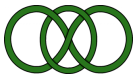
Università degli Studi di Genova

Dipartimento di Matematica

Tesi di Laurea Magistrale in

Matematica



Anno accademico 2024/2025

Tesi Magistrale

Modular Curves and arithmetic applications

Candidato
Giovanni Battista Isetti

Relatore
Prof. Stefano Vigni

Correlatore
Prof. Arvid Perego

Contents

Introduction

The study of the solutions to polynomial equations, or their zeros, within a given field (typically $\mathbb{Q}$ or its completions) represents one of the oldest and most profound pillars of number theory. While the problem of finding roots for a single polynomial in one variable is elegantly addressed by the Fundamental Theorem of Algebra and Galois theory, the complexity increases significantly when considering equations in two or more variables. This transition marks the shift from elementary algebra to the study of the arithmetic properties of algebraic curves.

Among these, elliptic curves occupy a central role. Defined by a cubic equation of the form

$$y^2 = x^3 + Ax + B,$$

these objects are not merely geometric curves but possess a rich group structure on their set of rational points. A fundamental result in this direction is the Mordell-Weil Theorem, which describes the algebraic structure of an elliptic curve.

> **Theorem.** *Let E be an elliptic curve over a number field K. The group $E(K)$ of K-rational points is a finitely generated abelian group.*

An immediate consequence of this result is that the group of K-rational points of E admits a decomposition:

$$E(K) \cong \mathbb{Z}^r \oplus E_{\text{tors}}(K)$$

where $E_{\text{tors}}(K)$ is the finite subgroup consisting of the torsion points of $E(K)$, and $r \in \mathbb{N}$ is the *rank* of $E(K)$.

While the torsion subgroup is effectively computable and its structure is constrained by deep results such as Mazur's Theorem, the rank r is a much more mysterious invariant; its determination remains one of the most challenging and central problems in the arithmetic of elliptic curves. Although the Mordell–Weil Theorem guarantees that r is a finite integer, it is essentially non-effective, as it does not provide a general algorithm to compute the rank for a given curve E.

In this thesis, we focus on a major breakthrough in this direction: the results obtained by Victor Kolyvagin. His work provides a powerful tool to bound the rank of an elliptic curve and represents one of the most significant pieces of evidence for the finiteness of the arithmetic invariants associated with E.

Roughly speaking, Kolyvagin's theorem establishes that, under certain conditions, the existence of a single point $y_K \in E(K)$ of infinite order is sufficient to control the structure of the entire group of rational points. Here, K is not an arbitrary number field, but a quadratic imaginary field. Specifically, his results allow us to prove that $r = 1$ in many cases where classical methods fail to provide an answer. More precisely, we will prove the following result:

> **Theorem.** *Assume that the elliptic curve $E/\mathbb{Q}$ does not have complex multiplication and that the point y_K has infinite order in $E(K)$. Then the rank of $E(K)$ is equal to* 1.

We remark that the assumption that E does not have complex multiplication is hardly a loss of generality in the rational case. Indeed, there are only thirteen possible j-invariants of elliptic curves over $\mathbb{Q}$ with complex multiplication.

The proof of this theorem is far from elementary and requires a vast theoretical framework that spans several areas of modern number theory. We will move from the classical geometry of algebraic curves and the analytic properties of modular forms to the sophisticated language of Galois cohomology and the theory of Complex Multiplication. This interplay between different mathematical disciplines is what makes Kolyvagin's result one of the most elegant achievements in arithmetic geometry.

The thesis is structured as follows:

Chapter 1 provides the necessary background on elliptic curves, covering their arithmetic over local and global fields and their complex analytic description.

Chapter 2 introduces the theory of modular curves and their moduli interpretation, culminating in the Eichler–Shimura construction which relates modular forms to elliptic curves.

Chapter 3 is devoted to the theory of Complex Multiplication. Here we define Heegner points and study their field of definition, providing the geometric "input" for Kolyvagin's machinery.

Chapter 4 contains the core of the work: the construction of the Euler system of cohomology classes and the complete proof of Kolyvagin's Theorem regarding the rank of $E(K)$ and the finiteness of the Shafarevich–Tate group.

Chapter 1

Elliptic Curves

1.1 Background on algebraic curves

Let K be a field and denote by $\overline{K}$ a fixed algebraic closure of K.

Definition 1.1.1. *The n-dimensional affine space over K is*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) := \{(x_1, \ldots, x_n) : x_i \in \overline{K} \text{ for all } i\}.$$

Note that if we consider

$$G_K := \mathrm{Gal}(\overline{K}/K) = \mathrm{Aut}_K(\overline{K}) = \{\sigma : \overline{K} \to \overline{K} : \sigma(x) = x \text{ for all } x \in K\},$$

then we have an action of G_K on $\mathbb{A}^n$ defined by the rule

$$P^\sigma := (\sigma(x_1), \ldots, \sigma(x_n))$$

for all $P = (x_1, \ldots, x_n) \in \mathbb{A}^n$ and $\sigma \in G_K$. In this sense we define the set of K-rational points of $\mathbb{A}^n$ as

$$\mathbb{A}^n(K) := (\mathbb{A}^n)^{G_K} := \{P \in \mathbb{A}^n | P^\sigma = P \text{ for all } \sigma \in G_K\}.$$

Definition 1.1.2. *Let $\overline{K}[X] := \overline{K}[x_1, \ldots, x_n]$ be the polynomial ring over $\overline{K}$.*

(a) If $I \subseteq \overline{K}[X]$ is an ideal we will call algebraic affine variety

$$\mathcal{V}(I) := \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Conversely, if $V \subseteq \mathbb{A}^n$ is an algebraic set, we will consider

$$\mathcal{I}(V) := \{f \in \overline{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

(b) An affine variety V is said to be defined over K if the ideal $\mathcal{I}(V)$ can be generated by polynomials over K. In this case we will write $V_{/K}$.

(c) If V is defined over K. Then, the set of K-rational points of V is

$$V(K) := V \cap \mathbb{A}^n(K).$$

Note that if V is an affine variety and we consider with a slight abuse of notation

$$\mathcal{I}(V_{/K}) := \{f \in K[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V\},$$

then V is defined over K if and only if $\mathcal{I}(V) = \mathcal{I}(V_{/K}) \cdot \overline{K}[X]$.

Definition 1.1.3. *The The affine coordinate ring of $V_{/K}$ is the quotient*

$$K[V] = K[X]/\mathcal{I}(V_{/K}).$$

In particular, if $\mathcal{I}(V)$ is a prime ideal of $K[X]$, then $K[V]$ is an integral domain and we can define the field of rational functions on $V_{/K}$ as its fraction field:

$$K(V) := \mathrm{Frac}(K[V]).$$

Analogously, one can define $\overline{K}[V] := \overline{K}[X]/\mathcal{I}(V)$ and consider $\overline{K}(V)$ if $\mathcal{I}(V)$ is a prime ideal of $\overline{K}[X] \cap \mathcal{I}(V) = \mathcal{I}(V/K)$. Hence, we obtain an embedding

$$K[V] \hookrightarrow \overline{K}[V],$$

and if it is possible to consider the field of fractions, we also obtain an embedding of the corresponding function fields

$$K(V) \hookrightarrow \overline{K}(V).$$

Using this notation, the absolute Galois group G_K acts on $\overline{K}[X]$ via its action on the coefficients, and consequently on $\overline{K}[V]$ and, where defined, on $\overline{K}(V)$. In particular

$$K[V] = \overline{K}[V]^{G_K}.$$

Definition 1.1.4. *Let $V_1, V_2 \subseteq \mathbb{P}^n$ be two projective varieties. A rational map between them is*

$$\varphi : V_1 \longrightarrow V_2$$

with $\varphi = [f_0 : \cdots : f_n]$ where the functions $f_0, \ldots, f_n \in \overline{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,

$$\varphi(P) = [f_0(P) : \cdots : f_n(P)] \in V_2.$$

Moreover φ is said to be defined over K if there exists $\lambda \in \overline{K}^\times$ such that

$$\lambda f_0, \ldots, \lambda f_n \in K(V_1).$$

Equivalently, φ is defined over K if and only if $\varphi^\sigma = \varphi$ for all $\sigma \in G_K$ where

$$\varphi^\sigma := [f_0^\sigma : \cdots : f_n^\sigma].$$

Proposition 1.1.5. *Let C_1, C_2 be two curves (i.e. projective varieties of dimension one) and let $\varphi : C_1 \to C_2$ be a morphism. Then φ is either constant or surjective.*

Proof. See [Har13, Chapter 2, Proposition 6.8]. □

Note that if C_1, C_2 are two curves defined over K and $\varphi : C_1 \to C_2$ is a nonconstant rational map defined over K, then we have an induced fields immersion

$$\varphi^* : K(C_2) \longrightarrow K(C_1), \qquad f \mapsto f \circ \varphi$$

which fixes K, i.e. is a K-immersion.

Proposition 1.1.6. *The field extension $K(C_1)/\varphi^*(K(C_2))$ is finite.*

Proof. See [Sil09, Chapter 1, Theorem 2.4]. □

Definition 1.1.7. *Let $\varphi : C_1 \to C_2$ be a rational maps between curves defined over K. We define the degree of φ to be*

$$\deg(\varphi) := \begin{cases} 0 & \text{if } \varphi \text{ is constant,} \\ [K(C_1) : \varphi^*(K(C_2))] & \text{otherwise.} \end{cases}$$

In the following chapters, we will frequently make use of the theory of divisors associated with a curve, as they provide a powerful framework for studying the geometry and the arithmetic of algebraic curves.

Let C be a curve.

Definition 1.1.8. *The divisor group $\mathrm{Div}(C)$ of C is defined as the free abelian group generated by the points of C. In other words, an element $D \in \mathrm{Div}(C)$ is a formal sum*

$$D = \sum_{P \in C} n_P P$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points P.

Definition 1.1.9. *The degree of $D = \sum_{P \in C} n_P P \in \mathrm{Div}(C)$ is*

$$\deg(D) := \sum P \in C n_P \in \mathbb{Z}.$$

We will denote the subgroup of the divisors of degree 0 by $\mathrm{Div}^0(C)$.

Note that if the curve C is defined over K, then the absolute Galois group G_K acts on $\mathrm{Div}(C)$ (or equivalently on $\mathrm{Div}^0(C)$) via

$$D^\sigma = \sum_{P \in C} n_P P^\sigma$$

where $D = \sum_{P \in C} P \in \mathrm{Div}(C)$.

Suppose now that C is smooth and let $f \in \overline{K}(C) \setminus \{0\}$. The divisor associated with f is

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot P$$

where $\mathrm{ord}_P(f)$ is the order of f at P. Moreover, a divisor $D \in \mathrm{Div}(C)$ is said to be principal if there exists $f \in \overline{K}(C) \setminus \{0\}$such that

$$\mathrm{div}(f) = D.$$

We will denote by $\mathrm{Princ}(C)$ the subgroup of the principal divisors. Moreover, it can be shown that for all $f \in \overline{K}(C) \setminus \{0\}$, the divisor $\mathrm{div}(f)$ has degree zero, i.e., $\deg(\mathrm{div}(f)) = 0$. This fundamental property allows us to state the following definition:

Definition 1.1.10. *The Picard group of C is the quotient*

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Princ}(C).$$

Similarly one defines

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C).$$

1.2 Elliptic curves

Definition 1.2.1. *An elliptic curve is a couple (E, O) where E is a nonsingular curve of genus 1 and $O \in E$. Moreover, (E, O) is said to be defined over K if E is defined over K as variety and O is rational, i.e. $O \in E(K)$.*

The definition above provides the abstract geometric characterization of an elliptic curve. In practice, every such curve can be embedded into the projective plane $\mathbb{P}^2$ and described by a specific cubic equation, known as a "Weierstrass equation".

Proposition 1.2.2. *Let E be an elliptic curve defined over K.*

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

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

gives an isomorphism of $E_{/K}$ onto a curve given by an equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

with coefficients $a_1, \ldots, a_6 \in K$ and satisfying $\phi(O) = [0, 1, 0]$. The equation 1.1 is called Weierstrass equation for the elliptic curve E.

(b) Any two Weierstrass equations for E are as in (a) are related by a linear change of variables of the form

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t,$$

with $u \in K^\times$ and $r, s, t \in K$.

(c) Conversely every smooth cubic curve C given by a Weierstrass equation as in (a) is an elliptic curve defined over K with base point O.

Proof. See [Sil09, Chapter 3, Proposition 3.1]. □

Now let E be an elliptic curve over a field K described by the Weierstrass equation

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

If we suppose $\mathrm{Char}(K) \neq 2$, we can reconstruct the squares and simplify the equation. More explicitly, doing the substitution $y = \frac{1}{2}(y - a_1x - a_2)$ we obtain

$$y^2 = ax^3 + b_2x^2 + 2b_4x + b_6,$$

where

- $b_2 := a_1^2 + 4a_2$,
- $b_4 := 2a_4 + a_1a_3$,
- $b_6 := a_3^2 + 4a_6$.

If we moreover define

- $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,
- $c_4 := b_2^2 - 24b_4$,
- $c_6 := -b_2^3 + 36b_2b_4 - 216b_6$,
- $\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$,
- $j := \dfrac{c_4}{\Delta}$ (if $\Delta = 0$ we put $j = \infty$),

we obtain the relations

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^2 - c_6^2.$$

Definition 1.2.3. *With notation above:*

(a) the quantity Δ is called the discriminant of the Weierstrass equation;

(b) the quantity j is the j-invariant of the Weierstrass equation.

Actually the j-invariant does not depend on the Weierstrass equation. More precisely, we have the following proposition.

Proposition 1.2.4. *The following properties hold.*

(a) Two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.

(b) Let $j_0 \in \overline{K}$. Then, there exists an elliptic curve defined over $K(j_0)$ with j-invariant j_0.

Proof. See [Sil09, Chapter 3, Proposition 1.4]. □

If we now suppose $\mathrm{Char}(K) \neq 2, 3$, we can eliminate the x^2 term with the substitutions

$$x = \frac{x - 3b_2}{36}, \qquad y = \frac{y}{108}$$

and we obtain the equation

$$y^2 = x^3 + Ax + B$$

where $A := -27c_4$ and $B := -54c_6$. In this case we have

$$\Delta = -16(4A^3 - 27B^2) \quad \text{and} \quad j := -1728\frac{(4A)^3}{\Delta}.$$

Proposition 1.2.5. *Let E be a curve described by a Weierstrass equation. Then the discriminant Δ with respect to it has the following geometric interpretation:*

(a) E is nonsingular if and only if $\Delta \neq 0$.

(b) E has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.

(c) E has a cusp if and only if $\Delta = c_4 = 0$.

Proof. See [Sil09, Chapter 3, Proposition 1.4]. □

Now we briefly recall the definition of the group law on an elliptic curve (E, O). Let P and Q be two points on E, and let L denote the line passing through P and Q (if $P = Q$, L is the tangent line to E at P). By Bezout's Theorem, L intersects E at a third point R. Let L' be the line passing through R and the point at infinity O. The sum $P + Q$ is defined as the third point of intersection of L' with E. In other words, $P + Q$ is the point such that $L' \cap E = \{R, O, P + Q\}$.

Proposition 1.2.6. *The composition law described above makes E into an abelian group with identity element O. Further, if E is defined over K, then*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0\}$$

is a subgroup of E.

Proof. See [Sil09, Chapter 3, Proposition 2.2]. □

Furthermore, the group operations induce two morphisms of varieties:

$$+ : E \times E \to E, \quad (P, Q) \mapsto P + Q$$

and

$$- : E \to E, \quad P \mapsto -P.$$

If E is defined over K, then these morphisms are also defined over K (for more details see [Sil09, Chapter 3, Proposition 3.6]).

Now let $(E, O), (E', O')$ be two elliptic curves.

Definition 1.2.7. *An isogeny $\varphi : E \to E'$ is a morphism such that $\varphi(O) = O'$.*

Example 1.2.8. *Let (E, O) be an elliptic curve. For each $m \in \mathbb{Z}$, we define the multiplication-by-m map*

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

inductively as follows. If $m > 0$, then

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}.$$

For $m < 0$, we define $[m]P = [-m](-P)$. Finally, for $m = 0$, we set $[0]P = O$ for all $P \in E$. Since the group law is a morphism, it follows by induction that $[m]$ is a morphism of varieties. Moreover, since $[m]O = O$, it is an isogeny.

Note that, given an isogeny $\varphi : E \to E'$, then by Proposition 1.1.5 we have only two possibilities:

- $\varphi(P) = O'$ for all $P \in E$, or
- φ is surjective.

Thus, except for the isogeny $[0]P = O'$ for all $P \in E$, every other isogeny φ induces the usual injection of function fields

$$\varphi^* : \overline{K}(E') \longrightarrow \overline{K}(E)$$

and we can consider the degree of φ defined as the degree of the finite extension $\overline{K}(E)/\varphi^*(\overline{K}(E'))$.

Definition 1.2.9. *Let $\varphi : E \to E'$ be a nonzero isogeny. We will say that φ is separable if the induced field extension $\overline{K}(E)/\varphi^*(\overline{K}(E'))$ has this property.*

Moreover, every isogeny is a group homomorphism. To see this we need a lemma.

Lemma 1.2.10. *Let (E, O) be an elliptic curve. Then the map*

$$E \to \mathrm{Pic}^0(E), \qquad P \mapsto [(P) - (O)]$$

is a group isomorphism.

Proof. See [Sil09, Chapter 3, Proposition 3.4]. □

Proposition 1.2.11. *Let $\varphi : (E_1, O_1) \to (E_2, O_2)$ be an isogeny. Then*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

i.e. φ is a group homomorphism.

Note that the converse is immediate, provided that φ is a morphism.

Proof. Note that if $\varphi(P) = O_2$ for all $P \in E_1$ the statement is trivial. Thus, suppose $\varphi \neq 0$ or equivalently that φ is surjective and consider the following group homomorphism:

$$\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2), \qquad \left[\sum_{P\in E_1} n_P(P)\right] \mapsto \left[\sum_{P\in E_1} n_P(\varphi(P))\right].$$

On the other hand by Lemma 1.2.10 we have an isomorphism of groups

$$\kappa_i : E_i \to \mathrm{Pic}^0(E_i), \qquad P \mapsto [(P) - (O)]$$

for $i = 1, 2$ and since $\varphi(O_1) = O_2$ the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \mathrm{Pic}^0(E_1) \\ \varphi\downarrow & & \downarrow\varphi_* \\ E_2 & \xrightarrow[\kappa_2]{} & \mathrm{Pic}^0(E_2) \end{array}$$

is commutative. Hence, doing the calculation, for all $P, Q \in E_1$ we have:

$$\begin{aligned} \varphi(P+Q) &= \kappa_2^{-1}(\varphi_*(\kappa_1(P+Q))) \\ &= \kappa_2^{-1}(\varphi_*(\kappa_1(P) + \kappa_1(Q))) \\ &= \kappa_2^{-1}(\varphi_*(\kappa_1(P)) + \varphi_*(\kappa_1(Q))) \\ &= \kappa_2^{-1}(\varphi_*(\kappa_1(P))) + \kappa_2^{-1}(\varphi_*(\kappa_1(Q))) \\ &= \varphi(P) + \varphi(Q). \end{aligned}$$

□

Putting together Proposition 1.2.11 and Example 1.2.8 we give the following definition.

Definition 1.2.12. *Let (E, O) be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The m-torsion subgroup of E, denoted by $E[m]$, is the set of points of E of order m, i.e.*

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

The torsion subgroup of E, denoted by E_{tors}, is the set of points of finite order, i.e.

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

Moreover, if E is defined over K, then $E_{\mathrm{tors}}(K)$ denotes the points of finite order in $E(K)$.

Proposition 1.2.13. *Let E be an elliptic curve defined over a field K and let $m \in \mathbb{Z}$ with $m \neq 0$. Then*

(a) $\deg([m]) = m^2$;

(b) if $\mathrm{Char}(K) = 0$ *or* $\mathrm{Char}(K) \nmid m$ *then*

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

Proof. See [Sil09, Chapter 3, Corollary 6.4]. □

We conclude this section by stating a Proposition whose corollary will be useful in the subsequent chapters.

Proposition 1.2.14. *Let E be an elliptic curve and let $\Phi \subseteq E$ be a finite subgroup of E. Then, there exists up to isomorphism an elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that* $\mathrm{Ker}(\varphi) = \Phi$.

Proof. See [Sil09, Chapter 3, Proposition 4.12]. □

Corollary 1.2.15. *Let $K \subset \mathbb{C}$ be a number field and E_1, E_2 be two elliptic curves defined over K. An isogeny $\varphi : E_1 \to E_2$ is defined over K if and only if its kernel* $\mathrm{Ker}(\varphi)$ *is invariant under the action of* $G_K = \mathrm{Gal}(\overline{K}/K)$.

Proof. Note that if φ is defined over K the statement is trivial since for all $\sigma \in G_K$ and $P \in \mathrm{Ker}(\varphi)$ one has

$$\varphi(P^\sigma) = \varphi(P)^\sigma = O^\sigma = O.$$

Conversely, assume that $\mathrm{Ker}(\varphi)$ is invariant under G_K, i.e., $\sigma(\mathrm{Ker}(\varphi)) = \mathrm{Ker}(\varphi)$ for all $\sigma \in G_K$. Given such a σ, consider the isogeny $\varphi^\sigma : E_1^\sigma \to E_2^\sigma$ obtained by applying σ to the coefficients of φ. Since E_1 and E_2 are defined over K then $E_i^\sigma = E_i$ for $i = 1, 2$. Moreover using the hypothesis

$$\mathrm{Ker}(\varphi^\sigma) = \mathrm{Ker}(\varphi)^\sigma = \mathrm{Ker}(\varphi).$$

Therefore φ and φ^σ are two isogenies from E_1 to E_2 with the same kernel and so, since K has characteristic 0, by Proposition 1.2.14 one has

$$\varphi^\sigma = \varphi$$

and by the generality of σ we conclude. □

1.3 Reduction of an elliptic curve

Definition 1.3.1. *Let K be a field. A discrete valuation on K is a map*

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

such that for all $x, y \in K$

(a) $v(x) = \infty$ *if and only if* $x = 0$*;*

(b) $v(xy) = v(x) + v(y)$

(c) $v(x + y) \geq \min\{v(x), v(y)\}$*;*

(d) $v(K)^\times$ *is a discrete subgroup of* $\mathbb{R}$*, that is* $v(K^\times) = a\mathbb{Z}$ *for some* $a \in \mathbb{Z}$*.*

Fixed a real number $c \in (0, 1)$, we may associate to each valuation v on K an absolute value

$$|\cdot|_v : K \longrightarrow \mathbb{R}_{\geq 0}$$

defined by

$$x \mapsto \begin{cases} c^{v(x)} & \text{if } x \neq 0, \\ 0 & \text{otherwise .} \end{cases}$$

that has the following property:

(a) $|x|_v = 0$ if and only if $x = 0$;

(b) $|xy|_v = |x|_v|y|_v$ for all $x, y \in K$;

(c) $|x + y|_v \leq \max\{|x|_v, |y|_v\} (\leq |x|_v + |y|_v)$.

Finally v induces a metric on K given by

$$d_v : K \times K \longrightarrow \mathbb{R}, \qquad (x, y) \mapsto |x - y|_v.$$

Two absolute values on K v, w are said to be equivalent if the two induced metrics d_v, d_w define the same topology on K and an equivalence class of equivalent absolute values on K is called place of K.

Definition 1.3.2. *Let* v *be a discrete valuation on field* K*. We say that* K *is a local field with respect to* v *if it is complete with respect to the metric* d_v*, that is, every Cauchy sequence with respect to* d_v *converges in* K*. Moreover, if* K *is not complete, we will denote by* K_v *the completion of* K *with respect to* v *and we have a natural inclusion* $K \hookrightarrow K_v$*.*

Definition 1.3.3. *Let* K *be a local field with respect to a valuation* v*.*

(a) We will call the valuation ring (or ring of integers) of K*,*

$$\mathcal{O}_v := \{x \in K : v(x) \geq 0\}$$

(b) We will call the units of $\mathcal{O}_v$ *(or of* K*),*

$$\mathcal{O}_v^\times := \{x \in K : v(x) = 0\}.$$

Note that $\mathcal{O}_v$ is a local PID with unique maximal ideal

$$m_v := \{x \in K : v(x) > 0\}.$$

Definition 1.3.4. *We will call $\pi \in \mathcal{O}_v$ such that $m_v = (\pi) = \pi\mathcal{O}_v$ the uniformizer and we will denote by $\kappa_v := \mathcal{O}_v/m_v$ the residue field of $\mathcal{O}_v$.*

In what follows we will suppose that v is normalized,that is $v(\pi) = 1$.

Example 1.3.5. *Let F be a number field and consider its ring of integers $\mathcal{O}_F$. Since $\mathcal{O}_F$ is a Dedekind domain, for each $x \in F$ we can write*

$$(x) = x\mathcal{O}_F = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

In particular we obtain a discrete valuation $v_{\mathfrak{p}}$ on $\mathcal{O}_F$ that can be extended to F putting

$$v_{\mathfrak{p}} : F = \mathrm{frac}(\mathcal{O}_F) \to \mathbb{Z} \cup \{\infty\}, \quad \frac{a}{b} \mapsto v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b).$$

We call the valuation $v_{\mathfrak{p}}$ on F the $\mathfrak{p}$-adic valuation on the number field F and we denote by $F_{\mathfrak{p}}$ the completion of F with respect to the $\mathfrak{p}$-adic metric.

Moreover, we have an explicit characterization of absolute values on a number field K.

Theorem 1.3.6 (Ostrowski)**.** *Any nontrivial absolute value on K is equivalent to a $\mathfrak{p}$-adic absolute value with $\mathfrak{p}$ a nonzero prime ideal of K or to an absolute value induced by an embedding of K in $\mathbb{C}$. In the first case we will call the absolute value nonarchimedean and in the second archimedean.*

We will use the following notation:

- $M_{\mathbb{Q}}^0 := \{|\cdot|_p : p \text{ is a prime number}\}$. This is a complete set of inequivalent nonarchimedean places for $\mathbb{Q}$.
- $M_{\mathbb{Q}}^\infty := \{|\cdot|_\infty\}$, where $|\cdot|_\infty$ is the absolute value on $\mathbb{Q}$ given by $|x|_\infty = \max x, -x$. This is the unique archimedean absolute value on $\mathbb{Q}$ up to equivalence.
- $M_{\mathbb{Q}} = M_{\mathbb{Q}}^0 \cup M_{\mathbb{Q}}^\infty$.

Let K be a local field with respect to a discrete valuation v and let E be an elliptic curve defined over K defined by the Weierstrass equation

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

for some $a_1, a_2, a_3, a_4, a_6 \in K$. Let $u \in K^\times$. Applying the change of variables

$$x = u^{-2}x', \quad y = u^{-3}y'$$

we obtain

$$(y')^2 + a_1u(x'y') + a_3u^3y' = (x')^3 + a_2u^2(x')^2 + a_4u^4x' + a_6u^6.$$

Thus the new coefficients are $a_i' = u^i a_i$ with valuation

$$v(a_i') = v(u^i a_i) = iv(u) + v(a_i)$$

for $i = 1, 2, 3, 4, 6$. In particular, by choosing u sufficiently large such that $iv(u) + v(a_i) \geq 0$ (for example an appropriate power of the uniformizer π), we obtain an equation of E with coefficients in $\mathcal{O}_v$.

Definition 1.3.7. *Let E be an elliptic curve defined over a local field K with respect to a valuation v. A Weierstrass equation for E*

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

with discriminant Δ is said to be minimal for E (at v), if $v(\Delta)$ is minimized subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_v$. This minimal value $v(\Delta)$ is called the valuation of the minimal discriminant of E at v.

Proposition 1.3.8. *Let E be an elliptic curve defined over a local field (K, v).*

(a) E admits a minimal Weierstrass equation.

(b) A minimal Weierstrass equation is unique up to a change of coordinates

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

with $u \in \mathcal{O}_v^\times$ and $r, s, t \in \mathcal{O}_v$.

(c) Conversely, if one starts with any Weierstrass equation whose coefficients are in $\mathcal{O}_v$, then any change of coordinates

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

used to produce a minimal Weierstrass equation satisfies $u, r, s, t \in \mathcal{O}_v$.

Proof. See [Sil09, Chapter 7, Proposition 1.3]. □

Let E be an elliptic curve defined over a local field (K, v) and fix a minimal Weierstrass equation for E at v. We may reduce its coefficients modulo m_v (or equivalently modulo the uniformizer π) and we obtain a new equation

$$y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}$$

with $\overline{a_i} \in \mathcal{O}_v/(\pi) = \kappa_v$ for all i. Note that this new curve could have singularities.

Definition 1.3.9. *With notations above, we denote by $\overline{E}$ the new curve obtained from E reducing the coefficients of any weierstrass modulo π and we call it the reduction of E modulo π.*

Note that if Δ is the minimal discriminant of E at v and $\overline{\Delta}$ is the discriminant of the curve obtained from E by reduction modulo m_v, then

$$v(\Delta) = 0 \iff \overline{\Delta} \neq 0 \iff \overline{E} \text{ is an elliptic curve over } \kappa.$$

Remark 1.3.10. *Let $P \in E(K)$. We can find homogeneous coordinates for $P = [x_0 : y_0 : z_0]$ with $x_0, y_0, z_0 \in \mathcal{O}_v^\times$. In this sense we have a reduction map*

$$\mathrm{red} : E(K) \to \overline{E}(\kappa_v), \qquad [x_0, y_0, z_0] \mapsto [\overline{x_0}, \overline{y_0}, \overline{z_0}].$$

Note that the set of nonsingular points of $\overline{E}(\kappa_v)$ form a group that we denote by $\overline{E}_{\mathrm{ns}}(\kappa_v)$. Moreover, consider

- $E_0(K) := \left\{P \in E(K) : \overline{P} \in \overline{E}_{\mathrm{ns}}(\kappa_v)\right\} = \mathrm{red}^{-1}\left(\overline{E}_{\mathrm{ns}}(\kappa_v)\right)$
- $E_1(K) := \left\{P \in E(K) : \overline{P} = \overline{O}\right\} = \mathrm{Ker}(\mathrm{red}) = \mathrm{red}^{-1}\left(\overline{O}\right)$

Proposition 1.3.11. *The short sequence of abelian groups*

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\mathrm{red}} \overline{E}_{\mathrm{ns}}(\kappa_v) \to 0$$

is exact.

Proof. See [Sil09, Chapter 7, Proposition 2.1]. □

Proposition 1.3.12. *Let E be an elliptic curve defined over a local field K with residue field κ and let $m \geq 1$ be an integer such that* $\gcd(\mathrm{Char}(\kappa), m) = 1$.

(a) The subgroup $E_1(K)$ has no nontrivial points of order m.

(b) Assume further that the reduced curve $\overline{E}$ over κ is nonsingular. Then the reduction map

$$E(K)[m] \longrightarrow \overline{E}(\kappa)$$

is injective.

Proof. For part (a), see [Sil09, Chapter 7, Proposition 3.1]. Suppose now that $\overline{E}$ is nonsingular over κ; that is, $E_0(K) = E(K)$ and $\overline{E}_{\mathrm{ns}}(\kappa) = \overline{E}(\kappa)$. Then, by Proposition 1.3.11, we have a short exact sequence

$$0 \to E_1(K) \longrightarrow E(K) \xrightarrow{\mathrm{res}} \overline{E}(\kappa) \to 0$$

which induces the left-exact sequence

$$0 \to E_1(K) \cap E[m] \longrightarrow E(K)[m] \xrightarrow{\mathrm{res}|_{E(K)[m]}} \overline{E}(\kappa).$$

By part (a), $E_1(K) \cap E[m] = \{O\}$, and thus $\mathrm{res}|_{E(K)[m]}$ is injective. □

We now focus on the case where the local field K has characteristic 0 and its residue field κ is finite.

Proposition 1.3.13. *Let K be a local field with respect to an absolute value $|\cdot|_K$ and let L/K be a finite field extension. Then there exists a unique absolute value on L $|\cdot|_L$ that extends $|\cdot|_K$.*

Proof. See [Ser13, Chapter 2, Section 2 Corollary 2]. □

In particular L inherits naturally the structure of local field. For example, let p be a prime of $\mathbb{Q}$ and let $L = \mathbb{Q}(\alpha)$ be a finite extension of $\mathbb{Q}$. Fix a prime $\mathfrak{p}$ of L such that $\mathfrak{p} \cap \mathbb{Q} = p$. In this case, one can check that the completion $L_{\mathfrak{p}}$ of L in $\mathfrak{p}$ coincides with $\mathbb{Q}_l(\alpha)$.

Definition 1.3.14. *Let L/K be a finite extension of local fields of degree $[L : K] = n$ with ring of integers R_K and R_L. Denote by m_K and κ_K (resp. m_L and κ_L) the maximal ideal and the residue field of K (resp. L). We write*

$$m_K R_L = m_L^e, \qquad f = [\kappa_L : \kappa_K]$$

for certain integers e, f greater then 1. We call:

(a) ramification index of L over K the integer e,

(b) residue degree of L over K the integer f.

Moreover, we say that the extension L/K is unramified if $e = 1$.

Note that if L/K and L'/K are two unramified extension of the local field K, then the compositum $L \cdot L'/K$ is unramified. Thus we can give the following.

Definition 1.3.15. *The maximal unramified extension K^{ur} of the local field K is the compositum of all (finite) unramified extension of K in a fixed algebraic closure $\overline{K}$.*

Remark 1.3.16. *The maximal unramified extension K^{ur} of K has the following properties:*

- *For every finite extension L/K such that $K \subseteq L \subseteq K^{\mathrm{ur}}$, L/K is unramified.*
- *The extension K^{ur}/K is Galois and we have an isomorphism of topological group*
$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Gal}(\overline{\kappa}/\kappa) =: G_\kappa$$
where $\overline{\kappa}$ is an algebraic closure of the residue field κ of K.

Definition 1.3.17. *We call the subgroup of $G_K = \mathrm{Gal}(\overline{K}/K)$*

$$I_K := \mathrm{Gal}(\overline{K}/K^{\mathrm{ur}})$$

the inertia subgroup of G_K.

In particular we have a short exact sequence of groups

$$0 \to I_K \to G_K \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \to 0$$

or equivalently

$$0 \to I_K \to G_K \to \mathrm{Gal}(\overline{\kappa}/\kappa) \to 0.$$

In other words, the inertia group I_K is the set of elements of G_K that act trivially on the residue field κ. Consider now a set X on which G_K acts.

Definition 1.3.18. *The set X is said to be unramified if I_K acts trivially on it, i.e.*

$$\sigma(x) = x$$

for all $x \in X$ and $\sigma \in I_K$.

Proposition 1.3.19. *Let (K, v) be a local field with a finite residue field κ. Let E be an elliptic curve defined over K and suppose that its reduction $\overline{E}$ is nonsingular over κ. Then, if $m \geq 1$ is an integer such that $\gcd(m, \mathrm{Char}(\kappa)) = 1$, then the set $E[m]$ is unramified.*

Proof. First of all the statement is consistent: recall that G_K acts on E through its action on the coordinates of the points and since the isogeny $[m]$ is defined over K the action restricts to $E[m] = \mathrm{Ker}([m])$. Let K'/K be a finite extension such that $E[m] \subseteq E(K')$ and fix the following notation:

- $R' :=$ ring of integers of K';
- $m' :=$ maximal ideal of R';
- $\kappa' := R'/m'$ the residue field of K';
- $v' :=$ the unique absolute value on K' which extends v.

Denoting by Δ the minimal discriminant of E, by the fact that $\overline{E}$ is non singular over κ, we have that

$$v'(\Delta) = v(\Delta) = 0.$$

In particular the minimal Weierstrass equation for E over K is a minimal equation of E over K' and $\overline{E}$ is nonsingular over κ'. Hence by Proposition 1.3.12 the reduction map

$$E(K')[m] \xrightarrow{\mathrm{red}} \overline{E}(\kappa')$$

is injective. Let now $P \in E[m]$ and $\sigma \in I_K$. From the characterization of inertia group, the element σ acts trivially on $\overline{E}(\kappa') \subseteq \overline{E}(\overline{\kappa})$, so

$$\mathrm{red}(P^\sigma - P) = \mathrm{red}(P^\sigma) - \mathrm{red}(P) = \mathrm{red}(P)^\sigma - \mathrm{red}(P) = \mathrm{red}(P) - \mathrm{red}(P) = \overline{O}.$$

Summing up, since $P^\sigma - P \in \mathrm{Ker}\left(E(K')[m] \xrightarrow{\mathrm{red}} \overline{E}(\kappa')\right)$ we obtain $P^\sigma = P$.

□

1.4 The case over $\mathbb{C}$

The goal of this section is to study elliptic curves over the complex numbers. We will outline the construction of elliptic curves over C and aim to classify them up to isomorphism. To begin with, we introduce a key group that will be used extensively in the subsequent chapters.

Definition 1.4.1. *The modular group is the multiplicative group of matrices*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

under matrix multiplication.

Now we introduce the concept of lattice in $\mathbb{C}$.

Definition 1.4.2. *A lattice Λ in $\mathbb{C}$ is a free $\mathbb{Z}$-submodule of $\mathbb{C}$ of rank 2, denoted by*

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z},$$

where $\{\omega_1, \omega_2\}$ forms a basis for $\mathbb{C}$ over $\mathbb{R}$.

Lemma 1.4.3. *let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ two lattices in $\mathbb{C}$ with $\omega_1/\omega_2 \in \mathcal{H}$ and $\omega_1'/\omega_2' \in \mathcal{H}$. Then $\Lambda = \Lambda'$ if and only if*

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

for some $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$.

Definition 1.4.4. *Given a lattice Λ of $\mathbb{C}$, a complex torus is the quotient*

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}.$$

Note that every complex torus is a compact Riemann surface. More generally, we have the following proposition to study the morphisms between them:

Proposition 1.4.5. *Any holomorphic map between complex tori $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is of the form*

$$\varphi(z + \Lambda) = mz + b + \Lambda'$$

for $m, b \in \mathbb{C}$ with $m\Lambda \subseteq \Lambda'$.Moreover, the map is invertible if and only if $m\Lambda = \Lambda'$. In other words, any holomorphic map between complex tori is the composition of a translation with a rotation.

Proof. See [DS05, Proposition 1.3.2]. □

Corollary 1.4.6. *Let*

$$\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda', \qquad z + \Lambda \mapsto mz + b + \Lambda'$$

be an holomorphic map between complex tori with $m\Lambda \subseteq \Lambda'$. Then, the following facts are equivalent:

(a) φ is an homomorphism of groups,

(b) $b \in \Lambda'$,

(c) $\varphi(0) = 0$.

Proof. The equivalence $(b) \iff (c)$ is immediate from the definition of φ, since $\varphi(0 + \Lambda) = b + \Lambda'$, which coincides with the identity element of $\mathbb{C}/\Lambda'$ if and only if $b \in \Lambda'$.

Now, suppose that (a) holds; if φ is a group homomorphism, it must map the identity to the identity. Thus, $\varphi(0+\Lambda) = b+\Lambda' = \Lambda'$, which implies $b \in \Lambda'$, proving $(a) \implies (b)$.

Conversely, if $b \in \Lambda'$, then for any $z_1, z_2 \in \mathbb{C}$ we have:

$$\varphi(z_1 + z_2 + \Lambda) = m(z_1 + z_2) + \Lambda' = (mz_1 + \Lambda') + (mz_2 + \Lambda') = \varphi(z_1 + \Lambda) + \varphi(z_2 + \Lambda),$$

which shows that φ is a group homomorphism, hence $(b) \implies (a)$. □

Remark 1.4.7. *Consider a complex lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\tau = \omega_1/\omega_2 \in \mathcal{H}$, and let $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$ be the lattice generated by $\{\tau, 1\}$. Since $\omega_2^{-1}\Lambda = \Lambda_\tau$, by Corollary 1.4.6, the map*

$$\varphi_\tau : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda_\tau, \qquad z + \Lambda \mapsto z/\omega_2 + \Lambda_\tau$$

is an isomorphism of groups. In particular, every complex torus is isomorphic to a torus generated by a basis of the form $\{\tau, 1\}$.

Moreover, while τ is not unique, it possesses a fundamental transformation property. Let Λ be a lattice and let $\tau = \omega_1/\omega_2$ and $\tau' = \omega_1'/\omega_2'$ be elements of $\mathcal{H}$ such that

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_{\tau'}.$$

Then $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are isomorphic via the map $z + \Lambda_\tau \mapsto (\omega_2/\omega_2')z + \Lambda_{\tau'}$. This implies that $(\omega_2/\omega_2')\Lambda_\tau = \Lambda_{\tau'}$, which can be rewritten as

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}.$$

Hence, by Lemma 1.4.3, there exists a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Explicitly solving for τ', we obtain

$$\tau' = \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} = \gamma(\tau).$$

Thus, every complex torus determines a point of the upper half-plane up to the action of the modular group $SL_2(\mathbb{Z})$. This association will be explored in greater detail in Section 2.2.

Definition 1.4.8. *For reasons that will become clear shortly, a non-zero holomorphic homomorphism between complex tori is called an isogeny.*

Remark 1.4.9. *Let N be any positive integer, let Λ be a lattice in $\mathbb{C}$, and consider the map*

$$[N] : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda, \qquad z + \Lambda \mapsto Nz + \Lambda.$$

Since $N\Lambda \subseteq \Lambda$, this map is clearly an isogeny. Letting E denote the torus $\mathbb{C}/\Lambda$ (again, for reasons that will be clear soon), the N-torsion subgroup is defined as the set

$$E[N] = \ker([N]) = \{z + \Lambda \in \mathbb{C}/\Lambda : [N](z + \Lambda) = 0\}.$$

Writing $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, we have

$$E[N] = \{z + \Lambda \in \mathbb{C}/\Lambda : Nz \in \Lambda\} = \{z \in \mathbb{C} : Nz \in \Lambda\}/\Lambda.$$

If $Nz \in \Lambda$, then $Nz = m\omega_1 + n\omega_2$ for some $m, n \in \mathbb{Z}$, which implies

$$z = \frac{m}{N}\omega_1 + \frac{n}{N}\omega_2.$$

By taking this modulo Λ, we can restrict m and n to the range $\{0, 1, \ldots, N-1\}$. Thus, we deduce that $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2, i.e.,

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

We now proceed to establish the connection between complex tori and elliptic curves over $\mathbb{C}$.

Definition 1.4.10. *Let Λ be a lattice. The weierstrass $\wp$-function with respect to Λ is $\wp(z) := \wp(z; \Lambda) : \mathbb{C} \longrightarrow \mathbb{C}$ given by*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The Eisenstein series of weight $2k$ (for Λ) is the series

$$G_{2k} := G_{2k}(\Lambda) := \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}.$$

Theorem 1.4.11. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice.*

(a) The Eisenstein series $G_{2k}(\Lambda)$ is absolutely convergent for all $k > 1$.

(b) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. The series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

(c) The Weierstrass $\wp$-function is even and Λ-periodic.

Proof. See [Sil09, Chapter 6, Theorem 3.2]. □

Remark 1.4.12. *In particular, it follows from Theorem 1.4.11 that the derivative $\wp'$ is analytic and can be obtained by term-by-term differentiation. Thus, for all $z \in \mathbb{C} \setminus \Lambda$, we have*

$$\wp'_\Lambda(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}.$$

Moreover, since $\wp'$ is also Λ-periodic, $\wp$ and $\wp'$ induce two meromorphic functions on the complex torus $\mathbb{C}/\Lambda$.

Proposition 1.4.13. *Let $\wp$ be the Weierstrass function with respect to a lattice Λ. Then for all $z \in \mathbb{C} \setminus \Lambda$, $\wp$ and its derivative satisfy the relation*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. See [Sil09, Chapter 6, Theorem 3.5]. □

Let τ be an element of the upper half plane. We will denote by E_τ the elliptic curve associated to the complex torus $\mathbb{C}$ via the last proposition.

It is standard notation, to set

$$g_2 = g_2(\Lambda), \qquad \text{and} \qquad g_3 = g_3(\Lambda) = 140G_6(\Lambda)$$

and next result says that the complex torus $\mathbb{C}/\Lambda$ is always isomorphic to an elliptic curve.

Proposition 1.4.14. *Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to a lattice $\Lambda \subseteq \mathbb{C}$.*

(a) The polynomial

$$f(x) = 4x^3 - g_2x - g_3$$

has distinct roots; thus, the discriminant

$$\Delta(\Lambda) := g_2^3 - 27g_3^2$$

is non-zero.

(b) Let E be the curve defined over $\mathbb{C}$ by

$$E : y^2 = 4x^3 - g_2x - g_3,$$

which, by part (a) and Proposition 1.2.5, is an elliptic curve. Then the map

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C}), \qquad z + \Lambda \mapsto [\wp(z) : \wp'(z) : 1]$$

is an isomorphism of Riemann surfaces that is also a group isomorphism.

Proof. See [Sil09, Chapter VI, Proposition 3.6]. □

According to the previous Proposition, every complex torus is biholomorphic to an elliptic curve. Conversely, since every elliptic curve has genus 1 by definition, it can be realized as a complex torus. Consequently, we find that complex tori (analytic objects) and elliptic curves (algebraic objects defined as the solution sets of cubic polynomials) are essentially interchangeable. Given this deep connection, from this point forward, we shall treat elliptic curves over $\mathbb{C}$ and complex tori as equivalent objects.

Chapter 2

Modular curves

2.1 Modular forms

To begin with, we want to study more closely the modular group $\mathrm{SL}_2(\mathbb{Z})$ introduced in the previous chapter (cf. Definition 1.4.1).

Proposition 2.1.1. *The modular group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the two matrices*

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \textit{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Proof. Let $G = \langle S, T \rangle$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S and T. We observe that for any integer n,

$$T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

The effects of left-multiplication by S and T^n on an arbitrary matrix are given by:

$$S \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix}, \qquad T^n \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+nc & b+nd \\ c & d \end{bmatrix}. \tag{2.1}$$

Now, let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. If $c \neq 0$, we can reduce the absolute value of the entries using the Euclidean algorithm. By multiplying by S if necessary, we may assume $|a| \geq |c|$. By the division algorithm, we can write $a = cq + r$ with $0 \leq r < |c|$. Then, as shown in (2.1), the matrix $T^{-q}\gamma$ has r as its upper-left entry. Applying S subsequently moves this r (with a sign change) to the lower-left position. By repeating this process, we can strictly decrease the absolute value of the lower-left entry at each step. Since these are non-negative integers, the process must terminate, meaning we can find an element $g \in G$ such that $g\gamma$ has a lower-left entry of 0. Since $g\gamma \in \mathrm{SL}_2(\mathbb{Z})$, it must be of the form:

$$g\gamma = \begin{bmatrix} \pm 1 & m \\ 0 & \pm 1 \end{bmatrix}.$$

Such a matrix can be written as $\pm T^m$. Noting that $S^2 = -I$ and $S^4 = I$, we have $-I \in G$, and thus $\pm T^m \in G$. It follows that $\gamma = g^{-1}(\pm T^m) \in G$, which completes the proof. □

A central role in our study will be played by the upper half-plane, defined as:

$$\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Let $\tau \in \mathcal{H}$. For each $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we consider the linear fractional transformation:

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

From the identity

$$\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

it follows that $\mathrm{Im}(\gamma(\tau)) > 0$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, ensuring that the action is well-defined on $\mathcal{H}$. Furthermore, this mapping satisfies the axioms of a group action:

- $I(\tau) = \tau$ for all $\tau \in \mathcal{H}$, where I is the identity matrix;
- $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$ for all $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Thus, we obtain a group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$:

$$\begin{aligned} \rho : \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} &\to \mathcal{H} \\ (\gamma, \tau) &\mapsto \gamma(\tau) \end{aligned}$$

In particular, this group of transformations is generated by the maps

$$\tau \mapsto \tau + 1 \quad \text{and} \quad \tau \mapsto -\frac{1}{\tau},$$

which correspond to the generators T and S of $\mathrm{SL}_2(\mathbb{Z})$, respectively.

Another class of objects that will be extensively used throughout this chapter is that of modular forms.

Definition 2.1.2. *Let k be an integer. A meromorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is weakly modular of weight k if*

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \quad \textit{for all } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \textit{ and } \tau \in \mathcal{H}.$$

Remark 2.1.3. *(a) Weak modularity of weight 0 corresponds to $\mathrm{SL}_2(\mathbb{Z})$-invariance, as the condition above reduces to $f(\gamma(\tau)) = f(\tau)$.*

(b) *As we will see in Remark 2.1.18, it suffices to verify the weak modularity condition on the generators S and T of $\mathrm{SL}_2(\mathbb{Z})$. Thus, f is weakly modular of weight k if and only if*

$$f(\tau+1) = f(\tau) \quad \text{and} \quad f(-1/\tau) = \tau^k f(\tau).$$

The periodicity condition $f(\tau+1) = f(\tau)$ implies that f admits a Fourier expansion (or q-expansion) in terms of $q = e^{2\pi i \tau}$.

(c) *Let f be a weakly modular function of weight k that is holomorphic on $\mathcal{H}$. With notation above, let $\mathbb{D}^* = \{q \in \mathbb{C} : 0 < |q| < 1\}$ be the punctured unit disk. We define the function $g : \mathbb{D}^* \to \mathbb{C}$ such that:*

$$g(q) = f\left(\frac{\log q}{2\pi i}\right).$$

Since f is holomorphic on $\mathcal{H}$, g is well-defined and holomorphic on $\mathbb{D}^*$. This allows us to represent f via its q-expansion:

$$f(\tau) = g(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Since $q \to 0$ as $\mathrm{Im}(\tau) \to \infty$, we can characterize the behavior of f "at the cusp" ∞ as follows:

- *f is holomorphic at infinity if g extends holomorphically to $q = 0$. In terms of the q-expansion, this means $a_n = 0$ for all $n < 0$.*
- *f is meromorphic at infinity if g has at most a pole at $q = 0$. This means $a_n = 0$ for all but finitely many $n < 0$.*

Definition 2.1.4. *Let k be an integer. A function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is a modular form of weight k if*

(a) *is holomorphic on $\mathcal{H}$,*

(b) *is weakly modular of weight k,*

(c) *is holomorphic at ∞.*

We will denote the set of modular forms of weight k with $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and the set of all modular forms with $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

Proposition 2.1.5. (a) *For all $k \in \mathbb{Z}$, the set $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathbb{C}$-vector space.*

(b) *The decomposition*

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$$

gives $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ the structure of a graded ring.

Proof. (a) Let $k \in \mathbb{Z}$ and $f, g \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. The sum $f+g$ is clearly holomorphic on $\mathcal{H}$ and at ∞, as these properties are preserved under linear combinations. Furthermore, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, we have:

$$\begin{aligned}(f+g)(\gamma(\tau)) &= f(\gamma(\tau)) + g(\gamma(\tau)) \\ &= (c\tau+d)^k f(\tau) + (c\tau+d)^k g(\tau) \\ &= (c\tau+d)^k (f+g)(\tau).\end{aligned}$$

Similarly, for any $\alpha \in \mathbb{C}$, the function αf satisfies the weight k transformation law and remains holomorphic, thus $\alpha f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

(b) From the previous part, it follows that $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is an abelian group for each k. The sum is direct because a non-zero modular form cannot satisfy the transformation law for two distinct weights simultaneously. Finally, if $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $g \in \mathcal{M}_l(\mathrm{SL}_2(\mathbb{Z}))$, their product fg is holomorphic on $\mathcal{H}$ and at ∞. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have:

$$\begin{aligned}(fg)(\gamma(\tau)) &= f(\gamma(\tau)) \cdot g(\gamma(\tau)) \\ &= (c\tau+d)^k f(\tau) \cdot (c\tau+d)^l g(\tau) \\ &= (c\tau+d)^{k+l} (fg)(\tau).\end{aligned}$$

Thus, $fg \in \mathcal{M}_{k+l}(\mathrm{SL}_2(\mathbb{Z}))$, confirming the graded ring structure.

□

A special type of modular forms are the cusp forms. These are modular forms that vanish at infinity, meaning that the constant term in their q-expansion is zero. More precisely, we give the following definition:

Definition 2.1.6. *A cusp form of weight k is a modular form of weight k whose Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n, \qquad q = e^{2\pi i \tau}$$

has constant term $a_0 = 0$. In other words, a modular form is a cusp form if

$$\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau) = a_0 + \sum_{n=1}^{\infty} a_n e^{-2\pi n \mathrm{Im}(\tau)} \cdot e^{2\pi i n \mathrm{Re}(\tau)} = a_0 = 0.$$

The set of cusp forms of weight k is denoted by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and the space of all cusp forms is denoted by $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}))$.

Proposition 2.1.7. *The following facts hold:*

(a) For all $k \in \mathbb{Z}$, $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathbb{C}$-vector space.

(b) The decomposition

$$\mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$$

gives $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}))$ *the structure of a graded ring.*

(c) $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}))$ *is an ideal of the modular forms ring* $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

Proof. Parts (a) and (b) follow by the same arguments presented in the proof of Proposition 2.1.5, as the properties of holomorphy and the modular transformation law are preserved under linear combinations and grading.

To prove (c), let $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $g \in \mathcal{S}_l(\mathrm{SL}_2(\mathbb{Z}))$, with q-expansions given by

$$f(\tau) = \sum a_n q^n \qquad \text{and} \qquad g(\tau) = \sum b_n q^n.$$

By the definition of cusp forms, we have $b_0 = 0$. The product fg is a modular form of weight $k+l$, and its constant term in the q-expansion is $a_0 b_0$. Since $b_0 = 0$, it follows that $a_0 b_0 = 0$, which implies that fg vanishes at infinity. Thus, $fg \in \mathcal{S}_{k+l}(\mathrm{SL}_2(\mathbb{Z}))$, confirming that $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}))$ is an ideal of $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$. □

Example 2.1.8. *We now introduce the fundamental examples of modular forms and functions. Similarly to the definitions associated with the Weierstrass* $\wp$*-function, for any even integer* $k > 2$*, let*

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(c\tau + d)^k}.$$

One can show that these sums converge absolutely and uniformly on compact subsets of $\mathcal{H}$*. In particular, we consider the normalized quantities:*

$$g_2(\tau) = 60G_4(\tau), \qquad g_3(\tau) = 140G_6(\tau).$$

We then define the modular discriminant as:

$$\Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2.$$

It can be shown that Δ *is a cusp form of weight* 12 *(i.e.,* $\Delta \in \mathcal{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$*) and satisfies* $\Delta(\tau) \neq 0$ *for all* $\tau \in \mathcal{H}$*. Thus, its only zero is at infinity.*

The modularity of G_k *follows from the fact that for any* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$*, the transformation*

$$(c', d') \mapsto (c'a + d'c, c'b + d'd) = (c', d') \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is a bijection of $\mathbb{Z}^2 \setminus \{(0,0)\}$*. This ensures* $G_k(\gamma(\tau)) = (c\tau + d)^k G_k(\tau)$.

Finally, we define the modular j*-invariant as:*

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}.$$

The function j is holomorphic on $\mathcal{H}$ and weakly modular of weight 0, making it $\mathrm{SL}_2(\mathbb{Z})$-invariant. Its q-expansion is given by:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots$$

Since j has a simple pole at $q = 0$, it is a modular function but not a modular form.

The j-function introduced above is closely related to an important polynomial that will be fundamental in the following chapters. Let N be a positive integer and consider

$$M^*(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) : \gcd(a,b,c,d) = 1, \det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = N \right\}.$$

One can prove that there is a decomposition of the form

$$M^*(N) = \coprod_{\substack{a,d>0 \\ ad=N}} \coprod_{0 \le b < d} \mathrm{SL}_2(\mathbb{Z}) \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

or equivalently, defining $\psi(N) = N \prod_{p|N}(1 + \frac{1}{p})$,

$$M^*(N) = \mathrm{SL}_2(\mathbb{Z}) \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^{\psi(N)} \mathrm{SL}_2(\mathbb{Z})\alpha_i.$$

With notation as above we can give the following.

Definition 2.1.9. *The classical modular polynomial is*

$$\Phi_N(Y) := \prod_{i=1}^{\psi(N)} (Y - j \circ \alpha_i)$$

where $j : \mathcal{H} \longrightarrow \mathbb{C}$ is the j-invariant introduced in example 2.1.8 and if $\alpha_i = \left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$, for all $\tau \in \mathcal{H}$

$$(j \circ \alpha_i)(\tau) = j\left(\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]\right)(\tau) = j\left(\frac{a\tau + b}{d}\right).$$

Proposition 2.1.10. *$\Phi_N(Y)$ is a polynomial in $\mathbb{Z}[j][Y]$.*

Proof. See [Lan87, Chapter 5, Section 2]. □

Thanks to proposition 2.1.10, replacing j, with another variable X we can consider

$$\Phi_N(X,Y) \in \mathbb{Z}[X,Y].$$

This new polynomial yields a key characterization of j-invariants.

Proposition 2.1.11. *Let $j_1, j_2 \in \mathbb{C}$. We have $\Phi_N(j_1, j_2) = 0$ if and only if there exist two elliptic curves E_1, E_2 and an isogeny $\varphi : E_1 \longrightarrow E_2$ such that j_1 and j_2 are respectively the j-invariants of E_1 and E_2 and $\mathrm{Ker}(\varphi) \cong \mathbb{Z}/N\mathbb{Z}$.*

Proof. We will only prove the case when N is prime since in this case the formulas become simpler. By Proposition 1.2.4 and the next section 2.2.2, we have a bijection

$$j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \longrightarrow \mathbb{C}$$

and hence each $j \in \mathbb{C}$ is of the form $j(\tau)$ for some $\tau \in \mathcal{H}$, and this association is well-defined up to the action of $\mathrm{SL}_2(\mathbb{Z})$. Then, doing the calculation, one can check that in our case:

$$\begin{aligned}\Phi_N(j(\tau), Y) &= (Y - j(N\tau)) \prod_{0 \le k < N} (Y - j(NST^k\tau)) \\ &= (Y - j(N\tau)) \prod_{0 \le k < N} \left(Y - j\left(\frac{\tau + k}{N}\right)\right),\end{aligned}$$

where S and T are the usual matrices. Let now $j_1 = j(\tau_1)$ and $j_2 = j(\tau_2)$ be the j-invariants of two elliptic curves over $\mathbb{C}$. Then:

$$\begin{aligned}\Phi_N(j_1, j_2) = 0 &\iff (j(\tau_2) - j(N\tau_1)) \prod_{0 \le k < N} \left(j(\tau_2) - j\left(\frac{\tau_1 + k}{N}\right)\right) = 0 \\ &\iff \tau_2 = g \cdot (N\tau_1) \text{ or } \tau_2 = g \cdot \left(\frac{\tau_1 + k}{N}\right) \\ &\qquad \text{for some } g \in \mathrm{SL}_2(\mathbb{Z}) \text{ and integer } 0 \le k < N \\ &\iff \mathbb{C}/\Lambda_{\tau_2} \cong \mathbb{C}/\Lambda_{N\tau_1} \text{ or } \mathbb{C}/\Lambda_{\tau_2} \cong \mathbb{C}/\Lambda_{\frac{\tau_1+k}{N}}.\end{aligned}$$

where the last equivalence follows from Remark 1.4.7 and if $\tau \in \mathcal{H}$, then $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$.

To conclude, the lattices $\Lambda_{N\tau_1}$ and $\Lambda_{\frac{\tau_1+k}{N}}$ are exactly all the sublattices of Λ_{τ_1} of index N. Since N is prime, the quotient group Λ_{τ_1}/Λ for any such sublattice is necessarily cyclic of order N. Thus, the inclusion $\Lambda \hookrightarrow \Lambda_{\tau_1}$ induces an isogeny $\varphi : E_1 \to E_2$ with $\mathrm{Ker}(\varphi) \cong \mathbb{Z}/N\mathbb{Z}$, which completes the proof. □

Until now, we have considered functions that are modular with respect to the full group $\mathrm{SL}_2(\mathbb{Z})$. However, for many arithmetic applications, it is essential to study functions that satisfy the modularity condition only for certain subgroups of finite index. For this reasons we give the following definition.

Definition 2.1.12. *Let N be a positive integer. The principal congruence subgroups of level N is*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\ N) \right\}$$

where the matrix congruence is interpreted term by term.

Remark 2.1.13. *(a)* $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$.

(b) Since the map $\pi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *is a surjective group homomorphism with kernel* $\Gamma(N)$*, it follows that* $\Gamma(N)$ *is a normal subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *and that the index is finite:*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| < \infty.$$

Definition 2.1.14. *A subgroup* Γ *of* $SL_2(\mathbb{Z})$ *is a congruence subgroup if* $\Gamma(N) \subseteq \Gamma$ *for some* $N \in \mathbb{Z}_{>0}$*, in which case* Γ *is a congruence subgroup of level* N*.*

In particular, every congruence subgroup Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$. Besides the principal congruence subgroups, the most important congruence subgroups are:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

where "$*$" means "unspecified".

Remark 2.1.15. *Let* N *be a positive integer. The chain of inclusions*

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$$

leads to the following considerations:

(a) The map

$$\Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \pmod{N}$$

is a surjective homomorphism with kernel $\Gamma(N)$*. Thus,* $\Gamma(N) \lhd \Gamma_1(N)$ *and the index* $[\Gamma_1(N) : \Gamma(N)] = N$ *is finite.*

(b) The map

$$\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod{N}$$

is a surjective homomorphism with kernel $\Gamma_1(N)$*. Thus,* $\Gamma_1(N) \lhd \Gamma_0(N)$ *and the index* $[\Gamma_0(N) : \Gamma_1(N)] = \phi(N)$ *is finite where*

$$\phi(N) = \#\{a \in \mathbb{Z} : 1 \leq a \leq N \text{ and } \gcd(a, N) = 1\}.$$

We now introduce two important notations.

- For any matrix $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(\mathbb{Z})$ the factor of automorphy $\delta(\gamma, \tau) \in \mathbb{C}$ for $\tau \in \mathcal{H}$ is

$$\delta(\gamma, \tau) = c\tau + d.$$

- For $\gamma \in SL_2(\mathbb{Z})$ and any integer k, the *weight-k* operator $[\gamma]_k$ on functions $f : \mathcal{H} \longrightarrow \mathbb{C}$ is
$$[\gamma]_k(f) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \qquad \tau \in \mathcal{H}.$$

The notion of weak modularity can be naturally extended to the case of congruence subgroups. Since a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane $\mathcal{H}$ in the same way as the full modular group, we can generalize the transformation law by restricting the set of matrices for which it must hold. More precisely, we give the following definition.

Definition 2.1.16. *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and let k be an integer. A meromorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is said to be weakly modular of weight k with respect to Γ if it is invariant under the weight-k action of Γ, that is, using the notation introduced above:*

$$[\gamma]_k(f) = f, \qquad \forall \gamma \in \Gamma.$$

Lemma 2.1.17. *For all $\gamma, \gamma' \in SL_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$,*

(a) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$,

(b) $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$,

(c) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$ *(this is an equalty of operators),*

(d) $Im(\gamma(\tau)) = \frac{Im(\tau)}{|j(\gamma,\tau)|^2}$

Proof. See [DS05, Chapter 1, Section 2, Lemma 1.2.2] □

Remark 2.1.18. *A consequence of Lemma 2.1.17 is that if a function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is weakly modular of weight k with respect to a set of matrices, then f is weakly modular of weight k with respect to the group generated by that set. In particular, since*
$$\mathrm{SL}_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle,$$
the condition of weak modularity for the full modular group can be verified by checking it only for the generators
$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

With the notion of weak modularity for congruence subgroups established, we can now define the corresponding spaces of modular and cusp forms.

Definition 2.1.19. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and k be an integer. A function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is a modular form of weight k with respect to Γ if:*

- *f is holomorphic on $\mathcal{H}$;*

- *f is weakly modular of weight k with respect to Γ;*
- *$[\alpha]_k(f)$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

The set of modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$.

As in the case of the full modular group, we can distinguish a specific subspace of modular forms that vanish at the boundaries of the upper half-plane. This leads to the following definition of cusp forms for a congruence subgroup:

Definition 2.1.20. *A modular form $f \in \mathcal{M}_k(\Gamma)$ is a cusp form of weight k with respect to Γ if the constant term a_0 in the Fourier expansion of $[\alpha]_k(f)$ is zero for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. The space of such forms is denoted by $\mathcal{S}_k(\Gamma)$.*

It is important to notice that for a general congruence subgroup Γ, a modular form f may not have a period of 1 at every cusp. For any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the function $[\alpha]_k(f)$ is periodic with some minimal period $h > 0$ (called the width of the cusp). Consequently, its Fourier expansion (or q-expansion) is given in terms of $q_h = e^{2\pi i\tau/h}$:

$$([f]_k\alpha)(\tau) = \sum_{n=0}^{\infty} a_n q_h^n.$$

The condition for f to be a cusp form is then $a_0 = 0$ for every such expansion. Since the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite, there are only finitely many non-equivalent cusps to check.

2.2 Modular curves

The study of modular forms and congruence subgroups is not merely an analytical endeavor; it possesses a profound geometric interpretation. Until now, we have viewed the upper half-plane $\mathcal{H}$ primarily as the domain for modular functions. However, the quotient of $\mathcal{H}$ by the action of a congruence subgroup Γ can be endowed with the structure of a Riemann surface. These quotient spaces, known as modular curves, are of fundamental importance in arithmetic geometry for two main reasons:

(a) Moduli Spaces: They serve as *moduli spaces*, where each point of the curve corresponds to an isomorphism class of elliptic curves equipped with a specific level-N structure (such as a torsion point of order N or a cyclic subgroup).

(b) Compactification: By adding the finite set of cusps to the quotient $\Gamma\backslash\mathcal{H}$, we obtain a compact Riemann surface, denoted by $X(\Gamma)$. This compactification is crucial as it allows us to employ the tools of algebraic geometry..

Definition 2.2.1. *Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be any congruence subgroup. The modular curve $Y(\Gamma)$ is defined as the quotient space of orbit of the action of Γ on $\mathcal{H}$, that is*

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

The modular curves for $\Gamma_0(N), \Gamma_1(N)$ and $\Gamma(N)$ are denoted

$$Y_0(N) = \Gamma_0(N)\backslash\mathcal{H} \quad Y_1(N) = \Gamma_1(N)\backslash\mathcal{H} \quad \text{and} \quad Y(N) = \Gamma(N)\backslash\mathcal{H}.$$

In the following, we will specifically focus on the modular curve $X_0(N)$, associated with the congruence subgroup $\Gamma_0(N)$. As we shall see, this curve plays a key role in arithmetic geometry as it parametrizes isomorphism classes of elliptic curves together with a cyclic subgroup of order N.

2.2.1 The Riemann surface $X_0(N)$

The goal of this subsection is to show that $Y_0(N)$ can be made into a Riemann surface that can be compactified.

Definition 2.2.2. *A Riemann surface is a 1-dimensional connected complex manifold.*

First of all, the upper half plane $\mathcal{H}$ inherits the euclidean topology as a subspace of $\mathbb{R}^2$. The natural surjection

$$\pi : \mathcal{H} \longrightarrow Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}, \qquad \pi(\tau) = \Gamma_0(N)\tau$$

gives $Y_0(N)$ the quotient topology, meaning a subset of $Y_0(N)$ is open if its inverse image under π in $\mathcal{H}$ is open. In order to show that $Y_0(N)$ is Hausdorff, we need a lemma.

Lemma 2.2.3. *Let $\tau_1, \tau_2 \in \mathcal{H}$ be given. Then there exist neighborhoods U_1 of τ_1 and U_2 of τ_2 in $\mathcal{H}$ with the property*

$$\text{for all } \gamma \in \mathrm{SL}_2(\mathbb{Z}), \text{ if } \gamma(U_1) \cap U_2 \neq \emptyset \text{ then } \gamma(\tau_1) = \tau_2.$$

Proof. See [DS05, Chapter 2, Section 1, Proposition 2.1.1]. □

Corollary 2.2.4. *The modular curve $Y_0(N)$ is Hausdorff.*

Proof. See [DS05, Chapter 2, Section 1, Proposition 2.1.2]. □

We now put local coordinates on $Y_0(N)$. This means finding for each point $\pi(\tau) \in Y_0(N)$ a neighborhood $\tilde{U}$ and a homeomorphism $\varphi : \tilde{U} \to V \subseteq \mathbb{C}$ such that the transition maps between the local coordinate systems are holomorphic. We have to distinguish two cases, depending on the so-called *isotropy subgroup*.

Definition 2.2.5. *Let τ be an element of $\mathcal{H}$. The isotropy group of τ is the τ-fixing subgroup of $\Gamma_0(N)$*

$$\Gamma_0(N)_\tau := \{\gamma \in \Gamma_0(N) : \gamma(\tau) = \tau\}.$$

A point $\tau \in \mathcal{H}$ is called elliptic if its isotropy group is nontrivial.

By Lemma 2.2.3, if τ is a point of $\mathcal{H}$ with trivial isotropy group, we can choose an open neighborhood U of τ that does not contain elliptic points. Moreover, one can show that the open neighborhood $\pi(U)$ equipped with the homeomorphism

$$\varphi : \pi(U) \longrightarrow U$$

gives a local chart. In contrast, for an elliptic point, the situation is more pathological. As a consequence of lemma 2.2.3, we can choose a neighborhood U of τ which has no elliptic points except possibly τ. For this reason, we can construct a chart for the elliptic point τ as follows: consider

$$\delta = \begin{bmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C}) \qquad \text{and} \qquad \rho : \tau \mapsto \tau^h$$

where $h \in \mathbb{N}^*$ is the period of the elliptic point τ (see [DS05, Chapter 2, Section 2] for more details). One can show that the composition

$$\psi : U \longrightarrow \mathbb{C}, \qquad \psi(\tau) := \rho(\delta(\tau))$$

induces a homeomorphism

$$\tilde{\psi} : \pi(U) \longrightarrow V := \mathrm{Im}(\psi).$$

For a complete proof that these families of open sets define an atlas and endow $Y_0(N)$ with the structure of a Riemann surface, see [DS05, Chapter 2, Section 2].

The goal is now to compactify $Y_0(N)$. First of all, define

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

One can check that a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ is

$$\mathcal{D} = \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) \in [-1/2, 1/2], \quad |\tau| \geq 1\}$$

(see [DS05, Chapter 2, Section 2]). This means that, as sets, we can write

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \ \simeq \ \mathcal{D}/\sim$$

where $\sim$ denotes the identifications induced by the action of $\mathrm{SL}_2(\mathbb{Z})$ on the boundary of the fundamental domain $\mathcal{D}$. Moreover, since by Remark 2.1.15

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = r < \infty,$$

we can write

$$\mathrm{SL}_2(\mathbb{Z}) = \coprod_{j=1}^{r} \beta_j \Gamma_0(N)$$

and one can check that

$$\mathcal{D}_N := \bigcup_{j=1}^{r} \beta_j^{-1}(\mathcal{D})$$

is a fundamental domain for $\Gamma_0(N)$. Hence we have at most r noncompact ends of $Y_0(N)$. For each $j = 1, \ldots, r$ we define

$$\beta_j^{-1}(\infty) := \lim_{\mathrm{Im}(\tau)\to\infty} \beta_j^{-1}(\tau)$$

and we say that, for each j, $\beta_j^{-1}(\infty)$ is a representative for a *cusp*. For example, if $\beta_j^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

$$\beta_j^{-1}(\infty) := \lim_{\mathrm{Im}(\tau)\to\infty} \frac{a\tau + b}{c\tau + d} = \lim_{\mathrm{Im}(\tau)\to\infty} \frac{a + b/\tau}{c + d/\tau} = \frac{a}{c} \in \mathbb{Q}.$$

This is the reason why we introduce $\mathbb{Q} \cup \{\infty\}$ and consider $\mathcal{H}^*$: we can consider cusps as the equivalence classes of $\mathbb{P}^1(\mathbb{Q})$ under the action of $\Gamma_0(N)$. More precisely, for all $\frac{m}{n} \in \mathbb{Q}$ and $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N)$ we define

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{m}{n} := \frac{am + bn}{cm + dn}$$

where this means to take ∞ to a/c and $-d/c$ to ∞ if $c \neq 0$ and to take ∞ to ∞ if $c = 0$. Note that the number of cusps of $Y_0(N)$ is in general less than or equal to r, and it may be strictly smaller, since some of the $\beta_j^{-1}(\infty)$ may be equivalent under the action of $\Gamma_0(N)$.

Definition 2.2.6. *In order to construct a Riemann surface, we topologize $\mathcal{H}^*$ by defining a neighborhood system $\mathcal{U}$ for each point $\tau \in \mathcal{H}^*$:*

- *if $\tau \in \mathcal{H}$ then $\mathcal{U} = \{D = D(\tau, r) : r > 0, \quad D \subseteq \mathcal{H}\}$;*
- *If $\tau = x \in \mathbb{Q}$ we set $\mathcal{U} = \{D(x + iy, y) \cup \{x\} : y > 0\}$;*
- *for $\tau = \infty$ we define $\mathcal{U} = \{\{\omega \in \mathbb{C} : \mathrm{Im}(\omega) > r\} : r > 0\}$.*

With this topology, the following facts hold:

- $\mathcal{H}^*$ is Hausdorff;
- $\mathcal{H}$ is open in $\mathcal{H}^*$;
- the action of $\Gamma_0(N)$ is continuous;

Definition 2.2.7. *We define $X_0(N) := \Gamma_0(N)\backslash\mathcal{H}^*$*

Note that, by definition, $X_0(N)$ is a compact Hausdorff topological space. One can prove that $X_0(N)$ is the compactification of $Y_0(N)$.

Definition 2.2.8. *Finally, we define the atlas $\{(\tilde{U}_\tau, \varphi_\tau)\}$ on $X_0(N)$. As we did for $Y_0(N)$, let*

$$\pi : \mathcal{H}^* \longrightarrow X_0(N)$$

be the quotient map, that is open. We distinguish the cases for $\tau \in \mathcal{H}^*$.

- *If $\tau \in \mathcal{H}$, the construction of local charts around τ has already been discussed.*

- *If $\tau \in \mathbb{P}^1(\mathbb{Q})$, choose $\beta \in \mathrm{SL}_2(\mathbb{Z})$ with $\beta(\tau) = \infty$. Then*

$$\beta\Gamma_0(N)_\tau\beta^{-1} = \left\{ \pm \begin{bmatrix} 1 & mh \\ 0 & 1 \end{bmatrix} : m \in \mathbb{Z} \right\},$$

where h is a fixed integer that depends on τ and $\Gamma_0(N)_\tau$ is the isotropy group of τ. Let $U_\tau := \beta^{-1}(\{\mathrm{Im}(\tau) > 2\})$. One can prove that $\gamma(U_\tau) \cap U_\tau = \emptyset$ for all $\gamma \in \Gamma_0(N)/\Gamma_0(N)_\tau$. We define $\tilde{U}_\tau := \pi(U_\tau)$ and $\varphi_\tau : \tilde{U}_\tau \to \mathbb{C}$ with $\varphi_\tau(\pi(z)) := e^{2\pi\beta(z)/h}$.

One can finally prove that these are compatible complex charts and thus with this atlas, $X_0(N)$ is a compact Riemann surface (for more details see [DS05, Chapter 2, Section 4]).

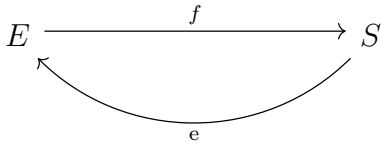
2.2.2 A moduli interpretation for $Y_0(N)$

Let N be a positive integer. In this section we will discuss how the points of the modular curve $Y_0(N)$ represent, in some sense, certain elliptic curves together with a fixed cyclic subgroup of order N. To begin with we will need some basic scheme-theoretic notions, which will be briefly summarized. We will call a scheme over $\mathrm{Spec}(\mathbb{Z}[1/N])$ a $\mathbb{Z}[1/N]$-scheme and we will denote by

$$\mathrm{Hom}_{\mathbb{Z}[1/N]}(S, T)$$

the set of arrows in the category $\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]}$ from S to T for all $\mathbb{Z}[1/N]$-schemes S and T.

Definition 2.2.9. *Let S be an arbitrary scheme. An elliptic curve over S is a proper smooth curve*



with geometrically connected fibers all of genus one, given with a section e. We will denote it by (E, e) or simply by E.

We now define a functor. For each $\mathbb{Z}[1/N]$-scheme S, let

$$F_0(N)(S) := \{(E \to S, C)\}/\cong_S,$$

where

- $E \to S$ is an elliptic curve over S;
- $C \subset E$ is a cyclic subgroup of order N, defined over S;

- two pairs $((E,e),C)$ and $((E',e'),C')$ are isomorphic, written

$$((E,e),C) \cong_S ((E',e'),C'),$$

if there exists an isomorphism of S-schemes $f : E \to E'$ sending e to e' and C to C'.

Note that in particular, if $K \subseteq \mathbb{C}$ is a field, then $F_0(N)$ coincides with the set

$$\left\{(E,C) \;\middle|\; \begin{array}{l} E \text{ is an elliptic curve defined over } K, \\ C \subseteq E \text{ is a cyclic subgroup of order } N \text{ defined over } K \end{array}\right\} \Big/ \cong_K$$

where the equivalence relation $\cong_K$ is defined as follows: we write

$$(E,C) \cong_K (E',C')$$

if there exists an isomorphism of elliptic curves

$$\varphi : E \longrightarrow E'$$

defined over K such that $\varphi(C) = C'$.

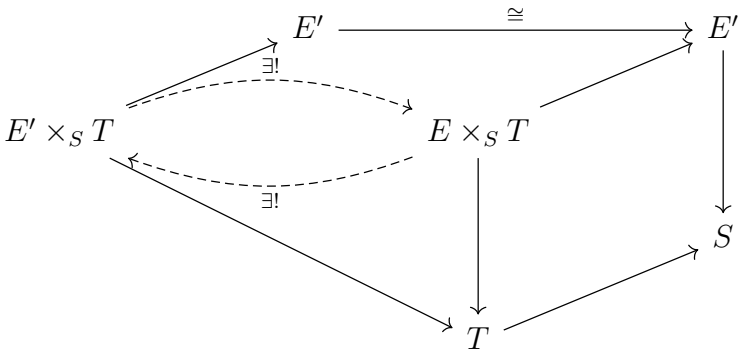
Moreover, let $f : T \to S$ be a morphism of $\mathbb{Z}[1/N]$-schemes. We want to define a map

$$F_0(N)(f) : F_0(N)(S) \longrightarrow F_0(N)(T).$$

Let $[(E,C)]$ be an element of $F_0(N)(S)$, then we can apply the base change to E and C

$$\begin{array}{ccc} E_T : E \times_S T & \longrightarrow & E \\ \downarrow & & \downarrow \\ T & \xrightarrow[f]{} & S \end{array} \qquad \begin{array}{ccc} C_T : C \times_S T & \longrightarrow & C \\ \downarrow & & \downarrow \\ T & \xrightarrow[f]{} & S \end{array}$$

and we put $F_0(N)(f)([(E,C)]) := [(E_T, C_T)]$. Note that this association is well defined thanks to the categorical definition of the fiber product:



Summing up, we obtain a functor

$$\begin{array}{rcl} F_0(N) : (\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]})^{op} & \longmapsto & \underline{Set} \\ S & \longmapsto & F_0(N)(S) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle F_0(N)(f)} \\ T & \longmapsto & F_0(N)(T) \end{array}$$

Recall that a functor $\mathcal{F} : \mathcal{C}^{op} \to \underline{\mathrm{Set}}$ is represented by $A \in \mathrm{Ob}(\mathcal{C})$ if there exists a natural isomorphism $\alpha : \mathcal{F} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\cdot, A)$. If $\mathcal{C} = \underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]}$ we will call the representing object (if it exists) of $\mathcal{F}$ a *fine moduli space* for the *moduli problem* $\mathcal{F}$. If we assume that $F_0(N)$ is representable, then there exists a scheme Y over $\mathbb{Z}[1/N]$ such that, for every $\mathbb{Z}[1/N]$-scheme S, there is a natural bijection

$$F_0(N)(S) \cong \mathrm{Hom}_{\mathbb{Z}[1/N]}(S, Y). \tag{2.2}$$

For example, if K is a number field, then $\mathrm{Spec}(K)$ is a $\mathbb{Z}[1/N]$-scheme thanks to the inclusions

$$\mathbb{Z}[1/N] \hookrightarrow \mathbb{Q} \hookrightarrow K$$

and (2.2) yields a bijection

$$F_0(N)(\mathrm{Spec}(K)) \cong \mathrm{Hom}_{\mathbb{Q}}(\mathrm{Spec}(K), Y),$$

so that each isomorphism class of objects parametrized by $F_0(N)$ over K corresponds to an arrow $\mathrm{Spec}(K) \to Y$, i.e. a K-rational point of Y.

Unfortunately, in general the functor $F_0(N)$ does not satisfy the representability property. Indeed, one can easily see that a necessary condition for the existence of a fine moduli space Y for $F_0(N)$ is that, if $f : S \to T$ is a monomorphism in $\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]}$, then $F_0(N)(f)$ has to be injective. But consider the inclusion $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$: it induces a map

$$F_0(N)(\mathrm{Spec}(\mathbb{Q})) \to F_0(N)(\mathrm{Spec}(\overline{\mathbb{Q}}))$$

that is not injective, because two elliptic curves over $\mathbb{Q}$ with the same j-invariant are isomorphic over $\overline{\mathbb{Q}}$, but in general not over $\mathbb{Q}$. For this reason, we must weaken the hypotheses.

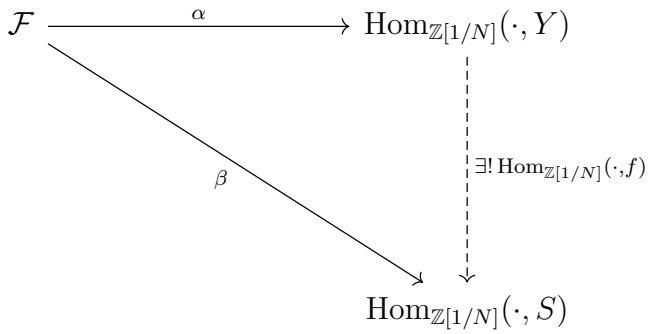
Definition 2.2.10. *Let $\mathcal{F} : (\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]})^{op} \to \underline{\mathrm{Set}}$ be a functor. A coarse moduli space is an object Y of $\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]}$ together with a natural transformation $\alpha : \mathcal{F} \to \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, Y)$ such that:*

(a) For all algebraically closed fields K equipped with a morphism $\mathrm{Spec}(K) \to \mathrm{Spec}(\mathbb{Z}[1/N])$, the induced map

$$\alpha_{\mathrm{Spec}(K)} : \mathcal{F}(\mathrm{Spec}(K)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[1/N]}(\mathrm{Spec}(K), Y)$$

is a bijection.

(b) If $S \in \mathrm{Ob}(\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]})$ and if $\beta : \mathcal{F} \to \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, S)$ is a natural transformation, there exists a unique arrow $f : Y \to S$ in $\underline{\mathrm{Sch}}_{\mathbb{Z}[1/N]}$ such that



is commutative.

One can check that the modular curve $Y_0(N)$ is a coarse moduli space for the moduli functor $F_0(N)$. In particular $Y_0(N)$ admits a model over $\mathbb{Q}$ by the base change

$$\begin{array}{ccc} Y_0(N) \times_{\mathrm{Spec}(\mathbb{Z}[1/N])} \mathrm{Spec}(\mathbb{Q}) & \longrightarrow & Y_0(N) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Q}) & \longrightarrow & \mathrm{Spec}(\mathbb{Z}[1/N]). \end{array}$$

Moreover, if K is a number field, then

$$\alpha_{\mathrm{Spec}(K)}([(E, C)]) \in \mathrm{Hom}_{\mathbb{Z}[1/N]}(\mathrm{Spec}(K), Y_0(N))$$

for each $[(E, C)] \in \{(E \to S, C)\}/\cong_{\mathrm{Spec}(K)}$. In conclusion, an elliptic curve E over K together with a fixed cyclic subgroup $C \subseteq E$ of order N corresponds via $\alpha_{\mathrm{Spec}(K)}$ to a K-rational point of $Y_0(N)$.

Without proving the universal property, we examine the isomorphism

$$\alpha_{\mathrm{Spec}(\mathbb{C})} : F_0(N)(\mathrm{Spec}(\mathbb{C})) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[1/N]}(\mathrm{Spec}(\mathbb{C}), Y_0(N))$$

appearing in the definition of a coarse moduli space. Note that an element of $F_0(N)(\mathrm{Spec}(\mathbb{C}))$ is of the form $[(E_\tau, \langle 1/N + \Lambda_\tau \rangle)]$, for some $\tau \in \mathcal{H}$, where

$$\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau, \quad \text{and} \quad E_\tau = \mathbb{C}/\Lambda_\tau.$$

Indeed, for each pair (E, C) where E is an elliptic curve over $\mathbb{C}$ and $C \subseteq E$ a fixed cyclic subgroup of order N, there exists $\tau \in \mathcal{H}$ such that

$$(E, C) \cong_{\mathbb{C}} (\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle).$$

To see this, write

$$E = \mathbb{C}/\Lambda_{\tau'}, \quad \text{and} \quad C = \langle \frac{c + d\tau'}{N} + \Lambda_{\tau'} \rangle$$

for some $c, d \in \mathbb{Z}$. Note that $\gcd(c, d, N) = 1$ since $P := (c + d\tau')/N$ has exact order N and we can write

$$ad - bc - kN = 1$$

for some $a, b, k \in \mathbb{Z}$. Consider now $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ and note that its reduction modulo N

$$\overline{\gamma} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$$

is an element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since the projection map

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

is surjective, and since modifying entries modulo N does not affect P, we may assume that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Finally, put $\tau := \gamma(\tau')$ and $m = c\tau' + d$. Thus

$$\begin{aligned} m \cdot \Lambda_\tau &= m \cdot (\mathbb{Z} \oplus \mathbb{Z}\tau) \\ &= \mathbb{Z}m \oplus \mathbb{Z}m\tau \\ &= \mathbb{Z}(c\tau' + d) \oplus \mathbb{Z}(a\tau' + b) \\ &= \mathbb{Z} \oplus \mathbb{Z}\tau' \\ &= \Lambda_{\tau'}, \end{aligned}$$

where in the fourth equality we used 1.4.3. Moreover,

$$m \cdot \left(\frac{1}{N} + \Lambda_\tau \right) = \frac{m}{N} + m \cdot \Lambda_\tau = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = P.$$

In conclusion, the isomorphism given by multiplication by m

$$[m] : \mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}/\Lambda_{\tau'}$$

sends $\langle 1/N + \Lambda_\tau \rangle$ to C.

We can give the following theorem:

Theorem 2.2.11. *Two points of $F_0(N)(\mathrm{Spec}(\mathbb{C}))$, $[E_\tau, \langle 1/N + \Lambda_\tau \rangle]$ and $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle]$, are equal if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Thus there is a bijection*

$$\alpha := \alpha_{\mathrm{Spec}(\mathbb{C})} : F_0(N)(\mathrm{Spec}(\mathbb{C})) \longrightarrow Y_0(N)(\mathbb{C}), \quad [E_\tau, \langle 1/N + \Lambda_\tau \rangle] \mapsto \Gamma_0(N)\tau.$$

Proof. Let $\tau, \tau' \in \mathcal{H}$ such that $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. This means that there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ such that $\gamma(\tau') = \tau$. As we did above, if we consider $m := c\tau' + d$, then

$$m \cdot \Lambda_\tau = \Lambda_{\tau'} \quad \text{and} \quad m \cdot \left(\frac{1}{N} + \Lambda_\tau \right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}.$$

Since $c = kN$ for some $k \in \mathbb{Z}$ and since

$$1 = \det(\gamma) = ad - bc = ad - Nkb,$$

we have that $\gcd(d, N) = 1$, and so

$$\langle \frac{c\tau' + d}{N} + \Lambda_{\tau'} \rangle = \langle \frac{d}{N} + \Lambda_{\tau'} \rangle = \langle \frac{1}{N} + \Lambda_{\tau'} \rangle.$$

In conclusion, the isomorphism $[m] : \mathbb{C}/\Lambda_\tau \to \mathbb{C}/\Lambda_{\tau'}$ sends $\langle 1/N + \Lambda_\tau \rangle$ to $\langle 1/N + \Lambda_{\tau'} \rangle$.

Conversely, let $m \in \mathbb{C}$ such that

$$m \cdot \Lambda_\tau = \Lambda_{\tau'} \quad \text{and} \quad \langle \frac{m}{N} + \Lambda_{\tau'} \rangle = \langle \frac{1}{N} + \Lambda_{\tau'} \rangle.$$

From the first condition and from Lemma 1.4.3, we can choose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}. \tag{2.3}$$

Moreover, from the second condition, there exists $k \in \mathbb{Z}$ with $\gcd(k, N) = 1$ such that

$$\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{m}{N} + \Lambda_{\tau'} = \frac{k}{N} + \Lambda_{\tau'}.$$

Hence $(c\tau' + d - k)/N \in \mathbb{Z} \oplus \mathbb{Z}\tau'$, which implies $c \equiv 0 \pmod{N}$, i.e., $\gamma \in \Gamma_0(N)$. In conclusion, from (2.3):

$$m\gamma(\tau') = m \cdot \frac{a\tau' + b}{c\tau' + d} = a\tau' + b = m\tau,$$

that is $\gamma(\tau') = \tau$. □

2.3 Eichler–Shimura theory

In this section we briefly introduce the Eichler–Shimura theory, which will be crucial in the next chapters. The aim is to construct a morphism defined over $\mathbb{Q}$

$$\psi \colon X_0(N) \longrightarrow E,$$

where E is an elliptic curve defined over $\mathbb{Q}$. We call ψ the modular parametrization of the elliptic curve E; it will be a fundamental tool for mapping points from $X_0(N)$ to E while preserving the field of definition of these points. Before stating the main theorem of this section, due to Eichler and Shimura, we need some preliminary results and definitions.

2.3.1 Preliminaries

The first important object that we want to define is the Jacobian variety associated to a compact Riemann surface.

Definition 2.3.1. *Let X be a compact Riemann surface and let $\{(U_i, \varphi_i)_{i\in I}\}$ be an atlas. A system $\{\omega_i\}_{i\in I}$ of scalar-valued functions ω_i on U_i is called a meromorphic differential if*

$$\omega_i \circ \varphi_i^{-1} = (\omega_j \circ \varphi_i^{-1}) \cdot (\varphi_j \circ \varphi_i^{-1})' \quad on \quad \varphi_i(U_i \cap U_j) \subseteq \mathbb{C} \tag{2.4}$$

whenever $U_i \cap U_j \neq \emptyset$.

We will denote the $\mathbb{C}$-vector space of meromorphic differentials by $\Omega(X)$. The derivative factor in (2.4) ensures that meromorphic differentials can be integrated, since the value of the integral does not depend on the choice of the chart U_i. For this reason, the classical notation that is used for $\omega_i \circ \varphi_i^{-1}$ is $\omega_i(\varphi_i^{-1}(z))dz$, where z is a local parameter. If $\omega = \{\omega_i\}_{i\in I}$ is a meromorphic differential and ω_i is holomorphic on U_i for all $i \in I$ we will call ω a holomorphic differential and we will denote by $\Omega_{\text{hol}}(X)$ the corresponding vector space.

Examples 2.3.2. *Let E be an elliptic curve over $\mathbb{C}$ described by the weierstrass equation*

$$f(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

Since by definition E is smooth, we have

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0, 0)$$

for all points $P \in E$. Since the two variables x, y can be viewed as meromorphic functions $E \to \mathbb{C}$, then also $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}$ are meromorphic. Moreover, $f|_E \equiv 0$, then

$$df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = 0$$

on E. In other words we obtain the equality

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

At points of $E(\mathbb{C})$ where $\frac{\partial}{\partial y} \neq 0$, x is a local coordinate of $E(\mathbb{C})$ and the left side defines locally a holomorphic differential. At points where $\frac{\partial}{\partial x} \neq 0$, y is a local coordinate and the right side defines locally a holomorphic differential. By a suitable change of coordinates, one can check that the holomorphy can be extended at the point ∞.

With the notations of the example 2.3.2 we give the following definition.

Definition 2.3.3. *Let $f_x := \frac{\partial f}{\partial x}$ and $f_y := \frac{\partial f}{\partial y}$. By the previous argument, it makes sense to define the holomorphic differential on E*

$$\omega := \frac{dx}{f_y} = -\frac{dy}{f_x}$$

and we will call it the invariant differential for E.

Let X be a compact Riemann surface of genus $g = g(X)$. Since X is in particular a closed orientable surface, the ordinary homology group $H^1(X, \mathbb{Z})$ is a free abelian group with $2g$ generators. Moreover, a consequence of the Riemann–Roch theorem is that $\Omega_{\text{hol}}(X)$ has dimension g as $\mathbb{C}$-vector space. For this reasons we give the following.

Definition 2.3.4. *With notation above, let $\omega_1, \ldots, \omega_g$ be a basis of $\Omega_{\text{hol}}(X)$ over $\mathbb{C}$ and let $c_1, \ldots, c_{2g}$ be a $\mathbb{Z}-$basis for $H_1(X, \mathbb{Z})$. We define the Jacobian variety of X as the g-dimensional complex torus $J(X) := \mathbb{C}^g/\Lambda(X)$ where*

$$\Lambda(X) = \begin{pmatrix} \int_{c_1} \omega_1 \\ \vdots \\ \int_{c_1} \omega_g \end{pmatrix} \mathbb{Z} \oplus \cdots \oplus \begin{pmatrix} \int_{c_{2g}} \omega_1 \\ \vdots \\ \int_{c_{2g}} \omega_g \end{pmatrix} \mathbb{Z}$$

One can check that the $2g$ vectors

$$\begin{pmatrix} \int_{c_k} \omega_1 \\ \vdots \\ \int_{c_k} \omega_g \end{pmatrix}, \quad k = 1 \ldots 2g$$

in $\mathbb{C}^g$ are linearly independent over $\mathbb{R}$. Moreover, the lattice $\Lambda(X)$ is unchanged if $\{c_k\}$ is replaced by a different $\mathbb{Z}-$basis and one can show that if $\{\omega_i\}$ is replaced by another basis of $\Omega_{\text{hol}}(X)$, the effect is to transform $\Lambda(X)$ by an element of $\text{Gl}_g(\mathbb{C})$.

The Jacobian variety is the first step for the construction of the modular parametrization since we will define ψ by a composition that passes through $J_0(N) = J(X_0(N))$.

Definition 2.3.5. *Let X be a compact Riemann surface of genus g and fix a point $x_0 \in X$. The Abel–Jacobi map with base point x_0 is*

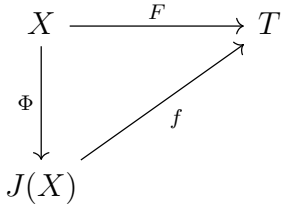
$$\Phi : X \longrightarrow J(X)$$

given by

$$x \longmapsto \left(\int_{x_0}^{x} \omega_1, \ldots, \int_{x_0}^{x} \omega_g \right).$$

The Abel–Jacobi map with base point $x_0 \in X$ has the following universal property.

Proposition 2.3.6. *If $F : X \to T$ is a holomorphic mapping of a compact Riemann surface of genus $g \geq 1$ into a complex torus, then F factors through the Jacobian variety: $F = f \circ \Phi$ for some holomorphic mapping $f : J(X) \to T$ that is the sum of a translation and a holomorphic homomorphism. In other words the diagram*



is commutative.

Proof. See [Kna92, Theorem 11.19]. □

Recall that an abelian variety A is a nonsingular projective variety over $\mathbb{C}$ with a distinguished point O and with an abelian group structure such that O is the identity and the operations of addition and negative are morphisms. A morphism $F : A \to B$ of abelian varieties is a morphism of varieties that is also a homomorphism of groups. Moreover, the abelian variety is said to be defined over $\mathbb{Q}$ if A is defined over $\mathbb{Q}$ as projective variety, O is in $A(\mathbb{Q})$ and addition and negative are defined over $\mathbb{Q}$.

The following theorem says that the Riemann surface X and the complex torus $J(X)$ can be actually viewed as nonsingular projective varieties, so it makes sense the name "Jacobian *variety*".

Theorem 2.3.7. *Let $\mathcal{C}$ be a nonsingular projective curve and consider $J(\mathcal{C})$ as the Jacobian variety of its underlying Riemann surface. Then $J(\mathcal{C})$ is an abelian variety, $\Phi : \mathcal{C} \to J(\mathcal{C})$ is a morphism of abelian varieties and we can rewrite the universal property in Proposition 2.3.6 in the following form:*
each morphism of varieties $F : \mathcal{C} \to A$ into an abelian variety, factors through $J(\mathcal{C})$ as $F = f \circ \Phi + F(x_0)$, where Φ is the Abel–Jacobi mapping with basis point $x_0 \in \mathcal{C}$. Moreover, if $\mathcal{C}$ is defined over $\mathbb{Q}$, then $J(\mathcal{C})$ can be defined over $\mathbb{Q}$ and the universal properties holds with all the structures defined over $\mathbb{Q}$.

Another concept that we need to develop for the Eichler–Shimura theory is that of so-called newforms. First of all we define the Hecke operators $\mathrm{T}_k(n)$ on the vector space $\mathcal{M}_k(\Gamma_0(N))$. To begin with consider

$$M(n) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) : \det(A) = N \right\}$$

and let

$$M(n, N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(n) : c \equiv 0 \pmod{N} \text{ and } \gcd(a, N) = 1 \right\}.$$

One can check that the matrices of the form

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

with $ad = n$, $d > 0$, $\gcd(a, N) = 1$ and $0 \leq b < d$ are a complete set of coset representatives for the right cosets of $\Gamma_0(N)$ on $M(n, N)$. In particular we have a finite disjoint union

$$M(n, N) = \coprod_i \Gamma_0(N)\alpha_i$$

where α_i satisfies the above condition for all i. Moreover, for all $f \in \mathcal{M}_k(\Gamma_0(N))$ and for all i, we define

$$(f \circ [\![\alpha_i]\!]_k)(\tau) := \delta(\alpha_i, \tau)^{-k} f(\alpha_i \cdot \tau) \det(\alpha_i)^{\frac{k}{2}}$$

where $\tau \in \mathcal{H}$. Now we are ready for the definition of Hecke operator.

Definition 2.3.8. *With notation above, the Hecke operator is the map*

$$\mathrm{T}_k(n) : \mathcal{M}_k(\Gamma_0(N)) \longrightarrow \mathcal{M}_k(\Gamma_0(N))$$

given by

$$\mathrm{T}_k(n)f := n^{\frac{k}{2}-1} \sum_i f \circ [\![\alpha_i]\!]_k.$$

Proposition 2.3.9. *The Hecke operator* $\mathrm{T}_k(n)$ *is well defined, i.e.*

$$\mathrm{T}_k(n)(\mathcal{M}_k(\Gamma_0(N))) \subseteq \mathcal{M}_k(\Gamma_0(N)).$$

Moreover, it carries $\mathcal{S}_k(\Gamma_0(N))$ *to itself.*

Proof. See [Kna92, Proposition 9.13]. □

Moreover, the following propetries holds.

Proposition 2.3.10. *On the space* $\mathcal{M}_k(\Gamma_0(N))$*, the Hecke operators satisfy:*

(a) for a prime power p^r *with* $r \geq 1$ *such that* $p \nmid N$*,*

$$\mathrm{T}_k(p^r)\mathrm{T}_k(p) = \mathrm{T}_k(p^{r+1}) + p^{k-1}\mathrm{T}_k(p^{r-1});$$

(b) for a prime power p^r *with* $r \geq 1$ *such that* $p \mid N$*,*

$$\mathrm{T}_k(p^r) = \mathrm{T}_k(p)^r;$$

(c) $\mathrm{T}_k(m)\mathrm{T}_k(n) = \mathrm{T}_k(mn)$ *if* m *and* n *are relatively prime;*

(d) The algebra generated by the $\mathrm{T}_k(n)$ *for* $n = 1, 2, 3, \ldots$ *is generated by the* $\mathrm{T}_k(p)$ *with* p *prime and is commutative.*

Proof. See [Kna92, Theorem 9.17]. □

Now we introduce the Petersson inner product on cusp forms that that will be a crucial ingredient in the definition of the newforms.

Definition 2.3.11. *The Patersson inner product on* $\mathcal{S}_k(\Gamma_0(N))$ *is*

$$\langle f, h\rangle = \int_{R_N} f(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}$$

for all $f, h \in \mathcal{S}_k(\Gamma_0(N))$*, where* R_N *is a fundamental domain for* $\Gamma_0(N)$*.*

Theorem 2.3.12 (Petersson)**.** *The Hecke operators* $\mathrm{T}_k(n)$ *with* $\gcd(n, N) = 1$*, on the space of cusp forms* $\mathcal{S}_k(\Gamma_0(N))$*, are self adjoint relative to the Petersson inner product. In other words, if* $\gcd(n, N) = 1$*, then*

$$\langle \mathrm{T}_k(n)f, h\rangle = \langle f, \mathrm{T}_k(n)h\rangle$$

for all $f, h \in \mathcal{S}_k(\Gamma_0(N))$*.*

Proof. See [Kna92, Theorem 9.18]. □

Before we continue, we need the following definition.

Definition 2.3.13. *An eigenvector cusp form under the* $\mathrm{T}_k(n)$ *with* $\gcd(N,n)=1$ *is called an eigenform.*

Since the Hecke operators $\mathrm{T}_k(n)$ commute and are self adjoint relative to the Petersson product whenever $\gcd(N,n)=1$, we can conclude that $\mathcal{S}_k(\Gamma_0(N))$ splits into the orthogonal sum of simultaneous eigenspaces for the operators $\mathrm{T}_k(n)$ with $\gcd(N,n)=1$. However, the dimension of these simultaneous eigenspaces is, in general, greater than 1. This degeneracy is due to some modular forms that arise from lower levels M (where M is a proper divisor of N) and are naturally embedded into $\mathcal{S}_k(\Gamma_0(N))$. More precisely we have two types of these cusp forms.

(a) Consider $f(\tau)\in\mathcal{S}_k(\Gamma_0(N/r))$, where $r\mid N$. Then, since

$$\Gamma_0(N)\subseteq\Gamma_0(N/r),$$

f is a cusp form of weight k also for $\Gamma_0(N)$. Moreover, if in addition f is an eigenform for

$$\mathrm{T}_k(N):\mathcal{S}_k(\Gamma_0(N/r))\longrightarrow\mathcal{S}_k(\Gamma_0(N/r))$$

where $\gcd(N,n)=1$, then the formula for $\mathrm{T}_k(n)f$ is the same relative to $\Gamma_0(N)$ as relative to $\Gamma_0(N/r)$. Summing up, an eigenform for $\Gamma_0(N/r)$ becomes an eigenform for $\Gamma_0(N)$ with the same eigenvalues.

(b) Consider $f(\tau)\in\mathcal{S}_k(\Gamma_0(N/r))$, where $r\mid N$. Then one can easily check that

$$f(r\tau)\in\mathcal{S}_k(\Gamma_0(N))$$

and letting $\mathrm{A}_k(r)$ be the operator

$$\mathrm{A}_k(r)f=f\circ\begin{bmatrix}r&0\\0&1\end{bmatrix}_k,$$

it carries $\mathcal{S}_k(\Gamma_0(N/r))$ to $\mathcal{S}_k(\Gamma_0(N))$ and satisfies

$$\mathrm{A}_k(r)\mathrm{T}_k(n)=\mathrm{T}_k(n)\mathrm{A}_k(r)\text{ if }\gcd(N,n)=1.$$

Consequently, if $f(\tau)$ is an eigenform for $\Gamma_0(N/r)$, then $f(r\tau)$ is an eigenform for $\Gamma_0(N)$ with the same eigenvalues.

Definition 2.3.14. *We call olforms the two types of eigenforms described above and we denote their spanned vector space*

$$\mathcal{S}_k^{\mathrm{old}}(\Gamma_0(N)):=\mathrm{Span}\{\textit{oldforms in }\mathcal{S}_k(\Gamma_0(N))\}.$$

Thanks to the Petersson inner product we can consider the orthogonal complement of $\mathcal{S}_k^{\text{old}}(\Gamma_0(N))$ in $\mathcal{S}_k(\Gamma_0(N))$

$$\mathcal{S}_k^{\text{new}}(\Gamma_0(N)) := \mathcal{S}_k^{\text{old}}(\Gamma_0(N))^{\perp}.$$

Definition 2.3.15. *We call newforms the eigenforms in $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$.*

A deep result by Atkin and Lehner shows that newforms are eigenvector for $\mathrm{T}_k(n)$ for all n. The following result explains why newforms are so important in our discussion.

Proposition 2.3.16. *Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ is an eigenform that is an eigenvector for all $\mathrm{T}_k(n)$, say with $\mathrm{T}_k(n)f = \lambda(n)f$. If the q expansion of f is $f(\tau) = \sum_{n=1}^{+\infty} c_n q^n$, then*

$$c_n = \lambda(n)c_1. \tag{2.5}$$

Consequently

(a) $f \not\equiv 0$ implies $c_1 \neq 0$;

(b) the system of eigenvalues $\{\lambda(n)\}$ determines f up to scalar.

Proof. See [Kna92, Proposition 9.20]. □

Under the assumption of Proposition 2.3.16, we can normalize f so that the q expansion $f(\tau) = \sum_{n=1}^{+\infty} c_n q^n$ has $c_1 = 1$. In particular equation (2.5) says that c_n is the eigenvalue of $\mathrm{T}_k(n)$.

Now we restrict our attention on cusp forms of weight 2 and on the compact Riemann surface $X = X_0(N)$ of genus $g = g(X_0(N))$. Recall that we defined, at the beginning of this section, the Jacobian variety $J_0(N)$ associated to $X_0(N)$: fixed a point $x_0 \in X_0(N)$ (for example one can take $x_0 = \pi(\infty)$, where $\pi : \mathcal{H}^* \to X_0(N)$ is the projection map), this two objects were moreover related by the Abel–Jacobi map

$$\Phi : X_0(N) \longrightarrow J_0(N), \qquad x \mapsto \left(\int_{x_0}^{x} \omega_1, \ldots, \int_{x_0}^{x} \omega_g \right)$$

where $\omega_1, \ldots, \omega_g$ is a $\mathbb{C}$-basis for $\Omega_{\text{hol}}(X_0(N))$. The goal is to associate to each Hecke operator $\mathrm{T}_2(n)$, an element $t_n \in \mathrm{End}(J_0(N))$. To do this, we will use the universal property of the couple $(J_0(N), \Phi)$ and the following proposition.

Proposition 2.3.17. *Let $\omega = \{\omega_i\}_{i \in I}$ be a holomorphic differential on $X_0(N)$, where by definition, each ω_i is defined on the chart (U_i, φ_i). Define the map $f_\omega : \mathcal{H} \to \mathbb{C}$ by*

$$f_\omega(\tau) := \omega_i(\pi(\tau))(\varphi_i \circ \pi)'(\tau), \text{ where } \tau \in U_i.$$

Then the association $\omega \mapsto f_\omega$ defines an isomorphism

$$\Omega_{\text{hol}}(X_0(N)) \cong \mathcal{S}_2(\Gamma_0(N)).$$

Proof. See [Kna92, Proposition 11.6]. □

In order to define an element of $\mathrm{End}(J_0(N))$ from each Hecke operator $\mathrm{T}_2(n)$, we will use the following other operator. As we did for the definition of Hecke operators, write

$$M(n,N) = \coprod_{i=1}^{k} \Gamma_0(N)\alpha_i$$

and define

$$\mathrm{T}(n) : X_0(N) \longrightarrow \mathrm{Div}(X_0(N)), \qquad \pi(\tau) \mapsto \sum_{i=1}^{k} \pi(\alpha_i \tau).$$

One can easily check that $\mathrm{T}(n)$ is well defined, i.e. that, if $\tau = \tau' \in \mathcal{H}^*$ are such that $\pi(\tau) = \pi(\tau')$, then

$$\sum_{i=1}^{k} \pi(\alpha_i \tau) = \sum_{i=1}^{k} \pi(\alpha_i \tau').$$

Now let

$$\Phi^{\#} : \mathrm{Div}(X_0(N)) \longrightarrow J_0(N)$$

be the linear extension of the Abel–Jacobi map Φ to the group of divisors on $X_0(N)$ and consider the composition

$$\mathrm{T}(n)^{\#} := \Phi^{\#} \circ \mathrm{T}(n) : X_0(N) \longrightarrow J_0(N).$$

We want to check that $\mathrm{T}(n)^{\#}$ is holomorphic and to do this we must understand how it acts. Recall that by Proposition 2.3.17, we have an isomorphism $\Omega_{\mathrm{hol}}(X) \cong \mathcal{S}_2(\Gamma_0(N))$. Thus, fixed a basis $\{\omega_1, \ldots, \omega_g\}$, one have that $\{f_1, \ldots, f_g\}$ is a basis of $\mathcal{S}_2(\Gamma_0(N))$ where f_i satisfies

$$\pi^*(\omega_i) = f_i(\tau) d\tau$$

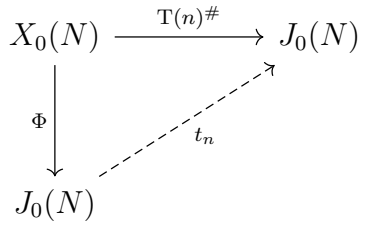
for all i. Hence, if Φ has basis point x_0 and $\tau_0 \in \pi^{-1}(x_0)$, we obtain

$$\begin{aligned} \mathrm{T}(n)^{\#}(\pi(\tau)) = (\Phi^{\#} \circ \mathrm{T}(n))(\pi(\tau)) &= \Phi^{\#}\left(\sum_{i=1}^{k} \pi(\alpha_i \tau)\right) \\ = \sum_{i=1}^{k} (\Phi \circ \pi)(\alpha_i \tau) &= \begin{pmatrix} \sum_i \int_{\tau_0}^{\alpha_i \tau} f_1(\zeta)\, d\zeta \\ \vdots \\ \sum_i \int_{\tau_0}^{\alpha_i \tau} f_g(\zeta)\, d\zeta \end{pmatrix}. \end{aligned}$$

Then $\mathrm{T}(n)^{\#}$ is holomorphic. Actually, $\mathrm{T}(n)^{\#}$ is a morphism of varieties and we will use this fact to apply the universal property of $(J_0(N), \Phi)$ to $\mathrm{T}(n)^{\#}$. This fact follows directly by the following theorem by Chow.

Theorem 2.3.18 (Chow)**.** *Let V_1, V_2 be smooth projective varieties over $\mathbb{C}$ and let $F : V_1 \to V_2$ be a holomorphic map between their underlying complex manifolds. Then F is a rational morphism over $\mathbb{C}$.*

Applying the universal property we obtain a commutative diagram



with $t_n \in \mathrm{End}(J_0(N))$. In particular for all $\tau \in \mathcal{H}^*$, we have the equality

$$\mathrm{T}(n)^{\#}(\pi(\tau)) = t_n(\Phi(\tau)) + \mathrm{T}(n)^{\#}(\pi(\tau_0))$$

that is

$$t_n \begin{pmatrix} \int_{\tau_0}^{\tau} f_1(\zeta)\, d\zeta \\ \vdots \\ \int_{\tau_0}^{\tau} f_g(\zeta)\, d\zeta \end{pmatrix} = \begin{pmatrix} \sum_i \int_{\tau_0}^{\alpha_i \tau} f_1(\zeta)\, d\zeta \\ \vdots \\ \sum_i \int_{\tau_0}^{\alpha_i \tau} f_g(\zeta)\, d\zeta \end{pmatrix}.$$

Moreover, one can calculate the differential dt_n from the previous formula, and one finally obtains the relation between t_n and the Hecke operator $\mathrm{T}_2(n)$:

$$dt_n \begin{pmatrix} f_1(\tau) \\ \vdots \\ f_g(\tau) \end{pmatrix} = \begin{pmatrix} \sum_i f_1 \circ [\![\alpha_i]\!]_2(\tau) \\ \vdots \\ \sum_i f_g \circ [\![\alpha_i]\!]_2(\tau) \end{pmatrix} = \begin{pmatrix} \mathrm{T}_2(n) f_1(\tau) \\ \vdots \\ \mathrm{T}_2(n) f_g(\tau) \end{pmatrix}. \tag{2.6}$$

Another important property of the endomorphisms t_n is the following.

Proposition 2.3.19. *The element $t_n \in \mathrm{End}(J_0(N))$ is defined over $\mathbb{Q}$ for all ≥ 1.*

Proof. See [Kna92, Lemma 11.76]. □

Another ingredient for the main statement of the Eichler–Schimura theory is the map

$$\mu : \mathcal{S}_2(\Gamma_0(N)) \longrightarrow \Omega_{\mathrm{hol}}(J_0(N))$$

defined as follows. We can use $z_1, \ldots, z_g$ as cordinates on $J_0(N)$ and the space $\Omega_{\mathrm{hol}}(J_0(N))$ is the $\mathbb{C}$-linear span of $dz_1, \ldots, dz_g$. Moreover, if $e_1, \ldots, e_g$ is the standard basis for the tangent space of $J_0(N)$ in O, then we have the natural pairing

$$\langle dz_i, e_j \rangle = \delta_{ij}.$$

Consider now

$$\tilde{\Phi} = \Phi \circ \pi : \mathcal{H}^* \longrightarrow J_0(N)$$

and let us check that for all $j = 1, \ldots, g$

$$\tilde{\Phi}^*(dz_j) = f_j(\tau) d\tau \tag{2.7}$$

where $\tilde{\Phi}^* : \Omega_{\text{hol}}(J_0(N)) \to \Omega_{\text{hol}}(\mathcal{H}^*)$ denotes the induced maps at the level of holomorphic differntials. In fact, at any point τ_1,

$$\tilde{\Phi}(\tau_1) = \begin{pmatrix} \int_{\tau_0}^{\tau_1} f_1(\zeta)d\zeta \\ \vdots \\ \int_{\tau_0}^{\tau_1} f_g(\zeta)d\zeta \end{pmatrix}$$

and the natural pairing gives

$$\langle \tilde{\Phi}^*(dz_j), \frac{d}{d\tau}\big|_{\tau_1} \rangle = \langle dz_j, d\tilde{\Phi}\left(\frac{d}{d\tau}\big|_{\tau_1}\right) \rangle = \langle dz_j, \begin{pmatrix} f_1(\tau_1) \\ \vdots \\ f_g(\tau_1) \end{pmatrix} \rangle = f_j(\tau_1).$$

Since by definition $\langle d\tau, \frac{d}{d\tau}\big|_{\tau_1} \rangle = 1$, we obtain (2.7). Since $\tilde{\Phi}^*$ maps basis to basis, we conclude that it is a vector space isomorphism. Therefore it makes sense to define

$$\mu : \mathcal{S}_2(\Gamma_0(N)) \longrightarrow \Omega_{\text{hol}}(J_0(N))$$

given by

$$\mu(f) := (\tilde{\Phi}^*)^{-1}(f(\tau)d\tau).$$

We now state the Shimura–Taniyama formula, that will help us in the proof of the Eichler–Shimura Theorem. Let f be an element in $\text{End}(J_0(N))$ and consider the endomorphism δf of $\Omega_{\text{hol}}(J_0(N))$ defined by

$$\langle (\delta f)u, v \rangle := \langle u, (df)_O v \rangle \text{ for } u \in \Omega_{\text{hol}}(J_0(N)) \text{ and } v \in \mathrm{T}_O(J_0(N)).$$

Here, $\mathrm{T}_O(J_0(N))$ denotes the tangent space of $J_0(N)$ at O and $(df)_O : \mathrm{T}_O(J_0(N)) \to \mathrm{T}_O(J_0(N))$ is the map induced at the level of tangent spaces.

Proposition 2.3.20 (Shimura–Taniyama)**.** *For f in $\mathcal{S}_2(\Gamma_0(N))$,*

$$(\delta t_n)(\mu(f)) = \mu(\mathrm{T}_2(n)f).$$

Proof. See [Kna92, Lemma 11.73]. □

2.3.2 The main theorem

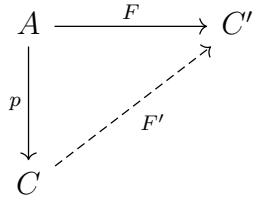
Now we are ready to state and prove the main theorem of Eichler–Shimura theory that gives for each newform $f \in \mathcal{S}_2^{\text{new}}(\Gamma_0(N))$, an elliptic curve constructed as a quotient of the Jacobian variety of $X_0(N)$, but first we have to explain exactly how we can consider the quotient of an abelian variety. Let A be an abelian variety and let B be an abelian subvariety of A, i.e. a subvariety that is an abelian group with the same group law of A. In this case the inclusion map $i : B \to A$ is a morphism. One can prove that if $F : A \to A'$ is a morphism of abelian varieties, then $\text{Ker}(F)$ is abelian subvariety of A and $\text{Im}(F)$ is an abelian subvariety of A'. Further, if A, A' and F are defined over $\mathbb{Q}$, then $\text{Ker}(F)$ and $\text{Im}(F)$ can be defined over $\mathbb{Q}$. The following proposition explains how we can define the quotient A/B as an abelian variety.

Proposition 2.3.21. *Let A be an abelian variety and let B be an abelian subvariety of A. Then there exists a pair (C, p) such that*

i) C is an abelian variety;

ii) $p : A \to C$ is a surjective morphism of abelian varieties with $\mathrm{Ker}(p) = B$;

iii) (C, p) satisfies the following universal property: for each morphism of abelian varieties $F : A \to C'$ with $B \subseteq \mathrm{Ker}(F)$, there exists a morphism of abelian varieties $F' : C \to C'$ such that the diagram



is commutative.

Moreover, if A, B, p are defined over $\mathbb{Q}$, then C can be defined over $\mathbb{Q}$ and in the universal property, if C' and F are defined over $\mathbb{Q}$, then the map F' is defined over $\mathbb{Q}$.

Proof. See [Pol03, Section 9.5]. □

Then, given an abelian variety A and an abelian subvariety B, we define the quotient A/B to be the abelian variety C of the theorem, with projection map $p\colon A \to A/B$.

Theorem 2.3.22. *Let $f(\tau) = \sum_{n=1}^{\infty} c_n e^{2\pi i n \tau}$ be a newform in $\mathcal{S}_2(\Gamma_0(N))$ normalized to have $c_1 = 1$ and suppose that all c_n are in $\mathbb{Z}$. Let $\Phi : X_0(N) \to J_0(N)$ be the Abel–Jacobi map with base point $x_0 \in X_0(N)$ and let $\tau_0 \in \mathcal{H}^*$ such that $\pi(\tau_0) = x_0$. Then there exists a pair (E, ν) such that*

i) E is an elliptic curve defined over $\mathbb{Q}$ and $\nu : J_0(N) \to E$ is a surjective morphism defined over $\mathbb{Q}$;

ii) the abelian subvariety $A := \mathrm{Ker}(\nu)$ of $J_0(N)$ is stable under the action of each $t_n \in \mathrm{End}(J_0(N))$ and the action of t_n on E corresponds to the multiplication by c_n for all $n \geq 1$;

iii) the properties i), ii) characterize the pair (E, ν) up to isomorphism over $\mathbb{Q}$;

iv) $\mu(f)$ is a non zero multiple of $\nu^*(\omega)$, where ω is the invariant differential of E

v) if

$$\Lambda_f = \left\{ \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta) d\zeta : \gamma \in \Gamma_(N) \right\},$$

then Λ_f is a lattice of $\mathbb{C}$ and E is isomorphic over $\mathbb{C}$ to $\mathbb{C}/\Lambda_f$.

In the course of proving Theorem 2.3.22 we will make crucial use of the following result by Wedderburn.

Lemma 2.3.23 (Wedderburn)**.** *Let $\mathbb{T}$ be a finite-dimensional associative and commutative algebra with identity defined over a field K and let $R = \mathrm{Nil}(\mathbb{T}) = \sqrt{(0)}$ be its nilradical. Then there exists $K_1, \ldots, K_r$ finite algebraic extensions of K such that*

$$\mathbb{T} = R \oplus K_1 \oplus \cdots \oplus K_r$$

as vector spaces.

Proof of Theorem 2.3.22. We want to give only a sketch of the proof of Theorem 2.3.22.

Let $\mathrm{End}_{\mathbb{Q}}(J_0(N)) := \mathrm{End}(J_0(N)) \otimes_{\mathbb{Z}} \mathbb{Q}$ and let $\mathbb{T}_{\mathbb{Q}}$ be the $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ generated by the set $\{t_n : n \geq 1\}$. We want to apply Lemma 2.3.23 to $\mathbb{T}_{\mathbb{Q}}$. Note that the members of $\mathrm{End}(J_0(N))$ are holomorphic and their differentials are consequently $\mathbb{C}$-linear maps from the tangent space (for example in the origin O) $\mathrm{T}_O(J_0(N)) \cong \mathbb{C}^g$ into itself. In this way we get an injective ring homomorphism of $\mathrm{End}(J_0(N))$ into the algebra of all g-by-g complex matrices $\mathrm{End}(J_0(N)) \to M_g(\mathbb{C})$. Since $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, we obtain

$$\mathrm{End}(J_0(N)) \hookrightarrow M_g(\mathbb{C}) \quad \text{given by } f \mapsto (df)_O.$$

By (2.6), dt_n corresponds to the matrix of $\mathrm{T}_2(n)$, then by Proposition 2.3.10, $\mathbb{T}_{\mathbb{Q}}$ is commutative and by proposition 2.3.19 this homomorphism restricts to

$$\mathbb{T}_{\mathbb{Q}} \longrightarrow M_g(\mathbb{Q}).$$

In conclusion, $\mathbb{T}_{\mathbb{Q}}$ is a commutative $\mathbb{Q}$-subalgebra of $M_g(\mathbb{Q})$. Applying Wedderburn's Lemma to the algebra $\mathbb{T}_{\mathbb{Q}}$ defined over $\mathbb{Q}$, we obtain a decomposition

$$\mathbb{T}_{\mathbb{Q}} = R \oplus (K_1 \oplus \cdots \oplus K_r)$$

where R is the nilradical of $\mathbb{T}_{\mathbb{Q}}$ and the K_i's are finite extensions of $\mathbb{Q}$. Thanks to the Shimura–Taniyama formula

$$\delta t_n(\mu(f)) = \mu(\mathrm{T}_2(n)f) = \mu(c_n f) = c_n \mu(f)$$

we have a well defined homomorphism

$$\rho : \mathbb{T}_{\mathbb{Q}} \longrightarrow \mathbb{Q}, \qquad t_n \mapsto c_n.$$

Note that if $t \in R$, then there exists $r \geq 1$ such that $t^r = 0$, hence

$$\rho(t)^r = \rho(t^r) = \rho(0) = 0 \in \mathbb{Q}.$$

In other words, $\rho(R) = 0$ and ρ acts only on the K_i's. Since the unit $\mathbb{1} \in \mathbb{T}_{\mathbb{Q}} \setminus R$, we can write

$$\mathbb{1} = e_1 + \cdots + e_r,$$

with e_i the unit of K_i for all $i = 1, \dots, r$. Applying ρ, we obtain

$$1 = \rho(\mathbb{1}) = \rho(e_1) + \cdots + \rho(e_r).$$

Without any loss of generality we can suppose that $\rho(e_1) = 1$ and $\rho(e_i) = 0$ for $i > 1$, that is $\rho(K_1) = \mathbb{Q}$. Finally, we define the ideal

$$U := R \oplus (K_2 \oplus \cdots \oplus K_r)$$

and

$$A := \sum_{\alpha \in U \cap \mathrm{End}(J_0(N))} \alpha(J_0(N)).$$

The latter will be in particular, the abelian subvariety of $J_0(N)$ that we will use to construct the elliptic curve E; more precisely, E will be the quotient $J_0(N)/A$, and ν will denote the projection map. We now show the main step of the proof.

(a) First one has to check that A is an abelian subvariety of $J_0(N)$ defined over $\mathbb{Q}$. If $\alpha \in U \cap \mathrm{End}(J_0(N))$, then we know that $\alpha(J_0(N)) = \mathrm{Im}(\alpha)$ is a subvariety of $J_0(N)$. Moreover, if B and B' are abelian subvarieties of $J_0(N)$, then we can see their sum as the image of the composition

$$B \times B' \hookrightarrow J_0(N) \times J_0(N) \xrightarrow{+} J_0(N), \quad (b, b') \mapsto b + b'.$$

In other words, A is an abelian subvarieties of $J_0(N)$. Moreover α, up to multiplication by an integer, is a polynomial in the t_n's and so it is defined over $\mathbb{Q}$ by Proposition 2.3.19. Then $\alpha(J_0(N))$ is an abelian subvariety defined over $\mathbb{Q}$ then so it is A.

(b) One defines $E := J_0(N)/A$.

(c) The fact that $A = \mathrm{Ker}(\nu)$ is stable under the action of the t_n's follows by the definition of A and by the fact that U is an ideal of $\mathbb{T}_{\mathbb{Q}}$.

(d) To study the action of the t_n's on E one applies the universal property of (E, ν) that we saw in Proposition 2.3.21 to the map $\nu \circ t_n$ and obtains the following commutative diagram

$$\begin{array}{ccc} J_0(N) & \xrightarrow{\quad\nu\quad} & E \\ {\scriptstyle t_n}\downarrow & & \downarrow{\scriptstyle \overline{t_n}} \\ J_0(N) & \xrightarrow[\quad\nu\quad]{} & E. \end{array} \tag{2.8}$$

Let $\rho' : \mathbb{Q} \to K_1$ be the inverse of ρ. Then, denoting by $[c_n]$ the multiplication by c_n,

$$t_n - [c_n] = t_n - \rho'(c_n) - ([c_n] - \rho'(c_n)) \in U \cap \mathrm{End}(J_0(N)).$$

In particular, in the quotient E, $\overline{t_n} = [c_n]$ and $ii)$ follows.

(e) Then one sees that $\dim(E) > 0$. To do this, one can prove equivalently that $A \neq J_0(N)$, showing a nontrivial element $\beta \in \mathrm{End}(J_0(N))$ that annihilates A.

(f) Then one shows that $\dim(E) = 1$ and $\mu(f) = k\nu^*(\omega)$ with $k \neq 0$. By the previous paragraph, we can find a nonzero member $\omega' \in \Omega_{\mathrm{hol}}(E)$. Let ν^* be the pullback mapping

$$\nu^* : \Omega_{\mathrm{hol}}(E) \longrightarrow \Omega_{\mathrm{hol}}(J_0(N))$$

induced by ν. Applying $(\cdot)^*$ to the commutative square (2.8) we have

$$\nu^* \circ \delta\overline{t_n} = \delta t_n \circ \nu^*$$

and since $\overline{t_n} = [c_n]$ implies $\delta\overline{t_n} = c_n \cdot (\cdot)$, we obatain

$$\delta t_n(\nu^*(\omega')) = c_n\nu^*(\omega').$$

If we define $f' = \mu^{-1}(\nu^*(\omega'))$, then $\mu(f') = \nu^*(\omega')$ and Shimura–Taniyama formula gives

$$\mu(\mathrm{T}_2(n)f') = \delta t_n(\mu(f')) = \delta t_n(\nu^*(\omega')) = c_n\nu^*(\omega') = c_n\mu(f')$$

that is

$$\mathrm{T}_2(n)f' = c_n f'.$$

If one suppose that $\dim(E) > 1$ then one can find ω', ω'' linearly independent. If we set $f'' = \mu^{-1}(\nu^*(\omega''))$, then f' and f'' are linearly independent and this is a contradiction since by the above argument

$$\mathrm{T}_2(n)f'' = c_n f''$$

for each n and two eigenforms with the same eigenvalues differ by the multiplication by a scalar (this is a direct consequence of Proposition 2.3.16). Moreover, if we put $\omega' = \omega$ the invariant differential, since $\mathrm{T}_2(n)f = c_n f$, one has that f and f' are linearly dependent and then, up to a scalar, $\mu(f) = \nu^*(\omega)$. Then we have *i*) and *iv*).

(g) To see that the pair (E, ν) is unique up to isomorphism let A', $(E' = J_0(N)/A', \nu')$ satisfying *i*) and *ii*) and let ω', ω be the invariant differential of E', E respectively. Then by the previous paragraph $\nu^*(\omega') = h\nu^*(\omega)$ for some $h \neq 0$. In particular they annihilate the same elements of the tangent space at O of A and A' respectively. Using Lie theory one shows that this implies that $A = A'$ and so by Proposition 2.3.21 $(E, \nu) \cong (E', \nu')$. Then we have *iii*)

(h) One now proves that Λ_f is a lattice in $\mathbb{C}$. Let $\mu(f)$ act on the tangent space $\mathrm{T}_O(J_0(N))$ via the identification $\Omega_{\mathrm{hol}}(J_0(N)) \cong \mathrm{T}_O(J_0(N))^\vee$. We know that if

$\{c_1, \ldots, c_{2g}\}$ is a basis of $H_1(X_0(N), \mathbb{Z})$, then the lattice $\Lambda(X_0(N))$ is generated on $\mathbb{R}$ by $\{u_1, \ldots, u_{2g}\}$ where

$$u_k = \begin{pmatrix} \int_{c_k} f_1(\zeta)d\zeta \\ \vdots \\ \int_{c_k} f_g(\zeta)d\zeta \end{pmatrix}, \text{ for } k = 1, dots, 2g.$$

One can prove that

$$\mu(f)(\Lambda(X_0(N))) = \sum_k \mathbb{Z} \int_{c_k} f(\zeta)d\zeta = \Lambda_f.$$

Doing the calculation and with some consideration of Lie theory, from the previous identity one proves that Λ_f is a lattice.

(i) Finally, the isomorphism $E \cong \mathbb{C}/\Lambda_f$ follows applying the universal property of (E, ν).

□

Before the ending of this section we briefly indroduce the concept of L-function associated to a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$. First of all we define the Atkin–Lehner involution w_N.

Definition 2.3.24. *Let $f \in \mathcal{M}_k(\Gamma_0(N))$. We define*

$$w_N(f) := f \circ [\![\alpha_N]\!]_k$$

where $\alpha_N := \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$.

It follows immediately by the definition of the matrix α_N that ω_N is an involution, provided that one checks that is well defined. For this purpose we have the following proposition.

Proposition 2.3.25. *The Atkin–Lehner involution w_N carries $\mathcal{M}_k(\Gamma_0(N))$ to itself ans $\mathcal{S}_k(\Gamma_0(N))$ to itself.*

Proof. See [Kna92, Proposition 9.7]. □

In particular from the previous proposition and by the fact that w_N is an involution, the two spaces $\mathcal{M}_k(\Gamma_0(N))$ and $\mathcal{S}_k(\Gamma_0(N))$ split as the sum of the eigenspaces for eigenvalues $+1$ and -1. For example for the cusp form we obtain the decomposition

$$\mathcal{S}_k(\Gamma_0(N)) = \mathcal{S}_k(\Gamma_0(N))^+ \oplus \mathcal{S}_k(\Gamma_0(N))^-$$

where

$$\mathcal{S}_k(\Gamma_0(N))^\epsilon = \{f \in \mathcal{S}_k(\Gamma_0(N)) : w_N(f) = \epsilon f\}$$

with $\epsilon \in \{\pm 1\}$.

We now define the L-function attached to a cusp form f and analyze its region of convergence.

Definition 2.3.26. *Let $f \in \mathcal{S}_k(\Gamma_0(N))$ be a cusp form and let $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ be its q-expansion at the cusp ∞. The L-function of f is the Dirichlet series*

$$L(s, f) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

The convergence is established in a theorem of Hecke.

Theorem 2.3.27 (Hecke)**.** *Let $f \in \mathcal{S}_k(\Gamma_0(N))$ be a cusp form in one of the eigenspaces $\mathcal{S}_k(\Gamma_0(N))^\epsilon$ of w_N, where $\epsilon = \pm 1$. Then $L(s, f)$ is initially defined for $\mathrm{Re}(s) > \frac{k}{2} + 1$ and extends to be entire in s. Moreover, the function*

$$\Lambda(s, f) = N^{\frac{s}{2}} (s\pi)^{-s} \Gamma(s) L(s, f)$$

satisfies the functional equation

$$\Lambda(s, f) = \epsilon(-1)^{\frac{k}{2}} \Lambda(k - s, f).$$

Proof. See [Kna92, Theorem 9.8]. □

Composing the Abel–Jacobi map with the morphism ν of Theorem 2.3.22, we obtain a map defined over $\mathbb{Q}$

$$\psi := \nu \circ \Phi : X_0(N) \xrightarrow{\Phi} J_0(N) \xrightarrow{\nu} E$$

that we will call modular parametrization of the elliptic curve E. From a theorem of Wiles we can deduce that the viceversa also holds over $\mathbb{Q}$.

Theorem 2.3.28. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then, there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N))$ such that:*

$$L(E, s) = L(E, f).$$

Furthermore, from results on the Tate's conjecture for abelian varieties proved by Faltings, it can be deduced that E is isogenous to the elliptic curve E_f obtained via the Eichler–Shimura construction.

Theorem 2.3.28 involves deep arithmetic invariants, specifically the conductor and the L-function of an elliptic curve. While a full treatment of these topics is beyond our current scope, we provide brief definitions to clarify the statement:

- The conductor N of an elliptic curve $E/\mathbb{Q}$ is a positive integer that encodes the "bad reduction" of the curve. Specifically, $p|N$ if and only if E has singular reduction at p.
- The L-function of E is defined via an Euler product $L(E, s) = \prod_p L_p(E, s)^{-1}$, where the local factors L_p depend on the number of points of E modulo p. For $p \nmid N$, $L_p(E, s) = 1 - a_p p^{-s} + p^{1-2s}$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

The equality $L(E, s) = L(f, s)$ is the bridge to the geometry. By the Faltings' Isogeny Theorem (formerly Tate's Conjecture), if two abelian varieties (like E and the E_f constructed via Eichler–Shimura) have the same L-function, they are isogenous over $\mathbb{Q}$.

2.4 Galois cohomology

The arithmetic of an elliptic curve E over a field K is fundamentally governed by the action of the absolute Galois group G_K on its points. In this section, we introduce the language of Galois cohomology as the formal tool to study the invariants of this action and to measure the obstruction to the existence of K-rational points.

To begin with let G be a profinite group, i.e. a topological group that is Hausdorff, compact and totally disconnected and let A be a left discrete G-module. This means that A is an abelian group together with an action of G

$$G \times A \longrightarrow A \qquad (\sigma, a) \mapsto \sigma \cdot a = a^{\sigma}$$

that is continuous if A is endowed with discrete topology.

Definition 2.4.1. *We define*

$$H^0(G, A) := A^G := \{a \in A : \sigma(a) = a \text{ for all } \sigma \in G\}$$

the so called G-invariants of A.

For an example, let K be a number field (for example an imaginary quadratic field) and consider the absolute Galois group

$$G := G_K = \mathrm{Gal}(\overline{K}/K).$$

Recall that for an elliptic curve E defined over K, G_K acts on its points via its action on their coordinates. In this case, we have:

$$H^0(G_K, E(\overline{K})) = E(K)$$

by the definition of K-rational points on E.

Consider now a short exact sequence of left G-module

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

Then it is induced another exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G. \tag{2.9}$$

Unlikely the homomorphism $B^G \longrightarrow C^G$ is in general not surjective. In other words the functor

$$A \mapsto A^G$$

is covariant, left-exact but in general it is not right-exact.

Proposition 2.4.2. *There exists a collection of functors $\{H^i(G, -)\}_{i \geq 0}$ such that for every short exact sequence of G-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

the exact sequence 2.9 extends to a long exact sequence of abelian groups

$$0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \longrightarrow H^1(G, A) \longrightarrow \dots$$

Proof. See [Sha72, Chapter 2] □

Definition 2.4.3. *The abelian group $H^i(G, A)$ is the i-th cohomology of G with coefficients in A.*

One way to define the groups $H^i(G, A)$ is to introduce the notions of *i-cocycles* and *i-coboundaries* and to set

$$H^i(G, A) = \frac{\{i\text{-cocycles}\}}{\{i\text{-coboundaries}\}}.$$

In what follows, we will only need the case $i = 0$ and $i = 1$. For $i = 0$ we already have an explicit definition of $H^0(G, A)$, whereas in the case $i = 1$ we can proceed with the following construction. A 1-cocycle (from G to A) is a continuous function $\eta : G \longrightarrow A$ such that

$$\eta(g_1 g_2) = \eta(g_1) + g_1 \cdot \eta(g_2)$$

for all $g_1, g_2 \in G$. A 1-coboundary (from G to A) is a continuous function

$$G \longrightarrow A, \qquad g \mapsto g \cdot a - a$$

for some $a \in A$. In what follows we will denote a 1-coboundary with respect to an element $a \in A$ with χ_a. It is easy to see that

$$\{1\text{-coboundaries}\} \subseteq \{1\text{-cocylcles}\}$$

and so we can consider the quotient $H^1(G, A)$.

Remark 2.4.4. *Note that if G acts trivially on A, then*

$$H^1(G, A) = \frac{\{\textit{continuous homomorphism } G \to A\}}{\{1\}} = \mathrm{Hom}_{\mathrm{cont}}(G, A).$$

Consider now a closed subgroup $H \subseteq G$ and take a left discrete G-module A. Since we can view A as an H-module, it is induced an homomorphism

$$\mathrm{res} := \mathrm{res}_i : H^i(G, A) \longrightarrow H^i(H, A)$$

called the restriction homomorphism. In particular, if $i = 0$

$$A^G \hookrightarrow A^H$$

is simply the inclusion. On the other hand, when $i = 1$, res is induced at the level of 1-cocycles from the restriction

$$(\eta : G \to A) \longmapsto (\eta|_H : H \to A).$$

In particular we can apply this construction to the special case of a local field whose Galois group acts on the points of an elliptic curve. In this sense, let E be elliptic curve over K, fix a place (finite or infinite) v of K and denote by K_v the completion

of K at v. The injective homomorphism $G_{K_v} \hookrightarrow G_K$ given by $\sigma \mapsto \sigma|_{\overline{K}}$ induces the composition res_v:

$$H^1(G_K, E(\overline{K})) \xrightarrow{\text{res}} H^1(G_{K_v}, E(\overline{K})) \longrightarrow H^1(G_{K_v}, E(\overline{K_v}))$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \searrow \quad \nearrow$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathrm{res}_v$$

where the second map is induced by the inclusion $E(\overline{K}) \hookrightarrow E(\overline{K_v})$ for a fixed embedding $\overline{K} \subseteq \overline{K_v}$.

The restriction map $\mathrm{res} = \mathrm{res}_1 : H^1(G, A) \to H^1(G, H)$ is moreover involved in a short exact sequence of groups called the "inflation–restriction" sequence. Since $H \subseteq G$ is a normal and closed subgroup of G, the quotient G/H is still a profinite group and A^H is a G/H-module. On the other hand, a 1-cocycle $f : G/H \to A^H$ induces another 1-cocycles $G \to A$ via the composition

$$G \twoheadrightarrow G/H \xrightarrow{f} A^H \hookrightarrow A.$$

In other words we obtain a map called "inflation" defined by

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

Proposition 2.4.5. *The sequence of groups*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A),$$

is exact; it is called the inflation–restriction sequence.

Proof. From the definitions, it is clear that $\mathrm{res} \circ \mathrm{inf} = 0$.

First, we prove the injectivity of inf. Let $\xi : G/H \to A^H$ be a 1-cocycle such that $\mathrm{inf}([\xi]) = 0$. This means there exists an $a \in A$ such that $\xi(\sigma) = \sigma \cdot a - a$ for all $\sigma \in G$. Since ξ depends only on the class of σ modulo H, for any $\tau \in H$ we have:

$$\tau \cdot a - a = \xi(\tau) = \xi(1) = 0$$

where we used the fact that τ and 1 represent the same class in G/H. Thus $\tau \cdot a = a$ for all $\tau \in H$, which implies $a \in A^H$. It follows that ξ is a coboundary and so $[\xi] = 0$ in $H^1(G/H, A^H)$.

Next, we show that $\ker(\mathrm{res}) \subseteq \mathrm{Im}(\mathrm{inf})$. Let $\eta : G \to A$ be a 1-cocycle such that $[\eta|_H] = 0$ in $H^1(H, A)$. This means there exists an $a \in A$ such that $\eta(\tau) = \tau \cdot a - a$ for all $\tau \in H$. By subtracting the coboundary $\sigma \mapsto \sigma \cdot a - a$ from η, we may assume that $\eta(\tau) = 0$ for all $\tau \in H$.

Under this assumption, the cocycle condition yields $\eta(\sigma\tau) = \eta(\sigma) + \sigma \cdot \eta(\tau) = \eta(\sigma)$ for all $\sigma \in G$ and $\tau \in H$. Thus η is constant on the right cosets of H, inducing a

well-defined map $\overline{\eta} : G/H \to A$. Finally, since H is normal in G, for every $\tau \in H$ and $\sigma \in G$ there exists $\tau' \in H$ such that $\tau\sigma = \sigma\tau'$. Then:

$$\begin{aligned}\tau \cdot \overline{\eta}(\bar{\sigma}) &= \tau \cdot \eta(\sigma) \\ &= \eta(\tau) + \tau \cdot \eta(\sigma) \\ &= \eta(\tau\sigma) = \eta(\sigma\tau') \\ &= \eta(\sigma) + \sigma \cdot \eta(\tau') \\ &= \eta(\sigma) = \overline{\eta}(\bar{\sigma}).\end{aligned}$$

This shows that the image of $\overline{\eta}$ lies in A^H. Therefore, $\overline{\eta}$ defines a class in $H^1(G/H, A^H)$ such that $\inf([\overline{\eta}]) = [\eta]$, proving the exactness at $H^1(G, A)$. □

Finally, in Section 2.4.2 we will give an idea of how to extend this sequence, obtaining the so-called Hochschild–Serre exact sequence.

2.4.1 The Selmer group and the Shafaverich-Tate group

Let $\varphi : E \to E'$ be a nonconstant isogeny of elliptic curves defined over a number field K and consider the induced exact sequence

$$0 \longrightarrow E[\varphi] \longrightarrow E \xrightarrow{\varphi} E' \longrightarrow 0,$$

where $E[\varphi]$ dentotes the kernel of φ. Taking the Galois cohomology, we obtain the long exact sequence

$$0 \to E(K)[\varphi] \to E(K) \xrightarrow{\varphi} E'(K) \xrightarrow{\delta} H^1(G_K, E[\varphi]) \xrightarrow{\iota} H^1(G_K, E) \xrightarrow{\varphi} H^1(G_K, E'), \tag{2.10}$$

where we are writing E and E' meaning $E(\overline{K})$ and $E'(\overline{K})$. From this we can form the following short exact sequence

$$0 \longrightarrow E'(K)/\varphi(E(K)) \xrightarrow{\kappa} H^1(G_K, E[\varphi]) \longrightarrow H^1(G_K, E)[\varphi] \longrightarrow 0. \tag{2.11}$$

Definition 2.4.6. *The sequence above is called Kummer sequence and the homomorphism κ is called Kummer map.*

Remark 2.4.7. *Before we continue, we want to study κ. The Kummer map is induced from the long exact sequence 2.10 in the following way:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\iota) & \longrightarrow & H^1(G_K, E[\varphi]) & \xrightarrow{\iota} & \mathrm{Im}(\iota) & \longrightarrow & 0 \\ & & \| & & & \nearrow_{\kappa} & & & \\ & & \mathrm{Im}(\delta) & & & & & & \\ & & \wr\| & & & & & & \\ & & \dfrac{E'(K)}{\mathrm{Ker}(\delta)} & & & & & & \\ & & \| & & & & & & \\ & & \dfrac{E'(K)}{\varphi(E(K))} & & & & & & \end{array}$$

Hence, in order to see the image of a class $[P] \in E'(K)/\varphi(E(K))$ we have to compute

$$\delta(P) \in H^1(G_K, E[\varphi]).$$

Note that $\delta(P)$ has the following explicit description. Since φ is surjective by Proposition 1.1.5, we can find a point $Q \in E(\overline{K})$ such that

$$P = \varphi(Q)$$

and we define

$$\delta(P)(\sigma) = \sigma \cdot Q - Q.$$

for all $\sigma \in G_K$. Since P is K-rational and φ is defined over K

$$\begin{aligned}\varphi(\delta(P)(\sigma)) &= \varphi(\sigma \cdot Q - Q) = \varphi(\sigma \cdot Q) - \varphi(Q) \\ &= \sigma \cdot P - P = P - P = 0\end{aligned}$$

and so $\delta(P)$ is a map from G_K to $E(K)[\varphi]$. In other words for all $[P] \in E(K)/\varphi(E(K))$, $\delta(P) = \chi_Q$ for some $Q \in E(\overline{K})$ such that $\varphi(Q) = P$.

Now we want to locally recreate an analogous of 2.11. For each place v of K, denoting with K_v the completion of K at v, we obtain with the same argument above an exact sequence

$$0 \longrightarrow E'(K_v)/\varphi(E(K_v)) \xrightarrow{\kappa_v} H^1(G_{K_v}, E[\varphi]) \longrightarrow H^1(G_{K_v}, E)[\varphi] \longrightarrow 0.$$

Summing up, we have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\varphi(E(K)) & \xrightarrow{\kappa} & H^1(G_K, E[\varphi]) & \longrightarrow & H^1(G_K, E)[\varphi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E'(K_v)/\varphi(E(K_v)) & \longrightarrow & \prod_v H^1(G_{K_v}, E[\varphi]) & \longrightarrow & \prod_v H^1(G_{K_v}, E)[\varphi] & \longrightarrow & 0 \end{array} \tag{2.12}$$

where the product is over all finite and infinite place of K.

Definition 2.4.8. *With notation above we give the following definitions.*

(a) The φ-Selmer group $\mathrm{Sel}(E/K)[\varphi]$ is the subgroup of $H^1(G_K, E[\varphi])$ defined as the kernel of the map $H^1(G_K, E[\varphi]) \to \prod_v H^1(G_{K_v}, E)[\varphi]$ in the diagram 2.12.

(b) The Shafarevic–Tate group of E/K, detoted by $Ш(E/K)$, is the subgroup of of $H^1(G_K, E)$ defined as the kernel of

$$\prod_v \mathrm{res}_v : H^1(G_K, E) \longrightarrow H^1(G_{K_v}, E)$$

where v ranges over all finite and infinite places of K.

Lemma 2.4.9. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of abelian groups. Then

$$0 \to A \xrightarrow{f} \mathrm{Ker}(g' \circ \beta) \xrightarrow{g|_{\mathrm{Ker}}} \mathrm{Ker}(\gamma) \to 0$$

is a short exact sequence.

Proof. Immediate from the definition of exactness and from the commutativity of the diagram. □

By applying Lemma 2.4.9, we obtain the exact sequence

$$0 \to E'(K)/\varphi(E(K)) \xrightarrow{\kappa} \mathrm{Sel}(E/K)[\varphi] \to Ш(E/K)[\varphi] \to 0, \tag{2.13}$$

which will be a key tool in the following sections. For example, it allows us to understand the meaning of the Shafarevic–Tate group. By definition

$$\mathrm{Sel}(E/K)[\varphi] = \bigcap_v \mathrm{Ker}\big(H^1(G_K, E[\varphi]) \xrightarrow{f_v} H^1(G_{K_v}, E[\varphi]) \xrightarrow{g_v} H^1(G_{K_v}, E)[\varphi]\big)$$

and if we take $[\eta : G_K \to E(\overline{K})[\varphi]] \in H^1(G_K, E[\varphi])$, then

$$[\eta_v] := (g_v \circ f_v)([\eta]) = [i_v \circ \eta \circ \mathrm{res}_v]$$

where $i_v : E(\overline{K})[\varphi] \hookrightarrow E(\overline{K_v})$ is the inclusion and $\mathrm{res}_v : G_{K_v} \hookrightarrow G_K$ is the restriction map. Thus, being in the Selmer group means that

$$[\eta_v] = [0] \qquad \text{for all place } v.$$

In other words a class $\eta \in H^1(G_K, E[\varphi])$ is in $\mathrm{Sel}(E/K)[\varphi]$ if for all v there exists a point $P_v \in E(\overline{K_v})$ such that

$$\eta_v = \chi_{P_v},$$

that is, it comes from a point in each of its localizations. Clearly, if a class comes from a global point $P \in E(\overline{K})$, then it comes from a point in each of its local version. In particular, this explains the inclusion

$$\frac{E'(K)}{\varphi(E(K))} \xhookrightarrow{\kappa} \mathrm{Sel}(E/K)[\varphi]$$

and allow us to view the left quotient as the subgroup of $\mathrm{Sel}(E/K)[\varphi]$ made of the classes of the form $[\chi_Q]$, for some $Q \in E(\overline{K})$ (note that $[\chi_Q]$ in this case is not always the zero class, since it is so only when Q lies in $\mathrm{Ker}(\varphi)$). Finally, thanks to the short exact sequence (2.13) we can interpret the Shafarevic–Tate group as the group of cohomology classes that come from points locally but not globally.

2.4.2 Spectral sequences

As announced earlier, this section aims to extend the inflation–restriction exact sequence

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

To this end, spectral sequences will play a crucial role, and we will now proceed to define them.

Definition 2.4.10. *Let R be a ring. A spectral sequence $\mathbb{E}$ consists of the following data:*

- *a family $\{E_r^{p,q}\}_{(p,q)\in\mathbb{Z}^2, r\in\mathbb{Z}_+}$ of R-modules;*
- *for each $r \in \mathbb{Z}_+$ and for each $(p,q) \in \mathbb{Z}^2$, a map of R-modules*

$$d_r^{p,q} : E_r^{p,q} \longrightarrow E_r^{p+r,q-r+1}$$

such that

  - $d_r^{p,q} \circ d_r^{p+r,q-r+1} = 0$;
  - $E_{r+1}^{p,q} = \mathrm{Ker}(d_r^{p,q})/\mathrm{Im}(d_r^{p-r,q+r-1})$.

It is useful to imagine the spectral sequence $\mathbb{E}$ as a "book" whose r-th page contains the family $\{E_r^{p,q}\}_{(p,q)}$ seen as a lattice, with homomorphisms $\{d_r^{p,q}\}_{(p,q)}$.

Definition 2.4.11. *Let $\mathbb{E}$ be a spectral sequence of R-modules and let $\{E^n\}_{n\in\mathbb{Z}}$ be a family of R-modules. We say that $\mathbb{E}$ is eventually constant if there exists $r_0 \in \mathbb{Z}_+$ such that $E_r^{p,q} = E_{r_o}^{p,q}$ for all $r \geq r_0$ and all $(p,q) \in \mathbb{Z}^2$. In this case we denote $E_\infty^{p,q} = E_{r_0}^{p,q}$ for each (p,q).*

For eventually constant spectral sequences we have the notion of convergence.

Definition 2.4.12. *Fix an eventually constant spectral sequence $\mathbb{E}$ of R-modules and a family $\{E^n\}_{n\in\mathbb{Z}}$ of R-modules. We say that $\mathbb{E}$ converges to $\{E^n\}_{n\in\mathbb{Z}}$ and we write*

$$E_r^{p,q} \Rightarrow E^{p+q}$$

if for each n there is a filtration of submodules of E^n

$$\cdots \subseteq F^{p+1}E^n \subseteq F^pE^n \subseteq F^{p-1}E^n \subseteq \ldots$$

such that:

- $\bigcap_{p\in\mathbb{Z}} F^pE^n = 0$;
- $\bigcup_{p\in\mathbb{Z}} F^pE^n = E^n$;
- $E_\infty^{p,q} \cong F^pE^{p+q}/F^{p+1}E^{p+q}$ *for all* (p,q).

The following theorem allows in many cases to construct eventually convergent spectral sequences.

Theorem 2.4.13. *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories and let*

$$F : \mathcal{A} \to \mathcal{B}, \quad G : \mathcal{B} \to \mathcal{C}$$

be two additive left exact functors such that also the composition $G \circ F$ is left exact. Suppose that we can construct the right derived functors of F, G and $G \circ F$ and that for each injective object I of $\mathcal{A}$ it holds $R^i G(F(I)) = 0$ for all $i > 0$. Then for each object A of $\mathcal{A}$ there is a spectral sequence $\mathbb{E}(A)$ such that

$$E_2^{p,q}(A) = R^p G(R^q F(A))$$

and

$$E_r^{p,q}(A) \Rightarrow R^{p+q}(G \circ F)(A).$$

The spectral sequence in Theorem 2.4.13 is called *Groethendieck spectral sequence of A*. From it, we can obtain an exact sequence.

Proposition 2.4.14. *In the hypotheses of Theorem 2.4.13, if we denote $L^{p+q} := R^{p+q}(G \circ F)(A)$, there is an exact sequence*

$$0 \to E_2^{1,0} \to L^1 \to E_2^{0,1} \to E_2^{2,0} \to \mathrm{Ker}(\mathrm{L}^2 \to \mathrm{E}_2^{0,2}) \to E_2^{1,1} \to E_2^{3,0}.$$

Now we want to apply these results to our situation. Let L/K be a finite Galois extension and consider the functors

- $F := (\cdot)^{G_L} : [G_K - \mathrm{mod}] \to [\mathrm{Gal}(L/K) - \mathrm{mod}]$
- $G := (\cdot)^{\mathrm{Gal}(L/K)} : [\mathrm{Gal}(L/K) - \mathrm{mod}] \to \underline{Ab}$.

Then they are left exact, and their composition $G \circ F = (\cdot)^{G_K}$ is left exact as well. Moreover the right derived functors of F, G and $G \circ F$ give exactly the Galois cohomologies, then for each G_K-module M we have the Groethendieck spectral sequence $\mathbb{E}(M)$ of M, with

$$E_2^{p,q}(M) = R^p G(R^q F(A)) = H^p(\mathrm{Gal}(L/K), H^q(G_L, M))$$

and

$$E_r^{p,q}(M) \Rightarrow H^{p+q}(G_K, M).$$

Then the exact sequence of Proposition 2.4.14 is

$$\begin{array}{l} 0 \longrightarrow H^1(\mathrm{Gal}(L/K), M^{G_L}) \xrightarrow{\ \inf\ } H^1(G_K, M) \\ \qquad\qquad\qquad\qquad\qquad\qquad \swarrow^{\ \mathrm{res}} \\ H^1(G_L, M)^{\mathrm{Gal}(L/K)} \longrightarrow H^2(\mathrm{Gal}(L/K), M^{G_L}) \longrightarrow H^2(G_K, M) \end{array} \tag{2.14}$$

This sequence is called the Hochschild–Serre sequence and following the proofs of Theorem 2.4.13 and Proposition 2.4.14, one sees that the first part of it is the restriction–inflation sequence.

Chapter 3

Heegner points

3.1 Orders in number fields

Let K be a number field.

Definition 3.1.1. *A subset $\mathcal{O} \subseteq K$ is said to be an order in K if all the following conditions holds:*

(a) $\mathcal{O}$ is a subring of K;

(b) $\mathcal{O}$ is finitely generated as $\mathbb{Z}$-module;

(c) $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

Since $\mathcal{O}$ is clearly torsion free, (b) and (c) are equivalent to $\mathcal{O}$ being a free $\mathbb{Z}$-module of rank two. Moreover (c) tell us that K is the field of fraction of $\mathcal{O}$.

Remark 3.1.2. *If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field with $d \in \mathbb{Z} \setminus \{0, 1\}$, we have an explicit description of orders in K. First of all we have the equality*

$$\{\textit{Orders in } K\} = \{\mathbb{Z}[a] : a \in \mathcal{O}_K \setminus \mathbb{Z}\}$$

where $\mathcal{O}_K$ is the ring of integers of K. Let us check the double inclusion. Let $a \in \mathcal{O}_K \setminus \mathbb{Z}$. Then $a = x + y\sqrt{d}$ for some $x \in \mathbb{Q}$ and $y \in \mathbb{Q}^\times$. Hence

$$\mathbb{Z}[a] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(a) = \mathbb{Q}(x + y\sqrt{d}) = \mathbb{Q}(\sqrt{d}) = K.$$

Moreover, $\mathbb{Z}[a]$ is clearly a subring of K and is finitely generated as $\mathbb{Z}$-module since a is an algebraic integer. Conversely, le $\mathcal{O} \subseteq K$ be an order of K. Since

$$rank_{\mathbb{Z}}(\mathcal{O}) = 2,$$

applying the elementary divisor theorem, we can find a basis of $\mathcal{O}$ over $\mathbb{Z}$ $\{1, a\}$, for some $a \in \mathcal{O}$. In other words $\mathcal{O} = \mathbb{Z}[a]$, $a \notin \mathbb{Z}$, and $a \in \mathcal{O}_K$ since $\mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}$-module.

More explicitly, since $\mathcal{O}_K = \mathbb{Z}[\omega_d]$ *with*

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

one has

$$\{\text{Orders in } K\} = \{\mathbb{Z}[a] : a \in \mathcal{O}_K \setminus \mathbb{Z}\} = \{\mathbb{Z}[c\omega_d] : c \in \mathbb{Z}_+\}.$$

Summing up, if K is a quadratic field, every order is contained in the maximal order $\mathcal{O}_K = \mathbb{Z}[\omega_d]$ and is uniquely determined by a positive non-zero integer c such that

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}c\omega_d =< 1, c\omega_d >_{\mathbb{Z}}.$$

Moreover, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\omega_d)$, where $\omega_d \in \mathbb{C}$ is the algebraic element defined in the previous remark.

Definition 3.1.3. *Let* $\mathcal{O}$ *be an order in a quadratic field* K*. We will call the unique integer* c *such that*

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}c\omega_d$$

the conductor of $\mathcal{O}$*. Moreover, the discriminant of* $\mathcal{O}$ *of conductor* c *is the integer*

$$d_{\mathcal{O}} = c^2 d_k$$

where d_k *is the discriminant of* K*.*

Given any order $\mathcal{O}$ in a quadratic field K, our goal is now to define a certain class group $Cl(\mathcal{O})$ associated to $\mathcal{O}$ in analogy with the classical ideal class group of $\mathcal{O}_K$. We give the following definitions:

Definition 3.1.4. *An ideal* $\mathfrak{a}$ *of* $\mathcal{O}$ *is said to be proper if*

$$\{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}.$$

Note that the inclusion

$$\mathcal{O} \subseteq \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}$$

always holds since $\mathfrak{a}$ *is an ideal of* $\mathcal{O}$*.*

Definition 3.1.5. *A fractional ideal of* $\mathcal{O}$ *(or a fractional* $\mathcal{O}$*-ideal) is a subset of* K *which is a nonzero finitely generated* $\mathcal{O}$*-module.*

Remark 3.1.6. *Every fractional ideal is of the form* $\alpha\mathfrak{a}$*, where* $\alpha \in K^\times$ *is an ideal of* $\mathcal{O}$*. Then a fractional* $\mathcal{O}$*-ideal* $\mathfrak{b}$ *is proper provided that*

$$\{\beta \in K : \beta\mathfrak{b} \subseteq \mathfrak{b}\} = \mathcal{O}.$$

Once we have fractional ideals, we can talk about invertible ideals.

Definition 3.1.7. *A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is said to be invertible if there is another fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.*

Note that any principal nonzero fractional ideal $\alpha\mathcal{O}$ with $\alpha \in K^\times$ is invertible since

$$(\alpha\mathcal{O})(\alpha^{-1}\mathcal{O}) = \alpha\alpha^{-1}\mathcal{O} = \mathcal{O}.$$

The basic result is that for orders in quadratic fields, the notions of proper and invertible coincides:

Proposition 3.1.8. *Let $\mathcal{O}$ be an order in a quadratic field K, and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.*

Proof. See [Cox22, Chapter 2, Section 7, Proposition 7.4]. □

We now give a useful characterization of nonzero fractional ideal of a given order $\mathcal{O}$ in a quadratic field K

Proposition 3.1.9. *Let $K = \mathbb{Q}(\omega_d)$ be a quadratic field and fix an order $\mathcal{O} \subseteq K$. Then, every nonzero fractional ideal $\mathfrak{b}$ of $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.*

Proof. Let $\mathfrak{b} = \alpha \cdot \mathfrak{a}$ be a nonzero fractional ideal of $\mathcal{O}$ with $\alpha \in K^\times$ and $\mathfrak{a} \subseteq \mathcal{O}$ an ideal. We divide the proof into several steps.

Step 1. First, we show that $\mathbb{Z}^* \cap \mathfrak{a} \neq \emptyset$. Let α be a nonzero element of $\mathfrak{a}$. Since

$$\mathfrak{a} \subseteq \mathcal{O} = \mathbb{Z} + c\omega_d\mathbb{Z},$$

where c is the conductor of the order $\mathcal{O}$, there exists $m, n \in \mathbb{Z}$, not both zero, such that

$$\alpha = m + c\omega_d n.$$

Consider now $\alpha' = \sigma(\alpha)$ with $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ the non trivial automorphism of K. Thus

$$\alpha' = \sigma(\alpha) = \sigma(m + c\omega_d n) = m + cn\sigma(\omega_d).$$

There are two cases to consider for ω_d. If $\omega_d = \sqrt{d}$, then

$$\alpha' = m - c\omega_d n \in \mathbb{Z} + c\omega_d\mathbb{Z} = \mathcal{O}.$$

Since $\mathfrak{a}$ is an ideal, $\alpha \cdot \alpha' = m^2 - c^2dn^2$ is an integer of $\mathfrak{a}$. Moreover, we may assume that d is not a square. Then c^2dn^2 cannot be a square, and hence $\alpha \cdot \alpha'$ is nonzero. Otherwise, if $\omega_d = \frac{1+\sqrt{d}}{2}$,

$$\alpha' = m + cn\left(\frac{1-\sqrt{d}}{2}\right) = (m + cn) - c\omega_d n \in \mathbb{Z} + c\omega_d\mathbb{Z} = \mathcal{O}.$$

Hence,

$$\alpha \cdot \alpha' = m^2 + cnm - c^2n^2\frac{d-1}{4} \in \mathfrak{a}.$$

Moreover, it is an integer since in this case $d \equiv 1 \pmod 4$. Suppose, for the sake of contradiction, that

$$m^2 + cnm - c^2n^2\frac{d-1}{4} = 0.$$

Then

$$4(m^2 + cnm) + c^2n^2 = c^2n^2d$$

that is

$$(2m + cn)^2 = c^2n^2d.$$

In other words c^2n^2d, would be a square, and we then conclude as in the previous case.

Step 2. Next, we prove that the quotient $\mathcal{O}/\mathfrak{a}$ is finite. From the previous step, we can choose a nonzero integer $m \in \mathfrak{a}$. Then $m\mathcal{O} \subseteq \mathfrak{a}$ and since

$$\mathcal{O}/m\mathcal{O} = \frac{\mathbb{Z} + c\omega_d\mathbb{Z}}{m(\mathbb{Z} + c\omega_d\mathbb{Z})} \cong \frac{\mathbb{Z} \oplus \mathbb{Z}}{m(\mathbb{Z} \oplus \mathbb{Z})} \cong (\mathbb{Z}/m\mathbb{Z})^2$$

we obtain

$$|\mathcal{O}/\mathfrak{a}| \leq |\mathcal{O}/m\mathcal{O}| \leq m^2.$$

Step 3. Finally, we complete the prove. Since $\mathcal{O} \cong \mathbb{Z} \oplus \mathbb{Z}$ and $\mathfrak{a} \subseteq \mathbb{Z} \oplus \mathbb{Z}$, $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank less then 2. Since the quotient $\mathcal{O}/\mathfrak{a}$ is finite for the the previous step, we conclude. □

Thanks to the proof of Proposition 3.1.9 (Step 2), we can define the norm of an ideal of an order.

Definition 3.1.10. *Let $\mathcal{O} \subseteq K$ be an order of an imaginary quadratic field and let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal. We define the norm of $\mathfrak{a}$ to be*

$$\mathrm{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|.$$

Moreover from Proposition 3.1.9, we obtain the following corollary.

Corollary 3.1.11. *Let $\mathcal{O}$ be an oder in a quadratic field K . Then, every proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is a lattice in $\mathbb{C}$.*

Remark 3.1.12. *Let $\mathfrak{b} \subseteq \mathcal{O}$ be a proper fractional ideal in an order of a quadratic imaginary field K. Then*

$$\mathrm{End}(\mathbb{C}/\mathfrak{b}) = \{\alpha \in K : \alpha \cdot \mathfrak{b} \subseteq \mathfrak{b}\} = \mathcal{O}.$$

In other words, we can define a map

$$\mathcal{I}(\mathcal{O}) \longrightarrow \{\mathbb{C}/\Lambda : \mathrm{End}(\mathbb{C}/\Lambda) = \mathcal{O}\}, \qquad \mathfrak{b} \mapsto \mathbb{C}/\mathfrak{b}$$

That we will study in more details in the next section.

Given an order $\mathcal{O}$ of a quadratic field K, denote by $\mathcal{I}(\mathcal{O})$ the set of proper fractional $\mathcal{O}$-ideals. By Proposition 3.1.8, $\mathcal{I}(\mathcal{O})$ is a group under multiplication. The principal $\mathcal{O}$-ideals give a subgroup $\mathcal{P}(\mathcal{O}) \subseteq \mathcal{I}(\mathcal{O})$. Hence we can form the quotient.

Definition 3.1.13. *The ideal class group of the order $\mathcal{O}$ is*

$$Cl(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

Now we want to give two alternative definitions of the ideal class group. Let n be a positive integer, $K = \mathbb{Q}(\sqrt{d})$ an imaginary quadratic field and consider

$$\mathcal{O}_n = \mathbb{Z} \oplus \mathbb{Z}n\omega_d$$

the order of K of conductor n.

Definition 3.1.14. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_n$. We say that $\mathfrak{a}$ is prime (or relatively prime) to n (or to $n\mathcal{O}_n$) if*

$$\mathfrak{a} + n\mathcal{O}_n = \mathcal{O}_n$$

Lemma 3.1.15. *Let $\mathfrak{a}, \mathfrak{b}$ be invertible ideals of $\mathcal{O}_n$. The following properties hold.*

(a) $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$*;*

(b) if τ denotes the non trivial element of $\mathrm{Gal}(K/\mathbb{Q})$*, then*

$$\mathfrak{a}\tau(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})\mathcal{O}_n.$$

Proof. See [Cox22, Chapter 2, Section 7, Lemma 7.14]. □

Lemma 3.1.16. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_n$.*

(a) $\mathfrak{a}$ is prime to n (i.e., $\mathfrak{a} + n\mathcal{O}_n = \mathcal{O}_n$) if and only if $\gcd(\mathrm{N}(\mathfrak{a}), n) = 1$.

(b) Every ideal of $\mathcal{O}_n$ prime to n is invertible.

Proof. (a) Let $m_n : \mathcal{O}_n/\mathfrak{a} \to \mathcal{O}_n/\mathfrak{a}$ be the multiplication-by-n map. Since $\mathcal{O}_n/\mathfrak{a}$ is a finite abelian group of order $\mathrm{N}(\mathfrak{a})$, we have:

$$\begin{aligned} \mathfrak{a} + n\mathcal{O}_n = \mathcal{O}_n &\iff m_n \text{ is surjective} \\ &\iff m_n \text{ is an isomorphism} \\ &\iff \gcd(\mathrm{N}(\mathfrak{a}), n) = 1. \end{aligned}$$

where the last equivalence follows from the structure theorem for finite abelian groups.

(b) Let $\mathfrak{a}$ be an $\mathcal{O}_n$-ideal which is prime to n. By Proposition 3.1.8, it suffices to prove that $\mathfrak{a}$ is proper. Recall that $\mathfrak{a}$ is proper if and only if its stabilizer in K is exactly $\mathcal{O}_n$, i.e., $\{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\} \subseteq \mathcal{O}_n$.

Let $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$. Since $\mathfrak{a}$ is an ideal, β is necessarily an integral element, so $\beta \in \mathcal{O}_K$. Using the hypothesis $\mathfrak{a} + n\mathcal{O}_n = \mathcal{O}_n$, we have:

$$\begin{aligned}\beta\mathcal{O}_n &= \beta(\mathfrak{a} + n\mathcal{O}_n)\\ &= \beta\mathfrak{a} + n(\beta\mathcal{O}_n)\\ &\subseteq \mathfrak{a} + n\mathcal{O}_K.\end{aligned}$$

Since $\mathfrak{a} \subseteq \mathcal{O}_n$ and $n\mathcal{O}_K \subseteq \mathcal{O}_n$ (as n is the conductor), it follows that:

$$\beta\mathcal{O}_n \subseteq \mathcal{O}_n + \mathcal{O}_n = \mathcal{O}_n.$$

This implies $\beta \in \mathcal{O}_n$, proving that $\mathfrak{a}$ is proper and thus invertible.

□

We now fix the following notation

- $\mathcal{I}(\mathcal{O}_n, n)$:= the subgroup of $\mathcal{I}(\mathcal{O}_n)$ generated by the $\mathcal{O}_n$-ideals prime to n;
- $\mathcal{P}(\mathcal{O}_n, n) := \{\mathfrak{a} \in \mathcal{I}(\mathcal{O}_n, n) : \mathfrak{a} \text{ is principal}\}$.

Our goal is to prove that the quotient $\mathcal{I}(\mathcal{O}_n, n)/\mathcal{P}(\mathcal{O}_n, n)$ is isomorphic to the ideal class group $Cl(\mathcal{O}_n)$. We need a lemma.

Lemma 3.1.17. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Given a nonzero integer M, then every ideal class in $Cl(\mathcal{O})$ constains a proper fractional $\mathcal{O}$-ideal whose norm is relatively prime to M.*

Proof. See [Cox22, Chapter 2, Section 7, Corollary 7.17]. □

Proposition 3.1.18.

$$\frac{\mathcal{I}(\mathcal{O}_n, n)}{\mathcal{P}(\mathcal{O}_n, n)} \cong \frac{\mathcal{I}(\mathcal{O}_n)}{\mathcal{P}(\mathcal{O}_n)} = Cl(\mathcal{O}_n)$$

Proof. Consider the composition

$$\mathcal{I}(\mathcal{O}_n, n) \to \mathcal{I}(\mathcal{O}_n) \to \mathcal{I}(\mathcal{O}_n)/\mathcal{P}(\mathcal{O}_n) = Cl(\mathcal{O}_n)$$

where the first map is the inclusion. Combining the two previous lemmas we obtain that it is surjective, hence to conclude we have to show that its kernel $\mathcal{I}(\mathcal{O}_n, n) \cap \mathcal{P}(\mathcal{O}_n)$ coincides with $\mathcal{P}(\mathcal{O}_n, n)$. Clearly we have an inclusion

$$\mathcal{P}(\mathcal{O}_n, n) \subseteq \mathcal{I}(\mathcal{O}_n, n) \cap \mathcal{P}(\mathcal{O}_n).$$

On the other hand, let $\alpha\mathcal{O}_n \in \mathcal{I}(\mathcal{O}_n, n) \cap \mathcal{P}(\mathcal{O}_n)$, then by definition, we can write $\alpha\mathcal{O}_n = \mathfrak{a}\mathfrak{b}^{-1}$, for some invertible ideals of $\mathcal{O}_n$ prime to n. Note that by Lemma

3.1.15, $\mathfrak{b}\tau(\mathfrak{b}) = \mathrm{N}(\mathfrak{b})\mathcal{O}_n$, that is $\mathrm{N}(\mathfrak{b})\mathfrak{b}^{-1} = \tau(\mathfrak{b})$, where τ denotes the complex conjugation. Thus

$$\mathrm{N}(\mathfrak{b})\alpha\mathcal{O}_n = \mathrm{N}(\mathfrak{b})\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathrm{N}(\mathfrak{b})\mathfrak{b}^{-1} = \mathfrak{a}\tau(\mathfrak{b}) \subseteq \mathcal{O}_n.$$

Then $\mathrm{N}(\mathfrak{b})\alpha\mathcal{O}_n \in \mathcal{P}(\mathcal{O}_n, n)$ and finally we conclude that

$$\alpha\mathcal{O}_n = \mathrm{N}(\mathfrak{b})\alpha\mathcal{O}_n(\mathrm{N}(\mathfrak{b})\mathcal{O}_n)^{-1} \in \mathcal{P}(\mathcal{O}_n, n).$$

□

Finally we see the third equivalent definition of the ideal class group of $\mathcal{O}_n$. We denote

- $\mathcal{I}_K(n)$:= the subgroup of $\mathcal{I}(\mathcal{O}_K)$ generated by the ideals of $\mathcal{O}_K$ prime to n;
- $\mathcal{P}_{K,\mathbb{Z}}(n) := \{\alpha\mathcal{O}_K : \alpha \equiv a \pmod{n\mathcal{O}_K}, a \in \mathbb{Z}, \gcd(a, n) = 1\}$.

Proposition 3.1.19. *There is a bijection*

$$\mathcal{I}_K(n) \longrightarrow \mathcal{I}(\mathcal{O}_n, n)$$

given by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}_n$. Its inverse is given by $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$. Moreover, this map preserves the norm and restricts to a bijection

$$\mathcal{P}_{K,\mathbb{Z}}(n) \longrightarrow \mathcal{P}(\mathcal{O}_n, n).$$

Proof. First of all, we check that $f : \mathcal{I}_K(n) \to \mathcal{I}(\mathcal{O}_n, n)$, $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}_n$ is well-defined. Given $\mathfrak{a} \in \mathcal{I}_K(n)$, consider the composition

$$\mathcal{O}_n \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}.$$

The kernel is $\mathfrak{a} \cap \mathcal{O}_n = f(\mathfrak{a})$. The induced injection $\mathcal{O}_n/f(\mathfrak{a}) \hookrightarrow \mathcal{O}_K/\mathfrak{a}$ implies $\mathrm{N}(f(\mathfrak{a})) \mid \mathrm{N}(\mathfrak{a})$. By Lemma 3.1.16, $f(\mathfrak{a})$ is prime to n since $\mathfrak{a}$ is. To show $\mathrm{N}(f(\mathfrak{a})) = \mathrm{N}(\mathfrak{a})$, consider

$$\phi : \mathcal{O}_n/f(\mathfrak{a}) \hookrightarrow \mathcal{O}_K/\mathfrak{a} \xrightarrow{n\cdot} \mathcal{O}_K/\mathfrak{a}$$

. Since $\gcd(n, \mathrm{N}(\mathfrak{a})) = 1$, the multiplication-by-$n$ map is an isomorphism. For any $[a] \in \mathcal{O}_K/\mathfrak{a}$, let $[a']$ be the unique class such that $[na'] = [a]$. Since $n\mathcal{O}_K \subseteq \mathcal{O}_n$, $na' \in \mathcal{O}_n$, so $\phi([na']) = [a]$, proving ϕ is surjective. Thus ϕ is an isomorphism and $\mathrm{N}(f(\mathfrak{a})) = \mathrm{N}(\mathfrak{a})$.

Now define $g : \mathcal{I}(\mathcal{O}_n, n) \to \mathcal{I}_K(n)$ by $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$. It is well-defined because $g(\mathfrak{b}) + n\mathcal{O}_K = (\mathfrak{b} + n\mathcal{O}_n)\mathcal{O}_K = \mathcal{O}_K$. To show $f \circ g = \mathrm{id}$, let $\mathfrak{b} \in \mathcal{I}(\mathcal{O}_n, n)$. The inclusion $\mathfrak{b} \subseteq \mathfrak{b}\mathcal{O}_K \cap \mathcal{O}_n$ is trivial. Conversely,

$$\mathfrak{b}\mathcal{O}_K \cap \mathcal{O}_n = (\mathfrak{b}\mathcal{O}_K \cap \mathcal{O}_n)(\mathfrak{b} + n\mathcal{O}_n) \subseteq \mathfrak{b} + n(\mathfrak{b}\mathcal{O}_K \cap \mathcal{O}_n) \subseteq \mathfrak{b} + \mathfrak{b}(n\mathcal{O}_K) \subseteq \mathfrak{b}.$$

To show $g \circ f = \mathrm{id}$, let $\mathfrak{a} \in \mathcal{I}_K(n)$. Then $(\mathfrak{a} \cap \mathcal{O}_n)\mathcal{O}_K \subseteq \mathfrak{a}$ is trivial. Conversely,

$$\mathfrak{a} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}_n + n\mathcal{O}_n) \subseteq (\mathfrak{a} \cap \mathcal{O}_n)\mathcal{O}_K + n\mathfrak{a}.$$

Since $n\mathfrak{a} \subseteq n\mathcal{O}_K \subseteq \mathcal{O}_n$, we have $n\mathfrak{a} \subseteq \mathfrak{a} \cap \mathcal{O}_n$, hence $\mathfrak{a} \subseteq (\mathfrak{a} \cap \mathcal{O}_n)\mathcal{O}_K$.

Finally, for the restriction to principal ideals: If $\alpha\mathcal{O}_K \in \mathcal{P}_{K,\mathbb{Z}}(n)$, then $\alpha \in \mathcal{O}_K$ and $\alpha \equiv a \pmod{n\mathcal{O}_K}$ with $\gcd(a,n) = 1$. Since $n\mathcal{O}_K \subseteq \mathcal{O}_n$, we have $\alpha \in \mathcal{O}_n$. Thus $f(\alpha\mathcal{O}_K) = \alpha\mathcal{O}_n$. Since $\alpha \equiv a \pmod{n\mathcal{O}_n}$ in $\mathcal{O}_n$, $\alpha\mathcal{O}_n \in \mathcal{P}(\mathcal{O}_n, n)$. Conversely, if $\alpha\mathcal{O}_n \in \mathcal{P}(\mathcal{O}_n, n)$, then $\alpha \in \mathcal{O}_n$ and $\alpha \equiv a \pmod{n\mathcal{O}_n}$ for some $a \in \mathbb{Z}$ prime to n. Since $n\mathcal{O}_n \subseteq n\mathcal{O}_K$, $\alpha \equiv a \pmod{n\mathcal{O}_K}$, so $g(\alpha\mathcal{O}_n) = \alpha\mathcal{O}_K \in \mathcal{P}_{K,\mathbb{Z}}(n)$. □

In conclusion we have

$$Cl(\mathcal{O}_n) = \frac{\mathcal{I}(\mathcal{O}_n)}{\mathcal{P}(\mathcal{O}_n)} \cong \frac{\mathcal{I}(\mathcal{O}_n, n)}{\mathcal{P}(\mathcal{O}_n, n)} \cong \frac{\mathcal{I}_K(n)}{\mathcal{P}_{K,\mathbb{Z}}(n)}. \tag{3.1}$$

3.2 The endomorphism ring

Let E be an elliptic curve over $\mathbb{C}$. By results of chapter 2, E is of the form

$$E = \mathbb{C}/\Lambda$$

for some lattice $\Lambda \subseteq \mathbb{C}$. Moreover, by Proposition 1.4.5 and Corollary 1.4.6 the endomorphism ring is

$$\begin{aligned} \mathrm{End}(E) &= \{\varphi : E \to E : \varphi \text{ is an isogeny}\} \\ &= \{[\alpha] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda : \alpha \in \mathbb{C},\ \alpha\Lambda \subseteq \Lambda\} \\ &= \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}. \end{aligned}$$

where $[\alpha]$ is the multiplication by $\alpha \in \mathbb{C}$. We have the following classification theorem for $\mathrm{End}(E)$.

Theorem 3.2.1. *Let $E = \mathbb{C}/\Lambda$ be an elliptic curve over $\mathbb{C}$ and let $\omega_1, \omega_2 \in \mathbb{C}$ be a basis for Λ over $\mathbb{Z}$. Consider the endomorphism ring of E*

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

Then one and only one of the following is true:

- $\mathrm{End}(E) = \mathbb{Z}$;
- $\mathbb{Q}(\frac{\omega_1}{\omega_2})$ *is an imaginary quadratic field and End(E) is an order in* $\mathbb{Q}(\frac{\omega_1}{\omega_2})$.

Proof. To begin with, up to lattice isomorphism, we may suppose that $\Lambda = \Lambda_\tau$ with $\tau = \frac{\omega_1}{\omega_2}$ (see Remark 1.4.7). By Remark 1.4.9, $\mathbb{Z} \subseteq \mathrm{End}(E)$, and if equality holds, there is nothing to prove. Suppose now that $\mathbb{Z} \subsetneq \mathrm{End}(E)$.

First of all, we prove that $\mathrm{End}(E)$ is integral over $\mathbb{Z}$. Let $\alpha \in \mathrm{End}(E)$ and consider the associated map

$$\begin{aligned} [\alpha] : \Lambda &\longrightarrow \Lambda \\ \lambda &\longmapsto \alpha\lambda. \end{aligned}$$

Since $[\alpha]$ is a homomorphism of $\mathbb{Z}$-modules of rank 2, we can consider its characteristic polynomial, which is of the form

$$p_\alpha(X) = X^2 + aX + b \in \mathbb{Z}[X].$$

By the Cayley–Hamilton theorem, $p_\alpha([\alpha])$ is the zero map, hence $p_\alpha(\alpha) = 0$.

We now prove that $\mathbb{Q}(\tau)$ is an imaginary quadratic field. Since $\mathbb{Z} \subsetneq \mathrm{End}(E)$, we may choose $\alpha_0 \in \mathrm{End}(E) \setminus \mathbb{Z}$. Since $\alpha_0 = \alpha_0 \cdot 1 \in \Lambda$, we can write

$$\alpha_0 = n + m\tau$$

for some $n, m \in \mathbb{Z}$ with $m \neq 0$. Using the notation above, we obtain

$$0 = p_{\alpha_0}(\alpha_0) = \alpha_0^2 + a\alpha_0 + b = (n + m\tau)^2 + a(n + m\tau) + b.$$

In other words, since $m \neq 0$, the element $\tau \in \mathbb{C}\setminus\mathbb{R}$ is a root of a quadratic polynomial with coefficients in $\mathbb{Z}$, and the claim follows.

It remains to prove that $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\tau)$. The endomorphism ring $\mathrm{End}(E)$ is a subring of $\mathbb{Q}(\tau)$, since for all $\alpha \in \mathrm{End}(E)$ we have

$$\alpha = \alpha \cdot 1 \in \Lambda = \mathbb{Z} + \mathbb{Z}\tau \subseteq \mathbb{Q}(\tau).$$

Moreover, since $\mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\tau)}$ and $\mathcal{O}_{\mathbb{Q}(\tau)}$ is finitely generated as a $\mathbb{Z}$-module, it follows that $\mathrm{End}(E)$ is finitely generated as a $\mathbb{Z}$-module.

Finally, we show that

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E) = \mathbb{Q}(\tau).$$

Since $\mathbb{Q}(\tau)$ is a field and $\mathrm{End}(E) \subseteq \mathbb{Q}(\tau)$ is a subring, the inclusion "$\subseteq$" is clear. Conversely, choosing $\alpha_0 \in \mathrm{End}(E) \setminus \mathbb{Z}$ as above, we have

$$\mathbb{Q}(\tau) = \mathbb{Q}(\alpha_0) = \mathbb{Q} \oplus \mathbb{Q}\alpha_0 = \mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z} \oplus \mathbb{Z}\alpha_0) \subseteq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E).$$

□

Definition 3.2.2. *An elliptic curve E over $\mathbb{C}$ is said to have complex multiplication if its endomorphism ring is isomorphic to an order in a quadratic imaginary field. More precisely, given such an order $\mathcal{O}$, one says that E has complex multiplication by $\mathcal{O}$ if* $\mathrm{End}(E) \cong \mathcal{O}$.

Proposition 3.2.3. *Let $\mathcal{O}$ be a an order in an imaginary quadratic field K. Then the map*

$$\begin{aligned} Cl(\mathcal{O}) &\longrightarrow \left\{ \begin{matrix} \textit{Elliptic curves } E \\ \textit{such that } \mathrm{End}(E) \cong \mathcal{O} \end{matrix} \right\} / \cong \\ [\mathfrak{a}] &\longmapsto [\![\mathbb{C}/\mathfrak{a}]\!] \end{aligned}$$

is a bijection.

In order to prove Proposition 3.2.3, we need a lemma whose proof can be found in [Cox22, Chapter 3, Section 10, Theorem 10.14].

Lemma 3.2.4. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice, and let $\wp(z)$ be the $\wp$-funcion with respect to Λ (Definition 1.4.10). Then, for a number $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, the following statements are equivalent:*

(a) $\wp(\alpha z)$ is a rational function in $\wp(z)$.

(b) $\alpha\Lambda \subseteq \Lambda$.

(c) There is an order $\mathcal{O}$ in an imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and there exists $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ such that

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\mathfrak{a}.$$

Now we are ready to prove proposition 3.2.3.

Proof. First of all we want to prove that the map is well defined. By Remark 3.1.12, $\mathbb{C}/\mathfrak{a}$ is an elliptic curve over $\mathbb{C}$ for all proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$. Moreover, by proposition 1.4.5

$$[\mathfrak{a}] = [\mathfrak{b}] \iff \mathbb{C}/\mathfrak{a} \cong \mathbb{C}/\mathfrak{b}$$

for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(\mathcal{O})$. This proves also injectivity. Finally, the equivalence of (b) and (c) of lemma 3.2.4 guarantees the surjectivity. □

3.3 Heegner points

Definition 3.3.1. *Let E, E' be two elliptic curves over $\mathbb{C}$ and let $\varphi : E \longrightarrow E'$ be an isogeny. We say that φ has degree $N \in \mathbb{Z}_{>0}$ if*

$$|\mathrm{Ker}(\varphi)| = |N|.$$

Moreover, we say that φ is cyclic of order N if $\mathrm{Ker}(\varphi) \cong \mathbb{Z}/N\mathbb{Z}$.

Given a positive integer N, the points of $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ may also be viewed as classifying triples (E, E', ϕ), where $\phi : E \longrightarrow E'$ is a cyclic isogeny of order N. Indeed, fixed a such triple, the couple $(E, ker(\phi))$ is a point of $Y_0(N)$ from the results of Section 2.2.2. Conversely, given any pair (E, C), with E an elliptic curve over $\mathbb{C}$ and C a cyclic subgroup in E of order N, we can consider $E' = E/C$ and the projection map

$$\phi : E \longrightarrow E'$$

which has clearly kernel isomophic to the cyclic group $\mathbb{Z}/N\mathbb{Z}$.

Let now K be an imaginary quadratic field.

Definition 3.3.2. *Let $\mathcal{O} \subseteq K$ be an order in K. We say that $x = (E, E', \phi) \in Y_0(N)(\mathbb{C})$ is a Heegner point associated to the order $\mathcal{O}$, if both E and E' have complex multiplication by $\mathcal{O}$.*

We have the following characterization of the set of Heegner points.

Proposition 3.3.3. *The set of heegner points is non-empty if and only if there exists an order $\mathcal{O}$ and an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that*

$$\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Proof. Suppose we have a Heegner point $x = (E, E', \phi)$ with

$$\mathrm{End}(E) = \mathrm{End}(E') = \mathcal{O}$$

for some order $\mathcal{O} \subseteq K$ and $\phi : E \longrightarrow E'$ such that

$$\mathrm{Ker}(\phi) \cong \mathbb{Z}/N\mathbb{Z}.$$

By proposition 3.2.3 there exist $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(\mathcal{O})$ such that

$$E \cong \mathbb{C}/\mathfrak{a}, \qquad E' \cong \mathbb{C}/\mathfrak{b}.$$

Then there exists some $\alpha \in K^\times$ such that $\phi = [\alpha]$. In other words, ϕ is the multiplication by α

$$\begin{aligned} \phi : \mathbb{C}/\mathfrak{a} &\longrightarrow \mathbb{C}/\mathfrak{b} \\ \overline{x} &\longmapsto \overline{\alpha x}. \end{aligned}$$

Note that

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

If we now set $\mathcal{N} := \alpha\mathfrak{a}\mathfrak{b}^{-1}$, then $\mathcal{N} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$ is an ideal and

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

Conversely, suppose that there is an ideal $\mathcal{N}$ of an order $\mathcal{O}$ such that

$$\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Choose an invertible fractional ideal $\mathfrak{a}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Note that both $\mathrm{End}(E)$ and $\mathrm{End}(E')$ are isomorphic to $\mathcal{O}$ by proposition 3.2.3. Consider now the isogeny

$$\phi : \mathbb{C}/\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \qquad \overline{x} \mapsto \overline{x}$$

which has kernel

$$\mathrm{Ker}(\phi) = (\mathfrak{a}\mathcal{N}^{-1})/\mathfrak{a} \cong \mathfrak{a}/\mathcal{N}\mathfrak{a} \cong \mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

□

By proposition 3.3 we deduce that a Heegner point $x \in Y_0(N)$ can be described as a triple

$$(\mathcal{O}, \mathcal{N}, [\mathfrak{a}])$$

where $\mathcal{O}$ is an order in an imaginary quadratic field K, $\mathcal{N} \subseteq \mathcal{O}$ is an $\mathcal{O}$-ideal such that $\mathcal{O}/\mathcal{N}$ is cyclic of order N and $[a] \in Cl(\mathcal{O})$.

Proposition 3.3.4. *Let K be a quadratic number field and let N be a positive integer. 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 $N = p_1^{e_1} \cdots p_r^{e_r}$ and suppose

$$p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \ldots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}.$$

Since for all i p_i splits in K, we have that

$$f = [\mathcal{O}_K/\mathfrak{p}_{ij} : \mathbb{Z}/p_i\mathbb{Z}] = 1.$$

Thus

$$\mathcal{O}_K/\mathfrak{p}_{11} \cong \mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1} \cong \mathbb{Z}/p_r\mathbb{Z}$$

and

$$\mathcal{O}_K/\mathfrak{p}_{11}^{e_1} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

Set now $\mathcal{N} = \mathfrak{p}_{11}^{e_1} \cdots \mathfrak{p}_{r1}^{e_r}$, then by chinese remainder theorem

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

□

Remark 3.3.5. *Let K be a quadratic field, $\mathcal{O} \subseteq K$ an order with conductor c and N be a positive integer. Suppose now that*

(a) $(c, N) = 1$;

(b) every prime p dividing N splits in K.

By proposition 3.3.4 we can find an ideal $\mathcal{N} \subseteq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Since $(c, N) = 1$, by construction of $\mathcal{N}$ we have

$$\mathcal{N} + c\mathcal{O}_K = \mathcal{O}_K.$$

In other words $\mathcal{N}$ is relatively prime to $c\mathcal{O}_K$, hence by (3.1) *$\mathcal{N}_\mathcal{O} := \mathcal{N} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal such that*

$$\mathcal{O}/\mathcal{N}_\mathcal{O} = \mathcal{O}/(\mathcal{O} \cap \mathcal{N}) \cong \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

*Finally, by Proposition 3.3.3 the set of Heegner points in $Y_0(N)$ associated to the order $\mathcal{O}$ is non-empty. Hence we can give the so called "*Heegner hypothesis*".*

HEEGNER HYPOTHESIS. In the above setting, the integer N is relatively prime to the conductor of the order and every prime p dividing N splits in K.

3.4 Ring class field

In this section, we introduce the theory of ring class fields, which provides the natural arithmetic framework for studying the rationality of Heegner points. As we shall see, these abelian extensions of imaginary quadratic fields are precisely the fields of definition for the points constructed via the theory of complex multiplication.

3.4.1 The Artin map

Let L/K be a Galois extension of number fields, $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ and $\mathfrak{P} \subseteq \mathcal{O}_L$ be a nonzero prime ideal lying over $\mathfrak{p}$. Set

$$\mathbb{F}_{\mathfrak{P}} := \mathcal{O}_L/\mathfrak{P}, \qquad \mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}.$$

Definition 3.4.1. *We define the decomposition group of $\mathfrak{P}$ (relatively to the extension L/K) to be the following subgroup of the Galois group:*

$$D_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

One can show that there is a surjective homomorphism

$$\begin{aligned} \Phi_{\mathfrak{P}} \colon D_{\mathfrak{P}} &\longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \\ \sigma &\longmapsto \overline{\sigma} \end{aligned}$$

where

$$\begin{aligned} \overline{\sigma} \colon \mathbb{F}_{\mathfrak{P}} &\longrightarrow \mathbb{F}_{\mathfrak{P}} \\ \overline{x} &\longmapsto \overline{\sigma(x)}. \end{aligned}$$

Definition 3.4.2. *We define the inertia group of $\mathfrak{P}$ (relatively to the extension L/K) to be*

$$I_{\mathfrak{P}} := \mathrm{Ker}(\Phi_{\mathfrak{P}}) = \{\sigma \in D_{\mathfrak{P}} : \sigma(x) - x \in \mathfrak{P}, \text{ for all } x \in \mathcal{O}_L\}.$$

Suppose now that $\mathfrak{p}$ does not ramifies in L, that is the ramification index e of $\mathfrak{P}$ over $\mathcal{O}_K$ is simply 1. In this case

$$|I_{\mathfrak{P}}| = e = 1$$

hence

$$D_{\mathfrak{P}} = D_{\mathfrak{P}}/I_{\mathfrak{P}} = D_{\mathfrak{P}}/\,\mathrm{Ker}(\Phi_{\mathfrak{P}}) \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$$

is cyclic. Since $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is canonically generated by

$$\overline{\sigma_{\mathfrak{P}}} : \mathbb{F}_{\mathfrak{P}} \longrightarrow \mathbb{F}_{\mathfrak{P}} \qquad \overline{x} \mapsto \overline{x}^q$$

where $q = |\mathcal{O}_K/\mathfrak{p}|$, we can give the following.

Definition 3.4.3. *We call the unique automorphism $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}$ such that*

$$\sigma_{\mathfrak{P}}(x) \equiv x^q \pmod{\mathfrak{P}}, \quad \forall x \in \mathcal{O}_L$$

the Frobenius automorphism at $\mathfrak{P}$.

Remark 3.4.4. *Let $\sigma \in \mathrm{Gal}(L/K)$ be a K-automorphism of L. Since*

$$D_{\tau(\mathfrak{P})} = \tau D_{\mathfrak{P}} \tau^{-1}$$

then

$$\sigma_{\tau(\mathfrak{P})} = \tau \sigma_{\mathfrak{P}} \tau^{-1}.$$

If moreover $\mathrm{Gal}(L/K)$ is abelian

$$\sigma_{\tau'(\mathfrak{P})} = \sigma_{\mathfrak{P}} \text{ for all } \tau' \in \mathrm{Gal}(L/K).$$

In other words, the Frobenius automorphism does not depend on the prime $\mathfrak{P}$ lying on $\mathfrak{p}$.

Definition 3.4.5. *Let L/K be an abelian extension of number fields and $\mathfrak{p}$ be a prime of K which does not ramify in L. The Artin symbol is*

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma_{\mathfrak{P}}$$

where $\mathfrak{P}$ is a prime lying on $\mathfrak{p}$.

Suppose now that L/K is an unramified abelian extension. In this case the Artin symbol is defined for all primes $\mathfrak{p}$ of K. Let $\mathfrak{a} \in \mathcal{I}(\mathcal{O}_K)$ be a fractional ideal with prime factorization

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i}, \quad r_i \in \mathbb{Z}.$$

We can define the Artin symbol

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

Moreover, it follows from the definition that

$$\left(\frac{L/K}{\mathfrak{ab}}\right) = \left(\frac{L/K}{\mathfrak{a}}\right) \cdot \left(\frac{L/K}{\mathfrak{b}}\right)$$

for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(\mathcal{O}_K)$

Definition 3.4.6. *Let L/K be an unramified abelian extension. The homomorphism*

$$\Phi_{L/K} := \left(\frac{L/K}{\cdot}\right) : \mathcal{I}(\mathcal{O}_K) \longrightarrow \mathrm{Gal}(L/K)$$

is called The Artin map.

3.4.2 Ring class field of conductor n

Let K be an imaginary quadratic field and fix an ideal $\mathfrak{m} \subseteq \mathcal{O}_K$. In this setting, denote by

- $\mathcal{I}_K(\mathfrak{m})$:= the subgroup of $\mathcal{I}(\mathcal{O}_K)$ generated by the ideals of $\mathcal{O}_K$ prime to $\mathfrak{m}$;
- $\mathcal{P}_{K,1}(\mathfrak{m}) := \{\alpha\mathcal{O}_K : \alpha \in \mathcal{O}_K, \alpha \equiv 1 \pmod{\mathfrak{m}}\}$.

Definition 3.4.7. *A subgroup $H \subseteq \mathcal{I}_K(\mathfrak{m})$ is called congruence subgroup for $\mathfrak{m}$ if it contains $\mathcal{P}_{K,1}(\mathfrak{m})$.*

Definition 3.4.8. *Let L/K be an abelian extension such that for all prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$*

$$\mathfrak{p} \nmid \mathfrak{m} \Rightarrow \mathfrak{p} \text{ does not ramify in } L.$$

We define the Artin map

$$\Phi_{\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

by putting

$$\Phi_{\mathfrak{m}}(\mathfrak{p}) := \left(\frac{L/K}{\mathfrak{p}}\right)$$

and extending the map to an homomorphism to every ideal $\mathfrak{b} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{b})}$ as we did before.

Fix now an imaginary quadratic field $K = \mathbb{Q}(\omega_d)$, a positive integer n and set

$$\mathcal{O}_n := \mathbb{Z} \oplus \mathbb{Z}n\omega_d$$

the order in K of conductor n. With this assumption, our goal is to find an abelian extension K_n/K such that

$$\mathrm{Gal}(K_n/K) \cong Cl(\mathcal{O}_n).$$

The existence of such extension is assured by the following important theorem.

Theorem 3.4.9 (Existence Theorem for quadratic imaginary fields)**.** *Let $\mathfrak{m}$ be an ideal of K quadratic imaginary field and let $H \subseteq \mathcal{I}_K(\mathfrak{m})$ be a congruence subgroup. Then there exists an unique abelian extension L/K such that*

(a) if $\mathfrak{p}$ is a prime of K that ramifies in L, then $\mathfrak{p} \mid \mathfrak{m}$;

(b) the kernel of the Artin map $\Phi_{L/K,\mathfrak{m}}$ is H.

Clearly it follows from the definition that $\mathcal{P}_{K,\mathbb{Z}}(n)$ is a congruence subgroup for $n\mathcal{O}_K$, i.e.

$$\mathcal{P}_{K,1}(n\mathcal{O}_K) \subseteq \mathcal{P}_{K,\mathbb{Z}}(n) \subseteq \mathcal{I}_K(n\mathcal{O}_K).$$

This motivates the following definition.

Definition 3.4.10. *The ring class field of K of conductor n is the abelian extension K_n of K corresponding to $\mathfrak{m} = n\mathcal{O}_K$ and $H = \mathcal{P}_{K,\mathbb{Z}}(n)$ in Theorem 3.4.9.*

Concretely, the ring class field of conductor n is an abelian extension K_n of K such that:

(a) if a prime ideal $\mathfrak{p}$ of K does not divide $n\mathcal{O}_K$, then it does not ramify in K_n;

(b) the prime ideals $\mathfrak{p} \in \mathcal{I}_K(n\mathcal{O}_K)$ that split completely in K_n are exactly those in $\mathcal{P}_{K,\mathbb{Z}}(n)$. Indeed, if $\mathfrak{p} \in \mathcal{I}_K(n\mathcal{O}_K)$, it does not ramify by the previous condition; hence:

$$\begin{aligned} \mathfrak{p} \in \mathcal{P}_{K,\mathbb{Z}}(n) &\iff \left(\frac{K_n/K}{\mathfrak{p}}\right) = \mathrm{id} \\ &\iff \mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}} \\ &\iff \mathfrak{p} \text{ splits completely in } K_n, \end{aligned}$$

where $\mathfrak{P}$ is any prime ideal of K_n lying over $\mathfrak{p}$, and $\mathbb{F}_{\mathfrak{P}}, \mathbb{F}_{\mathfrak{p}}$ denote the respective residue fields.

We now state the Tchebotarev density theorem which will be an useful tool during this work.

Definition 3.4.11. *Let K be a number field. Given a set M of prime ideals of K, we define the density of M to be the limit, if it exists,*

$$\lim_{n\to\infty} \frac{\#\{\mathfrak{p} \in M : \mathrm{N}(\mathfrak{p}) \leq n\}}{\#\{\mathfrak{p} \text{ prime of } K : \mathrm{N}(\mathfrak{p}) \leq n\}}.$$

where $\mathrm{N}(\cdot)$ is the norm of ideals of K in the extension $K/\mathbb{Q}$.

Remark 3.4.12. *Note that if the limit is not zero, then M is infinite.*

With the notion of density, we can give the theorem

Theorem 3.4.13 (Tchebotarev Density Theorem)**.** *Let L/K be a finite Galois extension of degree N, let $\sigma \in \mathrm{Gal}(L/K)$, let c be the cardinality of the conjugacy class of $\sigma \in \mathrm{Gal}(L/K)$ and let M be the set of prime ideals $\mathfrak{p}$ of K, unramified in L, such that there exists a prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$ with $\sigma = \sigma_{\mathfrak{P}}$. Then M has density c/N.*

We recall that the conjugacy class of $\sigma \in \mathrm{Gal}(L/K)$ is

$$\mathrm{Gal}(L/K)\sigma\mathrm{Gal}(L/K)^{-1} = \{\tau\sigma\tau^{-1} : \tau \in \mathrm{Gal}(L/K)\}.$$

Remark 3.4.14. *Let L/K be an abelian extension, $N = \#\mathrm{Gal}(L/K) = [L : K]$ and let $\mathfrak{m}$ be an ideal in $\mathcal{O}_K$ divisible by all the prime ideals of K that ramify in L. Then the Artin map*

$$\Phi_{\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

is surjective. Indeed, if we take $\sigma \in \mathrm{Gal}(L/K)$ *and if we consider the set*

$$M = \left\{ \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \mathfrak{p} \text{ is unramified in } L \text{ and } \sigma = \left(\frac{L/K}{\mathfrak{p}}\right) \right\},$$

Theorem 3.4.13 assures that M *has density*

$$c/N \neq 0$$

where c *is the cardinality of the conjugacy class of* σ*. Hence* M *has to be infinite and so, by our choice of* $\mathfrak{m}$*, there exists at least a prime ideals* $\mathfrak{p} \in \mathcal{I}_K(\mathfrak{m})$ *such that*

$$\Phi_{\mathfrak{m}}(\mathfrak{p}) = \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma.$$

Hence, for any positive integer n *we can consider* $\mathfrak{m} = n\mathcal{O}_K$ *and set*

$$H = \mathcal{P}_{K,\mathbb{Z}}(n).$$

By Theorem 3.4.9 and the three definitions of $Cl(\mathcal{O}_n)$ *in* (3.1) *we obtain*

$$\begin{aligned} \mathrm{Gal}(K_n/K) &= \mathrm{Im}(\Phi_{n\mathcal{O}_K}) \cong \mathcal{I}_K(\mathfrak{m})/\mathrm{Ker}(\Phi_{n\mathcal{O}_K}) \\ &= \mathcal{I}_K(\mathfrak{m})/H = \mathcal{I}_K(\mathfrak{m})/\mathcal{P}_{K,\mathbb{Z}}(n) \\ &\cong \mathrm{Cl}(\mathcal{O}_n). \end{aligned} \tag{3.2}$$

Moreover, if $\mathfrak{p}$ *is a prime ideal of* K *such that* $\mathfrak{p} \nmid n\mathcal{O}_n$*, then it does not ramify in* K_n*.*

3.4.3 Concrete construction

Let K be an imaginary quadratic field and let $\mathcal{O}_n$ be the order in K of conductor n for a positive integer n. We denote

$$\mathrm{Ell}_{\mathcal{O}_n}(\mathbb{C}) = \{j(E) \in \mathbb{C} : \mathrm{End}(E) \cong \mathcal{O}_n\}$$

the set of the j-invariants of all the elliptic curves with complex multiplication by $\mathcal{O}_n$. We define an action of the ideal class group $Cl(\mathcal{O}_n)$ on the set $\mathrm{Ell}_{\mathcal{O}_n}(\mathbb{C})$ that will help us during the section. In order to fix the notation, for any $[\mathfrak{a}] \in Cl(\mathcal{O}_n)$, consider

$$E_{\mathfrak{a}} := \mathbb{C}/\mathfrak{a} \text{ and } j(\mathfrak{a}) = j(E_{\mathfrak{a}}).$$

Definition 3.4.15. *The action of* $Cl(\mathcal{O}_n)$ *on* $\mathrm{Ell}_{\mathcal{O}_n}(\mathbb{C})$ *is defined as follows:*

(a) For all $E_{\mathfrak{a}}$ *with complex multiplication by* $\mathcal{O}_n$ *and for all* $[\mathfrak{b}] \in Cl(\mathcal{O}_n)$*, we define*

$$[\mathfrak{b}] \star E_{\mathfrak{a}} := E_{\mathfrak{a}\mathfrak{b}^{-1}} = \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1};$$

(b) For all $j(E_{\mathfrak{a}}) = j(\mathfrak{a}) \in \mathrm{Ell}_{\mathcal{O}_n}(\mathbb{C})$ *and for all* $[\mathfrak{b}] \in Cl(\mathcal{O}_n)$*, we define*

$$[\mathfrak{b}] \star j(E_{\mathfrak{a}}) := j([\mathfrak{b}] \star E_{\mathfrak{a}}).$$

Before proceeding, it is necessary to make an observation that will be crucial for the results to follow.

Remark 3.4.16. *Given al elliptic curve $E_{\mathfrak{a}}$ with complex multiplication by $\mathcal{O}_n$ and given $[\mathfrak{b}] \in Cl(\mathcal{O}_n)$ with $[\mathfrak{b}]$ an ideal in $\mathcal{O}_n$ there is a natural isogeny*

$$\varphi : E_{\mathfrak{a}} \longrightarrow E_{\mathfrak{a}\mathfrak{b}^{-1}} = [\mathfrak{b}] \star E_{\mathfrak{a}}$$

induced by the inclusion $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}^{-1}$. Moreover, φ has degree $\mathrm{N}(\mathfrak{b})$ since

$$\mathrm{Ker}(\varphi) = (\mathfrak{a}\mathfrak{b}^{-1})/\mathfrak{a} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_n/\mathfrak{b}$$

that is $|\mathrm{Ker}(\varphi)| = \mathrm{N}(\mathfrak{b})$.

Lemma 3.4.17. *If p is a prime number, then, the leading coefficient of $\Phi_p(X, Y)$ is -1.*

Lemma 3.4.18. *Every class of $Cl(\mathcal{O}_n)$ contains infinitely many ideals of prime norm.*

Proof. Recall that from (3.2) we have an isomorphism

$$Cl(\mathcal{O}_n) \cong \mathrm{Gal}(K_n/K)$$

which sends a class $[\mathfrak{p} \cap \mathcal{O}_n]$ to the Frobenius

$$\mathrm{Frob}_{K_n/K}(\mathfrak{p}) := \left(\frac{K_n/K}{\mathfrak{p}}\right)$$

with $\mathfrak{p} \in \mathcal{I}_K(n)$. Thus, fix a class in $Cl(\mathcal{O}_n)$ and consider its corresponding Frobenius $\sigma \in \mathrm{Gal}(K_n/K)$. By the Tchebotarev density Theorem 3.4.13 applied to the extension K_n/K, there exist infinitely many prime ideals $\mathfrak{p} \in \mathcal{I}_K(n)$ such that

$$\sigma = \mathrm{Frob}_{K_n/K}(\mathfrak{p}).$$

We want to show that infinitely many of these prime ideals have prime norm. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be such a prime and let $p = \mathfrak{p} \cap \mathbb{Q}$ be the corresponding prime ideal in $\mathbb{Q}$. Since $K/\mathbb{Q}$ is quadratic, we have three possibilities:

- p is inert in K, then $\mathrm{N}(\mathfrak{p}) = p^2$;
- p ramifies in K, then $\mathrm{N}(\mathfrak{p}) = p$;
- p splits in K, then $\mathrm{N}(\mathfrak{p}) = p$.

Thus, the norm $\mathrm{N}(\mathfrak{p})$ is prime if and only if p is not inert. This is equivalent to saying that the Frobenius automorphism of p over $\mathbb{Q}$ in the extension $K/\mathbb{Q}$ is trivial (for the split case) or the prime is ramified.

Since $K_n/\mathbb{Q}$ is a Galois extension and $\sigma \in \mathrm{Gal}(K_n/K) \leq \mathrm{Gal}(K_n/\mathbb{Q})$, we can apply the Tchebotarev density Theorem 3.4.13 again to $K_n/\mathbb{Q}$ for the element σ.

Then, there are infinitely many prime ideals p of $\mathbb{Z}$ such that their Frobenius class in $\mathrm{Gal}(K_n/\mathbb{Q})$ is the conjugacy class of σ. For any such prime p, let $\mathfrak{P}$ be a prime of K_n above it such that $\mathrm{Frob}_{K_n/\mathbb{Q}}(\mathfrak{P}) = \sigma$. Then, if we let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, we have:

$$\mathrm{Frob}_{K/\mathbb{Q}}(p) = \mathrm{Frob}_{K_n/\mathbb{Q}}(\mathfrak{P})|_K = \sigma|_K = \mathrm{id}$$

since $\sigma \in \mathrm{Gal}(K_n/K)$ by assumption. This implies that p is not inert in K. Therefore, $N(\mathfrak{p}) = p$, and since $\mathrm{Frob}_{K_n/K}(\mathfrak{p}) = \sigma$, the ideal $\mathfrak{p} \cap \mathcal{O}_n$ belongs to the required class. □

Theorem 3.4.19. *If E is an elliptic curve with complex multiplication, then its j-invariant $j(E)$ is an algebraic integer.*

Proof. Let E be an elliptic curve with complex multiplication by some order $\mathcal{O}_n$ in a quadratic field K. Applying lemma 3.4.18 to the trivial class $1 \in Cl(\mathcal{O}_n)$, we can find a prime ideal $\mathfrak{p}$ of $\mathcal{O}_n$ such that $1 = [\mathfrak{p}]$ and $N(\mathfrak{p}) = p$ with p a prime number. Then,

$$j([\mathfrak{p}] \star E) = [\mathfrak{p}] \star j(E) = 1 \star j(E) = j(E),$$

that is by proposition 1.2.4

$$[\mathfrak{p}] \star E \cong E.$$

As we saw in remark 3.4.16 we have a natural isogeny

$$\varphi : E \longrightarrow [\mathfrak{p}] \star E$$

that is cyclic of degree $\mathrm{N}(\mathfrak{p}) = p$. Hence, by proposition 2.1.11, we have that

$$\Phi_p(j(E), j(E)) = 0.$$

In other words, $j(E)$ is a root of the polynomial $-\Phi_p(X, X)$, that is in $\mathbb{Z}[X]$ by proposition 2.1.10 and it is monic by lemma 3.4.17. □

Remark 3.4.20. *Let E be an elliptic curve with complex multiplication. The fact that $j(E)$ is algebraic integer, implies that E can be defined over $\mathbb{Q}(j(E))$, that is a number field. Indeed, let*

$$E' : \begin{cases} y^2 + xy = x^3 - \frac{36}{j(E)-1728}x - \frac{1}{j(E)-1728} & \text{if } j(E) \neq 0, 1728 \\ y^2 + y = x^3 & \text{if } j(E) = 0 \\ y^2 = x^3 + x & \text{if } j(E) = 1728. \end{cases}$$

Then E' is clearly defined over $\mathbb{Q}(j(E))$ and its j-invariant satisfies

$$j(E') = j(E).$$

In other words by Proposition 1.2.4 E and E' are isomorphic over $\overline{\mathbb{Q}}$.

A consequence of these facts is the following explicit characterization of the ring class field of K.

Theorem 3.4.21. *Let $j \in \mathrm{Ell}_{\mathcal{O}_n}$, then*

$$K_n = K(j).$$

Proof. See [Cox22, Chapter 3, Section 11, Theorem 11.1]. □

Remark 3.4.22. *A fundamental property of the extension K_m/K that we will use frequently is the following: let $l \nmid m$ be a prime of $\mathbb{Q}$ which is inert in K, and let $\lambda = l\mathcal{O}_K$ be the corresponding prime ideal of K. By the definition of the ring class field, λ is unramified in K_m since l does not divide the conductor m. Furthermore, λ splits completely in K_m. Indeed, considering the Artin map:*

$$\Phi_{m\mathcal{O}_K} : \mathcal{I}_K(m\mathcal{O}_K) \longrightarrow \mathrm{Gal}(K_m/K), \quad \mathfrak{p} \longmapsto \left(\frac{K_m/K}{\mathfrak{p}}\right),$$

note that $\lambda = (l)$ is a principal ideal of $\mathcal{O}_K$ generated by the integer $l \in \mathbb{Z}$. Since $l \equiv l \pmod{m\mathcal{O}_K}$ and in our hypothesis $\gcd(l, m) = 1$, it follows that $\lambda \in \mathcal{P}_{K,\mathbb{Z}}(m)$, and thus $\Phi_{m\mathcal{O}_K}(\lambda)$ is the identity in $\mathrm{Gal}(K_m/K)$. This is equivalent to saying that the inertia group I_{λ_m} is trivial for each prime ideal λ_m of K_m lying over λ. Finally, if $n = lm$, the prime λ divides the conductor of K_n; consequently, each prime λ_m of K_m above λ is totally ramified in the extension K_n/K_m.

3.5 The rationality of Heegner points

One of the key properties of Heegner points, which will be essential for the arguments developed later, is their rationality over ring class fields. To begin with, let N be an integer and let $\mathcal{O}_n \subseteq K$ be an order of conductor n in an imaginary quadratic field satisfying the Heegner hypothesis. This means that N is relatively prime to n and every prime p dividing N splits in K. In this setting, we can consider a Heegner point $(\mathcal{O}_n, \mathcal{N}, [\mathfrak{a}])$ which consists explicitly of the isogeny

$$\varphi : E_1 \longrightarrow E_2,$$

where $E_1 = \mathbb{C}/\mathfrak{a}$ and $E_2 = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. By Proposition 3.2.3, both E_1 and E_2 have complex multiplication by the ring $\mathcal{O}_n$; hence, by Remark 3.4.20, they are defined over $\mathbb{Q}(j_1)$ and $\mathbb{Q}(j_2)$, respectively, where j_1 (resp. j_2) denotes the j-invariant of E_1 (resp. E_2). Applying Corollary 1.2.15 to $F = K(j_1, j_2)$, that is by Theorem 3.4.21 the ring class field K_n, we obtain that φ is defined over K_n. Moreover, also $C := \mathrm{Ker}(\varphi)$ is defined over K_n by the characterization of Corollary 1.2.15. Summing up, we obtain a pair (E_1, C) defined over K_n. In view of the moduli interpretation discussed in Section 2.2.2, this pair corresponds to a K_n-rational point of $Y_0(N)$ via the map

$$\alpha_{\mathrm{Spec}(K_n)} : F_0(N)(\mathrm{Spec}(K_n)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[1/N]}(\mathrm{Spec}(K_n), Y_0(N))$$

induced by the natural transformation $\alpha\colon F_0(N) \to \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, Y_0(N))$.

Chapter 4

Kolyvagin's Theorem

4.1 Statement and first considerations

Let N be a squarefree positive integer and let $X_0(N)$ be the usual modular curve. Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$ satisfying the Heegner hypotheses, i.e.

$$\text{every prime } p \text{ dividing } N \text{ splits in } K.$$

For simplicity, we assume $D \neq 3, 4$, so the integers $\mathcal{O}_K$ of K have unit group $\mathcal{O}_K^\times = \{\pm\}$. Let $f \in \mathcal{S}_2^{\text{new}}(\Gamma_0(N))$ be a newform and consider $E = E_f$ the elliptic curve defined over $\mathbb{Q}$ obtained via the Eichler–Shimura construction. In particular, we have a parametrization, that is, with notation used in Section 2.3, a map defined over $\mathbb{Q}$

$$\psi = \nu \circ \Phi : X_0(N) \longrightarrow E$$

where Φ is the Abel–Jacobi mapping. Note that without loss of generality, we may assume that Φ has base point $[\infty] = \pi(\infty)$ so that it is sent to the origin of E. The goal of this chapter is to study the rank of the group of K-rational point $E(K)$. More precisely, we will construct a point $y_K \in E(K)$ and what we want to prove is the following theorem by Kolyvagin.

In what follows, if m is an integer, we will denote by $\mathbb{Q}(E[m])$ the Galois extension of $\mathbb{Q}$ generated by the m-torsion points of E. Let us check that this definition is well-defined. More precisely, $\mathbb{Q}(E[m])$ is obtained from $\mathbb{Q}$ by adjoining the coordinates of all m-torsion points. Since the multiplication-by-m isogeny is defined over $\mathbb{Q}$, note that if $P \in E[m]$, then for each $\sigma \in G_\mathbb{Q} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$m\sigma(P) = \sigma(mP) = \sigma(O) = O.$$

In other words, the set $E[m]$ is invariant under the action of $G_\mathbb{Q}$, and thus the extension $\mathbb{Q}(E[m])/\mathbb{Q}$ is indeed Galois.

Theorem 4.1.1 (Kolyvagin)**.** *Assume that the modular curve E has not complex multiplication and that the point y_K has infinite order in $E(K)$. Then the group $E(K)$ has rank 1. Moreover, if p is an odd prime such that*

i) E has good reduction at p,

ii) the point y_K is not divisible by p in $E(K)$; that is, the equation $pQ = y_K$ has no solution $Q \in E(K)$,

iii) $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$,

then the p-torsion subgroup of the Shafarevic–Tate group $Ш(E/K)$ is trivial.

Remark 4.1.2. *First of all, look at the hypothesis of the prime p in the statement of theorem 4.1.1: these hold for almost all primes. Indeed,*

i) the prime p in which E has bad reduction are those that divides the discriminant and the discriminant admits only a finite number of prime divisors.

ii) The set of prime numbers p such that $y_K \in pE(K)$ is finite, since y_K has infinite order. Indeed, suppose by contradiction that there exists an infinite set $A \subset \mathbb{Z}_{\geq 1}$ such that for each $n \in A$ there exists a point $P_n \in E(K)$ with $nP_n = y_K$. By the Mordell–Weil theorem, we may choose a system of generators of $E(K)$ $\{Q_1, \ldots, Q_r, q_1, \ldots, q_t\}$, where the Q_i have infinite order and the q_j are torsion points. Then, for each $n \in A$, we can write

$$y_K = \sum_{i=1}^{r} a_i Q_i + \sum_{j=1}^{t} b_j q_j \quad \text{and} \quad P_n = \sum_{i=1}^{r} a_i^{(n)} Q_i + \sum_{j=1}^{t} b_j^{(n)} q_j$$

for suitable integer coefficients. Since $nP_n = y_K$, it follows that $a_i = na_i^{(n)}$ for all $i = 1, \ldots, r$, hence n divides a_i for every $n \in A$. As A is infinite, this implies that $a_i = 0$ for all i, and therefore y_K is a torsion point, contradicting our assumption.

iii) The action of the absolute Galois group $G_{\mathbb{Q}}$ on the the p-torsion subgroup $E[p]$ induces a representation

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p),$$

where the isomorphism holds because $E[p] \cong \mathbb{F}_p^2$. A Serre's theorem says that $\rho_{E,p}$ is surjective for $p >> 0$, then for almost all p

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[p]))} = \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Ker}(\rho_{E,p})} \cong \mathrm{GL}_2(\mathbb{F}_p).$$

To make the statement of Theorem 4.1.1 complete, we need to define the point y_K. The Heegner hypothesis on the number field K assures that we can find a point of $Y_0(N) \subseteq X_0(N)$ of the form

$$(\mathcal{O}_K, \mathcal{N}, [1])$$

with $\mathcal{N} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. This Heegner point corresponds to the isogeny

$$\mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$$

that is by definition cyclic of order N.

Definition 4.1.3. *We define x_1 as the point of $X_0(N)$ corresponding to the cyclic N-isogeny*

$$\mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}.$$

Moreover, denoting by K_1 the ring class field of the maximal order $\mathcal{O}_K$, we know from Section 3.5 that $x_1 \in X_0(N)(K_1)$.

Definition 4.1.4. *We define*

$$y_1 := \psi(x_1) \in E,$$

where ψ is the modular parametrization fixed at the beginning of the chapter.

Note that, since ψ is defined over $\mathbb{Q}$, it preserves fields of definition, and hence $y_1 \in E(K_1)$.

Definition 4.1.5. *Finally we define*

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

where the sum is in $E(K_1)$.

Remark 4.1.6. *Although the construction of the point depends crucially on the choice of the ideal, we are only interested in the fact that the point has infinite order. Indeed, one can check that every other point y'_K constructed as above is such that $y_K = \pm y'_K + (\text{torsion})$ (thus y_K has infinite order if and only if y'_K has infinite order).*

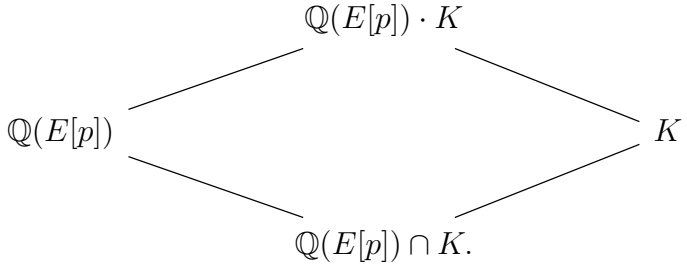
We will not prove directly Theorem 4.1.1 but we will pass through the following theorem.

Theorem 4.1.7. *Let p be an odd prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$, $p \nmid D$ and assume that p does not divide $y_K \in E(K)$. Then the Selmer group $\mathrm{Sel}(E/K)[p]$ is cyclic, generated by the image of the class of y_k under the Kummer map κ.*

Remark 4.1.8. *Let's see why Theorem 4.1.7 implies Theorem 4.1.1. Recall that, from Section 2.4, we have the short exact sequence of $\mathbb{F}_p$-vector spaces*

$$0 \to E(K)/p(E(K)) \xrightarrow{\kappa} \mathrm{Sel}(E/K)[p] \to Ш(E/K)[p] \to 0 \tag{4.1}$$

with κ the Kummer map. We want to show that the dimension over $\mathbb{F}_p$ of $E(K)/p(E(K))$ is exactly the rank of $E(K)$. To begin with, consider the following tower



Note that $\mathbb{Q}(E[p]) \cdot K = K(E[p])$ *and* $\mathbb{Q}(E[p]) \cap K = \mathbb{Q}$. *Indeed, looking at the ramified primes, we want to show that* $\mathbb{Q}(E[p]) \cap K$ *is a finite unramified extension of* $\mathbb{Q}$ *and so it has to coincide to* $\mathbb{Q}$ *itself. Let* l *be a prime number.*

- *If* $l \nmid D$, *then by definition of the discriminant,* l *does not ramify in* K, *then in* $\mathbb{Q}(E[p]) \cap K$.
- *If* $l \mid D$, *it is sufficient to show that the finite extension of local fields*

  $$\mathbb{Q}_l(E[p])/\mathbb{Q}_l$$

  is unramified. First of all we want to use Proposition 1.3.19. Note That
  - *The residue field of* $\mathbb{Q}_l$ *is finite since* $\kappa_{\mathbb{Q}_l} \cong \mathbb{Z}_l/l\mathbb{Z}_l \cong \mathbb{F}_l$.
  - E *has good reduction at* l. *Indeed, since* $l \mid D$, $l \nmid N$ *because we are assuming that every prime factor of* N *splits in* K. *Thus* l *does not divide the conductor of the elliptic curve* E, *that is,* E *has good reduction at* l.
  - *Since by hypothesis* $p \nmid D$, *i.e.* $p \neq l$, *we have*

    $$\gcd(\mathrm{Char}(\kappa_{\mathbb{Q}_l}), p) = \gcd(l, p) = 1.$$

  Hence by Proposition 1.3.19, the set $E[m]$ *is unramified, that is the inertia group* $I_{\mathbb{Q}_l}$ *acts trivially on it. In particular*

  $$\mathbb{Q}_l(E[p]) \subseteq \overline{\mathbb{Q}_l}^{I_{\mathbb{Q}_l}} = \overline{\mathbb{Q}_l}^{\mathrm{Gal}(\overline{\mathbb{Q}_l}/\mathbb{Q}_l^{\mathrm{ur}})} = \mathbb{Q}_l^{\mathrm{ur}}$$

  that is, $\mathbb{Q}_l(E[p])/\mathbb{Q}_l$ *is unramified.*

Then we have

$$\mathrm{Gal}(K(E[p])/K) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

and this implies that

$$E(K)[p] = E[p]^{\mathrm{Gal}(K(E[p])/K)} \cong E[p]^{\mathrm{GL}_2(\mathbb{F}_p)} \cong (\mathbb{F}_p^2)^{\mathrm{GL}_2(\mathbb{F}_p)} \cong (\mathbb{F}_p^2)^{\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^2)} = 0.$$

This means that $E(K)$ *does not contain nontrivial* p*-torsion points, then, writing*

$$E(K) \cong \mathbb{Z}^r \oplus E_{\mathrm{tors}}(K)$$

we must have $E(K)/pE(K) \cong \mathbb{Z}^r/p\mathbb{Z}^r \cong \mathbb{F}_p^r$ *that is,*

$$\dim_{\mathbb{F}_p}(E(K)/pE(K)) = r = \mathrm{Rank}(E(K)).$$

In the hypothesis of Theorem 4.1.1 the rank of $E(K)$ *is nonzero since the point* y_K *has infinite order. Summing up, if Theorem 4.1.7 holds, from the exactness of the sequence* (4.1)

$$\begin{aligned} 1 &= \dim_{\mathbb{F}_p}(\mathrm{Sel}(E/K)[p]) \\ &= \dim_{\mathbb{F}_p}(E(K)/pE(K)) + \dim_{\mathbb{F}_p}(Ш(E/K)[p]) \\ &= \mathrm{rank}(E(K)) + \dim_{\mathbb{F}_p}(Ш(E/K)[p]) \\ &\geq 1 + \dim_{\mathbb{F}_p}(Ш(E/K)[p]). \end{aligned}$$

that is $\mathrm{Rank}(E(K)) = 1$ *and* $Ш(E/K)[p] = 0$.

The next sections are devoted to the proof of Theorem 4.1.7. Following Kolyvagin, we divide the argument into three steps:

(a) First, we construct certain cohomology classes $c(n) \in H^1(G_K, E[p])$ from Heegner points of conductor n for K.

(b) Second, we study their local properties.

(c) Third, we use these results to calculate the Selmer group.

4.2 Construction of the cohomology classes $c(n)$

The goal of this section is to construct a family of cohomology classes $\{c_n\}$. The main idea is to regard y_1 as belonging to a family of additional rational points y_n. From them we will ultimately obtain certain cohomology classes that will play a crucial role in what follows. We will impose some conditions on the integers n indexing these families; chief among them is the requirement that n is squarefree and every prime factor l of n does not divide $N \cdot D \cdot p$. This last condition has an important consequence.

Proposition 4.2.1. *Under the above conditions, l does not ramify in the Galois extension $K(E[p])/\mathbb{Q}$.*

Proof. Note that, since by hypothesis $l \nmid D$, it suffices to show that λ does not ramify in $K(E[p])$ for all prime ideals λ of $\mathcal{O}_K$ lying above l. By assumption, such a λ does not divide the conductor $N\mathcal{O}_K$, hence the elliptic curve E has good reduction at λ. Moreover, since

$$\gcd(p, \mathrm{char}(\kappa_{K_\lambda})) = \gcd(p, l) = 1,$$

it follows from Proposition 1.3.19 that the action of the inertia group I_λ on $E[p]$ is trivial. This implies that the local extension of the completions $K_\lambda(E[p])/K_\lambda$ is unramified. Since ramification is a local property, the fact that the extension of the completions is unramified directly implies that the prime ideal λ does not ramify in the global extension $K(E[p])/K$. This concludes the proof. □

It follows from the previous proposition that, if $\mathfrak{p}$ is a prime ideal of $K(E[p])$ lying above l, the Frobenius automorphism at $\mathfrak{p}$ is well-defined; in this chapter, we will denote it by

$$\mathrm{Frob}(\mathfrak{p}) := \mathrm{Frob}_{K(E[p])/\mathbb{Q}}(\mathfrak{p}).$$

Recall that for all $\sigma \in \mathrm{Gal}(K(E[p])/\mathbb{Q})$ one has $\mathrm{Frob}(\sigma(\mathfrak{p})) = \sigma\mathrm{Frob}(\mathfrak{p})\sigma^{-1}$. Thus we can consider the conjugacy class

$$\mathrm{Frob}(l) = \{\mathrm{Frob}(\sigma(\mathfrak{p})) : \sigma \in \mathrm{Gal}(K(E[p])/\mathbb{Q})\}.$$

We assume that:

$$\tau \in \mathrm{Frob}(l), \tag{4.2}$$

where τ is the complex conjugation. One often says that a prime l satisfying (4.2) is a "Kolyvagin prime". Note that by Theorem 3.4.13 there is an infinite number of Kolyvagin primes.

Remark 4.2.2. *A consequence of the assumption* (4.2) *is that l remains inert in K. Note that, since K is an imaginary quadratic field, $K/\mathbb{Q}$ is abelian, and the conjugacy class* $\mathrm{Frob}_{K/\mathbb{Q}}(l)$ *consists of a single element, which, by an abuse of notation, we will also denote by* $\mathrm{Frob}_{K/\mathbb{Q}}(l)$*. Moreover, one has*

$$\mathrm{Frob}_{K/\mathbb{Q}}(l) = (\mathrm{Frob}_{K(E[p])/\mathbb{Q}}(l))|_K = \tau,$$

that is the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$*. Thus l is inert in K. Another useful fact in this context is that the prime ideal $\lambda := l\mathcal{O}_K \subseteq \mathcal{O}_K$ splits completely in $K(E[p])$ since*

$$\mathrm{Frob}_{K(E[p])/K}(\lambda) = (\mathrm{Frob}_{K(E[p])/\mathbb{Q}}(l))^2 = \tau^2 = \mathrm{id}.$$

Another consequence of assumption (4.2) is the following proposition

Proposition 4.2.3. *Assumption* (4.2) *implies that*

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

Proof. Note that since the complex conjugation τ is an involution, it satisfies the equation

$$X^2 - 1 = 0.$$

On the other hand, the characteristic polynomial of $\mathrm{Frob}_{\mathbb{Q}(E[p])/\mathbb{Q}}(l)$ acting on $E[p] \cong \mathbb{F}_p^2$ is $X^2 - a_l X + l$ (see [Sil09, Theorem 2.3.1]). Hence, assumption (4.2) implies the congruence

$$X^2 - 1 \equiv X^2 - a_l X + l \pmod{p}$$

from which we deduce that $a_l \equiv l + 1 \equiv 0 \pmod{p}$. □

Now, we want to introduce some families of objects that will play a fundamental role in the proof of Theorem 4.1.7. More precisely, we will need:

- a family $\{x_n\}_n$ of points of $X_0(N)$ such that each $x_n \in X_0(N)(K_n)$;
- a family $\{y_n\}_n$ of points of E such that each $y_n \in E(K_n)$;
- a family $\{P_n\}_n$ of points of E such that each $P_n \in E(K_n)$;
- a family $\{c(n)\}_n$ of cohomology classes such that each $c(n) \in H^1(G_K, E[p])$.

For the considerations made before, the index n of all these families will run over

$$\mathcal{R} := \{ \text{ squarefree integers } n \text{ relatively prime to } pND \text{ such that if } n = l_1 \cdots l_r, \text{ then } \tau \in \mathrm{Frob}(l_i), \text{ where } \tau \text{ is the complex conjugation } \}.$$

Let $\mathcal{O}_n = \mathbb{Z} \oplus n\mathcal{O}_K$ be the order in K of conductor n with $n \in \mathcal{R}$ and consider

$$\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n.$$

This is an ideal of $\mathcal{O}_n$ such that $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$ and as we saw in Chapter 3, the isogeny

$$\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/\mathcal{N}_n^{-1}$$

is cyclic of order N. Note that this construction is consistent since the conductor of the order is coprime with N.

Definition 4.2.4. *Let $n \in \mathcal{R}$. We define x_n as the point of $X_0(N)$ corresponding to the isogeny*

$$\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/\mathcal{N}_n^{-1}.$$

Note that, similarly to the case $n = 1$, we have $x_n \in X_0(N)(K_n)$, where K_n is the ring class field of K of conductor n.

Definition 4.2.5. *Let $n \in \mathcal{R}$. We define*

$$y_n := \psi(x_n)$$

where ψ is the modular parametrization. In particular, since ψ is defined over $\mathbb{Q}$, then $y_n \in E(K_n)$. We will again call each y_n a Heegner point and the family $\{y_n\}_{n\in\mathcal{R}}$ an Euler system.

Once we have the family $\{y_n\}_{n\in\mathcal{R}}$ we may study its properties. Fix the following notation:

- $n \in \mathcal{R}$;
- $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$;
- $G_n := \mathrm{Gal}(K_n/K_1)$;
- $\mathrm{Tr}_l = \sum_{\sigma\in G_l} \sigma \in \mathbb{Z}[G_l]$ if l is a prime factor of n.

Here $\mathbb{Z}[G_l]$ is the free abelian group generated by the elements of G_l, i.e.

$$\mathbb{Z}[G_l] = \bigoplus_{\sigma\in G_l} \mathbb{Z}\sigma.$$

Note that $\mathbb{Z}[G_l]$ has a natural ring structure defined as follows. If $\sum_\sigma n_\sigma\sigma, \sum_\tau m_\tau\tau$ are in $\mathbb{Z}[G_l]$, then

$$\left(\sum_\sigma n_\sigma\sigma\right)\cdot\left(\sum_\tau m_\tau\tau\right) = \sum_{\sigma,\tau} n_\sigma m_\tau\sigma\tau = \sum_\gamma \left(\sum_\tau n_{\gamma\tau^{-1}}m\tau\right)\gamma.$$

Remark 4.2.6. *Let $n = l\cdot m \in \mathcal{R}$ with l a prime factor. Then G_n and G_l have the following properties.*

(a) *Since* $K_n = K_l \cdot K_m$ *and* $K_l \cap K_m = K_1$, *we have*

$$G_l = \mathrm{Gal}(K_l/K_1) \cong \mathrm{Gal}(K_m \cdot K_l/K_m) = \mathrm{Gal}(K_n/K_m).$$

In particular we can apply Tr_l *to* y_n.

(b) *There is a decomposition* $G_n = \prod_{l|n} G_l$. *Indeed, if* $n = ll'$,

$$G_n = \mathrm{Gal}(K_l \cdot K_{l'}/K_1) \cong \mathrm{Gal}(K_l/K_1) \times \mathrm{Gal}(K_{l'}/K_1)$$

and we conclude by induction.

(c) *The group* G_l *is cyclic of order* $l+1$. *Indeed, by* (3.1)

$$G_l \cong \frac{\mathrm{Gal}(K_l/K)}{\mathrm{Gal}(K_1/K)} \cong \frac{Cl(\mathcal{O}_l)}{Cl(\mathcal{O}_K)} \cong \frac{\mathcal{I}_K(l) \cap \mathcal{P}(\mathcal{O}_K)}{\mathcal{P}_{K,\mathbb{Z}}(l)}$$

and by the short exact sequence

$$1 \to (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathcal{O}_K/l\mathcal{O}_K)^\times \longrightarrow \frac{\mathcal{I}_K(l) \cap \mathcal{P}(\mathcal{O}_K)}{\mathcal{P}_{K,\mathbb{Z}}(l)} \to 1$$

we have

$$G_l \cong \frac{(\mathcal{O}_K/l\mathcal{O}_K)^\times}{(\mathbb{Z}/l\mathbb{Z})^\times}.$$

Moreover, since l *is inert in* K *by Remark 4.2.2, if* λ *is the unique prime ideal of* K *over* l *and* $\mathbb{F}_\lambda$ *is its residue field, then*

$$G_l \cong \frac{(\mathcal{O}_K/l\mathcal{O}_K)^\times}{(\mathbb{Z}/l\mathbb{Z})^\times} \cong \frac{\mathbb{F}_\lambda^\times}{\mathbb{F}_l^\times} \cong \frac{\mathbb{F}_{l^2}^\times}{\mathbb{F}_l^\times}.$$

In particular, G_l *is cyclic of order* $l+1$.

Proposition 4.2.7. *Let* l *be a prime factor of* $n \in \mathcal{R}$, *write* $n = lm$ *and let* a_l *be the* l*-th coefficients of the Fourier series of the new form associated to* E. *Then*

(a) $\mathrm{Tr}_l(y_n) = a_l y_m$ *in* $E(K_m)$

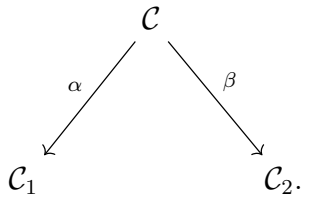
(b) *Each prime factor* $\lambda_n \subseteq \mathcal{O}_{K_n}$ *of* $\lambda = l\mathcal{O}_K$ *divides a unique prime ideal* λ_m *of* K_m *and we have the identity*

$$\mathrm{red}_{\lambda_n}(y_n) = \mathrm{red}_{\lambda_m}\left(\mathrm{Frob}_{K_m/\mathbb{Q}}(\lambda_m)(y_m)\right)$$

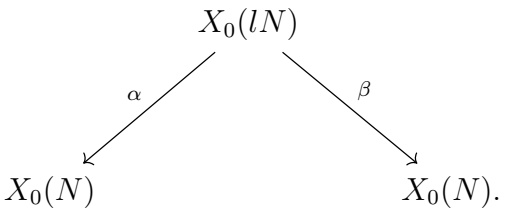
where $\mathrm{red}_{\lambda_n} : E(K_n) \to \overline{E}(\mathbb{F}_{\lambda_n})$ *is the reduction map.*

In order to prove this proposition, we need to interpret the Hecke operator $T_l := T_2(l)$ as an action on $\mathrm{Div}(X_0(N))$.

Definition 4.2.8. *Let $\mathcal{C}_1, \mathcal{C}_2$ be two curves. A correspondence $\mathcal{C}_1 \rightsquigarrow \mathcal{C}_2$ is a curve $\mathcal{C}$ together with two non constant morphisms*



In our case, we want to consider the Hecke operator T_l as a correspondence $X_0(N) \rightsquigarrow X_0(N)$ of the form



Recall that $X_0(N)$ classifies elliptic curves together with a cyclic subgroup of order N, up to isomorphism. More precisely, a point of $X_0(N)$ is a pair (E, C), where E is defined over $\mathbb{C}$ and $C \subset E$ is a cyclic subgroup with $C \cong \mathbb{Z}/N\mathbb{Z}$. Similarly, a representative of a point of $X_0(lN)$ is a pair $(E, C \oplus D)$, where $C \cong \mathbb{Z}/N\mathbb{Z}$ and $D \cong \mathbb{F}_l$. Using these notations, we can define α and β.

Definition 4.2.9. *We define*

- $\alpha : X_0(lN) \to X_0(N)$, $(E, C \oplus D) \mapsto (E, C)$;
- $\beta : X_0(lN) \to X_0(N)$, $(E, C \oplus D) \mapsto (E, (C + D)/D)$.

One can check, in the language of complex varieties, that

- α corresponds to the morphism $\alpha : \mathcal{H}/\Gamma_0(lN) \to \mathcal{H}/\Gamma_0(N)$ induced by the inclusion $\Gamma_0(pN) \subseteq \Gamma_0(N)$;
- β corresponds to the composition

$$\beta : \mathcal{H}/\Gamma_0(lN) \cong \mathcal{H}/\begin{bmatrix} l & o \\ 0 & 1 \end{bmatrix} \Gamma_0(lN) \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix}^{-1} \to \mathcal{H}/\Gamma_0(N)$$

  where the isomorphism is given by $z \to lz$ and the second map is induced by the inclusion

$$\begin{bmatrix} l & o \\ 0 & 1 \end{bmatrix} \Gamma_0(lN) \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix}^{-1} \subseteq \Gamma_0(N).$$

Correspondences induce maps of divisors, let's see it in our case. Let $x \in X_0(N)$, then we can view $\alpha^{-1}(x)$ as a divisor on $X_0(lN)$ as

$$\alpha^{-1}(x) = \sum_{P \in \alpha^{-1}(x)} \mathrm{mult}_P(\alpha) P \in \mathrm{Div}(X_0(lN)).$$

In this sense, $\beta(\alpha^{-1}(x)) \in \mathrm{Div}(X_0(N))$ and we obtain a map

$$\mathrm{Div}(X_0(N)) \xrightarrow{\beta \circ \alpha^{-1}} \mathrm{Div}(X_0(N))$$

given by

$$(E, C) \mapsto \sum_{\substack{D \subseteq E[l] \\ \#D = l}} (E, C \oplus D) \mapsto \sum_{\substack{D \subseteq E[l] \\ \#D = l}} (E, (C \oplus D)/D).$$

Another equation that we will use in the proof of Proposition 4.2.7 involves the reduction modulo l of T_l. One can prove that if $l \nmid N$, then $X_0(N)$ has good reduction at l, i.e. the curve $\overline{X_0(N)}$ obtained reducing modulo l the equation of $X_0(N)$ is nonsingular. In this sense we obtain an action on $\mathrm{Div}(\overline{X_0(N)})$

$$\overline{\mathrm{T}_l} : \mathrm{Div}(\overline{X_0(N)}) \to \mathrm{Div}(\overline{X_0(N)}).$$

Proposition 4.2.10. *The reduction of the Hecke operator* T_l *admits the decomposition*

$$\overline{\mathrm{T}_l} = \mathrm{Fr}_l + \mathrm{Fr}_l^t$$

where Fr_l *is the* l*-th Frobenius and* Fr_l^t *is its transpose. In other words, for all* $\overline{P} \in \overline{X_0(N)}$

$$\overline{\mathrm{T}_l}([\overline{P}]) = [\mathrm{Fr}_l(\overline{P})] + l[\overline{Q}]$$

where $\overline{Q} \in \overline{X_0(N)}$ *satisfies* $\mathrm{Fr}(\overline{Q}) = \overline{P}$.

Now we are ready for the proof of Proposition 4.2.7.

Proof of Proposition 4.2.7. Doing explicit calculation one can check that we have, at the level of divisors of $X_0(N)$, an equality

$$\mathrm{Tr}_l(x_n) = \mathrm{T}_l(x_m) \in \mathrm{Div}(X_0(N)).$$

Moreover, by Theorem 2.3.22 T_l, acts on E as multiplication by a_l and applying the modular parametrization, we have

$$a_l y_m = a_l \psi(x_m) = \psi(\mathrm{T}_l(x_m)) = \psi(\mathrm{Tr}_l(x_n)) = \mathrm{Tr}_l(\psi(x_n)) = \mathrm{Tr}_l(y_m).$$

Then we have proved (a).

Recall that by Remark 3.4.22 if λ_m is a prime ideal of K_m lying over l then it totally ramifies in K_n. In particular, if λ_n is the unique prime ideal of K_n lying over λ_m, then the residue fields coincide, that is

$$\mathbb{F}_{\lambda_n} \cong \mathbb{F}_{\lambda_m} \cong \mathbb{F}_{\lambda} \cong \mathbb{F}_{l^2}.$$

By Proposition 4.2.10 we have the congruence

$$\mathrm{T}_l \equiv \mathrm{Fr}_l + \mathrm{Fr}_l^t \pmod{l}.$$

Hence, passing modulo λ_n we have

$$\mathrm{T}_l(x_m) \equiv \mathrm{Fr}_l(x_m) + \mathrm{Fr}_l^t(x_m) \pmod{\lambda_n}.$$

In particular, there exists at least a point of the divisor $\mathrm{T}_l(x_m)$ that is equal to $\mathrm{Fr}_l(x_m) = \mathrm{Frob}_{(K_m/\mathbb{Q})}(\lambda_m)(x_m)$ modulo λ_n. On the other hand, from part (a), we know that

$$\mathrm{T}_l(x_m) = \mathrm{Tr}_l(x_n) = \sum_{\sigma \in \mathrm{Gal}(K_n/K_m)} \sigma(x_n).$$

Since λ_m is totally ramified in K_n, all the $\sigma(x_n)$'s are congruent to x_n modulo λ_n, so by the previous discussion we have that

$$x_n \equiv \mathrm{Frob}_{K_m/\mathbb{Q}}(\lambda_m)(x_m) \pmod{\lambda_n}.$$

Finally, applying the modular parametrization, we obtain the desired result. □

Now we are going to use the Euler system to construct cohomology classes in $H^1(G_K, E[p])$. Recall that by Remark 4.2.6

$$G_l = \mathrm{Gal}(K_l/K_1) \cong \mathrm{Gal}(K_n/K_m) \leq \mathrm{Gal}(K_n/K_1) = G_n$$

is a cyclic subgroup of order $l+1$ and let σ_l be a fixed generator.

Definition 4.2.11. *The augmentation ideal of the group ring $\mathbb{Z}[G_l]$ is the kernel of the map $\sum_{\sigma \in G_l} n_\sigma \sigma$.*

Note that, with notation above, the augmentation ideal is principal and generated by $\sigma - 1$ where $1 \in G_l$ is the identity. Indeed, the augmentation ideal is clearly generated by the element of the form $\sigma - \sigma'$, with $\sigma, \sigma' \in G_l$. This is exactly the set of elements of $\mathbb{Z}[G_l]$ of the form $\sigma - 1$ and the ideal generated by this set is the ideal $(\sigma_l - 1)$.

Definition 4.2.12. *We define D_l as the solution in $\mathbb{Z}[G_l]$ of the equation*

$$(\sigma_l - 1)X = l + 1 - \mathrm{Tr}_l. \tag{4.3}$$

Remark 4.2.13. *Note that a solution exists. For example Kolyvagin takes*

$$D_l^0 = \sum_{i_1}^{l} i \cdot \sigma_l^i = -\sum_{i=1}^{l+1} \frac{\sigma_l^i - 1}{\sigma_l - 1}.$$

Indeed:

$$(\sigma_l - 1) \cdot D_l^0 = -\sum_{i=1}^{l+1} (\sigma_l^i - 1) = l + 1 - \sum_{i=1}^{l+1} \sigma_l^i = l + 1 - \mathrm{Tr}_l.$$

Remark 4.2.14. *The solution D_l is well defined up to addition of elements in $\mathbb{Z}\mathrm{Tr}_l$. In fact, let $\sum_{i=0}^{l} n_i\sigma_l^i$ be a generic element of $\mathbb{Z}[G_l]$ and suppose that*

$$(\sigma_l - 1)\cdot\sum_{i=0}^{l} n_i\sigma_l^i = 0$$

or equivalently, that

$$\sum_{i=0}^{l} n_{-1}\sigma_l^i - \sum_{i=0}^{l} n_i\sigma_l^i = \sum_{i=0}^{l}(n_{i-1}-n_i)\sigma_l^i = 0$$

where $n_{-1} := n_l$. Then $n_i = n_{i-1}$ for all $i = 0,\dots,l$ that is

$$\sum_{i=0}^{l} n_i\sigma_l^i = k\mathrm{Tr}_l$$

for some $k \in \mathbb{Z}$. If we now have $D_l, D_l' \in \mathbb{Z}[G_l]$ satisfying 4.3, then

$$(\sigma_l - 1)\cdot(D_l - D_l') = 0$$

and by the previous discussion

$$D_l' = D_l + k\mathrm{Tr}_l$$

for some $k \in \mathbb{Z}$.

Definition 4.2.15. *Let $n \in \mathcal{R}$ and fix a solution $D_l \in \mathbb{Z}[G_l]$ for all prime factor $l \mid n$. We define D_n as the product*

$$D_n = \prod_{l|n} D_l \in \mathbb{Z}[G_n].$$

Proposition 4.2.16. *Let $n \in \mathcal{R}$. The point $D_n(y_n) \in E(K_n)$ gives a class $[D_n(y_n)] \in E(K_m)/pE(K_n)$ which is fixed by G_n.*

Proof. It suffices to show that for all $l \mid n$, $[D_n(y_n)]$ is fixed by the generator σ_l of G_l. In other words, we have to show that

$$(\sigma_l - 1)\cdot D_n(y_n) \in pE(K_n).$$

Note that

$$(\sigma_l - 1)\cdot D_n = (\sigma_l - 1)\cdot D_l \cdot D_m = (l + 1 - \mathrm{Tr}_l)\cdot D_m \in \mathbb{Z}[G_n].$$

Hence in y_n we have that

$$\begin{aligned}(\sigma_l - 1)\cdot D_n(y_n) &= (l+1)\cdot D_m(y_n) - D_m(\mathrm{Tr}_l(y_n)) \\ &= (l+1)\cdot D_m(y_n) - a_l\cdot D_m(y_m).\end{aligned}$$

where the last equality is guaranteed by Proposition 4.2.7. Finally, from Proposition 4.2.3 we have that

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

and the claim follows. □

Now we are ready to define the family $\{P_n\}_n$ where the index n runs over $\mathcal{R}$. Consider the exact sequence of groups

$$0 \to G_n \longrightarrow \mathcal{G}_n \longrightarrow \mathrm{Gal}(K_1/K) \to 0$$

and let S be a complete set of representatives for G_n in $\mathcal{G}_n$.

Definition 4.2.17. *We define*

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

with the request that if $m \mid n$, then we use the same set S to define P_m

Note that when $n = 1$, we recover the point $y_K \in E(K)$. Indeed, in this case we have

- $G_1 = \{1\}$,
- $\mathcal{G}_n = \mathrm{Gal}(K_1/K)$,
- $S = \mathcal{G}_1$.

Thus

$$P_1 = \sum_{\sigma \in \mathcal{G}_1} \sigma(D_1(y_1)) = \sum_{\sigma \in \mathcal{G}_1} \sigma(y_1) = \mathrm{Tr}_{K_1/K}(y_1) = y_K.$$

Proposition 4.2.18. *Let $n \in \mathcal{R}$. The point $P_n \in E(k_n)$ defines a class $[P_n] \in E(k_n)/pE(k_n)$ which is fixed by the action of the Galois group $\mathcal{G}_n = \mathrm{Gal}(k_n/K)$.*

Proof. Let $g \in \mathcal{G}_n$ and let S be a fixed complete set of representatives for the cosets of G_n in $\mathcal{G}_n$. By elementary group theory, the set

$$S' = gS = \{g \circ \eta : \eta \in S\}$$

is still a complete set of representatives for G_n in $\mathcal{G}_n$. By the definition of P_n, we have:

$$g(P_n) = g\left(\sum_{\eta \in S} \eta(D_n y_n)\right) = \sum_{\eta \in S} (g \circ \eta)(D_n y_n) = \sum_{\eta' \in S'} \eta'(D_n y_n).$$

By the property of coset representatives, for each $\eta' \in S'$ there exists a unique $\eta \in S$ such that $\eta' = \eta \circ \gamma_{\eta'}$ for some $\gamma_{\eta'} \in G_n$. Substituting this into the summation, we obtain:

$$g(P_n) = \sum_{\eta \in S} (\eta \circ \gamma_{\eta'})(D_n y_n) = \sum_{\eta \in S} \eta\big(\gamma_{\eta'}(D_n y_n)\big).$$

By Proposition 4.2.16, the class of $D_n y_n$ is fixed by G_n modulo $pE(k_n)$, which means $\gamma_{\eta'}(D_n y_n) = D_n y_n + pQ_{\eta'}$ for some $Q_{\eta'} \in E(k_n)$. Since η is an automorphism of $E(k_n)$, it maps $pE(k_n)$ into itself. Thus:

$$g(P_n) = \sum_{\eta \in S} \eta(D_n y_n + pQ_{\eta'}) = \sum_{\eta \in S} \eta(D_n y_n) + p \sum_{\eta \in S} \eta(Q_{\eta'}) \equiv P_n \pmod{pE(k_n)}.$$

This shows that the class $[P_n]$ is invariant under the action of $\mathcal{G}_n$. □

The family $\{P_n\}_{n\in\mathcal{R}}$ plays a crucial role in defining the cohomology classes $\{c(n)\}_{n\in\mathcal{R}}$. For this purpose, we construct an important commutative diagram. To begin with, consider the isogeny $[p] : E \to E$. Recall from section 2.4 that the short exact sequence

$$0 \to E[p] \longrightarrow E \xrightarrow{[p]} E \to 0 \tag{4.4}$$

induces the kummer sequence

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\kappa} H^1(G_K, E[p]) \longrightarrow H^1(G_K, E)[p] \longrightarrow 0.$$

In the same way, taking the Galois cohomology with respect to

$$G_{K_n} = \mathrm{Gal}(\overline{K_n}/K_n) = \mathrm{Gal}(\overline{K}/K_n)$$

to the sequence 4.4, we obtain the short exact sequence

$$0 \longrightarrow E(K_n)/pE(K_n) \xrightarrow{\kappa_n} H^1(G_{K_n}, E[p]) \longrightarrow H^1(G_{K_n}, E)[p] \longrightarrow 0.$$

Finally, applying the left-exact functor $(\cdot)^{\mathcal{G}_n}$ to the latter sequence, we obtain the exact sequence

$$0 \longrightarrow (E(K_n)/pE(K_n))^{\mathcal{G}_n} \xrightarrow{\kappa_n} H^1(G_{K_n}, E[p])^{\mathcal{G}_n} \longrightarrow H^1(G_{K_n}, E)[p]^{\mathcal{G}_n}.$$

Recall that the short exact sequence of Galois group acting on E

$$0 \to G_{K_n} \longrightarrow G_K \longrightarrow \mathrm{Gal}(K_n/K) \to 0$$

induces the inflation–restriction sequence

$$0 \to H^1(\mathrm{Gal}(K_n/K), E) \xrightarrow{\mathrm{inf}} H^1(G_K, E) \xrightarrow{\mathrm{res}} H^1(G_{K_n}, E).$$

Putting all these sequences together, we finally obtain the following commutative diagram with exact rows and column

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(\mathcal{G}_n, E(K_n))[p] & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{inf}} & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\kappa} & H^1(G_K, E[p]) & \longrightarrow & H^1(G_K, E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\kappa_n} & H^1(G_{K_n}, E[p])^{\mathcal{G}_n} & \longrightarrow & H^1(G_{K_n}, E)[p]^{\mathcal{G}_n}. & &
\end{array} \tag{4.5}$$

Note that the image of the map $\mathrm{res} : H^1(G_K, E[p]) \to H^1(G_{K_n}, E[p])$ is fixed by $\mathcal{G}_n$ by the Hochschild–Serre sequence. Moreover, we want to prove that it is an isomorphism.

Lemma 4.2.19. *E has no p-torsion rational over K_n.*

Proof. Suppose that $E(K_n)[p] \neq 0$. then there are only two possibilities:

- $E(K_n)[p] \cong \mathbb{F}_p$. In this case we have a tower of $\mathbb{F}_p$-subspaces of $E[p]$

$$1 \leq \mathbb{F}_p \cong E(K_n)[p] \leq \mathbb{F}_p^2 = E[p].$$

  Since $K_n/\mathbb{Q}$ is Galois and hence normal, then $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ has to preserve this tower of subspaces, but this cannot happen since in our hypothesis $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

- $E(K_n)[p] \cong \mathbb{F}_p^2$. In this case the entire p-torsion of E is K_n-rational, that is $\mathbb{Q}(E[p]) \subseteq K_n$. Thus, as observed in Remark 4.1.8, we have

$$\mathrm{GL}_2(\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{Gal}(K(E[p])/K) \cong \frac{\mathcal{G}_n}{\mathrm{Gal}(K_n/K(E[p]))}.$$

  In other words, we have a surjective homomorphism

$$\mathcal{G}_n \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

  and this is impossible whenever $p > 2$.

□

It follows immediately from Lemma 4.2.19 that

$$\mathrm{res} : H^1(G_K, E[p]) \to H^1(G_{K_n}, E[p])$$

is an isomorphism. Indeed, writing the Hochschild–Serre sequence

$$0 \longrightarrow H^1(\mathcal{G}_n, E(K_n)[p]) \xrightarrow{\inf} H^1(G_K, E[p])$$

$$\xrightarrow{\mathrm{res}} H^1(G_{K_n}, E[p])^{\mathcal{G}_n} \longrightarrow H^2(\mathcal{G}_n, E(K_n)[p]) \longrightarrow H^2(G_K, E[p])$$

we note by Lemma 4.2.19 that

$$H^1(\mathcal{G}_n, E(K_n)[p]) = H^2(\mathcal{G}_n, E(K_n)[p]) = 0$$

i.e. the restriction map is an isomorphism.

We can now rewrite the diagram by incorporating the isomorphism just obtained, and finally define the cohomology classes.

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & & & & & H^1(\mathcal{G}_n, E(K_n))[p] & & \\ & & & & & & \downarrow{\scriptstyle \inf} & & \\ 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\kappa} & H^1(G_K, E[p]) & \longrightarrow & H^1(G_K, E)[p] & \longrightarrow & 0 \\ & & \downarrow & & \wr\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\ 0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\kappa_n} & H^1(G_{K_n}, E[p])^{\mathcal{G}_n} & \longrightarrow & H^1(G_{K_n}, E)[p]^{\mathcal{G}_n}. & & \end{array} \tag{4.6}$$

Definition 4.2.20. *Let $n \in \mathcal{R}$. We define*

- $c(n) \in H^1(G_K, E[p])$ *the unique element such that* $\mathrm{res}(c(n)) = \kappa_n([P_n])$*;*
- $d(n) \in H^1(G_K, E)[p]$ *as the image of* $c(n)$*;*
- $\tilde{d}(n) \in H^1(\mathcal{G}_n, E)[p]$ *such that* $\inf(\tilde{d}(n)) = d(n)$.

Note that by the commutativity of the diagram and by the exactness of rows and columns $\tilde{d}(n)$ is well defined. Directly from the construction we deduce the following.

Proposition 4.2.21. *(a) The class $c(n) \in H^1(G_K, E[p])$ is trivial if and only if $P_n \in pE(K_n)$.*

(b) The classes $d(n) \in H^1(G_K, E)[p]$ and $\tilde{d}(n) \in H^1(\mathcal{G}_n, E)[p]$ are trivial if and only if $P_n \in pE(K_n) + E(K)$.

Proof. (a) By definition, $c(n)$ is the image of $\kappa_n(P_n)$ under the inverse of the restriction map (which is an isomorphism in this context). Thus, $c(n) = 0$ if and only if $\kappa_n(P_n) = 0$ in $H^1(G_{K_n}, E[p])$. By the injectivity of the local Kummer map $\kappa_n \colon E(K_n)/pE(K_n) \to H^1(G_{K_n}, E[p])$, this is equivalent to $P_n = 0$ in $E(K_n)/pE(K_n)$, which means $P_n \in pE(K_n)$.

(b) Since the inflation map $\inf \colon H^1(\mathcal{G}_n, E(K_n)) \to H^1(G_K, E)$ is injective, we have

$$d(n) = 0 \iff \tilde{d}(n) = 0.$$

Consider the following part of the diagram 4.6:

$$\begin{array}{ccc} E(K)/pE(K) & \xrightarrow{\kappa} & H^1(G_K, E[p]) \\ \downarrow & & \downarrow \mathrm{res} \\ (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\kappa_n} & H^1(G_{K_n}, E[p])^{\mathcal{G}_n} \end{array}$$

The class $d(n)$ is defined as the image of $c(n)$ in $H^1(G_K, E)[p]$. From the exactness of the Kummer sequence

$$0 \to E(K)/pE(K) \xrightarrow{\kappa} H^1(G_K, E[p]) \to H^1(G_K, E)[p] \to 0,$$

we have $d(n) = 0$ if and only if $c(n) \in \mathrm{im}(\kappa)$. By the commutativity of the diagram and the fact that res is an isomorphism, this is equivalent to $\kappa_n(P_n)$ being in the image of $E(K)/pE(K)$ via the map $\kappa_n \circ \mathrm{res}$. This happens if and only if $P_n \in pE(K_n) + E(K)$ as an element of $E(K_n)$. □

Remark 4.2.22. *William McCallum found a concrete description for the classes we have just constructed. More precisely, he observed that the class $c(n)$ is represented by the 1-cocycle*

$$f : G_K \to E[p], \quad \sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma-1)P_n}{p}$$

and the class $\tilde{d}(n)$ by

$$\tilde{f} : \mathcal{G}_n \to E, \quad \sigma \mapsto -\frac{(\sigma-1)P_n}{p}.$$

4.3 Preliminaries for the proof of theorem 4.1.7

In the last section we have introduced a family $\{c(n)\}_{n\in\mathcal{R}}$ of cohomology classes in $H^1(G_K, E[p])$ and now the goal is to study their properties. Recall that, in order to prove Theorem 4.1.1 we want to show that if p is an odd prime such that

- $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$,
- $p \nmid D$,
- $y_K \notin pE(K)$,

then the Selmer group $\mathrm{Sel}(E/K)[p]$ is cyclic generated by the image of the class of y_K under the Kummer map. To this end, we decompose the Selmer group into eigenspaces under the action of an involution. We then establish that one eigenspace is trivial, whereas the other is cyclic, generated by $\kappa(y_K)$.

Let τ be the complex conjugation, or equivalently, the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and consider the following action on $\mathrm{Sel}(E/K)[p]$

$$\tau : \mathrm{Sel}(E/K)[p] \longrightarrow \mathrm{Sel}(E/K)[p], \quad [\eta] \mapsto \tau \cdot [\eta] := [\tau \cdot \eta]$$

where $(\tau \cdot \eta)(\sigma) = \tau(\eta(\tau^{-1}\sigma\tau)) \in E[p]$ for all $\sigma \in G_K$. Since $\tau^2 = 1$, then its action on $\mathrm{Sel}(E/K)[p]$ is clearly an involution and we obtain a decomposition

$$\mathrm{Sel}(E/K)[p] = \mathrm{Sel}(E/K)[p]^+ \oplus \mathrm{Sel}(E/K)[p]^-.$$

The existence of a such decomposition is guaranteed by the following general lemma.

Lemma 4.3.1. *Let G be an abelian group endowed with an action of an involution τ such that the multiplication-by-2 map $[2]$ is invertible in $\mathrm{End}(G)$. then we can decompose G as*

$$G = G^+ \oplus G^-$$

where $G^\alpha = \{g \in G : \tau \cdot g = \alpha g\}$ for $\alpha \in \{\pm 1\}$.

Remark 4.3.2. *Note that in our hypotheses* $\mathrm{Sel}(E/K)[p]$ *is a finite dimensional* $\mathbb{F}_p$*-vector space and* p *is odd. Then* $[2] \in \mathrm{End}(\mathrm{Sel}(E/K)[p])$ *is invertible and we can apply the Lemma.*

Let f be the newform associated with E via Eichler–Shimura theory. Following the results of Section 2.3, we let $\epsilon \in \{\pm 1\}$ be the eigenvalue of f under the Atkin–Lehner involution, so that $f \in \mathcal{S}_2(\Gamma_0(N))^\epsilon$. With this notation, it is useful for our purpose to write the decomposition as

$$\mathrm{Sel}(E/K)[p] = \mathrm{Sel}(E/K)[p]^{-\epsilon} \oplus \mathrm{Sel}(E/K)[p]^{\epsilon}.$$

4.3.1 A generalization of the Selmer group

For a more precise study of the family $\{c(n)\}_{n\in\mathcal{R}}$ we need to generalize the Selmer group. Let T be a finite dimensional $\mathbb{F}_p$-vector space vith a discrete action of G_K (for example one can take $T = E[p]$). Note that if $v \in M_K$ is a place of K, then the restriction map

$$G_{K_v} \to G_K, \quad \sigma \mapsto \sigma|_{\overline{K}}$$

induces via composition an action on T. In this sense we can consider

$$H^1(G_K, T), \quad H^1(G_{K_v}, T).$$

Recall that

$$\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \cong \frac{\mathrm{Gal}(\overline{K_v}/K_v)}{\mathrm{Gal}(\overline{K_v}/K_v^{\mathrm{ur}})} = \frac{G_{K_v}}{I_v}$$

where I_v is the inertia group.

Definition 4.3.3. *Let* $v \in M_K$ *be a place of* K*.*

- *A local Selmer structure* $\mathcal{F}$ *fot* T *is a vector subspace* $H^1_{f,\mathcal{F}}(G_{K_v}, T)$ *of* $H^1(G_{K_v}, T)$*.*
- *The singular quotient of* $H^1_{f,\mathcal{F}}(G_{K_v}, T)$ *is the quotient*

$$H^1_{s,\mathcal{F}}(G_{K_v}, T) := H^1(G_{K_v}, T)/H^1_{f,\mathcal{F}}(G_{K_v}, T).$$

- *The unramified structure at* v *is the local Selmer structure*

$$H^1_{f,\mathcal{F}}(G_{K_v}, T) := H^1(\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v), T^{I_v}).$$

Remark 4.3.4. *It follows directly from the definition that the sequence*

$$0 \mapsto H^1_{f,\mathcal{F}}(G_{K_v}, T) \longrightarrow H^1(G_{K_v}, T) \longrightarrow H^1_{s,\mathcal{F}}(G_{K_v}, T) \to 0$$

is exact. Moreover, in the case of the unramified structure, the previous exact sequence becomes the following inflation–restriction sequence:

$$0 \to H^1(G^{\mathrm{ur}}_{K_v}, T^{I_v}) \xrightarrow{\mathrm{inf}} H^1(G_{K_v}, T) \xrightarrow{\mathrm{res}} H^1(I_v, T)^{G^{\mathrm{ur}}_{K_v}} \to 0$$

where $G^{\mathrm{ur}}_{K_v} := G_{K_v}/I_v \cong \mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$*.*

Given a local Selmer structure $\mathcal{F}$, we now proceed to construct a corresponding dual object $\mathcal{F}^*$. To begin with, we consider the $\mathbb{F}_p$ vector space $\boldsymbol{\mu}_p$ of the p-th roots of unity in $\overline{K_v}$ and we give the following.

Definition 4.3.5. *With notation above, we define:*

- $T^* := \mathrm{Hom}_{\mathbb{F}_p}(T, \boldsymbol{\mu}_p)$;
- *the cup product pairing is*

$$\cup : H^1(G_{K_v}, T) \otimes_{\mathbb{F}_p} H^1(G_{K_v}, T^*) \longrightarrow H^2(G_{K_v}, T \otimes_{\mathbb{F}_p} T^*)$$

given by

$$(\eta \cup \psi)(\sigma_1, \sigma_2) := \eta(\sigma_1) \otimes \sigma_1 \cdot \psi(g_2).$$

Note that the evaluation map

$$\mathrm{ev} : T \otimes_{\mathbb{F}_p} T^* \to \boldsymbol{\mu}_p, \quad x \otimes \varphi \mapsto \varphi(x)$$

induces a map in cohomology

$$\mathrm{ev} \circ (\cdot) : H^2(G_{K_v}, T \otimes_{\mathbb{F}_p} T^*) \longrightarrow H^2(G_{K_v}, \boldsymbol{\mu}_p)$$

and we can consider the composition

$$H^1(G_{K_v}, T) \otimes_{\mathbb{F}_p} H^1(G_{K_v}, T^*) \xrightarrow{\cup} H^2(G_{K_v}, T \otimes_{\mathbb{F}_p} T^*) \xrightarrow{\mathrm{ev}\circ(\cdot)} H^2(G_{K_v}, \boldsymbol{\mu}_p).$$

This is what we will call the Tate pairing. Before giving its definition, however, we slightly simplify the situation.

Lemma 4.3.6. *We have*

$$H^2(G_{K_v}, \boldsymbol{\mu}_p) \cong \mathbb{F}_p.$$

Proof. Taking the G_{K_v}-cohomology of the exact sequence of abelian group

$$0 \to \boldsymbol{\mu}_p \longrightarrow \left(\overline{K_v}\right)^\times \xrightarrow{(\cdot)^p} \left(\overline{K_v}\right)^\times \to 0$$

we obtain the long exact sequence

$$H^1\left(G_{K_v}, \overline{K_v}^\times\right) \to H^2\left(G_{K_v}, \boldsymbol{\mu}_p\right) \to H^2\left(G_{K_v}, \overline{K_v}^\times\right) \xrightarrow{(\cdot)^p} H^2\left(G_{K_v}, \overline{K_v}^\times\right).$$

Note that by Hilbert's Theorem 90, the first term is 0:

$$H^1\left(G_{K_v}, \overline{K_v}^\times\right) = 0.$$

Hence, by the exactness

$$H^2(G_{K_v}, \boldsymbol{\mu}_p) \cong \mathrm{Ker}\,((\cdot)^p) \cong \frac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \mathbb{F}_p$$

where the second isomorphism is due to the fact that

$$H^2\left(G_{K_v}, \overline{K_v}^\times\right) \cong \mathbb{Q}/\mathbb{Z}.$$

For more details, see [Mil11, Chapter 3]. □

Using the previous lemma we can give the following.

Definition 4.3.7. *The Tate pairing is the map*

$$< \cdot, \cdot >_v \colon H^1(G_{K_v}, T) \otimes_{\mathbb{F}_p} H^1(G_{K_v}, T^*) \longrightarrow \mathbb{F}_p$$

given by the composition

$$(\mathrm{ev} \circ (\cdot)) \circ \cup : H^1(G_{K_v}, T) \otimes_{\mathbb{F}_p} H^1(G_{K_v}, T^*) \longrightarrow H^2(G_{K_v}, \boldsymbol{\mu}_p) \cong \mathbb{F}_p$$

Proposition 4.3.8. *The Tate pairing is perfect. Moreover, let $v \in M_K^0$ a finite place of K and let $(l) = v \cap \mathbb{Z}$. If $l \neq p$, then $H^1(G_{K_v}^{\mathrm{ur}}, T)$ and $H^1(G_{K_v}^{\mathrm{ur}}, T^*)$ are exact orthogonal complements under the Tate pairing.*

Proof. See [Mil06, Chapter 3]. □

Definition 4.3.9. *Given a local Selmer structure $\mathcal{F}$ on T, we define its Cartier dual local Selmer structure $\mathcal{F}^*$ on T^* as the orthogonal complement $H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*)$ with respect to the Tate pairing. In other words*

$$H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*) = \{\psi \in H^1(G_{K_v}, T^*) :< \eta, \psi >_v = 0 \text{ for all } \eta \in H^1_{f,\mathcal{F}}(G_{K_v}, T)\}.$$

Remark 4.3.10. *Denote by $V^\vee = \mathrm{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p)$ the dual space of a $\mathbb{F}_p$-vector space V. Then the Tate pairing induces a perfect pairing*

$$H^1_{s,\mathcal{F}}(G_{K_v}, T) \otimes_{\mathbb{F}_p} H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*) \longrightarrow \mathbb{F}_p$$

and the resulting isomorphism

$$H^1_{s,\mathcal{F}}(G_{K_v}, T) \cong H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*)^\vee.$$

The local Selmer structures defined above serve as the building blocks for the global theory. Specifically, a global Selmer structure $\mathcal{F}$ on T is obtained by a collection of such local conditions, which in turn determines a subspace of the global Galois cohomology group $H^1(G_K, T)$.

Definition 4.3.11. *A global Selmer structure is a collection*

$$\{H^1_{f,\mathcal{F}}(G_{K_v}, T)\}_{v \in M_K}$$

of local Selmer structure, such that $H^1_{f,\mathcal{F}}(G_{K_v}, T)$ is the unramified structure at v for almost all $v \in M_K$. Given a global Selmer structure $\mathcal{F}$ on T $\{H^1_{f,\mathcal{F}}(G_{K_v}, T)\}_v$, the Selmer group is the subspace of $H^1(G_K, T)$ defined by

$$\mathrm{Sel}_{\mathcal{F}}(K, T) := \{c \in H^1(G_K, T) : c_v \in H^1_{f,\mathcal{F}}(G_{K_v}, T) \text{ for all } v \in M_K\}.$$

Here, the element c_v denotes the image of c under the restriction map

$$H^1(G_K, T) \to H^1(G_{K_v}, T).$$

Returning to our setting with $T = E[p]$, the following definitions determine the local Selmer structure used to recover the classical Selmer group $\mathrm{Sel}(E/K)[p]$. Recall that for each place v of K we have the Kummer local map

$$\kappa_v : E(K_v)/pE(K_v) \hookrightarrow H^1(G_{K_v}, E[p]).$$

Definition 4.3.12. *We define*

- *the geometric local Selmer structure at v $\mathcal{F}$ on $E[p]$ as*

$$H^1_{f,\mathcal{F}}(G_{K_v}, E[p]) := \mathrm{Im}(\kappa_v) \subseteq H^1(G_{K_v}, E[p]);$$

- *the geometric global Selmer structure $\mathcal{F}$ on $E[p]$ as the collection of all the geometric local Selmer structures on $E[p]$.*

Remark 4.3.13. *Note that by the Kummer sequence, $Im(\kappa_v)$ is a subspace of $H^1(G_{K_v}, E[p])$ and it coincides to the unramified local structure for each $v \in M_K$ such that $E[p]$ is unramified at v. But by Proposition 1.3.19 this happens for each place v of K where E has good reduction and such that $\gcd(p, \mathrm{Char}(\mathbb{F}_v)) = 1$, where $\mathbb{F}_v$ is the residue field of the local field K_v. In other words $Im(\kappa_v)$ coincides to the unramified structure for almost all place of K. Moreover, the geometric global Selmer structure gives*

$$\begin{aligned}\mathrm{Sel}_{\mathcal{F}}(K, E[p]) &= \{c \in H^1(G_K, E[p]) : c_v \in H^1_{f,\mathcal{F}}(G_{K_v}, E[p]) \text{ for all } v \in M_K\} \\ &= \{c \in H^1(G_K, E[p]) : c_v \in \mathrm{Im}(\kappa_v) \text{ for all } v \in M_K\} \\ &= \mathrm{Ker}(F) \\ &= \mathrm{Sel}(E/K)[p]\end{aligned}$$

where F is the map apperaring in the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\varphi(E(K)) & \xrightarrow{\kappa} & H^1(G_K, E[\varphi]) & \longrightarrow & H^1(G_K, E)[\varphi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{F}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & \prod_v E'(K_v)/\varphi(E(K_v)) & \longrightarrow & \prod_v H^1(G_{K_v}, E[\varphi]) & \longrightarrow & \prod_v H^1(G_{K_v}, E)[\varphi] & \longrightarrow & 0 \end{array} \tag{4.7}$$

We now proceed to a further generalization. Nevertheless, we keep in mind that in our setting T will be the $\mathbb{F}_p$-vector space $E[p]$, and in what follows we will identify the finite places of K with the corresponding prime ideals.

Definition 4.3.14. *Fix a global Selmer structure $\mathcal{F}$ on T and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. We define:*

- $\mathrm{Sel}_{\mathfrak{a}}(K, T) := \left\{c \in H^1(G_K, T) : c_v \in H^1_{f,\mathcal{F}}(G_{K_v}, T) \text{ for all } v \nmid \mathfrak{a}\right\}$;
- $\mathrm{Sel}^{\mathfrak{a}}(K, T^*) := \left\{c \in H^1(G_K, T^*) : c_v \in H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*) \text{ for all } v, \text{ and } c_v = 0 \text{ if } v \mid \mathfrak{a}\right\}$.

Note that it follows from the definition that

$$\mathrm{Sel}(G_K, E)[p] = \mathrm{Sel}_{\mathcal{F}}(K, E[p]) = \mathrm{Sel}_{\mathcal{O}_K}(K, E[p])$$

where $\mathcal{F}$ is the geometric global Selmer structure on $E[p]$. More generally, for a $\mathbb{F}_p$-vector space T, one has

$$\mathrm{Sel}_{\mathcal{F}}(K, T) = \mathrm{Sel}_{\mathcal{O}_K}(K, T) \quad \text{and} \quad \mathrm{Sel}_{\mathcal{F}^*}(K, T^*) = \mathrm{Sel}^{\mathcal{O}_K}(K, T^*).$$

Furthermore, if $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and T is the G_K-module under consideration, we obtain the following short exact sequences, whose exactness is immediate from the definition.

$$0 \longrightarrow \mathrm{Sel}_{\mathcal{F}}(K, T) \xrightarrow{d_1} \mathrm{Sel}_{\mathfrak{a}}(K, T) \xrightarrow{d_2} \oplus_{v|\mathfrak{a}} H^1_{s,\mathcal{F}}(G_{K_v}, T)$$

$$0 \longrightarrow \mathrm{Sel}^{\mathfrak{a}}(K, T^*) \xrightarrow{e_1} \mathrm{Sel}_{\mathcal{F}^*}(K, T^*) \xrightarrow{e_2} \oplus_{v|\mathfrak{a}} H^1_{f,\mathcal{F}^*}(G_{K_v}, T^*).$$

Using the isomorphism of Remark 4.3.10, one can splice these exact sequences together to obtain the following long exact sequence:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_{\mathcal{F}}(K, T) & \longrightarrow & \mathrm{Sel}_{\mathfrak{a}}(K, T) & \longrightarrow & \oplus_{v|\mathfrak{a}} H^1_{s,\mathcal{F}}(G_{K_v}, T) \\ & & & & & \swarrow & \\ & & \mathrm{Sel}_{\mathcal{F}^*}(K, T^*)^\vee & \longrightarrow & \mathrm{Sel}^{\mathfrak{a}}(K, T^*)^\vee & \longrightarrow & 0 \end{array} \tag{4.8}$$

4.3.2 Properties of the cohomology classes $c(n)$

Thanks to the generalized notion of Selmer groups introduced in the previous section, we now have the appropriate framework to formalize the local behavior of the cohomology classes $c(n)$. The first step consists in analyzing the action of complex conjugation on the classes $c(n)$, a property that will be crucial in the subsequent arguments.

As in the case of Selmer groups, complex conjugation acts on the entire cohomology group $H^1(G_K, E[p])$, yielding a decomposition analogous to that of the Selmer case

$$H^1(G_K, E[p]) = H^1(G_K, E[p])^{\epsilon} \oplus H^1(G_K, E[p])^{-\epsilon}.$$

Proposition 4.3.15. *Let $n \in \mathcal{R}$ and consider $r := \#\{l \text{ prime factor of } n\}$. Then*

$$c(n) \in H^1(G_K, E[p])^{(-1)^r \epsilon}.$$

Proof. One can chek that the complex conjugation τ acts on $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$ as a conjugation, i.e.

$$\tau\sigma = \sigma^{-1}\tau \text{ for all } \sigma \in \mathcal{G}_n.$$

Hence, if $S \subseteq \mathcal{G}_n$ is a complete set of representatives of G_n in $\mathcal{G}_n$

$$\begin{aligned}\tau(P_n) &= \tau\left(\sum_{\sigma\in S}\sigma D_n(y_n)\right) = \sum_{\sigma\in S}\tau\sigma D_n(y_n) = \sum_{\sigma\in S}\sigma^{-1}\tau D_n(y_n)\\ &= \sum_{\sigma\in S}\sigma^{-1}\tau\prod_{l|n}D_l(y_n) = \sum_{\sigma\in S}\sigma^{-1}\prod_{l|n}\tau D_l(y_n).\end{aligned}$$

We now rewrite the terms $\tau D_l(y_n)$, where $l \mid n$ is a prime factor. Recall that D_l satisfies the relation

$$(\sigma_l - 1)D_l = l + 1 - \mathrm{Tr}_l,$$

where σ_l is a fixed generator of the cyclic group G_l. Since both $(l+1)$ and Tr_l commute with τ, it follows that $(\sigma_l - 1)D_l$ also commutes with τ. Thus, we have

$$\begin{aligned}(\sigma_l - 1)D_l\tau = \tau(\sigma_l - 1)D_l &= (\sigma_l^{-1}\tau - \tau)D_l\\ &= (\sigma_l^{-1} - 1)\tau D_l = -\sigma_l^{-1}(\sigma_l - 1)\tau D_l.\end{aligned}$$

in $\mathbb{Z}[G_l]$. Applying σ_l to the last equality we have

$$\sigma_l(\sigma_l - 1)D_l\tau = -(\sigma_l - 1)\tau D_l$$

that is

$$(\sigma_l - 1)(\sigma_l D_l\tau + \tau D_l) = 0$$

in $\mathbb{Z}[G_l]$. By Remark 4.2.14 this means that

$$\tau D_l = -\sigma_l D_l\tau + k\mathrm{Tr}_l$$

for some $k \in \mathbb{Z}$. Then, applying these operators to y_n, we finally obtain

$$\tau D_l(y_n) = -\sigma_l D_l\tau(y_n) + k\mathrm{Tr}_l(y_n) = -\sigma_l D_l\tau(y_n) + ka_l y_{\frac{n}{l}}$$

where the last equality follows from Proposition 4.2.7. Thus, returning to the computation of $\tau(P_n)$ we have

$$\begin{aligned}\tau(P_n) &= \sum_{\sigma\in S}\sigma^{-1}\prod_{l|n}\tau D_l(y_n)\\ &= \sum_{\sigma\in S}\sigma^{-1}\prod_{l|n}\left(-\sigma_l D_l\tau(y_n) + ka_l y_{\frac{n}{l}}\right)\\ &\equiv (-1)^r\prod_{l|n}\sigma_l\sum_{\sigma\in S}\sigma^{-1}D_n\tau(y_n) \pmod{pE(K_n)}.\end{aligned}$$

where the congruence follows from Proposition 4.2.3. By Proposition 5.3 of [Gro91] there exists $\sigma_0 \in \mathrm{Gal}(K_n/K)$ such that

$$\tau(y_n) = \epsilon\sigma_0(y_n) + (\text{torsion}) \tag{4.9}$$

in $E(K_n)$. Note that if T is a torsion point of order $m \in \mathbb{Z}$ appearing in the equation 4.9, then $\gcd(m, p) = 1$, since by Proposition 4.2.19 $E(K_n)[p] = 0$. Thus

$$pa + bm = 1$$

for some $a, b \in \mathbb{Z}$ and we have

$$T = 1 \cdot T = (pa + bm) \cdot T = p \cdot aT.$$

In other words, we have

$$\tau(y_n) = \epsilon\sigma_0(y_n)$$

in the quotient $E(K_n)/pE(K_n)$. Since $\{\sigma^{-1}\}_{\sigma\in S}$ remains a complete set of representatives for $\mathrm{Gal}(K_n/K)$ and since the class of P_n is fixed by $\mathrm{Gal}(K_n/K)$ in $E(K_n)/pE(K_n)$ (by Proposition 4.2.18), it follows that

$$\begin{aligned}
\tau(P_n) &= \epsilon(-1)^r \prod_{l|n} \sigma_l \, \sigma_0 \sum_{\sigma\in S} \sigma^{-1} D_n(y_n) \\
&= \epsilon(-1)^r \prod_{l|n} \sigma_l \, \sigma_0 P_n \\
&= \epsilon(-1)^r \prod_{l|n} \sigma_l P_n \\
&= \epsilon(-1)^r P_n
\end{aligned}$$

in $E(K_n)/pE(K_n)$, where the last equality follows from the inclusions

$$G_l \subseteq \mathcal{G}_l \subseteq \mathcal{G}_n.$$

Finally, since the maps of the diagram 4.6 preserves the action of τ, we conclude. □

Recall that, under our hypotheses, every prime factor of $n \in \mathcal{R}$ is inert in K (cf. Remark 4.2.2). The following proposition is fundamental to characterizing the local behavior of the resulting cohomology classes.

Proposition 4.3.16. *Let $n = l_1 \cdots l_r \in \mathcal{R}$, let $\lambda_i := l_i\mathcal{O}_K$ for all $i \in \{1, \ldots, r\}$, and let $\mathfrak{a} := \lambda_1 \cdots \lambda_r$. Then $c(n) \in \mathrm{Sel}_{\mathfrak{a}}(K, E[p])$.*

Proof. We have to prove that for each place v of K which does not divide $\mathfrak{a}$, the class $[c(n)]_v$ in $H^1_{s,\mathcal{F}}(G_{K_v}, E[p])$ is trivial. We have three cases for v.

- $v = \infty$. In this case $K_v = \mathbb{C}$ and then

$$G_{K_v} = \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\}$$

that is $H^1(G_{K_v}, E[p]) = \{0\}$ regardless of the vector space $E[p]$.

- v is a finite place at which E has good reduction. In this case, since $v \nmid p$, the set $E[p]$ is unramified by Proposition 1.3.19, that is I_v acts trivially on $E[p]$. Then the local geometric structure is the unramified one and we have

$$\begin{aligned} H^1_{s,\mathcal{F}}(G_{K_v}, E[p]) &= \frac{H^1(G_{K_v}, E[p])}{H^1_{f,\mathcal{F}}(G_{K_v}, E[p])} = \frac{H^1(G_{K_v}, E[p])}{H^1(G^{\mathrm{ur}}_{K_v}, E[p]^{I_v})} \\ &\cong H^1(I_v, E[p])^{G^{\mathrm{ur}}_{K_v}} = \mathrm{Hom}(I_v, E[p])^{G^{\mathrm{ur}}_{K_v}} \end{aligned}$$

  where the isomorphism follows from Remark 4.3.4 and the last equality from Remark 2.4.4. Now let ω be a place of K_n lying over v. Thanks to the characterization of the extension K_n/K (cf. Theorem 3.4.9) and since v does not divide the conductor n of the extension, v does not ramify in K_n. In other words, $(K_n)_\omega/K_v$ is unramified. This implies that $(K_n)^{\mathrm{ur}}_\omega = K^{\mathrm{ur}}_v$ and since we can suppose $\overline{(K_n)_\omega} = \overline{K_v}$, we have

$$I_\omega = \mathrm{Gal}(\overline{(K_n)_\omega}/(K_n)^{\mathrm{ur}}_\omega) = \mathrm{Gal}(\overline{K_v}/K^{\mathrm{ur}}_v) = I_v.$$

  Then we have the following commutative diagram with exact rows

$$\begin{array}{ccccc} E(K_v)/pE(K_v) & \xrightarrow{\kappa_v} & H^1(G_{K_v}, E[p]) & \longrightarrow & \mathrm{Hom}(I_v, E[p])^{G^{\mathrm{ur}}_{K_v}} \\ & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{id}} \\ E((K_n)_\omega)/pE((K_n)_\omega) & \xrightarrow{(\kappa_n)_\omega} & H^1(G_{(K_n)_\omega}, E[p]) & \longrightarrow & \mathrm{Hom}(I_v, E[p])^{G^{\mathrm{ur}}_{K_v}}. \end{array}$$

  The first row is the sequence of Remark 4.3.4, recalling that, by definition,

$$H^1_{f,\mathcal{F}}(G_{K_v}, E[p]) = \mathrm{Im}(\kappa_v) \cong E(K_v)/pE(K_v).$$

  The second row is the same sequence for $(K_n)_\omega$ and then the vertical restriction is the composition

$$H^1(G_K, E[p]) \xrightarrow{\mathrm{res}_n} H^1(G_{K_n}, E[p]) \xrightarrow{\mathrm{res}_\omega} H^1(G_{(K_n)_\omega}, E[p]).$$

  By definition of $c(n)$

$$\mathrm{res}(c(n)_v) = (\kappa_n)_\omega((P_n)_\omega)$$

  where $c(n)_v \in H^1(G_{K_v}, E[p])$ is the image of $c(n)$ via res_n. Thus, from the exactness of the bottom row, the class $[c(n)]_v = 0$ in $\mathrm{Hom}(I_v, E[p])^{G^{\mathrm{ur}}_{K_v}} = H^1_{s,\mathcal{F}}(G_{K_v}, E[p])$.

- v is a finite place at which E has good reduction. See [Gro91, Proposition 6.2].

□

Before stating the main theorem of this section, we need one more lemma.

Lemma 4.3.17. *Let $n = ml \in \mathcal{R}$ with l a prime number and let $\lambda = l\mathcal{O}_K$. Then the class $[c(n)]_\lambda$ is zero in $H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])$ if and only if $P_m \in pE(K_\lambda)$.*

Proof. [Gro91, Proposition 6.2]. □

The preceding results can be summarized in the following theorem.

Theorem 4.3.18. *Suppose that the point $y_K \notin pE(K)$ and let $z \in E(\overline{K})$ such that $[p]z = y_K$. Let l be a Kolyvagin prime such that l does not split completely in the extension $K(E[p], z)/K(E[p])$. Let $\lambda := l\mathcal{O}_K$. Then the class $c(l) \in H^1(G_K, E[p])$ lies in the eigenspace $\mathrm{Sel}_\lambda(K, E[p])^{-\epsilon}$. Moreover, the class $[c(l)]_\lambda$ of $c(l)$ in the quotient $H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])$ is nonzero.*

In other words, Theorem 4.3.18 states that $c(l)$ satisfies the local conditions defined by the geometric Selmer structure $\mathcal{F}$ at all primes $\omega \neq l\mathcal{O}_K$, whereas it fails to lie in the local subgroup $H^1_{f,\mathcal{F}}(G_{K_\omega}, E[p])$ when $\omega = l\mathcal{O}_K$.

Proof. Propositions 4.3.15 and 4.3.16 imply directly that

$$c(l) \in \mathrm{Sel}_\lambda(G_K, E[p])^{-\epsilon}.$$

For the second part, recall that $P_1 = y_K$, hence by Lemma 4.3.17

$$[c(l)]_\lambda = 0 \iff y_K \in pE(K_\lambda).$$

Note that $L = K(E[p], z)$ is the minimal extension of $L_0 = K(E[p])$ in which y_K is divisible by p. In other words

$$y_K \in pE(K_\lambda) \iff L \subseteq K_\lambda(E[p]).$$

Indeed, if y_K is divisible by p in K_λ, by the minimality of L, $L \subseteq K_\lambda(E[p])$. Conversely, since $z \in K_\lambda$, then necessarely $y_K \in pE(K_\lambda)$. Let now $\mathfrak{P}$ be a prime ideal of L lying over λ, then trivially

$$y_K \in pE(K_\lambda) \iff L \subseteq K_\lambda(E[p]) \iff L_\mathfrak{P} \subseteq K_\lambda.$$

But λ splits completely in L_0 by remark 4.2.2 and $\mathfrak{p} = L_0 \cap \mathfrak{P}$ is a prime ideal of L_0 lying over λ, thus $(L_0)_\mathfrak{p} = K_\lambda$ and we have

$$y_K \in pE(K_\lambda) \iff L_\mathfrak{P} = (L_0)_\mathfrak{p}.$$

But $L_\mathfrak{P} = (L_0)_\mathfrak{p}$ holds if and only if λ splits completely in the extension L/L_0 and this cannot happen in our hypothesis. □

Another crucial result that we will apply in conjunction with Theorem 4.3.18 is the following.

Proposition 4.3.19. *Let l be a prime in $\mathcal{R}$, $\lambda := l\mathcal{O}_K$ and let $\eta \in \{\pm\}$. Suppose that there exists an element $c \in \mathrm{Sel}_\lambda(G_K, E[p])^\eta$ such that $[c]_\lambda \neq 0$ in $H^1_s(G_{K_\lambda}, E[p])$. Then, for all $s \in \mathrm{Sel}(E/K)[p]^\eta$, it holds that $s_\lambda = 0$ in $\mathrm{Im}(\kappa_\lambda)$.*

Proof. Thanks to Remark 4.3.23 (that we will discuss soon), we can rewrite the exact sequence (4.8) as follows:

$$0 \longrightarrow \mathrm{Sel}(K,E[p])^{\eta} \longrightarrow \mathrm{Sel}_{\lambda}(K,T)^{\eta} \xrightarrow{\alpha} H^1_s(G_{K_v},E[p])^{\eta}$$
$$(\mathrm{Sel}(K,E[p])^{\vee})^{\eta} \xrightarrow{\gamma} (\mathrm{Sel}^{\lambda}(K,E[p])^{\vee})^{\eta} \longrightarrow 0. \qquad (\beta)$$

By hypothesis, $\alpha(c) \neq 0$ in $H^1_s(G_{K_\lambda},E[p])^{\eta}$ and by the next Lemma (4.3.20)

$$\dim_{\mathbb{F}_p}(H^1_s(G_{K_\lambda},E[p])^{\eta}) = 1,$$

that is α is surjective. Thus by the exactness of the above sequence, γ is an isomorphism. Indeed, it is clearly surjective and by the exactness β is the zero-map since

$$H^1_s(G_{K_\lambda},E[p])^{\eta} = \mathrm{Im}(\alpha) = \mathrm{Ker}(\beta).$$

In conclusion, we obtain an isomorphism

$$(\mathrm{Sel}(K,E[p])^{\vee})^{\eta} \cong (\mathrm{Sel}^{\lambda}(K,E[p])^{\vee})^{\eta}$$

or equivalently

$$\mathrm{Sel}(K,E[p])^{\eta} \cong \mathrm{Sel}^{\lambda}(K,E[p])^{\eta}.$$

This in particular means, by the definition of $\mathrm{Sel}^{\lambda}(K,E[p])$, that for each $s \in \mathrm{Sel}(K,E[p])^{\eta}$, we have $s_\lambda = 0$.

□

It remains to prove the following lemma.

Lemma 4.3.20. *Let $l \neq p$ be a Kolyvagin prime at which E has good reduction and let $\lambda := l\mathcal{O}_K$. Then*

$$\dim_{\mathbb{F}_p}(H^1_{s,\mathcal{F}}(G_{K_\lambda},E[p])^{\pm}) = 1.$$

For the proof of Lemma 4.3.20, we need a special pairing

$$\mathrm{e}_p\colon E[p] \times E[p] \longrightarrow \boldsymbol{\mu}_p,$$

called the "Weil pairing". We now briefly recall its definition.

Let $T \in E[p]$. Then, there exists a function $f_T \in \overline{K}(E)$ such that

$$\mathrm{div}(f_T) = p(T) - p(O).$$

Consider now a point $T' \in E$ such that $[p]T' = T$. Since the order of T' is p^2 (as $[p^2]T' = [p]T = O$), there exists a function $g_T \in \overline{K}(E)$ such that

$$\mathrm{div}(g_T) = \sum_{R \in E[p]} \big((T'+R) - (R)\big).$$

Note that f_T and g_T satisfy

$$\operatorname{div}(f_T \circ [p]) = \operatorname{div}(g_T^p);$$

thus, up to scalar multiplication by an element in $\overline{K}^\times$, we can assume that $f_T \circ [p] = g_T^p$. Now, let $S \in E[p]$. For any $X \in E$, we have

$$g_T(X+S)^p = f_T([p]X + [p]S) = f_T([p]X) = g_T(X)^p.$$

Definition 4.3.21. *Using the notation above, we define the Weil pairing as*

$$\mathrm{e}_p \colon E[p] \times E[p] \to \boldsymbol{\mu}_p, \quad (S,T) \mapsto \frac{g_T(X+S)}{g_T(X)},$$

where $X \in E$ is any point such that $g_T(X+S)$ and $g_T(X)$ are both defined and nonzero.

Although g_T is defined only up to multiplication by scalars in $\overline{K}^\times$, it can be verified that e_p does not depend on this choice (for more details see [Sil09, Chapter 3, Section 8]).

Proposition 4.3.22. *The Weil pairing e_p is an alternating perfect pairing. Moreover it is Galois equivariant, i.e. it holds*

$$\sigma(\mathrm{e}_p(S,T)) = \mathrm{e}_p(\sigma(S), \sigma(T))$$

for all $S, T \in E[p]$ and $\sigma \in G_K$.

Proof. see [Sil09, Chapter 3, Section 8, Proposition 8.1] □

Remark 4.3.23. *It follows directly from Proposition 4.3.22 that*

$$E[p]^* = \operatorname{Hom}_{\mathbb{F}_p}(E[p], \boldsymbol{\mu}_p) \cong E[p].$$

We are now ready for the proof of Lemma 4.3.20.

Proof of lemma 4.3.20. We divide the proof into two steps.

Step 1. We are going to prove that

$$H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p]) \cong E[p]^{\mp}.$$

Since E has good reduction at λ, by Remark 4.3.13 the geometric local Selmer structure $\operatorname{Im}(\kappa_\lambda)$ coincides with the unramified one and by the exact sequence of Remark 4.3.4, we have

$$H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p]) = \frac{H^1(G_{K_\lambda}, E[p])}{H^1(G^{\mathrm{ur}}_{K_\lambda}, E[p]^{I_\lambda})} \cong H^1(I_\lambda, E[p])^{G^{\mathrm{ur}}_{K_\lambda}}.$$

Note that in our hypothesis, by Proposition 1.3.19 $E[p]$ is an unramified set (i.e. I_λ acts trivially on $E[p]$) and we can deduce that

$$H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p]) \cong \mathrm{Hom}(I_\lambda, E[p])^{G^{\mathrm{ur}}_{K_\lambda}}.$$

Moreover, one can check that every homomorphism

$$I_\lambda \longrightarrow E[p]$$

factors through $I_\lambda/pI_\lambda \cong \mathrm{Gal}(K^{\mathrm{ur}}_\lambda(l^{\frac{1}{p}})/K^{\mathrm{ur}}_\lambda) \cong \boldsymbol{\mu}_p$. Finally, since λ splits completely in $K(E[p])$ by Remark 4.2.2, if ω is a prime ideal of $K(E[p])$ lying over λ, then the residue fields are the same and ω appears with multiplicity 1 in the factorization of λ. This directly implies that

$$K(E[p]) \subseteq (K(E[p]))_\omega = K_\lambda,$$

that is $E[p] \subseteq K_\lambda$. Thus $E[p]$ is fixed by $G^{\mathrm{ur}}_{K_\lambda} = \mathrm{Gal}(K^{\mathrm{ur}}_\lambda/K_\lambda)$ and we get

$$H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p]) \cong \mathrm{Hom}(\boldsymbol{\mu}_p, E[p])^{G^{\mathrm{ur}}_{K_\lambda}} = \mathrm{Hom}(\boldsymbol{\mu}_p, E[p]).$$

Hence, we can conclude that

$$H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])^\pm \cong \mathrm{Hom}(\boldsymbol{\mu}_p, E[p])^\pm \cong E[p]^\mp$$

where the last isomorphism is given by

$$\mathrm{Hom}(\boldsymbol{\mu}_p, E[p]) \to E[p] \quad \varphi \mapsto \varphi(x_0)$$

where x_0 is a fixed primitive p-th root of unity.

Step 2. We now compute the dimensions of the eigenspaces. By the previous step it suffices to show that

$$\dim_{\mathbb{F}_p}(E[p]^\pm) = 1.$$

Note that since $\dim_{\mathbb{F}_p}(E[p]) = 2$, then

$$\big(\dim_{\mathbb{F}_p}(E[p]^+), \dim_{\mathbb{F}_p}(E[p]^-)\big) \in \{(1,1),(2,0),(0,2)\}.$$

Suppose, for example, that $\dim_{\mathbb{F}_p}(E[p]^+) = 2$ (the case for $E[p]^-$ is symmetric). In this case, we would have $E[p]^+ = E[p]$ and $E[p]^- = 0$. Consequently, for all $S, T \in E[p]$, it holds that $\tau S = S$ and $\tau T = T$. By the Galois equivariance of the Weil pairing (cf. Proposition 4.3.22), we have

$$\mathrm{e}_p(S,T) = \mathrm{e}_p(\tau S, \tau T) = \tau(\mathrm{e}_p(S,T)) = \mathrm{e}_p(S,T)^{-1},$$

where the last equality follows from the fact that τ acts on $\boldsymbol{\mu}_p$ by inversion. This implies $\mathrm{e}_p(S,T)^2 = 1$, and for $p > 2$, this means $\mathrm{e}_p(S,T) = 1$ for all $S, T \in E[p]$. This is a contradiction, as the Weil pairing is non-degenerate (perfect). Therefore, we must have

$$\dim_{\mathbb{F}_p}(E[p]^+) = \dim_{\mathbb{F}_p}(E[p]^-) = 1,$$

which completes the proof. □

4.4 Computation of the Selmer group

In this final part of the chapter, our goal is to compute the Selmer groups $\mathrm{Sel}(E/K)[p]^\eta$, for $\eta \in \{\pm\epsilon\}$. As announced at the beginning of the chapter, we prove that

$$\mathrm{Sel}(E/K)[p]^{-\epsilon} = 0 \quad \text{and} \quad \mathrm{Sel}(E/K)[p]^{\epsilon} = \langle \kappa(y_K) \rangle_{\mathbb{F}_p}.$$

As in the previous section, we want to understand how complex conjugation τ acts on our objects, and we now turn to the case of y_K.

Proposition 4.4.1. *Whit notation above,*

$$\tau(y_K) = \epsilon y_K$$

that is $y_K \in (E(K)/pE(K))^\epsilon$.

Proof. Recall that by Proposition 4.2.19 $E(K_1)$ has no nontrivial p-torsion and using Proposition 5.3 of [Gro91], we can choose an automorphism $\sigma \in \mathrm{Gal}(K_1/K)$ such that

$$\tau(y_K) = \epsilon\sigma(y_K)$$

in $E(K_1)/pE(K_1)$. Recall that τ acts as conjugation on $\mathrm{Gal}(K_1/K)$ and that the operator

$$\mathrm{Tr} = \sum_{\alpha \in \mathrm{Gal}(K_1/K)} \alpha,$$

used for the definition of y_K, preserves the inversion. Thus, since $\sigma \in \mathrm{Gal}(K_1/K)$, we obtain

$$\begin{aligned} \tau(y_K) &= \tau(\mathrm{Tr}(y_1)) = \mathrm{Tr}(\tau(y_1)) \\ &= \mathrm{Tr}(\epsilon\sigma(y_1)) = \epsilon \mathrm{Tr}(\sigma(y_1)) \\ &= \epsilon \mathrm{Tr}(y_1) = \epsilon y_K. \end{aligned}$$

□

We now fix some notation that we will largely use in next results. Let

- $L_0 := K(E[p])$;
- $L = L_0(z) = K(E[p], z)$ with $z \in E(\overline{K})$ such that $[p]z = y_K$.

Lemma 4.4.2. *We have*

$$H^i(\mathrm{Gal}(L_0/K), E[p]) = 0$$

for all i.

Proof. We want to use Proposition 2.4.13. Let $A := \mathbb{F}_p^2$ and fix the following left-exact functors:

- $F := (\cdot)^{\mathbb{F}_p^\times} : [\mathrm{GL}_2(\mathbb{F}_p) - \mathrm{mod}] \to \big[\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times - \mathrm{mod}\big]$;

- $G := (\cdot)^{\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times} : \left[\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times - \mathrm{mod}\right] \to \underline{Ab}$.

Since A is an object in the category $[\mathrm{GL}_2(\mathbb{F}_p) - \mathrm{mod}]$ and the composition $G \circ F = (\cdot)^{\mathrm{GL}_2(\mathbb{F}_p)}$ is still left-exact, we have the Groethendieck spectral sequence $\mathbb{E}(A)$ which verifies for all p, q:

- $\mathbb{E}(A)_2^{p,q} = R^pG(R^qF(A)) = H^p(\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times, H^q(\mathbb{F}_p^\times, \mathbb{F}_p^2))$;
- $H^p(\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times, H^q(\mathbb{F}_p^\times, \mathbb{F}_p^2)) \Rightarrow H^{p+q}(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2)$.

Note that $H^q(\mathbb{F}_p^\times, \mathbb{F}_p^2) = 0$ for all q. Indeed, for $q = 0$

$$H^0(\mathbb{F}_p^\times, \mathbb{F}_p^2) = (\mathbb{F}_p^2)^{\mathbb{F}_p^\times} = \{x \in \mathbb{F}_p^2 : \mathbb{F}_p^\times \cdot x = x\} = 0.$$

For $q > 0$, one can see [NSW13, Chapter 8, Corollary 1]. Thus

$$H^{p+q}(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2) = 0$$

for all p, q and we conlude. □

Lemma 4.4.2 has an important consequence.

Proposition 4.4.3. *The restriction map induces an isomorphism*

$$\mathrm{res} : H^1(G_K, E[p]) \cong H^1(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)} \cong \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(G_{L_0}, E[p]).$$

Proof. First of all we write the Hochschild–Serre exact sequence of Section 2.4.2 with $M = E[p]$. Then we have

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1(\mathrm{Gal}(L_0/K), E[p]^{G_{L_0}}) & \xrightarrow{\inf} & H^1(G_K, E[p]) \\ & & & \xleftarrow{\mathrm{res}} & \\ H^1(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)} & \longrightarrow & H^2(\mathrm{Gal}(L_0/K), E[p]^{G_{L_0}}) & \longrightarrow & H^2(G_K, E[p]). \end{array}$$

Since $E[p] \subseteq L_0$ is fixed by $G_{L_0} = \mathrm{Gal}(\overline{K}/L_0)$, by Lemma 4.4.2, one obtains

$$0 = H^i(\mathrm{Gal}(L_0/K), E[p]) = H^i(\mathrm{Gal}(L_0/K), E[p]^{G_{L_0}}).$$

Thus, by the exactness of the Hochschild-Serre sequence, the diagonal arrow

$$\mathrm{res} : H^1(G_K, E[p]) \to H^1(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)}$$

is an isomorphism. □

Thanks to Proposition 4.4.3, we can give the following.

Definition 4.4.4. *The restriction map induces a pairing*

$$[\cdot, \cdot] : H^1(G_K, E[p]) \times G_{L_0} \to E[p]$$

given by

$$[s, \rho] := \mathrm{res}(s)(\rho).$$

In order to study the properties of this pairing, we need to fix some other notation:

- S will be a finite-dimensional $\mathbb{F}_p$-vector space of $H^1(G_K, E[p])$ (for example we will put $S = \mathrm{Sel}(E/K)[p]$);
- $G_{L_0}^S := \{\rho \in G_{L_0} : [s, \rho] = 0 \text{ for all } s \in S\}$.
- L_0^S will be the subfield of $\overline{\mathbb{Q}}$ fixed by $G_{L_0}^S$.

Note in particular that

$$G_{L_0^S} = \mathrm{Gal}(\overline{\mathbb{Q}}/L_0^S) = \mathrm{Gal}(\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^{G_{L_0}^S}) = G_{L_0}^S.$$

Remark 4.4.5. *The pairing of Definition 4.4.4 induces another pairing*

$$S \times \mathrm{Gal}(L_0^S/L_0) \longrightarrow E[p].$$

First of all note that if $s \in S$, then $\mathrm{res}(s) : G_{L_0} \to E[p]$ factors through the quotient

$$\mathrm{Gal}(L_0^S/L_0) \cong \frac{G_{L_0}}{G_{L_0^S}}.$$

Indeed, if $\sigma \in G_{L_0^S} = G_{L_0}^S$, by definition $\mathrm{res}(s)(\sigma) = [s, \sigma] = 0$, that is $\sigma \in \mathrm{Ker}(\mathrm{res})$. Thus it is induced another map

$$\overline{\mathrm{res}}(s) : \mathrm{Gal}(L_0^S/L_0) \to E[p], \qquad [\sigma] \mapsto \mathrm{res}(s)(\sigma)$$

which defines a pairing

$$[\cdot, \cdot] : S \times \mathrm{Gal}(L_0^S/L_0) \to E[p] \qquad (s, \rho) \mapsto [s, \rho] := \overline{\mathrm{res}}(s)(\rho).$$

Proposition 4.4.6. *The induced pairing*

$$[\cdot, \cdot] : S \times \mathrm{Gal}(L_0^S/L_0) \longrightarrow E[p]$$

is non-degenerate. It induces the following isomorphism of $\mathrm{Gal}(L_0/K)$-modules

$$\mathrm{Gal}(L_0^S/L_0) \cong \mathrm{Hom}(S, E[p])$$

and the following isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules

$$S \cong \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(\mathrm{Gal}(L_0^S/L_0), E[p]).$$

Proof. First of all we show that

$$\mathrm{Gal}(L_0^S/L_0) \to \mathrm{Hom}(S, E[p]), \qquad \rho \mapsto [\cdot, \rho] \tag{4.10}$$

and

$$S \to \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(\mathrm{Gal}(L_0^S/L_0), E[p]), \qquad s \mapsto [s, \cdot] \tag{4.11}$$

are injective. Let $\rho \in \mathrm{Gal}(L_0^S/L_0)$ such that $[s,\rho] = 0$ for all $s \in S$. This means that $\rho = [\sigma]$ with

$$\sigma \in G_{L_0} \cap G_{L_0^S} = \mathrm{Gal}(\overline{\mathbb{Q}}/L_0) \cap \mathrm{Gal}(\overline{\mathbb{Q}}/L_0^S) = G_{L_0^S}.$$

Thus $\rho = [\sigma] = 1$ in $G_{L_0}/G_{L_0^S}$ and the map (4.10) is injective. As regards (4.11), let $s \in S$ such that $\overline{\mathrm{res}}(s)(\rho) = [s,\rho] = 0$ for all $\rho \in \mathrm{Gal}(L_0^S/L_0) = G_{L_0}/G_{L_0^S}$. Thus $\overline{res}(s)(\sigma) = 0$ for all $\sigma \in G_{L_0}$ and since the reduction map is an isomorphism by Proposition 4.4.3, necessarely $s = 0$ and the map (4.11) is injective. Now we prove that these two injections are actually isomorphisms. Since

$$\mathrm{Gal}(L_0/K) \cong \mathrm{GL}_2(\mathbb{F}_p) = \mathrm{Aut}(E[p]),$$

$E[p]$ is an irreducible $\mathrm{Gal}(L_0/K)$-module (this means that $E[p]$ does not have non-trivial submodule). Let $r := \dim_{\mathbb{F}_p}(S)$. Then, by the injectivity of (4.10) we know that $\mathrm{Gal}(L_0^S/L_0)$ is a $\mathrm{Gal}(L_0/K)$-submodule of

$$\mathrm{Hom}(S, E[p]) \cong E[p]^r.$$

Hence, by the irreducibility of $E[p]$, one has

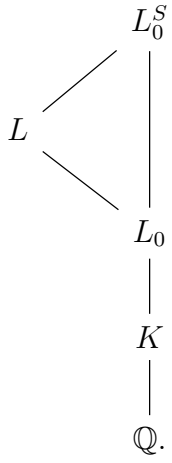
$$\mathrm{Gal}(L_0^S/L_0) \cong E[p]^t$$

for some $t \leq r$. But from the injectivity of (4.11), $S \cong \mathbb{F}_p^r$ is a subspace of

$$\mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(\mathrm{Gal}(L_0^S/L_0), E[p]) \cong \mathbb{F}_p^t$$

and this means that $t = r$ and (4.10) and (4.11) are isomorphisms. □

Now we want to apply Proposition 4.4.6 to the vector space $\mathrm{Sel}(E/K)[p]$ and to the following tower of fields



To do so, we first establish the following lemma.

Lemma 4.4.7. *There are isomorphisms between the eigenspaces*

$$E[p]^{\pm\epsilon} \cong \mathrm{Gal}(L/L_0)^{\pm}.$$

This in particular implies that $\dim_{\mathbb{F}_p}(\mathrm{Gal}(L/L_0)^{\pm}) = 1$.

Proof. First of all consider

$$c := \kappa(y_K)|_{G_{L_0}} : G_{L_0} \to E[p] \in H^1(G_{L_0}, E[p]) = \mathrm{Hom}(G_{L_0}, E[p])$$

where κ is the Kummer map. Recall that from Section 2.4 we have an explicit description of c:

$$c(\sigma) = \sigma(z) - z.$$

Moreover, note that

$$\mathrm{Ker}(c) = \{\sigma \in G_{L_0} : \sigma(z) = z\} = G_L.$$

Thus, if we prove that c is surjective, we obtain an induced isomorphism

$$\overline{c} : G_{L_0}/G_L \cong \mathrm{Gal}(L/L_0) \xrightarrow{\cong} E[p].$$

In order to prove that c is surjective, note that c is not the zero-map. Indeed, since $y_K \notin pE(K)$ and since the Kummer map κ is injective, one has

$$\kappa(y_K) \neq 0 \text{ in } H^1(G_K, E[p]).$$

But from propostion 4.4.3 we have an isomorphism

$$\mathrm{res} : H^1(G_K, E[p]) \xrightarrow{\cong} H^1(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)} = \mathrm{Hom}(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)}.$$

In other words, $c := \kappa(y_K)|_{G_{L_0}} = \mathrm{res}(\kappa(y_K))$ is a nonzero homomorphism $G_{L_0} \to E[p]$ that is also $\mathrm{Gal}(L_0/K)$-equivariant. Let $x \neq O$ be an element of $E[p]$ such that $x = c(\sigma_0)$ for some $\sigma_0 \in G_{L_0}$. Since the action of $\mathrm{Gal}(L_0/K)$ is transitive, for all $y \in E[p]$, there exists $\varphi \in \mathrm{Gal}(L_0/K)$ such that $\varphi(x) = y$. Thus, for the $\mathrm{Gal}(L_0/K)$-equivariance, we obtain

$$y = \varphi(x) = \varphi(c(\sigma_0)) = c(\sigma_0^{\varphi}).$$

Summing up, we have an isomorphism

$$\overline{c} : \mathrm{Gal}(L/L_0) \xrightarrow{\cong} E[p]$$

induced by c. We now study the action of the complex conjugation τ on $\kappa(y_K)$. One has for all $\sigma \in G_K$

$$\kappa(y_K)^{\tau}(\sigma) = \tau(\sigma^{\tau}(z) - z) = \sigma(\tau(z)) - \tau(z).$$

On the other hand in the quotient $E(K)/pE(K)$

$$[p]\tau(z) = \tau(pz) = \tau(y_K) = \epsilon y_K$$

where the last equality follows from Proposition 4.4.1. Hence

$$\kappa(y_K)^{\tau}(\sigma) = \epsilon\kappa(y_K)(\sigma)$$

and $\kappa(y_K)$ is an eigenvector for τ. Thus, if $\sigma \in \mathrm{Gal}(L/L_0)^{\pm}$, then

$$\epsilon\overline{c}(\sigma) = \overline{c}^{\tau}(\sigma) = \tau(\overline{c}(\sigma^{\tau})) = \tau(\overline{c}(\sigma^{\pm}))$$

and applying τ and multiplying by ϵ we finally obtain

$$\tau(\overline{c}(\sigma)) = \pm\epsilon\overline{c}(\sigma).$$

In other words, this means that via $\overline{c}$ we have the

$$E[p]^{\pm\epsilon} \cong \mathrm{Gal}(L/L_0)^{\pm}$$

□

Now we let the complex conjugation τ act on the Galois groups and in particular we consider the decompositions

$$\mathrm{Gal}(L_0^S/L_0) = \mathrm{Gal}(L_0^S/L_0)^+ \oplus \mathrm{Gal}(L_0^S/L)^-$$

$$\mathrm{Gal}(L_0^S/L) = \mathrm{Gal}(L_0^S/L)^+ \oplus \mathrm{Gal}(L_0^S/L)^-.$$

We denote $H := \mathrm{Gal}(L_0^S/L_0)$ and $I := \mathrm{Gal}(L_0^S/L)$. For example, using this notation,

$$H^+ = \{h \in H : h\tau = h\}.$$

Proposition 4.4.8. *The following properties hold.*

(a) $H^+ = \{(\tau h)^2 : h \in H\}$;

(b) $I^+ = \{(\tau i)^2 : i \in H\}$;

(c) $H^+/I^+ \cong \mathbb{F}_p$;

(d) let $s \in \mathrm{Sel}(E/K)[p]$. *The following conditions are equivalent:*

i) $s = 0$;

ii) $[s, \rho] = 0$ *for all* $\rho \in H$;

iii) $[s, \rho] = 0$ *for all* $\rho \in H^+$;

iv) $[s, \rho] = 0$ *for all* $\rho \in H^+ \setminus I^+$.

Proof. (a) We claim that

$$H^{\tau+1} = H^+$$

where $H^{\tau+1} = \{h^{\tau}h : h \in H\}$. Note that

$$(H^{\tau+1})^{\tau-1} = H^{\tau^2-1} = H^0 = \{\mathrm{id}\}.$$

Hence, if $\tau \in H$ then $(h^{\tau}h)^{\tau} = h^{\tau}h$, that is

$$H^{\tau+1} \subseteq H^+.$$

Conversely, if $h \in H^+$, then by definition $h^\tau h = h^2$ and since p is odd, 2 is an automorphism of H and we can write

$$h = (h^{\frac{1}{2}})^{\tau+1} \in H^{\tau+1}.$$

Summing up, expliciting the action of τ, we finally obtain

$$H^+ = H^{\tau+1} = \{h^\tau h : h \in H\} = \{(\tau h)^2 : h \in H\}.$$

(b) One uses the same argument of part (a).

(c) It follows directly from Lemma 4.4.7.

(d) By Proposition 4.4.6, we know that the map

$$S \to \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(\mathrm{Gal}(L_0^S/L_0), E[p]), \qquad s \mapsto [s, \cdot]$$

is an isomorphism; thus, the equivalence $(i) \iff (ii)$ is proved. Moreover, since the implications $(ii) \Rightarrow (iii) \Rightarrow (iv)$ are trivial, it suffices to prove $(iv) \Rightarrow (iii) \Rightarrow (ii)$.

Suppose that (iv) holds. Identifying s with a homomorphism $H \to E[p]$ via the isomorphism of Proposition 4.4.6, we have that $s|_{H^+ \setminus I^+}$ is the zero map. Since $I^+ \subsetneq H^+$ is a proper subgroup and s is a group homomorphism, the fact that s vanishes on the complement of a subgroup implies that $s|_{H^+}$ must be the zero map. Thus, the implication $(iv) \Rightarrow (iii)$ follows.

Now, suppose that (iii) holds. Note that since $\sigma([s, \rho]) = [s, \rho]$ for all $\sigma \in \mathrm{Gal}(L_0/K)$ (by the equivariance of the pairing), the map s preserves the eigenspaces, i.e.,

$$s|_{H^+} : H^+ \longrightarrow E[p]^+ \quad \text{and} \quad s|_{H^-} : H^- \longrightarrow E[p]^-.$$

By (iii), we have $s(H^+) = 0$. Consequently, the image $s(H) = s(H^-)$ is contained in $E[p]^-$. However, $s(H)$ must be a $\mathrm{Gal}(L_0/K)$-submodule of $E[p]$. Since $E[p]$ is irreducible (see proof of Proposition 4.4.6), its only submodules are $\{0\}$ and $E[p]$ itself. Since $E[p]^-$ is a proper subspace, we must have $s(H) = 0$, which proves (ii) and concludes the proof.

□

Before computing $\mathrm{Sel}(E/K)[p]^{-\epsilon}$, we need one more proposition.

Proposition 4.4.9. *Let l be a prime number inert in K and let $\lambda = l\mathcal{O}_K$. Assume that λ splits completely in L_0 and that λ is not ramified in L_0^S. Let λ_S be a prime ideal of L_0^S lying over λ. Then $\mathrm{Frob}_{L_0^S/K}(\lambda_S) \in \mathrm{Gal}(L_0^S/K)$ actually lies in $\mathrm{Gal}(L_0^S/L_0) = H$. Let $\mathrm{Frob}(\lambda)$ be the $\mathrm{Gal}(L_0/K)$-orbit of $\mathrm{Frob}_{L_0^S/K}(\lambda_S)$ and let $s \in \mathrm{Sel}(E/K)[p]$. The following conditions are equivalent:*

(a) $[s, \mathrm{Frob}_{L_0^S/K}(\lambda_S)] = 0$;

(b) $[s, \rho] = 0$ *for all* $\rho \in \mathrm{Frob}(\lambda)$*;*

(c) $s_\lambda = 0$ *in* $H^1(G_{K_\lambda}, E[p])$*.*

Proof. See [Gro91, Proposition 9.6]. □

Finally we are ready to prove that the negative eigenspace of $\mathrm{Sel}(E/K)[p]$ is trivial.

Theorem 4.4.10. $\mathrm{Sel}(E/K)[p]^{-\epsilon} = 0$.

Proof. Let $s \in \mathrm{Sel}(E/K)[p]^{-\epsilon}$. By Proposition 4.4.8, in order to show that $s = 0$, it suffices to prove that $[s, \rho] = 0$ for all $\rho \in H^+ \setminus I^+$. Fix such a ρ. Using Proposition 4.4.8 again, we can write $\rho = (\tau h)^2$ for some $h \in H$. By the Chebotarev Density Theorem (cf. Theorem 3.4.13), there exist infinitely many prime numbers l of $\mathbb{Q}$ such that

$$\tau h \in \mathrm{Frob}_{L_0^S/\mathbb{Q}}(l).$$

Fix such a prime l and let us study its properties. First, note that l is inert in K since

$$\tau = \mathrm{Frob}_{K/\mathbb{Q}}(l) \in \mathrm{Gal}(K/\mathbb{Q});$$

we denote the corresponding prime ideal by $\lambda = l\mathcal{O}_K$. Then, λ splits completely in L_0 because

$$\mathrm{id} = (\tau h|_{L_0})^2 \in \mathrm{Frob}_{L_0/K}(\lambda).$$

Furthermore, $\mathrm{Frob}_{L_0^S/L_0}(\lambda)$ is conjugated to $(\tau h)^2 = \rho \in H^+ \setminus I^+$, which is non-trivial. In other words, λ does not split completely in the extension L_0^S/L_0. Finally, since $\mathrm{Frob}_{L/L_0}(\lambda)$ is conjugated to $\rho|_L \notin I^+$, this Frobenius element is also non-trivial; thus, λ does not split completely in the extension L/L_0.

By Proposition 4.4.9, to prove that $[s, \rho] = 0$, it is equivalent to show that $s_\lambda = 0$ in $H^1(G_{K_\lambda}, E[p])$. Since λ does not split completely in L/L_0, by Proposition 4.3.18 the cohomology class $c(l)$ lies in $\mathrm{Sel}_\lambda(K, E[p])$ and satisfies $[c(l)]_\lambda \neq 0$ in $H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])$. Thus, applying Proposition 4.3.19 to the class $c(l)$, we obtain the thesis. □

Now we gather several results, most of which have been proved at different points earlier, into a single proposition.

Proposition 4.4.11. *Let* l *be a prime number unramified in* L_0^S *with* $\mathrm{Frob}_{L_0^S/\mathbb{Q}}(l)$ *conjugate to* τh *for some* $h \in H = \mathrm{Gal}(L_0^S/L_0)$*. Let* $\lambda = l\mathcal{O}_K$*. Then the following conditions are equivalent.*

(a) $c(l) = 0$ *in* $H^1(G_K, E[p])$*;*

(b) $c(l) \in \mathrm{Sel}(E/K)[p]$*;*

(c) $P_l \in pE(K_l)$*;*

(d) $d(l) = 0$ *in* $H^1(G_K, E)[p]$*;*

(e) $d(l)_\lambda = [c(l)]_\lambda = 0$ *in* $H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])$*;*

(f) $y_K \in pE(K_\lambda)$*;*

(g) $h^{\tau+1} = h^\tau h \in I^+ = \mathrm{Gal}(L_0^S/L)^+$.

Proof. The implication $(a) \Rightarrow (b)$ is clear. Regarding $(b) \Rightarrow (a)$, we know from Proposition 4.3.15 that $c(l) \in H^1(G_K, E[p])^{-\epsilon}$. Hence, if we assume (b), then $c(l) \in \mathrm{Sel}(E/K)[p]^{-\epsilon}$, which is trivial by Theorem 4.4.10; thus $c(l) = 0$.

The equivalence $(c) \iff (a)$ is exactly the first part of Proposition 4.2.21. Since $(E(K)/pE(K))^{-\epsilon} = 0$ by Theorem 4.4.10, the equivalence $(d) \iff (a)$ follows again from Proposition 4.2.21.

Moreover, the implication $(d) \Rightarrow (e)$ is trivial by localization. Conversely, since $c(l) \in \mathrm{Sel}^\lambda(K, E[p])^{-\epsilon}$, if we suppose that $[c(l)]_\lambda = 0$, then $c(l)$ falls into the full Selmer group $\mathrm{Sel}(E/K)[p]^{-\epsilon}$, which is zero by Theorem 4.4.10.

The equivalence $(e) \iff (f)$ follows from Lemma 4.3.17, keeping in mind that $P_1 = y_K$. Finally, for the equivalence $(f) \iff (g)$, we recall that $y_K \in pE(K_\lambda)$ if and only if λ splits completely in L/L_0.

Since λ splits completely in L_0/K (because $(\tau h|_{L_0})^2 = \mathrm{id}$), the condition for λ to split completely in the further extension L/L_0 is that its Frobenius element $\mathrm{Frob}_{L/L_0}(\lambda)$ is trivial. We calculate:

$$\mathrm{Frob}_{L/L_0}(\lambda) = (\tau h|_L)^2 = \tau h \tau h|_L = h^\tau h|_L.$$

Thus, $\mathrm{Frob}_{L/L_0}(\lambda) = \mathrm{id}$ if and only if $h^\tau h$ fixes L. Since $h^\tau h$ already belongs to H^+, this is equivalent to:

$$h^{\tau+1} = h^\tau h \in \mathrm{Gal}(L_0^S/L) \cap H^+ = I^+ \cap H^+ = I^+.$$

□

In order to prove that $\mathrm{Sel}(E/K)[p]^{+\epsilon}$ is cyclic generated by $\kappa(y_K)$ we need a lemma.

Lemma 4.4.12. $H^1(\mathrm{Gal}(L/K), E[p]) \cong \mathbb{F}_p \cdot \kappa(y_K)$.

Note that there is a slight abuse of notation in the statement since, formally, $\kappa(y_K) \in H^1(G_K, E[p])$. However, by the explicit description of the Kummer map, we have

$$\kappa(y_K)(\sigma) = \sigma(z) - z.$$

If $\sigma \in G_L$, then σ fixes z, hence $\kappa(y_K)(\sigma) = 0$. This implies that the cocycle $\kappa(y_K)$ factors through the quotient

$$\mathrm{Gal}(L/K) \cong G_K/G_L,$$

and the statement is well-defined.

Proof. By an argument entirely analogous to the proof of Proposition 4.4.3, but applied to the subgroup $\mathrm{Gal}(L/L_0) \leq \mathrm{Gal}(L/K)$, we obtain an isomorphism

$$H^1(\mathrm{Gal}(L/K), E[p]) \xrightarrow{\mathrm{res}} H^1(\mathrm{Gal}(L/L_0), E[p])^{\mathrm{Gal}(L_0/K)}.$$

Moreover, from Lemma 4.4.7 (more precisely, from its proof), we have $\mathrm{Gal}(L/L_0) \cong E[p]$ as $\mathrm{Gal}(L_0/K)$-modules. Since $\mathrm{Gal}(L/L_0)$ acts trivially on $E[p]$, the H^1 term becomes a Hom group:

$$\begin{aligned} H^1(\mathrm{Gal}(L/K), E[p]) &\cong H^1(\mathrm{Gal}(L/L_0), E[p])^{\mathrm{Gal}(L_0/K)} \\ &= \mathrm{Hom}(\mathrm{Gal}(L/L_0), E[p])^{\mathrm{Gal}(L_0/K)} \\ &\cong \mathrm{Hom}(E[p], E[p])^{\mathrm{Gal}(L_0/K)}. \end{aligned}$$

In Remark 4.1.8, we have seen that $\mathrm{Gal}(L_0/K) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Therefore,

$$\begin{aligned} H^1(\mathrm{Gal}(L/K), E[p]) &\cong \mathrm{Hom}(E[p], E[p])^{\mathrm{GL}_2(\mathbb{F}_p)} \\ &= \{\text{scalar homomorphisms } E[p] \to E[p]\} \\ &\cong \mathbb{F}_p. \end{aligned}$$

Finally, since $\kappa(y_K)$ is non-zero , it generates this one-dimensional $\mathbb{F}_p$-vector space, which yields the thesis. □

Now we are ready for the proof of the following Theorem.

Theorem 4.4.13. *The eigenspace* $\mathrm{Sel}(E/K)[p]^{+\epsilon}$ *has dimension* 1 *over* $\mathbb{F}_p$ *and is generated by* $\kappa(y_K)$.

Proof. Recall that by Proposition 4.4.6, we have an isomorphism

$$\mathrm{Sel}(E/K)[p] \cong \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(H, E[p]).$$

Let $s \in \mathrm{Sel}(E/K)[p]^{+\epsilon}$ and suppose that $[s, \rho] = 0$ for all $\rho \in I$. This implies that $I \subseteq \ker(s)$, so we can interpret s as an element of

$$\mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(H/I, E[p]) = \mathrm{Hom}_{\mathrm{Gal}(L_0/K)}(\mathrm{Gal}(L/L_0), E[p]) \cong \mathbb{F}_p \cdot \kappa(y_K),$$

where the last isomorphism follows from the proof of Lemma 4.4.12. Thus, to conclude the proof, it suffices to show that

$$s \in \mathrm{Sel}(E/K)[p]^{+\epsilon} \implies [s, \rho] = 0 \quad \text{for all } \rho \in I.$$

Furthermore, by the same argument used for Proposition 4.4.8, it suffices to prove that $[s, \rho] = 0$ for all $\rho \in I^+$.

Let q be a prime number of $\mathbb{Q}$ such that the class $c(q) \in H^1(G_K, E[p])$ is non-trivial. As seen in the proof of Theorem 4.4.10, we may choose q such that $\mathrm{Frob}_{L_0^S/\mathbb{Q}}(q)$ is conjugate to $\tau\sigma$ for some $\sigma \in H$ with $\sigma^{\tau+1} \notin I^+$. Now, let $c :=$

$c(q)|_{G_{L_0}} : G_{L_0} \to E[p]$. Since $E[p] \subseteq E(L_0)$, G_{L_0} acts trivially on $E[p]$, and hence c is a homomorphism. Let L' be the subfield of $\overline{K}$ fixed by $\ker(c)$. Explicitly, as $c(q) = \kappa(P_q)$, we have

$$\ker(c) = \{\sigma \in G_{L_0} : \sigma(z_q) = z_q\},$$

meaning $L' = L_0(z_q)$, where z_q satisfies $[p]z_q = P_q$. Moreover, since $c(q) \neq 0$, thanks to Proposition 4.4.11, $c(l) \in \mathrm{Sel}(E/K)[p]$ and with the same argument used to prove $\mathrm{Gal}(L/L_0) \cong E[p]$ we obtain $\mathrm{Gal}(L'/L_0) \cong E[p]$.

Now, let $s \in \mathrm{Sel}(E/K)[p]^{+\epsilon}$ and $\rho \in I^+$. To show $[s, \rho] = 0$, we write $\rho = (\tau i)^2$ for some $i \in I = \mathrm{Gal}(L_0^S/L)$ (using Proposition 4.4.8). Let l be a prime of $\mathbb{Q}$ such that:

- $\tau i \in \mathrm{Frob}_{L_0^S/\mathbb{Q}}(l)$;
- $\tau j \in \mathrm{Frob}_{L'/\mathbb{Q}}(l)$ for some $j \in \mathrm{Gal}(L'/L)$ such that $j^{\tau+1} \neq \mathrm{id}$.

Such a prime l exists because $L' \cap L_0^S = L$; thus, the two conditions are independent, and by the Chebotarev Density Theorem (Theorem 3.4.13), there are infinitely many such primes.

By Propositions 4.3.15 and 4.3.16, we have $c(lq) \in \mathrm{Sel}_{\lambda\mathfrak{q}}(K, E[p])^{+\epsilon}$, where $\mathfrak{q} = q\mathcal{O}_K$ and $\lambda = l\mathcal{O}_K$. In fact, $c(lq)$ lies in $\mathrm{Sel}_\lambda(K, E[p])^{+\epsilon}$. Indeed, since $i \in I$, Proposition 4.4.11 implies $P_l \in pE(K_\lambda)$, so $c(l) = 0$. Using Lemma 4.3.17, we obtain

$$c(lq) \in \mathrm{Sel}_\lambda(K, E[p])^{+\epsilon}.$$

Again by Lemma 4.3.17, the local class $[c(lq)]_\lambda$ vanishes if and only if $P_q \in pE(K_\lambda)$. As established in the proof of Theorem 4.3.18, this is equivalent to l splitting completely in $L' = L_0(z_q)$, i.e.,

$$\mathrm{id} = \mathrm{Frob}_{L'/L_0}(l) = (\tau j)^2 = j^{\tau+1},$$

which contradicts our choice of j. Therefore, $c(lq) \in \mathrm{Sel}_\lambda(K, E[p])^{+\epsilon}$ and its class $[c(lq)]_\lambda \in H^1_{s,\mathcal{F}}(G_{K_\lambda}, E[p])$ is non-trivial.

Finally, applying Proposition 4.3.19, we conclude $s_\lambda = 0$. By Proposition 4.4.9, this is equivalent to $[s, \rho] = 0$, which completes the proof. □

Bibliography

[Cox22] David A Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions*. Vol. 387. American Mathematical Soc., 2022.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.

[Gro91] Benedict H Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)* 153 (1991), pp. 235–256.

[Har13] Robin Hartshorne. *Algebraic geometry*. Springer Science & Business Media, 2013.

[Kna92] A.W. Knapp. *Elliptic Curves*. Mathematical Notes - Princeton University Press. Princeton University Press, 1992. ISBN: 9780691085593. URL: `https://books.google.it/books?id=-e_qVoKF8H8C`.

[Lan87] Serge Lang. "Elliptic functions". In: *Elliptic functions*. Springer, 1987, pp. 5–21.

[Mil06] James S Milne. *Arithmetic duality theorems*. BookSurge, LLC Charleston, SC, 2006.

[Mil11] James S Milne. *Class field theory*. JS Milne, 2011.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Vol. 323. Springer Science & Business Media, 2013.

[Pol03] Alexander Polishchuk. *Abelian varieties, theta functions and the Fourier transform*. 153. Cambridge University Press, 2003.

[Ser13] Jean-Pierre Serre. *Local fields*. Springer Science & Business Media, 2013.

[Sha72] Stephen S Shatz. *Profinite groups, arithmetic, and geometry*. 67. Princeton university press, 1972.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. 2. Springer, 2009.