^{\mathcal{G}_n} \longrightarrow 0
 \end{array}$$

As we have seen,

$$0 \rightarrow E(K)/pE(K) \xrightarrow{\delta} H^1(K, E_p) \rightarrow H^1(K, E)_p \rightarrow 0,$$

$$0 \rightarrow (E(K_n)/pE(K_n))^{\mathcal{G}_n} \xrightarrow{\delta_n} H^1(K_n, E_p)^{\mathcal{G}_n} \rightarrow H^1(K_n, E)_p^{\mathcal{G}_n} \rightarrow 0,$$

$$0 \rightarrow H^1(K_n/K, E_p) \xrightarrow{\text{Inf}} H^1(K_n, E)_p^{\mathcal{G}_n} \xrightarrow{\text{Res}} H^1(K_n, E)_p^{\mathcal{G}_n}$$

are exact sequences. To prove that  $H^1(K, E_p) \xrightarrow{\text{Res}} H^1(K_n, E_p)^{\mathcal{G}_n}$  is an isomorphism, we state the following lemma.

**Lemma 4.9.** *The elliptic curve  $E$  has no  $p$ -torsion rational over  $K_n$ .*

*Proof.* If  $E$  has  $p$ -torsion rational over  $K_n$ , then either  $E_p(K_n) = \mathbb{Z}/p\mathbb{Z}$  or

$E_p(K_n) = (\mathbb{Z}/p\mathbb{Z})^2$ . If  $E_p(K_n) = \mathbb{Z}/p\mathbb{Z}$ , then  $E_p$  has a cyclic subgroup scheme over  $\mathbb{Q}$ , as  $K_n$  is Galois over  $\mathbb{Q}$ . Hence, the Galois group of  $\mathbb{Q}(E_p)$  is contained in a Borel subgroup of  $GL_2(\mathbb{Z}/p\mathbb{Z})$ . If  $E_p(K_n) = (\mathbb{Z}/p\mathbb{Z})^2$ , then  $\mathbb{Q}(E_p)$  is a subfield of  $K_n$  and we have a surjective homomorphism  $\mathcal{G}_n \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$ . This is impossible because  $\mathcal{G} = Pic(\mathcal{O}_n) \rtimes \langle 1, \tau \rangle$ , but for  $p > 2$   $GL_2(\mathbb{Z}/p\mathbb{Z})$  is not a quotient of a group of dihedral type.  $\square$

The kernel of  $H^1(K, E_p) \xrightarrow{Res} H^1(K_n, E_p)^{\mathcal{G}_n}$  is  $H^1(K_n/K, E_p(K_n))$  via inflation. In addition, using the result of the Hochschild-Serre spectral sequence, the cokernel of  $Res$  is injected into  $H^2(K_n/K, E_p(K_n)) = 0$  by transgression (see [8, Theorem 2]). By lemma 4.9,  $ker(Res) = coker(Res) = 0$ , and then we have that  $H^1(K, E_p) \xrightarrow{Res} H^1(K_n, E_p)^{\mathcal{G}_n}$  is an isomorphism.

Looking at (\*\*), it is clear why we would find an element in  $E(K_n)/pE(K_n)$  fixed by  $\mathcal{G}_n$ . First, we study the action of  $G_n = Gal(K_n/K_1)$ , and by diagram (\*) we have  $G_n = (\mathcal{O}_K/n\mathcal{O}_K)^*/(\mathbb{Z}/n\mathbb{Z})^*$ . We consider only  $n$  square-free, so let  $n = \prod l_i$ . Let  $n = l \cdot m$ , with  $(l, m) = 1$ , and consider  $K_m$  and  $K_l$  the ring class fields of conductor respectively  $l$  and  $m$ . Define  $G_l = Gal(K_n/K_m)$  the subgroup of  $G_n$  fixing  $K_m$ . We have the diagram

$$\begin{array}{ccc}
 & K_n & \\
 & \swarrow & \searrow \\
 & & G_l \\
 & & \swarrow \\
 & & K_m \\
 G_n = \frac{(\mathcal{O}_K/lm\mathcal{O}_K)^*}{(\mathbb{Z}/lm\mathbb{Z})^*} & \swarrow & \searrow \\
 & & (\mathcal{O}_K/m\mathcal{O}_K)^*/(\mathbb{Z}/m\mathbb{Z})^* \\
 & & \swarrow \\
 & & K_1
 \end{array}$$

and then  $G_l \cong \frac{(\mathcal{O}_K/lm\mathcal{O}_K)^*/(\mathbb{Z}/lm\mathbb{Z})^*}{(\mathcal{O}_K/m\mathcal{O}_K)^*/(\mathbb{Z}/m\mathbb{Z})^*} \cong (\mathcal{O}_K/l\mathcal{O}_K)^*/(\mathbb{Z}/l\mathbb{Z})^*$ .

Since for every integer  $l_i, l_j$  dividing  $n$  we have  $K_{l_i} \cap K_{l_j} = K_1$ ,  $G_{l_i} \cap G_{l_j} = 1$  and  $K_n = \prod_i K_{l_i}$ , as all factors of  $n$  are pairwise, we get

$$G_n = \prod_i G_{l_i}.$$

Furthermore, since  $\lambda = (l)$  is the unique prime factor of  $l$  in  $K$  and is inert in  $K$ ,  $(\mathcal{O}_K/l\mathcal{O}_K)^* \cong F_\lambda^*$ , and then the subgroups  $G_l \cong F_\lambda/(\mathbb{Z}/l\mathbb{Z})^* = F_\lambda^*/F_l^*$  are cyclic of order  $l + 1$ . Let  $\sigma_l$  be a generator of  $G_l$ , then the augmentation ideal of the group ring  $\mathbb{Z}[G_l]$  is principal and generated by  $(\sigma_l - 1)$ . Let now  $Tr_l = \sum_{G_l} \sigma_l$  be the trace in  $\mathbb{Z}[G_l]$  and, following the work of Rubin in [11], we define

$$D_l = \sum_{i=1}^l i\sigma_l^i \in \mathbb{Z}[G_l].$$

The element  $D_l$  is constructed to satisfy the identity

$$(***) \quad (\sigma_l - 1) \cdot D_l = l + 1 - Tr_l$$

in  $\mathbb{Z}[G_l]$ . Then  $D_l$  is well defined up to the addition of elements in the subgroup  $\mathbb{Z} \cdot Tr_l$ , and finally, we can define  $D_n = \prod D_l \in \mathbb{Z}[G_l]$ .

**Proposition 4.10.** *The point  $D_n y_n \in E(K_n)$  gives a class  $\{D_n y_n\} \in E(K_n)/pE(K_n)$ , which is fixed by  $G_n$ .*

*Proof.* It suffices to show that  $\{D_n y_n\}$  is fixed by  $\sigma_l$ , for all  $l|n$ , as these elements give  $\sigma_n$ , a generator of  $G_n$ . Hence, we must prove that  $(\sigma_l - 1)D_n y_n$  lies in  $pE(K_n)$ .

Write  $n = l \cdot m$ . By the definition of  $D_l$ , we have

$$(\sigma_l - 1)D_n = (\sigma_l - 1)D_l D_m = (l + 1 - Tr_l)D_m$$

in  $\mathbb{Z}[G_n]$ . Hence

$$\begin{aligned} (\sigma_l - 1)D_n y_n &= (l + 1 - Tr_l)D_m y_n = \\ &= (l + 1)D_m y_n - Tr_l D_m y_n = (l + 1)D_m y_n - D_m(Tr_l y_n) \end{aligned}$$

. Since  $l + 1 \equiv 0 \pmod{p}$ , it suffices to prove that  $Tr_l y_n$  lies in  $pE(K_n)$ . This follows from part (i) of the next proposition and from the congruence  $a_l \equiv 0 \pmod{p}$ .  $\square$

**Proposition 4.11.** *Let  $n = l \cdot m$ , let  $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$ .*

(i)  $Tr_l(y_{lm}) = a_l y_m$  in  $E(K_m)$ .

(ii) Each prime factor  $\lambda_n$  of  $l$  in  $K_n$  divides a unique prime  $\lambda_m$  of  $K_m$ , and we have the congruence  $y_n \equiv \text{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}$

*Proof.*

(i) This follows from the corresponding facts about the points  $x_n, x_m$  on  $X_0(N)$  over  $K_n$ . Let  $\phi$  be a modular parameterization  $\phi : X_0(N) \rightarrow E$  and let  $T_l$  denotes the Hecke correspondence defined above, which is self-dual of bidegree  $l + 1$ . By Theorem (4.4) we have  $\text{Tr}_q(x_{nq}) = T_q(x_n)$ , and by Eichler-Shimura theory we obtain  $\phi \circ T_l = a_l \phi$ . Then,

$$\text{Tr}_l(y_{lm}) = \text{Tr}_l(\phi(x_{lm})) = \phi(\text{Tr}_l(x_{lm})) = \phi(T_l(x_m)) = a_l(\phi(x_m)) = a_l y_m.$$

(ii) The prime  $\lambda = (l)$  in  $K$  is principal and is generated by an integer  $l$  prime to  $m$ , and then, by class field theory,  $\lambda$  splits completely in  $K_m/K$ . The factors  $\lambda_m$  of  $\lambda$  in  $K_m$  are totally ramified in  $K_n$ :  $\lambda_m = (\lambda_n)^{l+1}$ . In particular, the residue field  $F_{\lambda_n}$  has  $l^2$  elements and is canonically isomorphic to  $F_\lambda$ . We have the congruence:  $x_n \equiv \text{Frob}(\lambda_m)(x_m)$  on  $X_0(N)$  over  $F_{\lambda_n}$ . Indeed, by definition, the points in the divisor  $T_l(x_m)$  are the conjugates of  $x_n$  over  $K_m$ , and these are all congruent to  $x_n \pmod{\lambda_m}$  since  $\lambda_m$  is totally ramified in  $K_n/K_m$ . Using the Eichler-Shimura congruence relation  $T_l \equiv \text{Fr}_l + \text{Fr}_l^l \pmod{l}$ , we see that at least one point in the divisor  $T_l x_m$  is congruent to  $\text{Frob}(\lambda_m)(x_m) \pmod{\lambda_n}$ . Hence all points in the divisors are congruent to  $\text{Frob}(\lambda_m)(x_m)$ . This also follows from the fact that the residue field  $F_{\lambda_m}$  has  $l^2$  elements, and then  $a^l \equiv a^{\frac{1}{l}}$ .  $\square$

Since the collection of points  $y_n$  satisfy these properties, they form an Euler system, that we call the *Euler system of Heegner points*, in the language of Kolyvagin,. We will use elements of this system to construct Kolyvagin's cohomology classes  $c(n)$  in  $H^1(K, E_p)$ , which will be useful to study the Selmer group and, consequently, the Šafarevič-Tate group.

Now we return to find an element in  $E(K_n)/pE(K_n)$  fixed by  $\mathcal{G}_n$ . Observe that since  $\text{Tr}_l y_n = a_l y_m \in pK_m \subset pK_n$ , the class  $\{D_n y_n\} \in E(K_n)/pE(K_n)$  is independent on the choice of solutions  $D_l$  of  $(***)$ , but depends on the choice of

generators  $\sigma_l$  for  $G_l$ , for  $l|n$  up to scaling by  $(\mathbb{Z}/p\mathbb{Z})^\times$  ( $p$  is coprime with  $l$ ).

The group  $\mathcal{G}_n$  sits in the exact sequence

$$0 \rightarrow G_n \rightarrow \mathcal{G}_n \rightarrow Gal(K_1/K) \rightarrow 0$$

. Let  $S$  be a set of coset representatives for  $G_n$  in  $\mathcal{G}_n$ , and define

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K_n)$$

and, by Proposition 4.9, the class  $\{P_n\}$  in  $E(K_n)/pE(K_n)$  is fixed by  $\mathcal{G}_n$ , is independent on the choice of  $S$  and depends on the choice of generators  $\sigma_l$  of  $G_l$ , for  $l|n$ , only up to scaling by  $(\mathbb{Z}/p\mathbb{Z})^\times$ .

## 4.2 Kolyvagin's cohomology classes

In this section we define Kolyvagin's cohomology classes that, as claimed before, are useful to study  $Sel(E/K)_p$  and  $\text{III}(E/K)_p$ .

Define  $c(n)$  to be the unique class in  $H^1(K, E_p)$  such that:

$$Res c(n) = \delta_n \{P_n\}$$

using notation in (\*\*), recalling that  $\delta_n : (E(K_n)/pE(K_n))^{\mathcal{G}_n} \rightarrow H^1(K_n, E_p)^{\mathcal{G}_n}$  and  $Res : H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$ . We also want to associate to each  $c(n)$  in  $H^1(K, E_p)$  an element in  $H^1(K, E)_p$ , so define  $d(n)$  the image of  $c(n)$  in  $H^1(K, E)_p$ . By the commutativity of (\*\*) and the exactness of the bottom row follows that  $Res d(n) = 0$ , and then there is a unique class  $\tilde{d}(n)$  in  $H^1(K_n/K) = H^1(\mathcal{G}_n, E(K_n))_p$  such that:

$$Inf \tilde{d}(n) = d(n)$$

in  $H^1(K, E)_p$ . Summing up, we are working with the following diagram:

$$\begin{array}{ccccccc}
& & & & & & 0 \\
& & & & & & \downarrow \\
& & & & & & H^1(K_n/K, E_p) \\
& & & & & & \tilde{d}(n) \\
& & & & & & \downarrow \text{Inf} \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p \longrightarrow 0 \\
& & \downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} \\
& & & & c(n) & \longrightarrow & d(n) \\
& & & & \sim \downarrow \text{Res} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & H^1(K_n, E)_p^{\mathcal{G}_n} \longrightarrow 0 \\
& & \{P_n\} & \longrightarrow & \delta_n \{P_n\} = \text{Res } c(n) & \longrightarrow & 0
\end{array}$$

In McCallum work [9], we can also find the 1-cocycles that represent  $c(n)$  and  $d(n)$ .

**Lemma 4.12.** (a) *The class  $c(n)$  is represented by the cocycle:*

$$\sigma \rightarrow \sigma \left( \frac{1}{p} P_n \right) - \frac{1}{p} P_n - \frac{(\sigma - 1)P_n}{p}$$

on  $\text{Gal}(\overline{K}/K)$ , where  $\frac{(\sigma-1)P_n}{p}$  is the unique  $p$ -division point of  $(\sigma - 1)P_n$  in  $E(K_n)$  and  $\frac{1}{p}P_n$  is a fixed  $p$ -root of  $P_n$  in  $E(\overline{K})$ .

(b) *The class  $d(n)$  is represented by the cocycle*

$$\sigma \rightarrow \frac{(\sigma - 1)P_n}{p}$$

*Proof.* (a) The existence and the uniqueness of the  $p$ -division point follows from the fact that  $P_n \in (E(K_n)/pE(K_n))^{\mathcal{G}_n}$  and from Lemma 4.9. The uniqueness implies that  $\frac{(\sigma-1)P_n}{p}$  is a cocycle, and then the expression in the statement is a cocycle. The cocycle clearly takes values in  $E_p$ , and the first term disappears if we restrict to  $K_n$ , hence it satisfies the condition of  $c(n)$ .

(b) Regarded as a cocycle with values in  $E$ , we see that  $\sigma \rightarrow \sigma \left( \frac{1}{p} P_n \right) - \frac{1}{p} P_n$  is a coboundary, and then we obtain the statement.  $\square$

**Proposition 4.13.** (1) *The class  $c(n)$  is trivial in  $H^1(K, E_p)$  if and only if  $P_n$  is in*

$pE(K_n)$ .

(2) the class  $d(n) \in H^1(K, E)$  and the class  $\tilde{d}(n) \in H^1(K_n/K)$  are trivial if and only if  $P_n \in pE(K_n) + E(K)$ .

*Proof.* These statements follow from the definitions and from the diagram (\*\*).  $\square$

**Remark 4.14.** The class  $c(1)$  is trivial if and only if the basic Heegner point  $P_1 = y_k$  is divisible by  $p$  in  $E(K)$ , and the classes  $d(1)$  and  $\tilde{d}(1)$  are always globally trivial.

We now observe the action of  $Gal(K/\mathbb{Q}) = \langle 1, \tau \rangle$  on  $c(n)$ . Since  $p$  is odd, we have a direct sum decomposition into eigenspaces for  $\tau$ :

$$H^1(K, E_p) = H^1(K, E_p)^+ \oplus H^1(K, E_p)^-$$

We will see that the class  $c(n)$  lies in one of these eigenspaces, whose sign depends both on  $E$  and the number of primes dividing  $n$ . In the previous section, we have seen that  $\tau$  lifts to an involution of  $K_n$  and acts on  $Gal(K_n/K)$  by  $\tau\sigma\tau^{-1} = \sigma^{-1}$ , and hence  $\tau$  acts on the point  $y_n \in E(K_n)$ .

Define *canonical involution* (or *Fricke involution*)  $w_N : X_0(N) \rightarrow X_0(N)$  as the operator that takes the point  $x = (E \xrightarrow{\phi} E')$  to the point  $w_N(x) = (E' \xrightarrow{\phi'} E)$ , where  $\phi'$  is the dual isogeny (see [14, §III.6]). The action of  $w_N$  on  $X_0(N)$  is induced by the Fricke involution on  $\mathbb{H}^*$ :

$$w_N(z) = -\frac{1}{Nz}.$$

If a lattice  $\Lambda \subset \mathbb{C}$  has oriented basis  $\langle \omega_1, \omega_2 \rangle$ , the action of canonical involution  $w_N$  sends a lattice  $\Lambda \subset \mathbb{C}$  with oriented basis  $\langle \omega_1, \omega_2 \rangle$  to the involuted lattice  $w_N(\Lambda)$  with oriented basis  $\langle -\frac{1}{N}\omega_2, \omega_1 \rangle$ , and interchanges the cusps  $\infty$  and  $0$ .

Let  $\epsilon = \pm 1$  be the eigenvalue of the Fricke involution  $w_N$  on the eigenform  $f = \sum a_n q^n$  associated to the modular curve  $E$ :

$$f|w_n = \epsilon \cdot f$$

**Note 4.15.** In the next two propositions and in Chapter 5, we will study the con-

nection between the eigenvalue of the Fricke involution  $w_N$ , the eigenvalue of the complex conjugation  $\tau$  and the sign of the functional equation of the  $L$ -series of  $E$  over  $\mathbb{Q}$  (see §5.2.1).

**Proposition 4.16.** *We have  $y_n^\tau = \epsilon \cdot y_n^\sigma + (\text{torsion}) \in E(K_n)$ , for some  $\sigma \in \mathcal{G}_n$ .*

*Proof.* Let  $x_n = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\}) = \phi(y_n)$ . By [5, §4, §5], we have the identities  $x_n^\tau = (\mathcal{O}_n, \mathcal{N}_n^\tau, \{\mathfrak{a}^\tau\} = \{\mathfrak{a}\}^{-1})$ ,  $w_N((\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\}) = (\mathcal{O}_n, \mathcal{N}_n^\tau, \{\mathfrak{a}\mathcal{N}^{-1}\})$ . By proposition 4.2, we also know that  $x_n$  is rational over  $K_n$ , which is an abelian extension of  $K$  with Galois group  $\mathcal{G}_n \cong \text{Pic}(\mathcal{O}_n)$ . Then, if we consider  $\mathfrak{b}$  an ideal of  $\mathcal{O}_n$  not dividing  $n$  and  $\sigma_{\mathfrak{b}}$  the Artin symbol of  $\{\mathfrak{b}\}$  in  $\mathcal{G}_n$ , we have the formula  $(\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\})^{\sigma_{\mathfrak{b}}} = (\mathcal{O}_n, \mathcal{N}_n, \{\mathfrak{a}\mathfrak{b}^{-1}\})$ . Then  $w_N(x_n^\sigma) = (\mathcal{O}_n, \mathcal{N}_n^\tau, \{\mathfrak{a}\mathcal{N}^{-1}\mathfrak{b}^{-1}\})$ , and if we define  $\mathfrak{b}^*$  as the ideal such that  $\{\mathfrak{a}\mathcal{N}^{-1}\mathfrak{b}^{-1}\} = \{\mathfrak{a}\}^{-1}$  and  $\sigma = \sigma_{\mathfrak{b}^*} \in \mathcal{G}_n$ , we obtain the identity  $x_n^\tau = w_N(x_n^\sigma)$ . We also use the result in [6, p.228], which says that the class of the divisor  $c = (x_n) - (\infty)$  defines an element in the Jacobian  $J(K_1)$ . Hence

$$(x_n - \infty)^\tau = w_N(x_n - \infty)^\sigma + (w_n \infty - \infty).$$

Since  $w_N \infty = 0$  is the cusp of  $X_0(N)$ , and the class of  $(0 - \infty)$  is torsion in the Jacobian, this gives the claim on the curve  $E$ .  $\square$

**Proposition 4.17.** *Define  $\epsilon_n = \epsilon \cdot (-1)^{f_n}$ , where  $f_n = \{l : l|n\}$ .*

- (1) *The class  $\{P_n\}$  lies in the  $\epsilon_n$ -eigenspace for  $\tau$  in  $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$*
- (2) *The class  $c(n)$  lies in the  $\epsilon_n$ -eigenspace for  $\tau$  in  $H^1(K, E_p)$ , and the class  $d(n)$  lies in the  $\epsilon_n$ -eigenspace for  $\tau$  in  $H^1(K, E)_p$ .*

Observe that, since  $d(n) \in H^1(K, E)_p^{\epsilon_n}$ , we may refine Proposition 4.13 with the following corollary:

**Corollary 4.18.** *The class  $d(n)$  is trivial in  $H^1(E, K)_p^{\epsilon_n}$  if and only if  $P_n$  is in  $pE(K_n) + E(K_n)^{\epsilon_n}$*

*Proof.* Recall that we defined  $P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K_n)$ , for  $S$  a set of coset representatives for  $G_n$  in  $\mathcal{G}_n$ . Remember also that  $\tau$  acts on  $\mathcal{G}_n$  by  $\tau \sigma \tau^{-1} = \sigma^{-1}$ ,

hence  $\tau P_n = \sum_{\sigma \in S} \sigma^{-1} \tau D_n y_n$ .

We defined  $D_n = \prod_{l|n} D_l \in \mathbb{Z}[G_n]$ , where we defined  $D_l \in \mathbb{Z}[G_l]$  to be the solution of  $(\sigma_l - 1) \cdot D_l = l + 1 - Tr_l$  in  $\mathbb{Z}[G_l]$  and well-defined up to addition of elements in the subgroup  $\mathbb{Z} \cdot Tr_l$ . Applying  $\tau$  on the right and left of this identity, we find:  $(\sigma_l - 1)D_l \tau = \tau(\sigma_l - 1)D_l = (\sigma_l^{-1} - 1)\tau D_l = -\sigma_l^{-1}(\sigma_l - 1)\tau D_l$ . Hence

$$\tau D_l = -\sigma_l D_l \tau + m Tr_l,$$

for some  $m \in \mathbb{Z}$ , as  $\tau D_l + \sigma_l D_l \tau$  is annihilated by  $(\sigma_l - 1)$ .  $Tr_l y_n = a_l y_{n/l} \equiv 0$  in  $pE(K_n)$ , then we have

$$\tau P_n \equiv (-1)^{f_n} \cdot \prod_{l|n} \sigma_l \cdot \sum_{\sigma \in S} \sigma^{-1} \cdot D_n(\tau y_n) \pmod{pE(K_n)}.$$

Remember that by the above proposition,  $y_n^\tau = \epsilon \cdot \sigma'(y_n) + (\text{torsion}) \in E(K_n)$  for some  $\sigma' \in \mathcal{G}_n$ , and by Lemma 4.9,  $E(K_n)_p = 0$ , then  $y_n^\tau = \epsilon \cdot y_n^\sigma$ . Hence:

$$\tau P_n \equiv \epsilon_n \cdot \prod_{l|n} \sigma_l \cdot \sigma' \cdot \sum_{\sigma \in S} \sigma^{-1} \cdot D_n y_n \pmod{pE(K_n)}.$$

Note that  $\sum_{\sigma \in S} \sigma^{-1} \cdot D_n y_n \equiv P_n$ , as  $\{D_n y_n\}$  is fixed by  $G_n$  and, since  $S$  is a set of cosets representatives for  $G_n$  in  $\mathcal{G}_n$ , so is  $\{\sigma^{-1} : \sigma \in S\}$ . Since  $\{P_n\}$  is fixed by  $\mathcal{G}_n$ , we have  $\tau P_n \equiv \epsilon_n \cdot P_n \pmod{pE(K_n)}$ , which proves (1). The statements in (2) follow from (1) and from the fact that the maps in the diagram (\*\*) commute with the action of  $Gal(K/\mathbb{Q}) = \langle 1, \tau \rangle$ .  $\square$

### 4.3 Localization of Kolyvagin's classes

In this section, we study local properties of Kolyvagin's classes in  $H^1(K, E_p)$  and in  $H^1(K, E)_p$ . This will allow us to decide if the class  $c(n)$  is in the Selmer group  $Sel(E/K)_p$ , that is, if the class  $d(n)$  is locally trivial in all places  $\lambda$  of  $K$ . By Remark 4.14,  $d(1)$  and  $\tilde{d}(1)$  are always globally trivial, and then  $c(1) \in Sel(E/K)_p$ .

Let  $\lambda$  be the unique prime of  $K$  above the integer prime  $l$ , and let  $\lambda_n$  represent a prime of  $K_n$  above  $\lambda$ . We denote the completion of  $K_n$  at  $\lambda_n$  by  $K_{\lambda_n}$ . Suppose

that  $n = l \cdot m$ . The prime ideal  $\lambda$  is principle, generated by the number  $l$  prime to  $m$ , and hence splits completely in  $K_m$  by the class field theory, and each prime factor  $\lambda_m$  of  $l$  in  $K_m$  ramifies totally in  $K_n$ . In particular, there is an embedding  $K_m \hookrightarrow K_\lambda$ , and from the fact that  $P_m \in (E(K_m)/pE(K_m))^{\mathcal{G}_m}$  the resulting image of  $P_m$  in  $E(K_\lambda)/pE(K_\lambda)$  is independent on the choice of embedding.

**Proposition 4.19.** (1) *The class  $d(n)_v$  is locally trivial in  $H^1(K_v, E)_p$  at the archimedean place  $v = \infty$  and at all finite places  $v$  of  $K$  which do not divide  $n$ .*

(2) *If  $n = l \cdot m$  and  $\lambda$  is the unique prime of  $K$  dividing  $l$ , the class  $d(n)_\lambda$  is locally trivial in  $H^1(K_\lambda, E)_p$  if and only if  $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$  for one (and hence all) places  $\lambda_m$  of  $K_m$  dividing  $\lambda$ .*

*Proof.* (1). If  $v = \infty$ , then  $K_\infty = \mathbb{C}$  is algebraically closed, and then the Galois cohomology of  $E$  is trivial. If  $v \nmid n$ , then the class  $\tilde{d}(n)$  in  $H^1(K_n/K, E)_p$  satisfies  $d(n) = \text{Inf } \tilde{d}(n)$ , and  $\tilde{d}(n)$  is unramified at  $v$ . Hence  $d(n)_v$  lies in the subgroup  $H^1(K_v^{un}/K_v, E)$ , where  $K_v^{un}$  is the maximal unramified extension of  $K_v$ . This group is trivial when  $E$  has good reduction at  $v$  see [10, Chapter I, §3], so  $d(n)_v = 0$  for  $v \nmid N$ .

If  $v|N$  the curve  $E$  has a bad reduction. In this case, we can consider  $E$  as a group scheme over  $K$ , specifically, we use the Néron model [14, §C.15, p 446-448]. Let  $E^0$  be the connected component of the Neron model and  $\Phi = E/E^0$  be the group of components. Then  $H^1(K_v^{un}/K_v, E^0) = 0$ , so  $H^1(K_v^{un}/K_v, E^0) = 0$  injects into  $H^1(K_v, \Phi)$ , see [10, Chapter I, Proposition 3.8], Ch I, Prop.3.8]. But  $d(n)_v$  is represented by a cocycle with values in a subgroup  $E'$  of  $E$  with  $[E' : E^0]$  prime to  $p$ . Indeed, if  $J$  be the Jacobian of  $X_0(N)$ , then for any place  $w$  dividing  $v$  in  $K_n$ , the class of the Heegner divisor  $(x_n) - (\infty)$  in  $(K_n)_w$  lies in  $J^0$ , up to translation by the rational torsion point  $(0) - (\infty)$ , see [5, Ch. I, §3]]. Hence  $y_n$  is, up to translation by rational torsion on  $E$ , in  $E^0$ . Since  $E(\mathbb{Q})_p = 0$  by assumption, the points  $y_n$ , and consequently  $D_n y_n$  and  $P_n$ , lie in the subgroup  $E'$ , whose image in  $\Phi$  has order prime to  $p$ . Since  $d(n)_v$  is represented by a cocycle with values in the subgroup  $E'$ , we obtain  $d(n)_v = 0$ .

(2). As noted at the beginning of this section, the prime  $\lambda \in K$  splits completely in  $K_m$ , and each factor  $\lambda_m|\lambda$  in  $K_m$  is totally ramified, of degree  $l + 1$ , in  $K_n$ . The

localization  $d(n)_\lambda$  is represented by the cocycle  $\sigma \rightarrow \frac{(\sigma-1)P_n}{p}$  on  $Gal(K_{\lambda_n}/K_{\lambda_m}) \cong G_l$  with values in  $E(K_{\lambda_n})$ . Since  $n$  is prime with  $N$ ,  $l \nmid N$ , and the curve  $E$  has good reduction at  $\lambda$ . Since  $E'$  is a pro- $l$ -group and  $l \neq p$ , the cohomology group  $H^1(G_l, E^1(K_{\lambda_n}))_p = 0$ . Hence  $d(n)_\lambda$  is trivial if and only if it has trivial image in  $H^1(G_l, \tilde{E}(K_{\lambda_n}))_p = Hom(G_l, \tilde{E}(F_\lambda)_p)$ , where  $\tilde{E} = E/E^1$  is the reduced curve. The image of  $d(n)_\lambda$  is represented by the cocycle  $\sigma \rightarrow \text{reduction of } -\frac{(\sigma-1)P_n}{p}$ . Since  $G_l$  is cyclic, generated by  $\sigma_l$ , we see that the local class  $d(n)_\lambda$  is trivial if and only if:  $Q_n = \frac{(\sigma_l-1)P_n}{p}$  has trivial reduction mod  $\lambda_n$ . Since  $\sigma_l$  acts trivially on  $\tilde{E}(F_{\lambda_n}) = \tilde{E}(F_\lambda)$ , the reduction  $\tilde{Q}_n$  is contained in  $\tilde{E}(F_\lambda)_p$ .

Since we defined  $P_n = \sum_{\sigma \in S} \sigma D_n y_n = \sum_{\sigma \in S} \sigma D_m D_l y_n$  and we constructed  $D_l$  such that  $(\sigma_l - 1) \cdot D_l = l + 1 - Tr_l$ , we have

$$Q_n = \sum_{\sigma \in S} \sigma D_m \left( \frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right)$$

by Proposition 4.11,(i). By part (ii) of the same proposition, we have the congruence:

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)Frob(\lambda_m) - a_l}{p} y_m \pmod{\lambda_n}$$

at all places  $\lambda_n$  dividing  $\lambda$  in  $K_n$ . For any  $\sigma \in \mathcal{G}_n$ , we conjugate this congruence (mod  $\sigma^{-1}\lambda_n$ ) by  $\sigma$  to obtain:

$$\sigma \left( \frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \sigma \left( \frac{(l+1)Frob(\sigma^{-1}\lambda_m) - a_l}{p} \right) y_m \pmod{\lambda_n}$$

but we also see that  $\sigma \cdot Frob(\sigma^{-1}\lambda_m) = Frob(\lambda_m) \cdot \sigma$ , so we obtain:

$$\sigma \left( \frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \left( \frac{(l+1)Frob(\lambda_m) - a_l}{p} \right) \sigma y_m \pmod{\lambda_n}$$

and then:

$$Q_n \equiv \frac{(l+1)Frob(\lambda_m) - a_l}{p} P_m \pmod{\lambda_n}$$

The reduction  $\tilde{P}_m$  lies in the  $\epsilon_m$ -eigenspace for  $Frob(l)$  on  $\tilde{E}(F_\lambda)/p\tilde{E}(F_\lambda)$ . Since  $(l+1)Frob(l) - a_l$  annihilate  $\tilde{E}(F_\lambda)$ , and since the  $\epsilon_m$ -eigenspace of  $p$ -torsion is cyclic, then  $\tilde{Q}_n = 0$  if and only if  $\tilde{P}_m \in p\tilde{E}(F_\lambda)$ . As  $E^1$  is  $p$ -divisible, this is

equivalent to the divisibility  $P_m \in pE(K_{\lambda_m})$ .  $\square$

**Remark 4.20.** Let us now consider  $n = l$  prime. By Corollary 4.18, we know that the class  $d(l)$  is globally trivial if and only if  $P_l \in pE(K_l) + E(K)$ . Now we can state that  $d(l)$  is locally trivial at all places  $v \neq l$  of  $K$ , and is locally trivial at  $\lambda$  if and only if  $P_1 = y_K \in pE(K_\lambda)$ .

To conclude this study on localization of Kolyvagin's cohomology classes  $c(n)_\lambda$ , we now apply the Tate pairing described in Chapter 3 in this specific local situation. As before, we consider  $K$  an imaginary quadratic extension of  $\mathbb{Q}$ ,  $\lambda = (l)$  an inert prime in  $K$  and  $K_\lambda$  the completion of  $K$  at  $\lambda$ . Assume also that  $p$  is odd and  $l$  satisfies congruences  $l + 1 \equiv a_l \equiv 0 \pmod{p}$ . The elliptic curve  $E$  is defined over  $\mathbb{Q}$ , so  $\text{Gal}(K/\mathbb{Q}) = \text{Gal}(K_\lambda/\mathbb{Q}_l) = \langle 1, \tau \rangle$  acts on the  $\mathbb{Z}/p\mathbb{Z}$ -vector spaces  $E(K_\lambda)/pE(K_\lambda)$  and  $H^1(K_\lambda, E)_p$ .

**Proposition 4.21.** (1) *The eigenspaces  $(E(K_\lambda)/pE(K_\lambda))^\pm$  and  $H^1(K_\lambda, E)_p^\pm$  for  $\text{Gal}(K_\lambda/\mathbb{Q}_l)$  each have dimension 1 over  $\mathbb{Z}/p\mathbb{Z}$ .*

(2) *The Tate pairing  $\langle, \rangle$  induces a non-degenerate pairing of  $\mathbb{Z}/p\mathbb{Z}$ -vector spaces*

$$\langle, \rangle^\pm : (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(K_\lambda, E)_p^\pm \rightarrow \mathbb{Z}/p\mathbb{Z}$$

*In particular, if  $d_\lambda \neq 0$ , lies in  $H^1(K_\lambda, E)_p^\pm$  and  $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^\pm$  satisfies  $\langle s_\lambda, d_\lambda \rangle = 0$ , then  $s_\lambda \equiv 0 \pmod{pE(K_\lambda)}$ .*

*Proof.* (1) We have isomorphisms of  $\text{Gal}(K_\lambda, \mathbb{Q}_l)$ -modules:

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} E(K_\lambda)_p, \quad H^1(K_\lambda, E)_p \xrightarrow{\sim} \text{Hom}(\mu_p(K_\lambda), E(K_\lambda)_p)$$

. Since  $l + 1 \equiv 0 \pmod{p}$ ,  $\mu_p(K_\lambda) = \mu_p(K_\lambda)^-$ . Hence

$$E(K_\lambda)_p^\pm \cong (E(K_\lambda)/pE(K_\lambda))_p^\pm \cong H^1(K_\lambda, E)_p^\mp$$

, and all eigenspaces have dimension 1.

(2) It suffices to check that the  $\pm$ -eigenspaces for  $\tau$  are orthogonal under  $\langle, \rangle$ . But the Tate pairing satisfies  $\langle c_1^\tau, c_2^\tau \rangle = \langle c_1, c_2 \rangle$ , because  $\tau$ , which we defined to be

the complex conjugation in  $Gal(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$  with  $D$  prime to  $p$ , acts trivially on  $H^2(K_\lambda, \mu_p) = \mathbb{Z}/p\mathbb{Z}$ . Since  $p$  is odd, the result follows.  $\square$

## 5 Kolyvagin's work on Modular Elliptic Curves

### 5.1 Description of $Sel(E/K)_p$

In this section, we want to give a concrete description of the  $Sel(E/K)_p$ .

First, we apply Proposition 4.21 to the specific subgroup  $Sel(E/K)_p$  of  $H^1(K, E)_p$ , where we use the full power of global class field theory studied in Chapter 2.

**Proposition 5.1.** *Assume that the class  $d \in H^1(K, E)_p^\pm$  is locally trivial for all places  $v \neq \lambda$  of  $K$ , but that  $d_\lambda \neq 0$  in  $H^1(K_\lambda, E)_p^\pm$ . Then, for any class  $s$  in the subgroup  $Sel(E/K)_p^\pm \subset H^1(K, E)_p^\pm$ , we have  $s_\lambda = Res_{K_\lambda}(s) = 0$  in  $H^1(K_\lambda, E_p)^\pm$ .*

*Proof.* We remark that  $Sel(E/K)_p = ker(H^1(K, E)_p \rightarrow \prod_{all\ v} H^1(K_v, E)_p)$ . By this definition, the restriction  $s_\lambda$  lies in  $(E(K_\lambda)/pE(K_\lambda))^\pm$ . Then it suffices, by Proposition 4.21, to show that  $\langle s_\lambda, d_\lambda \rangle = 0$ . To do this, following diagram (\*\*), we lift  $d \in H^1(K, E)_p$  to a class  $c \in H^1(K, E_p)$ , which is well defined modulo the image  $\delta(E(K)/pE(K))$ . The global pairing  $\langle s, c \rangle_K$ , induced by the cup-product, lies in  $H^2(K, \mu_p) = Br(K)_p = \bigoplus_{all\ v} Br(K_v)_p$ , and by Corollary 3.4 it is completely determined by its local components  $\langle s_v, c_v \rangle \in Br(K_v)_p$  for all places  $v$  in  $K$ . But  $\langle s_v, c_v \rangle = 0$  for all  $v \neq \lambda$ , as  $d_v = 0$  in  $H^1(K_v, E)_p$  by assumption. By the reciprocity law of the global class field theory (see Theorem 3.5), the sum of local invariants of a global class is 0, and then we must have  $\langle s, c \rangle_K = \sum_{all\ v} \langle s_v, c_v \rangle = \langle s_\lambda, c_\lambda \rangle = \langle c_\lambda, d_\lambda \rangle = 0$  □

We now return to the study of cohomology classes  $d(n) \in H^1(K, E)_p$  constructed in Chapter 4, whose local properties are stated in Proposition 4.19, and we consider only global classes satisfying Proposition 5.1. Following Kolyvagin's idea, this will allow us to bound the order of  $Sel(E/K)_p$ .

Recall that we are under the hypothesis that  $p$  is an odd prime and that the Galois group of  $\mathbb{Q}(E_p)$  is isomorphic to  $GL_2(\mathbb{Z}/p\mathbb{Z}) \cong Aut(E_p)$ . Let  $L = K(E_p)$ . We consider  $K$  imaginary quadratic field of discriminant  $-D$  prime to  $N \cdot p$ , and then  $K$  and  $\mathbb{Q}(E_p)$  are disjoint. Let  $L = K(E_p)$ . Hence  $\mathcal{G} = Gal(L/K)$  is isomorphic to  $GL_2(\mathbb{Z}/p\mathbb{Z})$ , and contains the central group  $Z \cong (\mathbb{Z}/p\mathbb{Z})^*$  of homotheties of  $E_p$ .

Since  $Z$  has order  $|\mathbb{Z}/p\mathbb{Z}| = p - 1$ , which is prime to  $p$ , we have  $H^1(Z, E_p) = 0$  for  $n \geq 1$ . Since  $p$  is odd, then  $Z \neq 1$  and  $H^0(Z, E_p) = E_p^Z = 0$ .

**Proposition 5.2.** *We have  $H^n(\mathcal{G}, E_p) = 0$  for all  $n \geq 0$ . The restriction of classes gives an isomorphism of  $\text{Gal}(K/\mathbb{Q})$ -modules:*

$$\text{Res} : H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(\text{Gal}(\overline{\mathbb{Q}}/L), E_p(L))$$

*Proof.* We have seen  $H^1(Z, E_p) = 0$  for  $n \geq 0$ . Furthermore, by the spectral sequence  $H^m(\mathcal{G}/Z, H^n(Z, E_p)) \Rightarrow H^{m+n}(\mathcal{G}, E_p)$ , follows the disappearance of the cohomology of  $\mathcal{G}$  in  $E_p$  (see [12]). The kernel of  $\text{Res}$  is  $H^1(\mathcal{G}, E_p) = 0$  and the cokernel injects into  $H^2(\mathcal{G}, E_p) = 0$  via transgression in the Hochschild-Serre spectral sequence (see [8]), and then the restriction is an isomorphism.  $\square$

From this proposition, we obtain the pairing:

$$[\cdot, \cdot] : H^1(K, E_p) \times \text{Gal}(\overline{\mathbb{Q}}/L) \rightarrow E_p(L)$$

which satisfies  $[s^\sigma, \rho^\sigma] = [s, \rho^\sigma] = [s, \rho]^\sigma$  for all  $s \in H^1(K, E_p), \rho \in \text{Gal}(\overline{\mathbb{Q}}/L)$  and  $\sigma \in \mathcal{G} = \text{Gal}(L/K)$ . Note that, by injectivity of restriction, if  $[s, \rho] = 0$  for all  $\rho \in \text{Gal}(\overline{\mathbb{Q}}/L)$ , then  $s \equiv 0$ .

We wish to exploit this pairing in case of specific subgroups of  $H^1(K, E_p)$ . Consider a finite subgroup  $S \subset H^1(K, E_p)$  (i.e., finite-dimensional vector space over  $\mathbb{Z}/p\mathbb{Z}$ ). Let  $\text{Gal}_S(\overline{\mathbb{Q}}/L)$  be the subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/L)$  such that, if  $\rho \in \text{Gal}_S(\overline{\mathbb{Q}}/L)$ , then  $[s, \rho] = 0$  for all  $s \in S$ . Let  $L_S$  be the fixed field of  $\text{Gal}_S(\overline{\mathbb{Q}}/L)$ . Then  $L_S$  is a finite normal extension of  $L$ .

We want to see how the previous pairing behaves with  $\text{Sel}(E/K)_p \subset H^1(K, E_p)$ .

**Proposition 5.3.** *The induced pairing  $[\cdot, \cdot] : S \times \text{Gal}(L_S/L) \rightarrow E_p(L)$  is non-degenerate.*

*It induces an isomorphism of  $\mathcal{G}$ -modules:*

$$\text{Gal}(L_S/L) \xrightarrow{\sim} \text{Hom}(S, E_p(L))$$

and an isomorphism of  $\text{Gal}(K, \mathbb{Q})$ -modules:

$$S \xrightarrow{\sim} \text{Hom}_{\mathcal{G}}(\text{Gal}(L_S/L), E_p(L))$$

*Proof.* If there exists  $\rho \in \text{Gal}(L_S/L)$  such that  $[s, \rho] = 0$  for all  $s \in S$ , then  $\rho \in \text{Gal}_S(\overline{\mathbb{Q}}/L)$ , but by definition  $L_S$  is the fixed field of  $\text{Gal}_S(\overline{\mathbb{Q}}/L)$ , and the fact that  $\rho \in \text{Gal}(L_S/L)$  implies that  $\rho$  is the trivial element. Then the induced pairing is non-degenerate. By the definition of  $L_S$  and the injectivity of restriction  $H^1(K, E_p) \xrightarrow{\sim} \text{Hom}_{\mathcal{G}}(\text{Gal}(\overline{\mathbb{Q}}/L), E_p(L))$ , pairing  $[\cdot, \cdot] : S \times \text{Gal}(L_S/L) \rightarrow E_p(L)$  induces injections  $\text{Gal}(L_S/L) \hookrightarrow \text{Hom}(S, E_p)$  and  $S \hookrightarrow \text{Hom}_{\mathcal{G}}(\text{Gal}(L_S/L), E_p)$ . If we define  $r = \dim(S)$ , then these two injections show that  $\text{Gal}(L_S/L)$  is a  $\mathcal{G}$ -module of  $\text{Hom}(S, E_p) \cong E_p^r$ . Since  $E_p$  is a simple  $\mathcal{G}$ -module,  $E_p^r$  is semi-simple. Any submodule of a semi-simple module is semi-simple, hence we have an isomorphism of  $\mathcal{G}$ -modules  $\text{Gal}(L_S/L) \xrightarrow{\sim} E_p^s$ , for  $s \leq r$ . Then

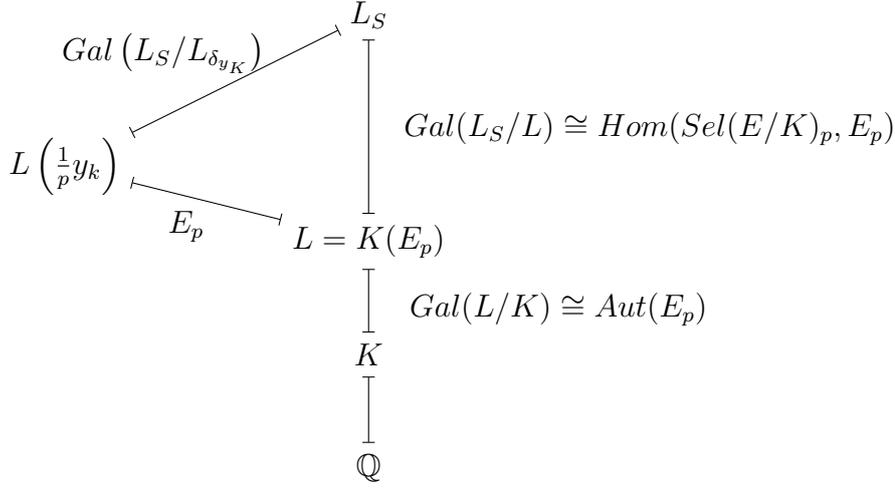
$$\text{Hom}_{\mathcal{G}}(\text{Gal}(L_S/L), E_p) \cong (\mathbb{Z}/p\mathbb{Z})^s,$$

but  $\text{Hom}_{\mathcal{G}}(\text{Gal}(L_S/L), E_p)$  contains  $S$  and  $S \cong (\mathbb{Z}/p\mathbb{Z})^r$ . Then  $s = r$  and the previous injections are both isomorphisms.  $\square$

First, we apply Proposition 5.3 to the finite subgroup  $S = \text{Sel}(E/K)_p$  of  $H^1(K, E_p)$ .

In order to prove the main theorem, assume that  $y_K \in E(K)$ , the basic Heegner point, has infinite order in  $E(K)$ . By the Mordell-Weil theorem, the group  $E(K)$  is finitely generated, and then the point  $y_K$  is not infinitely divisible in  $E(K)$ , that is, there are only finitely many integers  $n$  such that  $y_K = nP$  with  $P \in E(K)$ .

Consider  $p$  an odd prime that satisfies the conditions imposed so far and that does not divide  $y_K$  in  $E(K)$ . To  $y_K \in (E(K)/pE(K))^\epsilon$  we associate the point  $\frac{1}{p}y_K$  in  $E(K)_p^\epsilon$ . Let  $\delta y_K$  be the non-zero image of  $\text{Sel}(E/K)_p^\epsilon$ , then  $L\left(\frac{1}{p}y_K\right) = L_{\delta y_K}$ . Here is a field diagram.



Observe that the extension  $L_{\delta_{y_K}}$  of  $L = K(E_p)$  has Galois group isomorphic to  $E_p$ . For simplicity in notation, we let  $H = \text{Gal}(L_S/L)$  and  $I = \text{Gal}(L_S/L_{\delta_{y_K}})$  be the subgroup of  $H$  which fixes the subfield  $L\left(\frac{1}{p}y_k\right) = L_{\delta_{y_K}}$ . Let  $\tau$  be a fixed complex conjugation in  $\text{Gal}(L_S/\mathbb{Q})$ , and let  $H^\pm$  and  $I^\pm$  denote the  $\pm$ -eigenspace for  $\tau$ , acting by conjugation, on  $H$  and  $I$ .

**Proposition 5.4.** *With previous notation, the following statements hold:*

1. We have  $H^+ = \{(\tau h)^2 : h \in H\}$ ,  $I^+ = \{(\tau i)^2 : i \in I\}$  and  $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$ .
2. Let  $s \in \text{Sel}(E/K)_p^\pm$ . Then the following are equivalent:
  - (a)  $[s, \rho] = 0 \quad \forall \rho \in H$
  - (b)  $[s, \rho] = 0 \quad \forall \rho \in H^+$
  - (c)  $[s, \rho] = 0 \quad \forall \rho \in H^+ - I^+$
  - (d)  $s = 0$

*Proof.* (1). Since  $p$  is odd,  $H^+ = H^{\tau+1} = \{h^\tau \cdot h : h \in H\}$ . But  $\tau$  act by conjugation and  $h^\tau = \tau h \tau^{-1} = \tau h \tau$ , so  $h^\tau h = (\tau h)^2$ . The same works for  $I^+$ . Finally, as can be seen from the diagram above,  $E_p = H/I$ , and then we obtain  $H^+/I^+ = (H/I)^+ = E_p^+ \cong \mathbb{Z}/p\mathbb{Z}$ .

(2). Clearly, (d) $\Rightarrow$ (a), and from the fact that the induced pairing  $[, ]$  in Proposition 5.3 is nondegenerate, (a) $\Rightarrow$ (d). Also,  $H^+ - I^+ \subset H^+ \subset H$ , and then (a) $\Rightarrow$ (b) $\Rightarrow$ (c). So,

it suffices to prove (c) $\Rightarrow$ (b) $\Rightarrow$ (a). Note that  $s : H^+ \rightarrow E_p$  is a group homomorphism and  $L_{\delta_{y_k}} \subsetneq L_S \Rightarrow I^+ \subsetneq H^+$ . Hence, the fact that  $s$  vanishes on  $H^+ - I^+$  implies that  $s$  vanishes on the entire group  $H^+$ . From the second isomorphism in Proposition 5.3,  $s \in Sel(E/K)_p^\pm$  induces a  $\mathcal{G}$ -homomorphism  $H \rightarrow E_p$ , which maps  $H^+ \rightarrow E_p^\pm, H^- \rightarrow E_p^\mp$ . If  $s$  vanishes on  $H^+$ , the image  $s(H)$  is therefore contained in  $E_p^\mp$ , so we have seen in previous proof that  $s(H)$  is a  $\mathcal{G}$ -submodule of the simple module  $E_p$ , either  $s(H) = E_p$  or  $s(H) = 0$ .  $\square$

Let now see local properties of  $Sel(K/K)_p$ .

**Proposition 5.5.** *For  $s \in Sel(E/K)_p \subset H^1(K, E_p)$  the following are equivalent:*

- (a)  $[s, \rho] = 0$ , where  $\rho$  is the Frobenius substitution associated to the factor  $\lambda_{L_S}$  of  $\lambda$  in  $H = Gal(L_S/L)$
- (b)  $[s, Frob(\lambda)] = 0$
- (c)  $s_\lambda \equiv 0$  in  $H^1(K_\lambda, E_p)$

*Proof.* For the previous observation on the properties of pairing  $[, ]$ , we have that  $[s^\sigma, \rho^\sigma] = [s, \rho^\sigma] = [s, \rho]^\sigma$  for all  $s \in H^1(K, E_p), \rho \in Gal(\overline{\mathbb{Q}}/L), \sigma \in \mathcal{G}$ . For every  $\rho$  exists  $\sigma \in \mathcal{G}$  such that  $\rho = Frob(\lambda)^\sigma$ , and then

$$0 = [s, \rho] = [s, Frob(\lambda)^\sigma] = [s, Frob(\lambda)]^\sigma.$$

Hence (a) $\Leftrightarrow$ (b).

To prove (a) $\Leftrightarrow$ (c), we assume  $s_\lambda \equiv P_\lambda$  in  $E(K_\lambda)/pE(K_\lambda) \hookrightarrow H^1(K_\lambda, E_p)$ . Then  $\frac{1}{p}P_\lambda$  is rational over  $L_{S\bar{\lambda}}$ , where  $\bar{\lambda} = \lambda_{L_S}$  divides  $\lambda$  in  $L_S$ , and we obtain  $[s, \rho] = \left(\frac{1}{p}P_\lambda\right)^{\rho^{-1}}$  in  $E(L_{S\bar{\lambda}})_p \cong E(L_S)_p$ . Hence we have  $[s, \rho] = 0$  if and only if  $P_\lambda \in pE(K_\lambda)$ , and by Proposition 4.19 we have this if and only if  $s_\lambda$  is locally trivial in  $H^1(K_\lambda, E_p)$   $\square$

Now we again exploit the notions derived from the study of  $E$  as a modular curve. Let  $\epsilon$  be the eigenform of the Fricke involution on the eigenform  $f$  associated to  $E$ , described in Section 4.2. By Proposition 4.16, we know that the basic Heegner point  $y_k = P_1$  lies in the  $\epsilon_1 = \epsilon$ -eigenspace for complex conjugation  $\tau$  on  $E(K)/pE(K)$ . By previous hypothesis, we also consider  $p$  such that

$\delta y_K \in Sel(E/K)_p$ , and then we see that  $\delta y_K$  lies in  $Sel(E/K)_p^\epsilon$ .

$Sel(E/K)_p^\epsilon$  is not empty; we want to prove in following proposition that the same is not true for the  $-\epsilon$ -eigenspace.

**Proposition 5.6.**  $Sel(E/K)_p^{-\epsilon} = 0$

*Proof.* Assume  $s \in Sel(E/K)_p^{-\epsilon} = 0$ . By Proposition 5.4, to prove  $s = 0$  it is enough to show  $[s, \rho] = 0$  for all  $\rho \in H^+ - I^+$ . By the same proposition, we also know that if  $\rho \in H^+ - I^+$ , then exists  $h \in H$  such that  $\rho = (\tau h)^2$ .

By Chebotarev's density theorem, there exist infinitely many rational primes that are unramified in the extension  $L_S/\mathbb{Q}$  and that have a factor  $\lambda_{L_S}$  in  $L_S$  whose Frobenius substitution is equal to  $\tau h$  in  $Gal(L_S/\mathbb{Q})$ . Let  $l$  be one of them primes. Then, by class field theory,  $(l) = \lambda$  is inert in  $K$  and splits completely in  $L = K(E_p)$ . By Proposition 5.5,  $[s, \rho] = 0$  if and only if  $s_\lambda \equiv 0$  in  $H^1(K_\lambda, E_p)$ . Note that  $F_{\lambda_{L_S}}/F_\lambda \cong L_S/K$ , and then the Frobenius substitution of  $F_{L_S}/F_\lambda$  is equal to  $(\tau h)^2 = \rho$ .

Let  $c(l) \in H^1(K, E_p)$  be the cohomological class constructed in the previous chapter, and let  $d(l)$  be its image in  $H^1(K, E)_p$ . We consider  $l$  prime and then, by Proposition 4.16, both classes lie in the  $\epsilon_l = -\epsilon$ -eigenspace for  $\tau$ . By Proposition 4.19,  $d(l)_v \neq 0$  if  $v \neq \lambda$  and  $d(l)_\lambda$  is trivial if and only if  $y_K \in pE(K_\lambda)$ . Note that  $y_K \in pE(K_\lambda)$  is equivalent to saying that the prime  $\lambda \in K$  splits completely in the extension  $L \left( \frac{1}{p}y_K \right) = L_{\delta y_K}$ . Since we defined  $Frob(\lambda) = \rho$  not in  $I^+ = H^+ \cap I$ , this splitting does not occur, and then we we claim  $d(l)_\lambda \neq 0$ .

Hence are verified hypothesis to apply Proposition 5.1, and we conclude that  $s_\lambda \equiv 0$  in  $H^1(K_\lambda, E_p)^{-\epsilon}$ , and we obtain the statement.  $\square$

**Proposition 5.7.** *Assume that  $y_K$  is not divisible by  $p$  in  $E(K)$ . Let  $l$  be a rational prime which is unramified in  $L_S/\mathbb{Q}$  and has a factor  $\lambda_{L_S}$  whose Frobenius substitution is equal to  $\tau h$  in  $Gal(L_S/\mathbb{Q})$ , with  $h \in H = Gal(L_S/L)$ . Then  $\lambda = (l)$  is inert in  $K$  and splits completely in  $L = K(E_p)$ . The following are equivalent:*

- (1)  $c(l) \equiv 0$  in  $H^1(K, E_p)$
- (2)  $c(l) \in Sel(E/K)_p \subset H^1(K, E_p)$
- (3)  $P_l$  is divisible by  $p$  in  $E(K_l)$

- (4)  $d(l) \equiv 0$  in  $H^1(K, E)_p$   
(5)  $d(l)_\lambda \equiv 0$  in  $H^1(K_\lambda, E)_p$   
(6)  $P_1 = y_K$  is locally divisible by  $p$  in  $E(K_\lambda)$   
(7)  $h^{1+\tau}$  lies in the subgroup  $I^+ = I \cap H^+$  of  $H^+$ .

*Proof.* (1) $\Leftrightarrow$ (2): If  $c(l) \in \text{Sel}(E/K)_p$ , then  $c(l) \in \text{Sel}(E/K)_p^{-\epsilon} = 0$  by previous proposition. Conversely, if  $c(l) \equiv 0$  then  $c(l) \in \text{Sel}(E/K)_p$  by definition of Selmer group.

(1) $\Leftrightarrow$ (3) because, by Proposition 4.19,  $c(l) \equiv 0$  if and only if  $P_l \in pE(K_l)$ .

(1) $\Leftrightarrow$ (4): by exactness of sequence in theorem 1.28,  $\text{Sel}(E/K)_p^{-\epsilon} = 0$  implies  $E(K)/pE(K) = 0$ , and  $c(l) \equiv 0$  is equivalent to  $d(l) \equiv 0$ .

(4) $\Leftrightarrow$ (5) By Proposition 4.19,  $d(l)_v$  is locally trivial at every place except perhaps, and by Proposition 5.6 follows that  $\text{III}(E/K)_p^{-\epsilon} = 0$ , hence  $d(l) \equiv 0$  if and only if  $d(l)_\lambda = 0$ .

(5) $\Leftrightarrow$ (6) by remark 4.20,  $d(l)$  is locally trivial at all places  $v \neq l$  of  $K$ , and is locally trivial at  $\lambda$  if and only if  $P_1 = y_K \in pE(K_\lambda)$ .

(6) $\Leftrightarrow$ (7)  $y_K \in pE(K_\lambda)$  is equivalent to say that the prime  $\lambda$  splits completely in the extension  $L \left( \frac{1}{p}y_K \right)$ , and then  $\tau h \in I$ , from which it follows that  $h^{1+\tau} \in I \cap H^+$ .  $\square$

**Proposition 5.8.**  $\text{Sel}(E/K)^\epsilon \cong \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$ .

*Proof.* Let  $s \in \text{Sel}(E/K)_p^\epsilon$ .  $\text{Sel}(E/K)_p^\epsilon$  can have at most dimension 1 over  $\mathbb{Z}/p\mathbb{Z}$ , so I want to prove that  $s$  is a multiple of  $\delta y_K$ . If we prove  $[s, \rho] = 0$  for all  $\rho \in I$ , then  $s \in \text{Hom}_{\mathcal{G}}(H/I, E_p)$ . Indeed, since the induced pairing  $[, ]$  described in Proposition 5.3 is non-degenerate, the fact that  $[s, \rho] = 0 \quad \forall \rho \in I$  implies that  $I$  is trivial, and then

$$H \cong H/I = \text{Gal}(L_S/L) / \text{Gal}(L_S/L_{\delta y_K}) \cong L_{\delta y_K} / L = L \left( \frac{1}{p}y_K \right) / L$$

for the fundamental theorem of Galois theory. By Proposition 5.3, we have the isomorphism  $S \xrightarrow{\sim} \text{Hom}_{\mathcal{G}}(H, E_p(L)) \cong \text{Hom}_{\mathcal{G}}(H/I, E_p)$ , and since  $\mathcal{G} = \text{Aut}(E_p)$  and  $\text{Gal}(H/I) \cong E_p$ , we obtain  $\text{Hom}_{\mathcal{G}}(H/I, E_p) \cong \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$ . By Proposition 5.4, to prove  $[s, \rho] = 0$  for all  $\rho \in I$  it suffices to prove  $[s, \rho] = 0$  for all  $\rho \in I^+$ ,

and by Proposition 5.4 follows that, if  $\rho \in I^+$ , then  $\rho = (\tau i)^2$  for some  $i \in I$ .

Consider  $l'$  to be a prime such that  $c(l')$  is non-trivial in  $H^1(K, E_p)$ . By Proposition 5.7,  $c(l')$  is not in  $\text{Sel}(E/K)_p$ , so the extension  $L' = L_{c(l')}$  of  $L = K(E_p)$  has Galois group isomorphic to  $E_p$  and is disjoint from the extension  $L_S/L$ . By Proposition 5.7, we can obtain  $l'$  as a rational prime which is unramified in  $L_S/\mathbb{Q}$  with a factor  $\lambda_{L_S}$  whose Frobenius substitution is equal to  $\tau h$ , taking  $h \in H$  such that  $h^{1+\tau} \notin I^+$ . If a prime ideal  $\lambda = (l) \in K$  splits completely in  $L$ , it splits completely also in  $L'$  if and only if  $P_{l'} \in pE(K_{\lambda'}) = pE(K_\lambda)$ , for all factors  $\lambda_{l'}$  of  $\lambda$  in  $K_{l'}$ .

We want a prime  $l$  such that  $c(l) \in \text{Sel}(E/K)_p$ . Let  $l$  be a prime whose Frobenius substitution is conjugate to  $\tau i \in \text{Gal}(L_S/\mathbb{Q})$ , with  $i \in I = \text{Gal}(L_S/L_{\delta y_K})$ , and such that  $\tau i$  is conjugate to  $\tau j \in \text{Gal}(L'/\mathbb{Q})$ , where  $j \in \text{Gal}(L'/L)$  and satisfies  $j^{1+\tau} \neq 1$ . These two conditions can be satisfied simultaneously because  $(l) = \lambda$  splits completely both in  $L_S$  and  $L'$ , and  $L'/L$  is disjoint from  $L_S/L$  ( $L' \cap L_S = L$ ). We want to compare  $c(l)$  and  $c(l')$ , then claim that the class  $d(l \cdot l')$  in  $H^1(K, E)_p^\epsilon$  is locally trivial for all places  $v \neq \lambda$ , but  $d(l)_\lambda \neq 0$ . By Proposition 4.19 follows the triviality for all  $v \neq \lambda, \lambda'$ , where  $\lambda'$  is prime in  $K$  dividing  $l'$ . Since Frobenius substitution of  $l$  is conjugate to  $\tau i$  with  $i \in I$ , by Proposition 5.7  $c(l) \equiv 0$ , and  $P_l \in pE(K_l)$ . Since  $P_l \in pE(K_l)$ , then it is divisible by  $p$  at  $E(K_{\lambda'}) = E(K_{\lambda'})$ , and then by Proposition 4.19 we obtain that  $d(l \cdot l')_{\lambda'}$ . Then it remains to be proven that  $d(l \cdot l') \neq 0$ , but we know that  $d(l \cdot l')_\lambda$  is trivial if and only if  $P_{l'} \in pE(K_\lambda)$ , and this is equivalent to claim that  $\lambda$  splits in  $L'$ , or equivalently that  $(\tau j)^2 = j^{\tau+1} = 1$ , and this contradicts our hypothesis on  $j$ .

We have proved that the class  $d = d(l \cdot l') \in H^1(K; E)_p^\epsilon$  satisfies hypothesis of Proposition 5.1, and then  $s_\lambda = 0$  for all  $s \in \text{Sel}(E/K)$ , and then  $[s, \rho] = 0$  with  $\rho = (\tau i)^2$  defined above.

Now, for every  $\rho = i^{1+\tau} \in I^+$  we can find a couple of primes  $l, l'$  that satisfies conditions as above, and then we obtain that  $s(I^+) = s(I) = 0$ .  $\square$

In conclusion, we can state the following proposition.

**Proposition 5.9.** *Let  $p$  be an odd prime such that  $\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ , and assume that  $p$  does not divide  $y_K$  in  $E(K)$ . Then the group  $\text{Sel}(E/K)_p$  is cyclic,*

generated by  $\delta y_K$ .

## 5.2 Birch and Swinnerton-Dyer conjecture and Kolyvagin's theorem

In this section we present some important results on the group of rational points  $E(K)$  of an elliptic curve  $E$  over an imaginary quadratic field  $K$ , under specific hypothesis.

Let  $X_0(N)$  be a modular curve over  $\mathbb{Q}$ . We recall that, by remark 1.10,  $X_0(N)$  classifies elliptic curves with a cyclic  $N$ -isogeny. Let  $K = \mathbb{Q}(\sqrt{-D})$  be an imaginary quadratic field of discriminant  $-D$ , where all prime factors of  $N$  are split. For simplicity, we assume that  $D \neq 3, 4$ , so the ring of integers  $\mathcal{O}_K$  of  $K$  has unit group  $\mathcal{O}_K^\times = \langle \pm 1 \rangle$ . Choose an ideal  $\mathcal{N}$  of  $\mathcal{O}_K$  with  $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ . Then the complex tori  $\mathbb{C}/\mathcal{O}$  and  $\mathbb{C}/\mathcal{N}^{-1}$  define elliptic curves related by a cyclic  $N$ -isogeny, and hence a point  $x_1 \in X_0(N)$ . We have seen in Chapter 2 that the point  $x_1$  is rational over the Hilbert class field  $K_1$  of  $K$ .

Let  $E$  be an elliptic curve of conductor  $N$  over  $\mathbb{Q}$ , and let us fix a parametrization  $\phi : X_0(N) \rightarrow E$  which maps the cusp  $\infty$  of  $X_0(N)$  to the origin  $O$  of  $E$ . Once  $\phi$  has been fixed, there is a unique invariant differential  $\omega$  on  $E$  over  $\mathbb{Q}$  such that  $\phi^*(\omega)$  is the differential  $\sum a_n q^n dq/q$  associated to a normalized newform on  $X_0(N)$ . Consider  $\omega_0$  a Néron differential on  $E$ , then it is known that exists an integer  $c \geq 1$  such that  $\omega_0 = c\omega$ .

In the next section, we define some elements that are necessary to state the Birch and Swinnerton-Dyer conjecture and the Kolyvagin's theorem, of which we will write the statement and a partial demonstration in the second section.

### 5.2.1 L-series and the conjecture of Birch and Swinnerton-Dyer

The  $L$ -series of an elliptic curve is a generating function that records information about the reduction of the curve modulo every prime. Known results are fragmentary, but conjecturally such  $L$ -series contain a large amount of information concerning the set of global points on the curve. Further, there are intimate relations

connecting  $L$ -series on elliptic curves defined over  $\mathbb{Q}$  and the theory of modular forms. Let  $E/K$  be an elliptic curve and let  $v$  be a finite place at which  $E$  has good reduction. We denote the residue field of  $K$  at  $v$  by  $k_v$ , the reduction of  $E$  at  $v$  by  $\tilde{E}_v$ , and let  $q_v = \#k_v$  be the norm of the prime ideal corresponding to  $v$ . We recall from [14, V, §2] that the *Zeta function* of  $\tilde{E}_v/k_v$  is the power series

$$Z(\tilde{E}_v/k_v; T) = \exp\left(\sum_{n=1}^{\infty} \tilde{E}_v(k_{v,n}) \frac{T^n}{n}\right)$$

where  $k_{v,n}$  is the unique extension of  $k_v$  of degree  $n$ .

**Theorem 5.10.** *Let  $\tilde{E}_v/k_v$  be an elliptic curve, and let  $a_v = q_v + 1 - \tilde{E}_v(k_v) \in \mathbb{Z}$ .*

*Then*

$$Z(\tilde{E}_v/k_v, T) = \frac{1 - a_v T + q_v T^2}{(1 - T)(1 - q_v T)}.$$

*Further,*

$$Z(\tilde{E}_v/k_v, 1/q_v T) = Z(\tilde{E}_v/k_v, T),$$

*and  $1 - a_v T + q_v T^2 = (1 - \alpha T)(1 - \beta T)$ , with  $|\alpha| = |\beta| = \sqrt{q_v}$ .*

*Proof.* See [14, §V, 2.4]. □

Define  $L_v(T) = 1 - a_v T + q_v T^2 \in \mathbb{Z}[T]$ , then  $Z(\tilde{E}_v/k_v, T)$  is a rational function,  $Z(\tilde{E}_v/k_v, T) = \frac{L_v(T)}{(1-T)(1-q_v T)}$ . We extend the definition of the function  $L_v(T)$  to the case where  $E$  has a bad reduction by setting

$$L_v(T) = \begin{cases} 1 - T & \text{if } E \text{ has split multiplicative reduction at } v \\ 1 + T & \text{if } E \text{ has nonsplit multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v \end{cases}$$

Then in all cases we have the relation

$$L_v(1/q_v) = \tilde{E}_{ns}(k_v)/q_v$$

Let us define  $M_K^0$  to be the set of the nonarchimedean absolute values in  $K$ .

**Definition 5.11.** The  $L$ -series of  $E/K$  is defined by the Euler product

$$L(E/K, s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1}.$$

The product defined above converges and gives an analytic function for all  $s$  such that  $\operatorname{Re}(s) > \frac{3}{2}$  (see [14, §V, 2.4]).

**Theorem 5.12.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . The  $L$ -series  $L(E/\mathbb{Q}, s)$  has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at  $s$  and  $2 - s$ .*

*Proof.* See [14, §C.16.1]. □

We want to better analyze the functional equation in Theorem 5.12. Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and let  $N$  be the conductor of  $E/\mathbb{Q}$ . The  $L$ -function  $L(E, s)$  is a Dirichlet series  $\sum_{n \geq 1} a_n n^{-s}$  defined by an Euler product which determines the number of points on  $E \pmod{p}$  for all primes  $p$  (see [6, §I.7, p.231]). We know that the function  $f_E(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$ , called "inverse Mellin transform" of  $L$ , is a newform of weight 2 and level equal to  $N$  (see [14, § C.16, Theorem 16.4.a]). We define a new function:

$$L^*(E/\mathbb{Q}, s) = \int_0^\infty f\left(\frac{iy}{\sqrt{N}}\right) y^s \frac{dy}{y} = N^{s/2} (s\pi)^{-s} \Gamma(s) L(E/\mathbb{Q}, s)$$

where  $\Gamma$  is the gamma function (see [6, Chapter 1, §7]). Then Theorem 5.12 has the following more precise formulation.

**Theorem 5.13.** *Let  $E/\mathbb{Q}$  be an elliptic curve. Then the function  $L^*(E, s)$  has an analytic continuation to the entire complex plane and satisfies the functional equation*

$$L^*(E/\mathbb{Q}, s) = \epsilon_L L^*(E/\mathbb{Q}, 2 - s), \quad \text{for some } \epsilon_L = \pm 1$$

*Proof.* See [6, Ch 5] □

**Remark 5.14.** Note that, because of the sign inversion  $s \rightarrow s + 1$ , if we derive in  $s$  we obtain

$$\frac{d^r}{ds^r} L^*(E/\mathbb{Q}, s) = (-1)^r \epsilon_L \cdot \frac{d^r}{ds^r} L^*(E/\mathbb{Q}, 2 - s)$$

Observe that, if we consider this equality for  $s = 1$ , we obtain

$$L(E/\mathbb{Q}, 1) = \epsilon_L L(E/\mathbb{Q}, 1),$$

and consequently  $L'(E/\mathbb{Q}, 1) = -\epsilon_L L'(E/\mathbb{Q}, 1)$ . Hence, if we assume by hypothesis that  $L(E/\mathbb{Q}, 1) = 0$  and  $L'(E/\mathbb{Q}, 1) \neq 0$ , then we must consider  $\epsilon_L = -1$ . In general, we have that

$$\text{ord}_{s=1} L(E/\mathbb{Q}, s) \text{ is odd} \iff \epsilon_L = -1$$

The modularity of elliptic curves over  $\mathbb{Q}$  and its implications for  $L$ -series are described in the next result (see [14, §C.16, Theorem 16.4]).

**Theorem 5.15.** *Let  $E/\mathbb{Q}$  be an elliptic curve of conductor  $N$ , let  $L(E, s) = \sum_{n \geq 1} a_n n^{-s}$  be its  $L$ -series and let  $f_E(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$  be the inverse Mellin transform of  $L$ . (1) For each prime  $p \nmid N$ , let  $T(p)$  be the associated Hecke operator, and let  $w_N$  be the Fricke involution defined by  $(w_N f)(\tau) = f(-\frac{1}{N\tau})$ . Then:*

$$T(p)f_E = a_p f_E \quad \text{and} \quad w_N f_E = \epsilon_L f_E$$

where  $\epsilon_L = \pm 1$  is the sign of the functional equation in Theorem 5.13.

(2) Let  $\omega$  be an invariant differential on  $E/\mathbb{Q}$ . Then there exists a finite morphism  $\phi : X_0(N) \rightarrow E$  defined over  $\mathbb{Q}$  such that  $\phi^*(\omega)$  is a multiple of the differential form on  $X_0(N)$  represented by  $f(z)dz$ .

**Remark 5.16.** Let  $\epsilon_N = \pm 1$  be the eigenvalue of the Fricke involution  $w_N$  on the eigenform  $f$  associated to the modular curve  $E$  defined in §4.2 ( $f|w_N = \epsilon f$ ). The equality  $L^*(E/\mathbb{Q}, s) = \epsilon_L L^*(E/\mathbb{Q}, 2 - s)$ , and in particular the reflection respect to  $s \rightarrow 2 - s$ , implies that there is an inversion of symmetry between the Fricke involution and the functional equation (observe that in Theorem 5.15 we use the inverse Mellin transform  $f_E$  of the eigenform  $f$ , that changes the sign respect to the canonical involution  $w_N$ ). Then the  $L$ -function of  $E$  over  $\mathbb{Q}$  satisfies a functional

equation with sign  $\epsilon_L = -\epsilon_N$ , and then we obtain the functional equation:

$$L^*(E/\mathbb{Q}, s) = -\epsilon_N L^*(E/\mathbb{Q}, 2 - s),$$

see [6, §IV, 0.2].

The next conjecture involves the behavior of the  $L$  series of elliptic curves around  $s = 1$ .

**Conjecture 5.17.** (Birch and Swinnerton-Dyer) *Let  $E/\mathbb{Q}$  be an elliptic curve.*

(i)  $L(E/\mathbb{Q}, s)$  has a zero at  $s = 1$  of order equal to the rank of  $E(\mathbb{Q})^2$ .

(ii) Let  $r = \text{rank } E(\mathbb{Q})$ . Then:

$$\lim_{s \rightarrow 1} \frac{L(E/\mathbb{Q}, s)}{(s - 1)^r} = \frac{\int_{E(\mathbb{R})} |\omega| \cdot \#\text{III}(E/\mathbb{Q}) R(E/\mathbb{Q}) \prod_p \mathfrak{m}_p}{\#E_{\text{tors}}(\mathbb{Q})^2}$$

where  $R(E/\mathbb{Q})$  is the elliptic regulator of  $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$ , computed using the canonical height pairing (see [14, §VIII.9, p. 253]), and  $\mathfrak{m}_p = \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ , with  $E_0(\mathbb{Q}_p)$  the set of points of  $E(\mathbb{Q}_p)$  with non-singular reduction.

As described by Tate in 1974, “this remarkable conjecture relates the behavior of a function  $L$  at a point where it is not at present known to be defined to the order of a group III which is not known to be finite!” Now we want to study this conjecture in our case.

**Remark 5.18.** The conjecture of Birch and Swinnerton-Dyer predicts that the integer  $r = \text{ord}_{s=1} L(E/\mathbb{Q}, s)$  is equal to the rank of the finitely generated abelian group  $E(\mathbb{Q})$  of rational points.

**Theorem 5.19.** *Let  $K$  be an imaginary quadratic field with class number 1, and  $E$  be an elliptic curve defined over  $K$  or  $\mathbb{Q}$ , with complex multiplication by the ring of integers  $\mathcal{O}_K$  of  $K$ . If  $F$  is  $K$  or  $\mathbb{Q}$  and  $\text{rank}(E/F) \geq 1$ , then  $L(E/F, s)$  vanishes at  $s = 1$ .*

*Proof.* See [2, §6]. □

In the following statement, we also see a partial converse to previous theorem.

**Remark 5.20.** A partial converse to the previous theorem is stated in [4]. Assume that  $E$  is an elliptic curve defined over  $\mathbb{Q}$  with complex multiplication by the ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . If  $L(E/\mathbb{Q}, s)$  has an odd order zero at  $s = 1$ , then either  $E(\mathbb{Q})$  has rank  $\geq 1$  or the  $p$ -primary subgroup of  $\text{III}(E/\mathbb{Q})$  is infinite for all primes  $p$  where  $E$  has good, ordinary reduction (except possibly  $p = 2, 3$ ). Note that the latter possibility is unlikely, to say the least.

### 5.2.2 Kolyvagin's theorem

In this last section, we want to link  $L$ -series with the results we obtained on the Kolyvagin system of Heegner points, and we will study a particular case of Birch and Swinnerton-Dyer conjecture.

First, we introduce the definition of *canonical height* of a point in  $E$ , which gives us information about the subgroup  $E(K)/E_{\text{tors}}(K)$ .

**Definition 5.21.** The *canonical* (or *Néron-Tate*) *height* on  $E/K$ , denoted by  $\hat{h}$  or  $\hat{h}_E$ , is the function

$$\hat{h} : E(\overline{K}) \rightarrow \mathbb{R}$$

defined by

$$\hat{h}(P) = \frac{2}{\deg(f)} \lim_{N \rightarrow \infty} 4^{-N} h_f([2^N]P),$$

where  $f \in K(E)$  is any nonconstant even function and  $h_f$  is the *height on  $E$  relative to  $f$*  (see [14, §VIII.6]).

We use the canonical height  $\hat{h}$  because it is independent on the function  $f$  (see [14, §VIII.9.1]) and gives important information about the order of a point in  $E$ .

**Theorem 5.22.** (*Néron-Tate*) *Let  $E/K$  be an elliptic curve,  $\hat{h}$  be the canonical height on  $E$  and  $P \in E(\overline{K})$ . Then:*

- (i)  $\hat{h}(P) \geq 0$
- (ii)  $\hat{h}(P) = 0$  if and only if  $P$  is a torsion point.

*Proof.* See [14, p. VIII.9.3.d] □

By the definition of the basic Heegner point:  $y_K = \text{Tr}_{K_1/K}(y_1) \in E(K)$  in §4.1, where  $y_1 = \phi(x_1) \in K_1$ . Observe that, if we consider an ideal  $\mathcal{N}' \neq \mathcal{N}$

that satisfies the same condition  $\mathcal{O}_K/\mathcal{N}' \cong \mathbb{Z}/p\mathbb{Z}$ , then any Heegner point  $y'_1$  of conductor 1 relative to  $\mathcal{N}'$  is conjugate to  $y_K$ . Hence, if we construct the basic Heegner point  $y'_K = \text{Tr}_{K_1/K}(y'_1)$ , we see that  $y'_K = \pm y_K + (\text{torsion})$ . Then, by theorem 5.18, the canonical height  $\hat{h}(y_K)$  is well defined, independent of the choice of the ideal  $\mathcal{N}$ . Thanks to Gross and Zagier's work, we can link the notions of L-series and canonical height with the limit formula [6, §1.6.5]:

$$L'(E/K, 1) = \frac{\int \int_{E(\mathbb{C})} \omega \wedge \bar{i}\omega}{\sqrt{D}} \cdot \hat{h}(y_K).$$

Observe that it follows that the point  $y_K$  has infinite order if and only if

$$L'(E/K, 1) \neq 0.$$

By comparing this with Birch and Swinnerton-Dyer conjecture, following the work of Gross and Zagier (see [6, Chapter V, 2.2]), we obtain the following conjecture.

**Conjecture 5.23.** *Assume that  $\hat{h}(y_K) \neq 0$ . Then:*

- (i) *the group  $E(K)$  has rank 1, so the index  $I_K = [E(K) : \mathbb{Z}y_K]$  is finite,*
- (ii) *the Tate-Shafarevic group  $\text{III}(E/K)$  is finite, and its order is given by*

$$\#\text{III}(E/K) = \left( \frac{I_K}{c \cdot \prod_{p|N} \mathfrak{m}_p \cdot \mathfrak{u}_K} \right)^2$$

where  $\mathfrak{u}_K = \text{Card}(\mathcal{O}_K^\times / \langle \pm 1 \rangle)$  (recall that we are considering cases where  $\mathfrak{u}_K = 1$ ), using notation for Néron model (see [14, §C.15]), where  $\mathfrak{m}_p = \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$  and  $c$  the integer such that  $\omega_0 = c\omega$ .

Note that both the index  $I_K$  and the integer  $c$  are such that  $\omega_0 = c\omega$  depends on the fixed parameterization  $\phi$ , but the ratio  $I_K/c$  is independent of  $\phi$ .

Note also that, since  $\#\text{III}(E/K)$ ,  $I_K$  and the local factors  $\mathfrak{m}_p$  are integers, the formula in (ii) predicts that  $\#\text{III}(E/K)$  should always divide  $(I_K)^2$ . By the existence of Cassels-Tate pairing  $\langle, \rangle : \text{III}(E/K) \rightarrow \text{III}((E/K)^\vee)$ , this implies that the group  $\text{III}(E/K)$  should always be annihilated by  $I_K$ .

Kolyvagin has proved a large part of this conjecture, and we will sketch the proof of a slightly weaker result to illustrate Kolyvagin's main theorem.

**Remark 5.24.** As we have seen in §5.1, the group  $E(K)$  is finitely generated, according to the Mordell-Weil theorem, and then the point  $y_K$  is not infinitely divisible in  $E(K)$

By Theorem 1.29, we have the exact sequence

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} Sel(E/K)_p \longrightarrow \text{III}(E/K)_p \longrightarrow 0$$

and using this fact, from Proposition 5.9 we deduce the following proposition.

**Proposition 5.25.** *Let  $p$  be an odd prime such that  $Gal(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$ , and assume that  $p$  does not divide  $y_K$  in  $E(K)$ . Then:*

- (1) *the group  $E(K)$  has rank 1,*
- (2) *the  $p$ -torsion subgroup  $\text{III}(E/K)_p$  is trivial.*

*Proof.* By Proposition 5.9, we see that  $Sel(E/K)_p$  is cyclic and generated by the image of the non-trivial element  $y_K$  in  $E(K)/pE(K)$  through the injective function  $\delta : E(K)/pE(K) \rightarrow Sel(E/K)_p$ . Because of the exact sequence  $0 \rightarrow E(K)/pE(K) \xrightarrow{\delta} Sel(E/K)_p \xrightarrow{g} \text{III}(E/K)_p \rightarrow 0$ , it follows that  $Sel(E/K)_p = Im(\delta) = Ker(g)$ , and then  $Im(g) = \text{III}(E/K)_p$  is trivial. By Remark 1.10 and by results in §4.1, almost all odd primes satisfies required hypothesis, and then, by Proposition 5.9,  $E(K) = \langle y_K \rangle + E_{tors}(K)$ .  $\square$

When  $y_K$  has infinite order in  $E(K)$ , i.e.,  $\hat{h}(y_K) \neq 0$ , this proposition applies for almost all primes  $p$ . Observe that our hypotheses imply that  $p$  does not divide the index  $I_K = [E(K) : \mathbb{Z}y_K]$ , so the conclusion is consistent with part (ii) of the conjecture. By refining the argument for primes  $p$  which divide  $y_K$ , using the fact that  $p^n$  does not divide  $y_K$  for large  $n$ , Kolyvagin obtains the following theorem.

**Theorem 5.26.** *(Kolyvagin) Assume that the point  $y_K$  has infinite order in  $E(K)$ . Then*

- (1) *the group  $E(K)$  has rank 1.*

(2) the group  $\text{III}(E/K)$  is finite, of order dividing  $t_{E/K} \cdot (I_K)^2$ , where  $t_{E/K}$  is an integer  $\geq 1$ , whose prime factors depend only on the curve  $E$ .

**Remark 5.27.** By Remark 1.28, the Shafarevich-Tate group  $\text{III}(E/K)$  is the group of homogeneous spaces, modulo equivalence, that are everywhere locally trivial.

In Proposition 5.14, we have considered primes  $p$  that do not divide the Heegner point  $y_K$  of finite order. To describe  $\text{III}(E/K)$ , we could analyze  $\text{III}(E/K)_p$  for primes  $p$  that divide  $y_K$  in  $E(K)$ . The cohomology classes  $d(n) \in H^1(K, E)_p$  constructed in §4.2 are candidates for non-trivial elements in  $\text{III}(E/K)_p$ .

Let us conclude by citing more recent studies, which relate the Gross, Zagier and Kolyvagin studies on  $E(K)$  to the points of  $E(\mathbb{Q})$ . In the previous section, we stated results on  $L(E/\mathbb{Q}, s)$ , now we want to connect these propositions with  $L(E/K, s)$ , where  $K = \mathbb{Q}(\sqrt{-D})$  is the imaginary quadratic field of discriminant  $D$ .

**Theorem 5.28.** *Let  $f$  be cuspidal newform of even weight  $k$  with trivial character for the group  $\Gamma_0(N)$ , and let  $S$  be a finite set of primes including all those dividing  $N$ . Let  $\epsilon_L$  denote the sign in the functional equation of  $f$ .*

(i) *There exists a quadratic field  $\mathbb{Q}(\sqrt{D})$ , with  $D$  a fundamental discriminant, and  $\epsilon_L \cdot D < 0$ , such that every prime in  $S$  splits in  $\mathbb{Q}(\sqrt{D})$ , and  $L(f, s, \chi_D)$  has a simple zero at  $s = k/2$ , where  $\chi_D$  is the quadratic Dirichlet character associated with  $K$ .*

(ii) *There exists a quadratic field  $\mathbb{Q}(\sqrt{D})$ , with  $D$  a fundamental discriminant, and  $\epsilon_L \cdot D > 0$ , such that every prime in  $S$  splits in  $\mathbb{Q}(\sqrt{D})$ , and  $L(f, k/2, \chi_D) \neq 0$ .*

*Proof.* See [1, §1]. □

Let  $f$  be a modular form of weight two associated with an elliptic curve  $E$  defined over  $\mathbb{Q}$ . The significance of the point (ii) is that if  $L(f, 1) = L(E/\mathbb{Q}, 1) \neq 0$ , then according to the results of Gross and Zagier, the existence of such a twist implies the non-vanishing of the associated Heegner point in the twisted curve  $E^K$  whose  $L$ -function is  $L(E, s, \chi_D)$ . By Kolyvagin's work, this in turn implies the finiteness of  $E(\mathbb{Q})$ , and of the Tate-Shafarevich group  $\text{III}(E/\mathbb{Q})$ .

Let us now return to the assumptions imposed in Kolyvagin's work, assume  $L(f, s) = L(E/\mathbb{Q}, 1) = 0$  and  $L'(E/\mathbb{Q}, 1) \neq 0$  (i.e.  $\epsilon_L = -1$ ). By the formula

$$L(E/K, s) = L(E^K/\mathbb{Q}, s) \cdot L(E/\mathbb{Q}, s),$$

where  $E^K/\mathbb{Q}$  is the twisted curve  $E/\mathbb{Q}$  on the field  $K$ , we obtain:

$$L'(E/K, s) = L(E^K/\mathbb{Q}, s) \cdot L'(E/\mathbb{Q}, s) + L'(E^K/\mathbb{Q}, s) \cdot L(E/\mathbb{Q}, s).$$

By hypothesis,  $L'(E/K, 1) = L(E^K/\mathbb{Q}, 1) \cdot L'(E/\mathbb{Q}, 1)$ , and Theorem 5.28 states that there exists an imaginary quadratic field  $K$  that satisfies hypothesis for Kolyvagin's theorem and such that  $L(f, 1, \chi_D) = L(E^K/\mathbb{Q}, 1) \neq 0$ , and consequently  $L'(E/K, 1) \neq 0$ . Then, the basic Heegner point  $y_K$  has infinite order, and by Kolyvagin's theorem the group  $E(K)$  has rank 1, so  $E(K) \cong \mathbb{Z} \oplus E_{tors}(K)$ . Since  $E(\mathbb{Q}) \subset E(K)$ , results that  $r_{\mathbb{Q}} = \text{rank } E(\mathbb{Q}) \leq 1$ .

Our claim now is to demonstrate that  $y_K \in E(\mathbb{Q})$ . Let  $\epsilon_N$  be the eigenvalue of the Fricke involution  $w_N$  on the eigenform associated to  $E$  and  $\epsilon_L$  be the sign of the functional equation relative to the  $L$ -function of  $E$ . By Remarks 5.14 and 5.16 we know that, under the previous hypothesis on  $L$  and  $L'$ ,  $\epsilon_L = -1$  and then  $\epsilon_N = +1$ . Moreover, by Proposition 4.17,  $y_K = P_1$  lies in the  $\epsilon_N$ -eigenspace for the complex conjugation  $\tau$  in  $E(K)$ .

$$y_K \in E(K)^+ = E(K)^{\tau=+1} = \left\{ \frac{(x, y) + \tau(x, y)}{2} \in K^2 : (x, y) \in E(K) \right\}.$$

We have  $\frac{(x, y) + \tau(x, y)}{2} = (\Re(x), \Re(y)) \in \mathbb{Q}^2$ , and if  $(x, y)$  satisfies the Weierstrass equation of the curve  $E$ , so does  $(\Re(x), \Re(y))$ . Then  $E(K)^+ \subset E(\mathbb{Q})$ , and thus  $y_K \in E(\mathbb{Q})$ .

Since  $y_K \in E(\mathbb{Q}) \cong \mathbb{Z}^{r_{\mathbb{Q}}} + E_{tors}(K)$  is of infinite order in  $E(K)$ , it is of infinite order  $E(\mathbb{Q})$ , and then  $r_{\mathbb{Q}} = 1$ .

In conclusion, the results of Kolyvagin and Gross-Zagier imply the following cases of the point (i) in the Birch and Swinnerton-Dyer conjecture for elliptic curves

defined over  $\mathbb{Q}$ :

$$L_E(1) \neq 0 \quad \Rightarrow \quad \text{rank } E(\mathbb{Q}) = 0$$

$$L_E(1) = 0 \text{ and } L'_E(1) \neq 0 \quad \Rightarrow \quad \text{rank } E(\mathbb{Q}) = 1$$

## Bibliography

- [1] D. Bump, S. Friedberg, and J. Hoffstein. “Nonvanishing theorems for L-functions of modular forms and their derivatives”. In: *Inventiones mathematicae* 102, pp. 543-618 (1990).
- [2] J. Coates and A. Wiles. “On the Conjecture of Birch and Swinnerton-Dyer”. In: *Inventiones mathematicae* 39, pp. 223-251 (1977).
- [3] D. A. Cox. *Primes of the Form  $x^2 + ny^2$ , 2nd Edition*. Wiley, 2013.
- [4] R. Greenberg. “On the Birch and Swinnerton-Dyer Conjecture”. In: *Inventiones mathematicae* 72, pp. 241-265 (1983).
- [5] B. H. Gross. “Heegner points on  $X_0(N)$ ”. In: *Modular forms (R.A.Rankin)* (1984).
- [6] B. H. Gross and D.B.Zagier. “Heegner points and derivatives of L-series”. In: *Inventiones mathematicae* 84, pp. 225-232 (1986).
- [7] B. Gross. “Kolyvagin’s work on modular elliptic curves”. In: *Cambridge Univ. Press* 153, pp.235-256 (1991).
- [8] G. Hochschild and J. Serre. “Cohomology of group extensions”. In: *Trans. Amer. Math. soc.* 74, pp. 110-134 (1953).
- [9] W. G. McCallum. “Kolyvagin’s work on Shafarevich-Tate groups”. In: *University of Arizona* (2003).
- [10] J. S. Milne. *Arithmetic duality theorems*. Vol. 1. Perspective in Mathematics. Academic Press, 1986.
- [11] K. Rubin. *Appendix to S. Lang, Cyclotomic fields I and II*. Springer-Verlaag, 1990.
- [12] J. Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”. In: *Inventiones mathematicae* 15 (1972).
- [13] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, 1994.

- [14] J. H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition*. Vol. 106. Graduate Texts in Mathematics. Springer, 2009.
- [15] J. Tate. “Duality theorems in Galois cohomology over number fields”. In: *Proc. ICM Stockholm (1962)*.
- [16] J. T. Tate. *Global Class Field Theory*. Algebraic number theory, pp. 162-203. J. Cassels and A. Frohlich, 1967.