Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”

Corso di Laurea Triennale in Matematica

Elliptic Curves with Complex Multiplication

Relatore:
Prof. Longo Matteo

Laureando: Luca Marchesini
Matricola: 1236266

Anno Accademico 2021/2022

21 Luglio 2022

Contents

Chapter I

Introduction

A central question in the arithmetic of plane algebraic curves is deciding whether a given curve defined over a number field K has finitely or infinitely many K-rational points, especially $\mathbb{Q}$-rational points in this work. Restricting to smooth curves, it is reasonable to think that this problem depends first on the degree of the curve, assuming that the curves have equations with coefficients in $\mathbb{Q}$.

1. A degree one projective curve is a *line* in the projective plane, so it always has infinite $\mathbb{Q}$-rational points.

2. A degree two projective plane curve is called a *conic*. In this case, it is easy to prove that if it has one point, then it has infinitely many points; in particular, it is isomorphic to a projective line.

3. A degree three projective curve C is a *cubic*. If C is smooth, then the curve is not rational and the criteria for distinguishing the ones with finitely many points from the ones with infinitely many rational points are still conjectural in many cases. These curves define the family of *elliptic curves.*

4. A smooth curve C with degree greater than three always has geometric genus $g(C) > 1$, see [GH94, The genus formula, pg. 220-221] for a proof. Then, by a conjecture of Mordell, now called *Faltings's Theorem*, by Gerd Faltings, who proved it in 1983, all curves defined over $\mathbb{Q}$ with genus greater than one have only a finite number of $\mathbb{Q}$-rational points.

The aforementioned conjectural criterion for an elliptic curve E is the *Weak Birch and Swinnerton-Dyer conjecture.* This conjecture relates the rank of the group of $\mathbb{Q}$-rational points of the elliptic curve to the order of the vanishing at 1 of a complex-valued function $L(E, s)$, called the *Hasse-Weil L-function*, built by gluing local information of E. However, following the definition of $L(E, s)$, it was not clear whether the function was defined in $s = 1$. Thus, the problem of the existence of the analytic continuation of the Hasse-Weil L-function became crucial for the well-posedness of the conjecture. Now, we know that if E is defined over $\mathbb{Q}$ then $L(E, s)$ extends to a holomorphic function defined on all the complex plane, where $s = 1$ is the point of symmetry of the functional equation, as a consequence of the *Modularity Theorem*, proven by by Conrad, Diamond and Taylor, based on the work of Wiles. So, the general result was known to hold only in 2001, but at that time the problem was already solved for some special curves.

Historically, the first families of elliptic curves whose L-function was known to be entire are the following:

$$\begin{aligned} G^n &: y^2 = x^3 - nx \\ E^n &: y^2 = x^3 + n, \end{aligned} \tag{I.1}$$

where $n \in \mathbb{Z}$ and $n \neq 0$. For such curves, one can proceed by directly computing the local information as described in [Kob93, Chapter II]. Afterwards, this result was reinterpreted as a consequence of the theory of elliptic curves with *complex multiplication*.

An elliptic curve E, defined over a field of characteristic zero, has complex multiplication if its ring of endomorphisms $End(E)$ is larger than $\mathbb{Z}$. In such cases, the additional structure gives rise to a rich and fascinating theory, where geometry, analysis and algebra intersect. As a consequence of this theory, the local information of an elliptic curve with such properties acquires more regularity and this finally leads to the analytic continuation of $L(E, s)$ and to an elegant functional equation.

The aim of this work is to demonstrate the analytic continuation and the functional equation of an elliptic curve, with associated Weierstrass equation with coefficients in $\mathbb{Q}$, with complex multiplication by the full ring of integers of an imaginary quadratic extension of $\mathbb{Q}$. We will develop the basic theory of complex multiplication following mainly [Sil09] and [Sil91] to conclude with the aforementioned results by a natural generalization of the arguments presented in [Kob93, Chapter II]. The above restrictions play an important role, simplifying many arguments and making the treatment of the subject more elementary while exhausting the problem for a family of curves which is a natural extension of the ones described in (I.1).

In the next chapter, we will define and study the main geometric objects of this work, hence varieties and elliptic curves. Furthermore, we will focus on isogenies following the treatment of [Was08], the main reference for [Sut17a] and [Sut17b].

In the third chapter, we will deal with the elliptic curves defined over $\mathbb{C}$ and their relationship to *complex tori*, following [Mir95]. This connection will enable us to prove many properties of such curves, culminating in the characterization of the endomorphism ring $End(E)$.

In the fourth chapter, we will develop the associated algebraic theory and in particular we will study the properties of the reductions of elliptic curves with respect to a prime $\mathfrak{p}$, generalizing and making explicit the results proved in the previous chapter.

In the fifth chapter, we will use the theory introduced before to obtain the local information associated with such elliptic curves, proving the Weil conjectures in such cases and treating the cases of "bad reduction". The regularity of the local information and the proof of the analytic continuation and of the functional equation will be discussed in the last chapter.

Finally, we will develop, in parallel with the general theory, the examples of the curves of the form (I.1), where their special structure allows for more direct computations, which are presented in §V.3 and §VI.3.

Chapter II

Geometric Structure

II.1 Algebraic Curves

We fix the setting of this work.

Definition II.1.1. The *Affine n-space* over the field K is the set of n-tuples

$$\mathbb{A}^n(K) = \{(x_1, \dots, x_n) \mid x_i \in K\}.$$

Given $x \in \mathbb{A}^n(K)$, x_i is said to be the *i-th coordinate* of x.

Definition II.1.2. The *Projective n-space* over the field K is the set

$$\mathbb{P}^n(K) = \frac{\mathbb{A}^{n+1}(K) \setminus \{O\}}{\sim}$$

where $x \sim y \iff \exists\ \lambda \in K^*$ such that $x_i = \lambda y_i$, for every $0 \leq i \leq n$. The equivalence class of $(x_0, x_1, \dots, x_n) \in \mathbb{A}^{n+1}(K)$ is denoted by $[x_0, x_1, \dots, x_n]$ and the single x_i are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n(K)$.

Now we focus on the objects of algebraic geometry. In particular, the following definition establishes a connection between algebraic objects, represented by polynomials, and geometric objects, represented by subsets of $\mathbb{A}^n(\bar{K})$ or $\mathbb{P}^n(\bar{K})$.

Definition II.1.3. Let $\bar{K}[x] = \bar{K}[X_1, \dots, X_n]$ be the polynomial ring in n variables, and let $I \subset \bar{K}[X]$ be an ideal. The *affine algebraic set* associated to I is:

$$V_I = \{P \in \mathbb{A}^n(\bar{K}) \mid f(P) = 0\ \forall f \in I\}.$$

Moreover given $V \subset \mathbb{A}^n(\bar{K})$ the *ideal generated* by S is:

$$I(V) = \{f \in \bar{K}[X] \mid f(P) = 0\ \forall P \in V\}.$$

Similarly let $\bar{K}[X]_h = \bar{K}[X_0, \dots, X_n]_h$ denote the set of homogeneous polynomials in $n + 1$ variables. We write $I \subset \bar{K}[X]_h$ if we can choose generators of I that belong to $\bar{K}[X]_h$. So we can define a *projective algebraic set* associated to the ideal $I \subset \bar{K}[X]_h$ and we can define the *ideal* $I(S) \subset \bar{K}[X]_h$ *generated* by $S \in \mathbb{P}^n(\bar{K})$.

Remark II.1.4. By the Hilbert Basis Theorem, each ideal of $K[X]$ is finitely generated, hence finding the related algebraic set is equivalent to finding the zeros of a system of polynomial equations over an algebraically closed field, a much more familiar problem.

The next theorem measures, for any ideal I, how far this connection is from being an equivalence.

Theorem II.1.5 (Hilbert Nullstellensatz). *Let $I \in \bar{K}[X]$ be an ideal. Then*

$$I(V_I) = \sqrt{I}$$

where $\sqrt{I} = \{f \in \bar{K}[X] \mid f^n \in I, \textit{for some}\, n \in \mathbb{N}\}$.

Remark II.1.6. We note that if the ideal $I = P_1 P_2 \dots P_n \subset \bar{K}[X]$ is a product of distinct prime ideals, then $\sqrt{I} = I$, so that $I(V_I) = \sqrt{I} = I$. As a consequence, we can consider I or V_I without losing information. Moreover $V(I) = \bigcup_{i=1}^{n} V(P_i)$. This means that the decomposition of the ideal into distinct factors corresponds to the decomposition of the algebraic set into the union of distinct algebraic sets.

Definition II.1.7 (Variety)**.** An affine algebraic set V is called a *(affine) variety* if the ideal $I(V) \subset \bar{K}[X]$ is a prime ideal. Similarly, a projective algebraic set V is called a *(projective) variety* if the ideal $I(V) \subset \bar{K}[X]_h$ is a prime ideal.

From the perspective of diophantine geometry we are interested in studying the points of a variety, hence by the above remark limiting to the prime ideals is not a real restriction. Moreover, instead of looking at the variety over algebraically closed fields, it is also interesting to look at it over smaller fields.

Definition II.1.8. A variety V is *defined over* K if there exist generators $f_i \in K[X]$ of $I(V)$. We denote it by V/K. Moreover, if V is affine and defined over K, we define the *K-rational points* as

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

Similarly we define the K-rational points for a projective variety with the convention that $[x_0, \ldots, x_n] \in \mathbb{P}^n(K)$ if $(\frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}) \in \mathbb{A}^n(K)$, for some $0 \leq i \leq n$ such that $x_i \neq 0$.

Remark II.1.9. We stress that even if a variety V/K is defined over K the points of V lie in an algebraically closed field extension of K.

Remark II.1.10. Historically, (x, y) and (x, y, z) are the oriented basis for the affine spaces $\mathbb{A}^2(K)$ and $\mathbb{A}^3(K)$. So, given a point $P \in \mathbb{A}^2(K)$ or $P \in \mathbb{A}^3(K)$, we will denote its first coordinate by P_x or x_P, its second coordinate by P_y or y_P and, if $P \in \mathbb{A}^3(K)$, its third coordinate by z_P or P_z.

Example II.1.11. Let $(y) \subset \mathbb{C}[x, y, z]$ be an ideal. Then $V_{(y)} = \{P \in \mathbb{A}^3(\mathbb{C}) \mid P_y = 0\}$ is an affine variety V, because by Theorem II.1.5 the ideal $I(V) = \sqrt{(y)} = (y)$ is irreducible in a UFD, hence prime. In general a variety generated by a proper principal ideal, i.e. generated by a single polynomial of non-zero degree, is called a *hypersurface*. The variety V is also defined over $\mathbb{Q}$ and we can look for its rational points, which are $V[\mathbb{Q}] = \{(a, 0, c) \in \mathbb{A}^3(\mathbb{Q}) \mid a, c \in \mathbb{Q}\}$.

Next, we focus on a subfamily of the varieties we defined.

Definition II.1.12 (Plane Algebraic Curve)**.** A variety V/K is called a plane algebraic curve if it is a hypersurface in $\mathbb{P}^2(\bar{K})$ or $\mathbb{A}^2(\bar{K})$.

A hypersurface V is generated by $(f) = I(V)$, where the polynomial f is unique up to an invertible element of $\bar{K}[x]$ and hence a constant. For this reason, we will define the variety V by the polynomial f.

Definition II.1.13. The *degree* of a plane algebraic curve V/K is the degree of the polynomial $f \in K[x]$, such that $I(V) = (f)$.

Remark II.1.14. So far, we have stressed the similarity between affine theory and projective theory. In fact, given a projective variety V, we can associate with it its *affinization* V^a with respect to a hyperplane $H \subset \mathbb{P}^n(\bar{K})$, $V \not\subseteq H$, which is an affine variety. Furthermore, given an affine variety V_1 we can associate with it its *projective closure* $\bar{V}_1$, again by fixing a hyperplane in $H \subset \mathbb{P}^n(\bar{K})$. If such operations are done with respect to the same hyperplane, then they are one inverse of the other for a variety. This result tells us that we can pass from the affine to the projective description of a curve and vice versa, losing only a finite number of points, i.e. the ones in $V \cap \mathbb{H}$.

If we move to the study of the points of a plane algebraic curve, we can divide them into two classes.

Definition II.1.15. Given a plane algebraic curve $f \in K[X]$, a point $P \in V_{(f)}$ is *singular* if and only if

$$\nabla f(P) = 0$$

where $\nabla_i f(P) = \frac{\partial f(P)}{\partial x_i}$ is the vector of formal derivatives with respect to x_i. A point $P \in V$ is *smooth* if it is not singular. A variety is *smooth* if it has no singular points.

Now, let's state a useful application of the smoothness condition, which will be useful later to prove that some algebraic sets are varieties.

Proposition II.1.16. *Let $f \in K[X]_h$ be a polynomial such that $\nabla f(P) \neq 0$ for every $P \in \mathbb{P}^n(\bar{K})$. Then $V_{(f)}$ is a projective variety.*

Proof. Since $\bar{K}[X]$ is an UFD, it is enough to show that (f) is irreducible in $\bar{K}[X]$ to show that (f) is prime. Assume, by contradiction, that $f = gh$ with $g, h \in \bar{K}[X]_h$ and $\deg(g), \deg(h) \geq 1$. Then by the *Bézout Theorem*, see [Wal00] for a proof, the set $C = V_{(f)} \cap V_{(g)} \neq \emptyset$. As a result, if we fix a point $P \in C$, then $g(P) = h(P) = 0$, so that

$$\nabla f(P) = \nabla(gh)(P) = \nabla g(P)h(P) + g(P)\nabla h(P) = 0.$$

This is the contradiction. □

II.2 Algebraic Maps

So far we only presented the algebraic objects, now we look at the algebraic functions associated.

Definition II.2.1. Given an affine variety V/K the *coordinate ring* is the ring

$$K[V] = \frac{K[X]}{I(V) \cap K[X]} .$$

Similarly if $V/\bar{K}$ is a projective variety the *coordinate ring* is the ring

$$K[V] = \frac{K[X_0, \dots, X_n]}{I(V) \cap K[X_0, \dots, X_n]} .$$

Remark II.2.2. With the above definition we are simply identifying two polynomials if and only if they are equal as functions from V to $\bar{K}$.

Since $I(V)$ is prime, the coordinate ring is always a domain. As a result, we can consider its field of fractions $\bar{K}(V)$, called the field of *rational functions*. In the case of projective varieties, the field of *rational functions* $K(V)_h$ is the subfield of the field of fractions of $K[V]$ whose elements have the form $\frac{f}{g}$, where the polynomials $f, g \in \bar{K}[V]$ are homogeneous and have the same degree.

Definition II.2.3. Let $V_1/K, V_2/K$ be projective varieties. A *rational map* ϕ is a map of the form

$$\phi : V_1 \to V_2 \quad \phi = [f_0, \dots, f_n]$$

where the functions $f_0, \dots, f_n \in \bar{K}(V_1)_h$ have the property that for every point $P \in V_1$ at which $\phi(P)$ is defined then $\phi(P) \in V_2$. Moreover, if for each point $P \in V_1$ for which $\phi(P)$ is not defined there exists $g \in \bar{K}(V)_h$ such that

1. $(gf_i)(P) \in \bar{K}$, for every $1 \leq i \leq n$
2. $(gf_i) \neq 0$ for some i

then we define $\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$ and we say that ϕ is a *morphism.* We say that ϕ is *defined over* L if $f_0, \ldots, f_n \in L(X)_h$.

Definition II.2.4. A morphism $\phi : V_1 \to V_2$ is an isomorphism if there exists a morphism $\phi^{-1} : V_2 \to V_2$ such that $\phi^{-1} \circ \phi = id_{V_1}$ and $\phi \circ \phi^{-1} = id_{V_2}$. If such ϕ exists, then V_1 and V_2 are said to be isomorphic. In particular, if ϕ is defined over K, then V_1 and V_2 are said to be isomorphic over K.

Remark II.2.5. Consider a rational map of projective varieties $\phi : V_1 \to V_2$ and let $\phi = [f_0, \ldots, f_n]$ with $f_0, \ldots, f_n \in \bar{K}(V_1)_h$. There is an alternative way to describe the map. In fact, we can multiply all the homogeneous coordinates by the denominators of $f_0, \ldots, f_n$ to obtain the same map $\phi = [g_0, \ldots, g_n]$, where $g_0, \ldots, g_n \in \bar{K}[V_1]$ are homogeneous polynomials of the same degree.

A morphism of affine varieties is defined by requiring that the projective closure of the map, i.e. the homogenization of the rational functions that define ϕ, is a morphism for the projective closure of the affine varieties. As a result, any morphism of affine varieties can be transformed into a morphism of the projective closure of such varieties. In contrast, a morphism $\phi : V_1 \to V_2$ of projective varieties can be transformed into a morphism of the affinization of such varieties only if $\phi(V_1) \not\subseteq H$, where $H \subset V_2$ is the hyperplane with respect to we perform the affinization of V_2.

Example II.2.6. Let $f = x_1^2 x_2 - x_1^3 - x_2 x_0 \in K[x_1, x_2, x_3]$ be a homogeneous polynomial. Just assume $\nabla(f)(P) \neq 0$, for every $P \in \mathbb{P}^2(\bar{K})$. Then by Proposition II.1.16 $V_{(f)} = E$ is a smooth projective plane algebraic curve. In fact, E is a special case of plane algebraic curves called *elliptic curves.* Focusing on its morphisms, we see that E is defined over $\mathbb{Q}(i)$ and that over this field there is an isomorphism $\phi : E \to E$ given by $\phi = [-x_0, ix_1, x_2]$, with inverse $\phi^{-1} : E \to E$ given by $\phi^{-1} = [-x_0, -ix_1, x_2]$. For the affinization $f^a = y^2 - x^3 - x$, with respect to the fundamental hyperplane H_2, the related isomorphism is $\phi = (-x, iy)$ and the inverse morphism is $\phi^{-1} = (-x, -iy)$.

Remark II.2.7. We stress that two isomorphic varieties $V_1/\bar{K}$, $V_2/\bar{K}$ are not necessarily isomorphic over any subfield $L \subset \bar{K}$. In fact, if the isomorphism $\phi : V_1 \to V_2$ isn't defined over L then some L-rational points of V_1 could be sent to points not in $\mathbb{P}^2(L)$. That is the reason why for varieties V_1/L and V_2/L we will restrict ourselves to the morphisms defined over L.

II.3 Elliptic Curves

We begin our study of the *elliptic curves.*

Definition II.3.1 (Elliptic curve)**.** An *elliptic curve* is a pair (E, O), where E is a smooth curve of degree three and $O \in E$. A curve is defined over E, written E/K, if E is defined over K and $O \in K$.

We generally denote the elliptic curve by E or E/K, supposing that the point O exists.

II.3.1 Weierstrass Form

The general equation for an elliptic curve may be quite complicated and long:

$$\begin{aligned} e_9X_1^2X_2 + e_0X_1^3 + e_1X_1^2X_0 + e_2X_1X_0^2 + e_3X_0X_1X_2 + e_4X_1X_2^2 = \\ = e_5X_0^3 + e_6X_0^2X_2 + e_7X_0X_2^2 + a_8X_2^3. \end{aligned}$$

However it turns out that in most cases an elliptic curve is isomorphic, as a variety, to an elliptic curve with a simpler equation.

Proposition II.3.2 (Weiestrass form)**.** *Let $E/\bar{K}$ be an elliptic curve. If the characteristc of the field $char(\bar{K}) \neq 2, 3$, then the curve is isomorphic to a curve with equation*

$$X_1^2X_2 = X_0^3 + AX_0X_2^2 + BX_2^3.$$

This curve is the Weierstrass form of the elliptic curve.

Proof. We will suppose that any elliptic curve has an inflection point, we will not show this, but one can see [Wal00, Theorem III.6.4] for a proof. After a change of projective basis, we can assume $O = [0, 1, 0]$ to be an inflection point with tangent $X_2 = 0$ so that $e_0, e_1, e_2 = 0$. Moreover, we can assume $e_9, e_5 = 1$ because the curve is an irreducible cubic. As a result, we end up with a curve of the form:

$$X_1^2X_2 + a_1X_0X_1X_2 + a_3X_1X_2^2 = X_0^3 + a_2X_0^2X_2 + a_4X_0X_2^2 + a_6X_2^3.$$

From now on we will consider the affinization of the curve with respect to X_2:

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

This is called the *generalized Weierstrass form* for an elliptic curve, and, as we have shown, it exists for any field of definition $\bar{K}$. Now, if $char(\bar{K}) \neq 2$ then we can make the substitution:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3),$$

then

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

where

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

Next, if $char(\bar{K}) \neq 3$ we can make the substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right),$$

which yields the final equation:

$$E^a : y^2 = x^3 - 27c_4x - 54c_6$$

with

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

All the maps we presented are linear and invertible, hence we built an isomorphism of elliptic curves. □

Remark II.3.3. Given an elliptic curve $E/\bar{K}$, the above construction shows us that the Weierstrass form is not unique. However, all its Weierstrass forms are isomorphic over $\bar{K}$. Then from now on the Weierstrass form associated to an elliptic curve will be simply one of such forms.

From now on, we will say that an elliptic curve E/K is *defined over the ring* R if it has an associated Weierstrass form with affine equation $y^2 = x^3 + Ax + B$, with $A, B \in R$.

The Weierstrass form will simplify the study of these curves. In particular, we start by presenting two interesting quantities that play a key role in the description of an elliptic curve.

Definition II.3.4. Given an elliptic curve $E/\bar{K}$ with affine Weierstrass equation $y^2 = x^3 + Ax + B$, we define the *discriminant*

$$\Delta = 16Disc(x^3 + Ax + B) = -16(4A^3 + 27B^2)$$

and the *j-invariant*

$$j_E = -1728\frac{(4A)^3}{\Delta}.$$

Proposition II.3.5. *Consider $char(\bar{K}) \neq 2, 3$.*

1. *A curve given by a Weierstrass equation is smooth if and only if $\Delta \neq 0$.*
2. *Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.*

Proof. 1. First, we notice that the only point of the elliptic curve that is not in the affinization of the curve is $O = [0, 1, 0]$, which is smooth, being an inflection point. Then, by Euler's identity on homogeneous polynomials f of degree n:

$$nf = X_0\frac{\partial f}{\partial X_0} + X_1\frac{\partial f}{\partial X_1} + X_2\frac{\partial f}{\partial X_2},$$

a point $P \notin H_2$ is singular if and only if

$$f(P) = 0 \quad \frac{\partial f}{\partial X_0}(P) = 0 \quad \frac{\partial f}{\partial X_1}(P) = 0.$$

This is true if and only if

$$f^a(P^a) = 0 \quad \frac{\partial f^a}{\partial x} = 0 \quad \frac{\partial f^a}{\partial y} = 0.$$

We reduced the smoothness condition of a curve in Weierstrass form to

$$\begin{cases} y^2 = x^3 + Ax + B \\ 2y = 0 \\ \frac{d(x^3+Ax+B)}{dx} = 0. \end{cases} \tag{II.1}$$

But $MCD(f, f') \neq 0 \iff f$ has distinct roots $\iff Disc(f) = 0$. Then, since $\Delta = 16Disc(x^3 + Ax + B)$ and $char(\bar{K}) \neq 2$, we conclude that E/K is smooth if and only if $\Delta(E) \neq 0$, $\text{char}(K) \neq 2, 3$.

2. An isomorphism between two elliptic curves yields an isomorphism between their Weierstrass form, but the only isomorphism that preserves this form is

$$(x,y) \mapsto \big(u^2x, u^3y\big) \qquad u \neq 0,$$

with the new affine equation given by

$$E' : y^2 = x^3 + Au^4x + Bu^6.$$

As a result

$$\Delta' = u^{12}\Delta \qquad j_{E'} = -1728\frac{u^{12}(4A)^3}{u^{12}\Delta} = j_E$$

and this settles the first part. Now we have to show that two curves with the same j-invariant are isomorphic. Given the two associated Weierstrass equations

$$y^2 = x^3 + Ax + B \qquad y'^2 = x'^3 + A'x' + B',$$

the equality of the j-invariant is equivalent to

$$\frac{1728(4A)^3}{16(4A^3+27B^2)} = \frac{1728(4A')^3}{16(4A'^3+27B'^2)} \iff A'^3B^2 = A^3B'^2.$$

We distinguish three cases.

(a) The invariant $j_E = 0$. Then the coefficients have the property that $A = A' = 0$, so that the isomorphism is obtained with the above substitution with $u = (\frac{B'}{B})^{\frac{1}{6}}$.

(b) The invariant $j_E = 1728$. Then the coefficients have the property that $B = B' = 0$, so that the isomorphism is obtained with $u = (\frac{A'}{A})^{\frac{1}{4}}$.

(c) The invariant $j_E \neq 0, 1728$. Then we set $u = (\frac{A'}{A})^{\frac{1}{4}} = (\frac{B'}{B})^{\frac{1}{6}}$.

□

Remark II.3.6. We stress that the j-invariant completely describes the isomorphism classes over $\bar{K}$. However, if we restict only to the isomorphisms defined over a field $K \subset \bar{K}$, there could be many more isomorphism classes. Consider, as an example, an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ in Weierstrass form. Then the curves $E/\mathbb{Q} : y^2 = x^3 + An^2x + Bn^3$, with $n \in \mathbb{Z}^*$ square-free, are an infinite family of elliptic curves with the same j-invariant but not isomorphic over $\mathbb{Q}$. Except for $j_E = 0, 1728$, it turns out that these are all the additional isomorphism classes over $\mathbb{Q}$ and are called *twists* of $E/\mathbb{Q}$.

II.3.2 The Group Law

After having introduced a normal form for the elliptic curves, we focus on the structure carried by the geometry of such curves. Consider an elliptic curve with an equation with coefficients in K, then, by the definition, there is a K-rational point $O \in E$. A simple corollary of *Bézout Theorem* for algebraic curves states that:

Theorem II.3.7. *Given a projective plane algebraic curve $C/\bar{K}$ of degree d, a projective line l intersects C in d points, counted with multiplicity.*

The multiplicity of intersection, in general, is subtle to define, but in this case it is simply the multiplicity of a point as the root of the homogeneous polynomials obtained by substituting the equation of the line into the equation of the curve. Now, consider two points $P_1, P_2 \in E[L]$, for a field $L \supseteq K$. We would like to define a geometric sum of these points, then, encouraged by Theorem II.3.7, we define

$$P_1 * P_2 = P_3,$$

where the point P_3 is the third intersection with E of the unique line passing through P_1 and P_2, with multiplicity. This means that if $P_1 = P_2$ then we have to take the tangent line of $P_1 \in E/K$ and if P_1 is an inflection point $P_1 * P_1 = P_1$. The operation is stable in the following sense: since E has an equation with coefficients in K, it turns out that the third point will belong to $E[L]$ as well. However, the sum lacks an identity, which is the reason why we had to fix a point O.

Definition II.3.8. Let $(E/K, O)$ be an elliptic curve with an equation with coefficients in K with a K-rational point O. Then given $P_1, P_2 \in E/K$ we define:

$$P_1 + P_2 = O * (P_1 * P_2).$$

Proposition II.3.9. *The addition structure of an elliptic curve $(E/K, O)$ turns the K-rational points of E into an abelian group. In particular:*

1. *O is the identity,*

2. *$(O * O) * P_1 = -P_1$,*

3. *if we choose another K-rational point O' then $(E/K, O) \cong (E/K, O')$ by the translation:*
$$\tau_{o'} : P_1 \mapsto P_1 + O'.$$

Proof. We notice that the addition is obviously commutative; in fact, the difficult part is establishing the associativity of this operation, see [Sil09, Prop III.2.2e].

1. $O + P_1 = O * (O * P_1) = O * P_2 = O$ since the three points O, P_1, P_2 are collinear.

2. $(O * O) * P_1 + P_1 = O * (((O * O) * P_1) * P_1) = O * (O * O) = O + O = O$ and we conclude by commutativity.

3. First, $\tau_{O'}(O) = O'$. Now, we have to verify that given two points of the form $P - O'$, $Q - O'$, then $P + Q - O' = P +' Q$ holds. We rewrite the expression as $P + Q = (P +' Q) + O'$ and we realize that it is equal to
$$(P +' Q) + O' = O * (O' * (O' * (P * Q)))) = O * (P * Q) = P + Q$$
since the points $O', P * Q, O' * (P * Q)$ are collinear.

□

Remark II.3.10. The proposition we just proved shows that the choice of the base point $O \in E/K$ does not affect the structure of the group. Therefore, in general, we will not specify this point supposing that it exists. However, if we have a curve in the Weierstrass form, we will always choose $O = [0, 1, 0]$, hence the point at infinity. There are some reasons for this; the geometrical one is a question of symmetry. Setting an inflection as the base point is convenient, since in this case $O * O = O$ and, as a consequence, the negation is obtained by $-P_1 = O * P_1$, so that $P + Q = O * (P * Q) = -(P * Q)$ which is equivalent to changing the sign of the y coordinate of the affinization of $P * Q$. For example, this will make it easier to write some morphisms of elliptic curves explicitly.

Example II.3.11. Given an elliptic curve E/K in Weiestrass form, the addition of $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$, two points in the affinization of the curve, is easy to write. Set $s = \frac{y_P - y_Q}{x_P - x_Q}$. Then

$$\begin{cases} y^2 = x^3 + Ax + B \\ y = s(x - x_P) + y_P \end{cases} \qquad \begin{cases} s^2x^2 - 2xx_Ps^2 + x_P^2s^2 = x^3 + Ax + B \\ y = s(x - x_P) + y_P. \end{cases} \tag{II.2}$$

But we know that the roots of the last polynomial are x_P, x_Q, x_{P*Q}. So that

$$-s^2 = -x_P - x_Q - x_{P*Q}$$

and

$$x_{P+Q} = s^2 - x_P - x_Q \qquad y_{P+Q} = s(x_P - x_{P+Q}) - y_P,$$

where we recall that $x_{P+Q} = x_{P*Q}$ and that $y_{P+Q} = -y_{P*Q}$, since $P + Q = O * (P * Q) = -P * Q$ and $O = [O : 1 : O]$ is an inflection point.

II.3.3 Torsion Points

Investigating the structure of the group E/K is first of all studying an abelian group. An important property of an element of such groups is the following.

Definition II.3.12. Let G be an abelian group. An element $g \in G$ is a torsion element if it has finite order. Then we define $G_{Tor} = \{h \in G \mid |h| < \infty\}$ to be *the torsion subgroup* of G.

This is the finite-order part of our group. In the same way, we could study the infinite part.

Definition II.3.13. Let G be an abelian group. Then $\text{rank}(G)$ is the dimension of $\frac{G}{G_{Tor}} \otimes \mathbb{Q}$, the $\mathbb{Z}$-module with $\mathbb{Q}$ coefficients, as a $\mathbb{Q}$-vector space.

Remark II.3.14. The definition is well-posed, since $\frac{G}{G_{Tor}}$ is torsion-free and abelian. Moreover, if G is finitely generated, then obviously $\text{rank}(G) < \infty$.

Now, we transfer these definitions to the elliptic curves.

Definition II.3.15 (n-Torsion Point)**.** Let (E/K, O) be an elliptic curve, $n \in \mathbb{N}^*$. Then the group of n-Torsion Points is:

$$E[n] = \{P \in E/K \mid nP = O\}.$$

Remark II.3.16. We emphasize that $E_{Tor} = \bigcup_{n \in N} E[n]$.

Example II.3.17 (2-Torsion Points)**.** Let E/K be an elliptic curve in Weierstrass form with affine equation $y^2 = x^3 + Ax + B$. We want to describe the points of 2-torsion. We first note that $P + P = O$ if and only if $P = -P$ and, looking at the affinization, this means that $P_y = -P_y = 0$. Then the 2-torsion points have the form $[\xi_i : 0 : 1]$ with ξ_i the roots of $x^3 + Ax + B$, which are distinct since $\Delta_E \neq 0$.

Definition II.3.18 (Rank)**.** Let E/K be an elliptic curve. Then $rank(E[K])$ is the rank of the abelian group of the K-rational points of the curve.

The following famous result implies that the rank of an elliptic curve is always finite over $\mathbb{Q}$.

Theorem II.3.19 (Mordell's Theorem)**.** *Let E/K be an elliptic curve defined over $\mathbb{Q}$. Then the group of rational points is finitely generated.*

Remark II.3.20. As a consequence $rank(E[\mathbb{Q}]) = 0$ if and only if the curve has finite rational points. Therefore, to distinguish the curves with a finite number of rational points from those with an infinite number of rational points, the determination of the rank is fundamental. The theory we will expose builds a conjectural bridge between the rank and other objects associated to the elliptic curve of simpler evaluation.

II.4 Isogenies

Since the elliptic curves carry both the structure of an algebraic variety and of an abelian group, it is natural to define a map for such curves in the following way.

Definition II.4.1 (Isogeny)**.** Let $E_1/K, E_2/K$ be elliptic curves. A map $\phi : E_1 \to E_2$ is an *isogeny* if it is a morphism of varieties from E_1/K to E_2/K and a homomorphism of groups. An isogeny $\phi : E_1 \to E_1$ is called an endomorphism.

Example II.4.2 (Isomorphism)**.** We have already met some simple isogenies. Let E_1/K, E_2/K be elliptic curves in Weierstrass form with affine equation given by $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + Au^4x + Bu^6$, $u \in K^*$. Then the isomorphism $\phi : E_1 \to E_2$ of the affine curves

$$\phi : (x, y) \mapsto \left(xu^2, yu^3\right)$$

is an isogeny:

1. $\phi(O) = \phi([0 : 1 : 0]) = [0 : \frac{1}{u} : 0] = [0 : 1 : 0] = O'$,
2. $\phi(P+Q) = \phi(P) +' \phi(Q)$ since the map is linear and so preserves the projective lines, hence it respects the geometric addition law.

It is an isomorphism since we can write the inverse isogeny $\phi^{-1} : (x, y) \to \left(\frac{x}{u^2}, \frac{y}{u^3}\right)$.

Example II.4.3 (multiplication-by-2 map)**.** Let E/K an elliptic curve with affine Weierstrass equation $f : y^2 = x^3 + Ax + B$ and consider a point $P = (x_P, y_P) \in E$. We want to prove the sum $P + P = 2P$ is an isogeny. Following the definition of the geometric group law it's enough to express the intersection of the tangent line to P with the curve in terms of rational functions of x_P, y_P.

$$t_P : \frac{\partial f}{\partial x}(P)(x - x_P) + \frac{\partial f}{\partial y}(P)(y - y_P) = 0$$
$$t_P : y = \frac{3x_P^2 + A}{2y_P}(x - x_P) + y_P$$

Substituting in the equation of the curve we get:

$$x_{2P} = \frac{(3x_P^2 + A)^2}{4y_p^2} - 2x_P = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4(x_P^3 + Ax_P + B)}$$
$$y_{2P} = \frac{x_P^6 + 5Ax_P^4 + 20Bx_P^3 - 5A^2x_P^2 - 4ABx_P - A^3 - 8B^2}{8(x_P^3 + Ax_P + B)^2} y_P$$

where we substituted $y_P^2 = x^3 + Ax + B$. Further, it's easy to check the rational map is a morphism so that $[2] : E \to E$ is an isogeny.

As for the addition formula we could obtain an algebraic expression also in the case E/K is not in Weierstrass form, repeating the procedure.

Now we are ready to state the following notable result.

Theorem II.4.4. *Let $E_1/K, E_2, K$ be elliptic curves. Then the isogenies from E_1 to E_2 have a natural group structure.*

Proof. The homomorphisms of an abelian group have a natural group structure $(\phi + \psi) = \phi_1(a) + \psi(a)$. As a consequence it's enough to prove that if $\phi, \psi : E_1 \to E_1$ are isogenies then $\phi + \psi$ can be written as a rational map too. Then we can use the fact that the addition and duplication operations are given by algebraic maps on the coordinates of the points.

1. Case $\phi = \psi$. Then $\phi + \psi = 2\psi = [2] \circ \psi : E_1 \to E_2$, where $[2] : E_2 \to E_2$ is the multiplication-by-2 map on E_2.

2. Case $\phi = -\psi$. Then $\phi + \psi$ is the multiplication-by-0 morphism, given by $[X_0 : X_1 : X_2] \mapsto O$.

3. Otherwise the addition formula is a rational map of the coordinates of the two points P, Q we have to sum. Then, if we substitute instead of the coordinates of the points the rational maps which define, coordinate by coordinate, the isogenies we get a rational map which is equal to $\phi + \psi$.

□

Corollary II.4.5. *The multiplication-by-m maps, $m \in \mathbb{Z}$, are isogenies. Moreover, if the equation of the elliptic curve in Weiertrass form is $y^2 = x^3 + Ax + B$ then the rational maps that define the isogeny have coefficients in $\mathbb{Z}[A, B]$.*

Proof. First, we recall that the identity map is the multiplication-by-1 isogeny and that the multiplication-by-(-1) is an isogeny with coefficients in $\mathbb{Z}$, in fact notice that $[-1] : (x, y) \mapsto (x, -y)$. Then, by the above theorem we conclude that the maps $[m] = [1] + [1] + \cdots + [1]$ and $[-m] = [-1] + [-1] + \cdots + [-1]$ are isogenies. Moreover the addition and duplication formula have rational maps with coefficients in $\mathbb{Z}[A, B]$. As a consequence we conclude that any isogeny $[m]$ has coefficients defined in $\mathbb{Z}[A, B]$. □

II.4.1 Standard Form

In this section, in order to simplify the notation, the term "isogeny" will stand for "non-zero isogeny".

For elliptic curves in Weierstrass form the example II.4.3 suggests the existence of a special form for an endomorphism. In fact the following result holds for all isogenies of such curves.

Proposition II.4.6 (Standard form)**.** *Let $E_1/K, E_2/K$ be elliptic curves in Weierstrass form with equations $y^2 = f_1$, $y^2 = f_2$ and let $\phi : E_1 \to E_2$ be an isogeny. Then ϕ can be defined through the affine rational maps:*

$$\phi(x, y) = \left(\frac{r(x)}{v(x)}, \frac{t(x)}{w(x)} y \right)$$

where the polynomials $r(x), s(x), v(x), w(x) \in K[x]$. Moreover $gcd_{K[x]}(r(x), v(x)) = 1$ and $gcd_{K[X]}(t(x), w(x)) = 1$, $v^3 | w^2$ and $w^2 | v^3 f_1$. This expression is unique.

Proof. Uniqueness. The rational maps are defined over $\bar{K}(E)$, then the only possible substitution is $y^2 \mapsto x^3 + Ax + B$. So, consider an isogeny with two standard forms: their difference coordinate by coordinate is the zero element in $\bar{K}(E)$ but it's evident that we can't make substitutions if the isogeny is in standard form, so their difference is zero, which means two such forms are equal.
Existence. The proof of the existence of such a form is quite elementary, however for the sake of brevity we won't prove it generally, see [Sut17a] or [Was08] for the proof. Such form will arise naturally for the endomorphisms of some elliptic curves we will see later. □

This is called the *standard form* and plays a crucial role in simplifying the theory needed to study the isogenies, at the cost of restricting many general results to $char(K) \neq 2, 3$.

Remark II.4.7. Consider $v_1(x) = \frac{v(x)}{gcd(v(x), f_1(x))}$ and $w_1(x) = \frac{w(x)}{gcd(w(x), f_1(x))}$. Then the polynomial $v_1^3 | w_1^2$ and $w_1^2 | v_1^3$ hence $v_1(x) = u_1^2(x)$ and $w_1(x) = u_1^3(x)$. Moreover also $gcd(v(x), f_1(x)) \mid gcd(w(x), f_1(x))$.

Proposition II.4.8. *Let $E_1/K, E_2/K$ be elliptic curves in Weierstrass form and let $\alpha : E_1 \to E_2$ be an isogeny. Then α is surjective.*

Proof. Restricting to the case of an isogeny in standard form, $\alpha = \left(\frac{r(x)}{v(x)}, \frac{t(x)}{w(x)} y \right)$. Let $(a, b) \in E_2$ and consider the polynomial $g_a(x) = r(x) - av(x)$, where a is different from the ratio of the leading coefficients of $r(x)$ and $v(x)$. Then g_a is a non-constant polynomial, hence it has at least a solution $x_0 \in \bar{K}$, so that $\frac{r(x_0)}{v(x_0)} = a$. Let $P = (x_0, y_0), -P = (x_0, -y_0) \in E_1$ be the points having x_0 as x-coordinate. Supposing $y_0 \neq 0$, P is not a 2-torsion point, then $\phi(\{P, -P\}) = \{(a, b), (a, -b)\}$, since they are the only points with x-coordinate equal to a. If P is a 2-torsion point then also (a, b) is a 2-torsion point, this means that there is only one point in E_2 which has x-coordinate equal to a. As a result necessarily $\phi(P) = (a, b)$. Moreover since the zeros are the only points at infinity of the elliptic curves and the zero of E_1 is mapped to the zero of E_2 we have almost concluded. It remains to prove the case in which the point $P = (a, b)$ has x-coordinate a equal to the ratio of the leading coefficients of $r(x)$ with $v(x)$. Then we can choose another point $P' \neq 0$, with $P'_x \neq a$ and such that $(P - P')_x \neq a$, this is possible since the elliptic curve E_2 has infinite affine points over $\bar{K}$ while there are at most two points with the same x-coordinate. This means there exist points Q_1, Q_2 such that $\alpha(Q_1) = P'$ and $\alpha(Q_2) = P - P'$ and since α is an isogeny $\alpha(Q_1 + Q_2) = \alpha(Q_1) +' \alpha(Q_2) = P$ and $E_1 \supset \alpha^{-1}(P) \neq \emptyset$. □

The standard form gives important information on the kernel of the isogenies.

Proposition II.4.9. *Let $E_1/K, E_2/K$ be elliptic curves and let $\alpha : E_1 \to E_2$ be an isogeny of standard affine form $\left(\frac{r(x)}{v(x)}, \frac{t(x)}{w(x)} y\right)$. Then the affine kernel is*

$$\ker_{\mathrm{a}}(\alpha) = \{P \in E_1 \mid v(P_x) = 0\}.$$

Proof. If $\bar{\alpha}(P) = [0 : 1 : 0]$ then $\alpha(P) \notin \mathbb{A}^2(\bar{K})$. This happens only if $v(P_x) = 0$ or $w(P_x) = 0$ because the numerator and denominator of α in standard form have no common roots. Since these two polynomials have the same roots we can restrict to $v(P_x) = 0$. We show now that the condition is sufficient by passing to the homogeneization of the isogeny. Then the morphism has the form $\bar{\alpha} : [\bar{r}(x_0, x_2)\bar{w}(x_0, x_2) : \bar{t}(x_0, x_2)\bar{v}(x_0, x_2)x_1 : \bar{w}(x_0, x_2)\bar{v}(x_0, x_2)]$. Now, We distinguish two cases. If $P_y \neq 0$ then, since $v^3 | w^2$, each root of v of multiplicity k has at least multiplicity $k + 1$ as a root of w so that normalizing by $\bar{w}(x_0, x_2)$ we obtain $\bar{\alpha}(P) = [0 : 1 : 0]$. If $P_y = 0$ then P_x is a root of the polynomial $f_1(x)$ such that the Weierstrass form of the curve is $y^2 = f_1(x)$. Then we can multiply the coordinates of $\bar{\alpha}$ by $x_2 x_1$ and divide them by the polynomial with the roots of $\bar{f}_1(x)$ in $\bar{w}(x)$. Thanks to the substitution $x_2 x_1^2 = \bar{f}_1(x_0, x_2)$ we can normalize the second homogeneous coordinate and make it nonzero. Finally, after normalizing $\bar{v}, \bar{w}$ as in the first passage, we obtain the desired result. □

This proves the following corollary.

Corollary II.4.10. *Let $E_1/K, E_2, /K$ be elliptic curves* $\mathrm{char}(K) \neq 2, 3$ *and let the map $\alpha : E_1 \to E_2$ be an isogeny. Then α has finite kernel.*

Proof. Considering the associated Weierstrass form of such curves then the isogenies have a standard form $\phi(x, y) = \left(\frac{r(x)}{v(x)}, \frac{t(x)}{w(x)} y\right)$. Since $\deg(v) < \infty$ and the affine points in the kernel have x-coordinate which is a root of $v(x)$ then $\#\ker(\alpha) \leq \deg(v) + 1$. In fact, except for the 2-torsion points that have y-coordinate equal to 0, all the other points have y-coordinate different from zero. So for each x-coordinate there are two choices of y, but these are the roots of $v_1 = \frac{v(x)}{gcd(v(x), f_1(x))}$, as in remark II.4.7, so that they are already counted twice. □

Example II.4.11 (Frobenius isogeny)**.** We show now an isogeny with trivial kernel which is not an isomorphism. Let $E/\bar{F_p}$ be an elliptic curve, defined over $\mathbb{F}_p$, with $char(K) = p > 0$. There is a morphism of the field that is called the *Frobenius automorphism*, given by $\phi_p : x \mapsto x^p$. Moreover $\phi(x) = x \iff x \in \mathbb{F}_p$. From the fact ϕ_p is a morphism of fields we obtain that given any rational map $\psi(x, y)$ with coefficients in $\mathbb{F}_p$ then $\phi_p(\psi(x, y)) = \psi(\phi_p(x), \phi_p(y))$. In particular it commutes with the map defining the sum of two points of the elliptic curve and the equation defining the elliptic curve. This means that $\phi_p : (x, y) \mapsto (x^p, y^p)$ defines an isogeny: if a point P respects the equation of the elliptic curve then $\phi_p(P)$ does the same and $\phi_p(P + Q) = \phi_p(P) + \phi_p(Q)$, for the above considerations. Its kernel is trivial since it is, coordinate by coordinate, a morphism of fields, hence injective. Moreover if E is in Weierstrass form $y^2 = x^3 + Ax + B$ then

$$\phi_p = (x^p, (x^3 + Ax + B)^{\frac{p-1}{2}} y)$$

in standard form, by making the substitution $y^2 \mapsto x^3 + Ax + B$. This tells us that no isogeny can be the inverse of such map: suppose ϕ_p^{-1} has a standard form then the x-coordinate should respect the equation $(\phi_x^{-1})^p = x$, which has no solutions in $\bar{K}(E)$. In general if E/K, K a perfect field, is not defined in $\mathbb{F}_p$ then the Frobenius morphism still defines an isogeny $\phi_p : E \to E^p$ but is not an endomorphism anymore: in fact the coefficients of the equation defining the elliptic curve change when raised to the p^{th}-power.

II.4.2 Degree

The considerations on the Frobenius isogeny lead to a distinction between the order of the kernel of an isogeny and the degree of the polynomials that define it.

Definition II.4.12 (Degree)**.** Let $E_1/K, E_2/K$ be elliptic curves, let $\alpha : E_1 \to E_2$ be an isogeny with standard form $\left(\frac{s(x)}{v(x)}, \frac{t(x)}{w(x)} y\right)$. We define the *degree* of the isogeny to be $\deg(\alpha) = \max\{\deg(s), \deg(v)\} = \deg(\bar{s}(x)) = \deg(\bar{v}(x))$ the projective closure of the polynomials.

We want to clarify the relationship between the degree and the kernel of an isogeny.

Proposition II.4.13 (Separability)**.** *Let α be an isogeny in standard form, where $\alpha : \left(\frac{s(x)}{v(x)}, \frac{t(x)}{w(x)} y\right)$ is defined over K. Then the following conditions are equivalent.*

1. $\frac{d\left(\frac{u}{v}\right)}{dx} = 0$.
2. $u' = v' = 0$.
3. $u = f(x^p)$ *and* $v = g(x^p)$ *with* $char(K) = p > 0$

Then α is inseparable *if it meets one of the following conditions. Otherwise it is called* separable.

Proof.

$1 \to 2$. $(\frac{u}{v})' = 0 \iff \frac{u'v-v'u}{v^2} = 0 \iff u'v - v'u = 0$. Then $gcd(u,v) = 1$ since it is in standard form, so that $v|v'$ and $u|u'$ but $\deg(v') < \deg(v)$ and $\deg(u') < \deg(u)$. As a consequence necessarily $v' = u' = 0$.

$2 \to 3$. This is obvious from the definition of formal derivatives of polynomials: the exponent of the monomials has to be divisible by p for its derivative to vanish.

$3 \to 1$. $u' = 0$ and $v' = 0$ so $\frac{u'v-v'u}{v^2} = 0$ then $(\frac{u}{v})' = 0$.

□

Corollary II.4.14. *All the isogenies in standard form are composition of a purely inseparable part, given by a power of the frobenius isogeny, and a separable part.*

Proof. If the isogeny is separable we have nothing to prove. If it is inseparable we obtain the result by repeatedly applying the third condition in the proposition above. □

Corollary II.4.15. *All the isogenies defined over K, $char(K) = 0$, are separable.*

By Corollary II.4.14 it makes sense to define the *separable degree* and *inseparable degree* of an isogeny which are the degree of the separable and purely inseparable parts, this last part is a power of the frobenius morphism. Therefore, the inseparable degree is a power of $p = char(K)$. Now, we are ready to state the following result that links the degree and the order of the kernel.

Theorem II.4.16. *Let $\alpha : E_1 \to E_2$ be an isogeny defined over K. Then the order of the kernel of α is $\#\ker(\alpha) = \deg_{sep}(\alpha)$.*

Proof. Since an isogeny can be decomposed as $\alpha = \alpha_{sep} \circ (\phi_p)^n$, where the purely inseparable part, being injective, does not contribute to the kernel, we can restrict our attention to the separable isogenies. As always we will assume $char(K) \neq 2, 3$. Now let $\alpha = \left(\frac{s(x)}{v(x)}, \frac{t(x)}{w(x)}y\right)$ be a separable isogeny in standard form. Then consider $(a,b) \in E_2$ and define $S(a,b) = \#\alpha^{-1}((a,b))$. Now, we look at the solutions of $\frac{s(x)}{v(x)} = a$. Consider $a, b \neq 0$ then define $g_a = s(x) - av(x)$, where we require a to be different from the ratio of the leading coefficients of $s(x)$ and $v(x)$, this is possible since E_2 has infinite points. Hence $\deg(g_a) = \deg(\alpha)$. Further, we choose a such that $g_a(x)$ has no double roots. In fact, consider a double root x_0 of g_a then we obtain that $s(x_0) = av(x_0)$ and $av'(x_0) = s'(x_0)$. Multiplying the first and second terms we obtain $a(s(x_0)v'(x_0) - s'(x_0)v(x_0)) = 0$, so that x_0 is a root of $v^2\left(\frac{u}{v}\right)'$ and since α is separable this polynomial has only a finite number of roots. So we can choose between the infinite number of points $(a,b) \in E_2$ one such that $g_a(x)$ and $s(x)v'(x) - v(x)s'(x)$ have no common zeros: then $g_a(x)$ has exactly $\deg(\alpha)$ distinct solutions, hence $S(a,b) = \deg(\alpha)$.

We know that $S(a,b)$ is constant for $(a,b) \in E_2$ since an isogeny is a surjective homomorphism, moreover we know necessarily $S(a,b) \leq \deg(\alpha)$ and from what we proved $S(a,b) \geq \deg(\alpha)$. As a result, $\#\ker(\alpha) = S(a,b) = \deg(\alpha)$. □

Proposition II.4.17. *Let $\alpha : E_1 \to E_2$, $\beta : E_2 \to E_3$ be isogenies. Then the degree $\deg(\beta \circ \alpha) = \deg(\beta)\deg(\alpha)$. The same holds for the separable and inseparable degrees.*

Proof. For the separable degrees since isogenies are surjective and are homomorphisms we know that $\#\ker(\beta \circ \alpha) = \#\ker(\alpha)\#\ker(\beta)$. For the inseparable degrees since $\alpha = \alpha_{sep} \circ \phi_p^n$ and $\beta = \beta_{sep} \circ \phi_p^m$ then $\beta \circ \alpha = \beta_{sep} \circ \alpha'_{sep} \circ \phi_p^{n+m}$, where α'_{sep} exists has obviously the same degree of α_{sep}. As a result the inseparable degree is effectively $p^n p^m$. Finally, since the degree is obviously the product of the separable and inseparable degrees, we conclude. □

Corollary II.4.18. *The isogeny $\alpha : E_1 \to E_2$ is an isomorphism if and only if $deg(\alpha) = 1$.*

Proof. Case $char(K) \neq 2, 3$. Obviously since the degree is multiplicative it can't be greater then 1 and since it is surjective can't have degree 0. Moreover if we consider E_1 and E_2 in Weierstrass form then $\alpha = (\xi_1 x, \xi_2 y)$, where $\xi_1, \xi_2 \neq 0$, in standard form, since the degree of the denominator is 0 by the fact the isogeny has no affine zeros. As a result $\alpha^{-1} = \left(\frac{x}{\xi_1}, \frac{y}{\xi_2}\right)$ is the inverse isogeny. □

Theorem II.4.19. *The automorphism group $Aut(E) \subset End(E)$ of an elliptic curve E/K with $charK \neq 2, 3$ is isomorphic to:*

$$Aut(E) \simeq \begin{cases} \mu_6 & j(E) = 1728 \\ \mu_4 & j(E) = 0 \\ \mu_2 & otherwise \end{cases}$$

where μ_n is the group of the n^{th} roots of unity. In particular $Aut(E)$ is finite.

Proof. Consider the equation in Weierstrass form $y^2 = x^3 + Ax + B$, we recall that every isogeny of degree 1 has standard form $\alpha = (\xi^2 x, \xi^3 y)$, for some $\xi \in \bar{K}$.

1. If $j(E) = 0$ then $A = 0$ and after simplifying we obtain the new equation $y^2 = x^3 + \xi^6 B$. Necessarily $\xi^6 = 1$ since the map has to preserve the Weierstrass form. Then, taking ξ to be a generator of the group of the roots of unity $x^6 = 1$, which are 6 since $char(K) \neq 2, 3$, we conclude.

2. If $j(E) = 1728$ then $B = 0$ and the relation ξ has to respect is $y^2 = x^3 + \xi^4 Ax$. As a result $\xi^4 = 1$ and since $char(K) \neq 2$ we conclude.

3. Otherwise both $A, B \neq 0$ and the relation becomes $y^2 = x^3 + \xi^4 Ax + \xi^6 B$. Hence $\xi^4 = 1$ and $\xi^6 = 1$ which implies $\xi^2 = 1$ and since $char(K) \neq 2$ we conclude.

□

Chapter III

Analytic Structure

III.1 Riemann Surfaces

To grasp the idea of a Riemann surface we can define them as topological spaces that are locally "equal" to an open set of $\mathbb{C}$. More formally, let X be a topological space.

Definition III.1.1 (complex chart)**.** A *complex chart*, or *chart*, on X is a homeomorphism $\phi : U \to U$, where $U \subset X$ is an open set in X, and $V \subset \mathbb{C}$ is an open set in the complex plane $\mathbb{C}$. Then U is called the *domain* of the chart ϕ.

These homeomorphisms "pull back" the structure of $\mathbb{C}$ into our topological space, giving, for example, local coordinates on U, the domain of the chart. Now, the fundamental idea is to cover X with such domains, but first, in order to deal with nontrivial spaces, hence spaces which are not the disjoint union of copies of the complex plane, we have to handle the intersection of such domains. In particular, the homeomorphisms should be compatible in a complex sense.

Definition III.1.2. Let $\phi_1 : U_1 \to V_1$ and $\phi_2 : U_2 \to V_2$ be two complex charts on X. We say that ϕ_1 and ϕ_2 are compatible if either $U_1 \cap U_2 = \emptyset$ or

$$\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$$

is biholomorphic, hence holomorphic with inverse holomorphic. The composition $\phi_2 \circ \phi_1^{-1}$ is called the *transition map.*

Now we are ready to define the complex atlas.

Definition III.1.3. A *complex atlas*, or simply *atlas*, $\mathcal{A}$ on the topological space X is a collection $\mathcal{A} = \{\phi_\alpha : U_\alpha \to V_\alpha\}$ of pairwise compatible complex charts whose domain cover X, hence $\bigcup_\alpha U_\alpha = X$.

Remark III.1.4. Since bijective holomorphic functions are, in fact, biholomorphic, it is enough to require the transition map to be simply holomorphic.

We would like to always take a maximal atlas to have the finest structure.

Definition III.1.5. Two complex atlases $\mathcal{A}_1$ and $\mathcal{A}_2$ of X are equivalent $\mathcal{A}_1 \sim \mathcal{A}_2$ if $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$ is a complex atlas of X.

The one described above is an equivalence relation on the atlases of X.

Definition III.1.6. A *complex structure* on X is a maximal complex atlas, hence the union of all the atlases of an equivalence class.

Now we are ready to define the Riemann surfaces:

Definition III.1.7 (Riemann surface)**.** A *Riemann surface* X is a second countable Hausdorff connected topological space endowed with a complex structure.

Example III.1.8. The projective line $\mathbb{P}^1(\mathbb{C})$ with the quotient topology can be given a complex atlas $\mathbb{A} = \{\phi_0 : \mathbb{P}^1 \setminus H_0 \to \mathbb{C}, \phi_1 : \mathbb{P}^1 \setminus H_1 \to \mathbb{C}\}$ where

$$\phi_0 : [z, w] \mapsto \frac{w}{z} \qquad \phi_1 : [z, w] \mapsto \frac{z}{w}.$$

These are homeomorphisms with the inverse given respectively by $\phi_0^{-1} : z \mapsto [1, z]$ and $\phi_1^{-1} : z \mapsto [z, 1]$. Furthermore, we verify that the map $\phi_1 \circ \phi_0^{-1} : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ is holomorphic in $\mathbb{C} \setminus \{0\}$:

$$(\phi_1 \circ \phi_0^{-1})(z) = \phi_1([1 : z]) = \frac{1}{z}.$$

Hence $\mathcal{A}$ is an atlas and we can associate to it the complex structure $\bar{\mathcal{A}}$ so that $\mathbb{P}^1$, which is a second countable connected Hausdorff topological space, becomes a Riemann surface.

It turns out that the algebraic and projective smooth algebraic plane curves V over $\mathbb{C}$ are naturally Riemann surfaces, we quickly sketch the construction, for the details see [Mir95, chapter I]. For the affine case, let f be the defining equation of the curve. By the definition of smoothness at each point $P = (x, y) \in V$ at least one coordinate of the gradient vector $\nabla f(P)$ is nonzero, suppose $\nabla_y f(P) \neq 0$, the case $\nabla_x f(P) \neq 0$ is similar. Then a holomorphic version of the implicit function theorem ensures that there is a biholomorphic function $h_P : V_x \to V_y$ defined on a neighborhood V_x of x such that $f(z, h(z)) = 0$. The map $\phi_P : V_x \to U_P$ such that $\phi_P(z) = (z, h(z))$ is a homeomorphism with the inverse given by the projection $\pi_P : (x, y) \mapsto x$. Then, if we also add the charts for $\nabla_x f(P) \neq 0$, constructed in an analogous way, $\mathcal{A} = \{\pi_P : U_P \to V_P \mid P \in V\}$ can be shown to be an atlas, due to the fact that h_P are biholomorphic.

The projective case is similar if we consider $V = V_0 \cup V_1 \cup V_2$ as the union of three affine algebraic plane curves, i.e. the affinization with respect to the three fundamental planes of the projective variety. Each affine variety has a Riemann structure on it with an atlas $\mathcal{A}_i$, then we define the atlas of V as $\mathcal{A} = \bar{\mathcal{A}}_0 \cup \bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2$ where $\bar{\mathcal{A}}_1 = \{\pi_i \circ \phi_P \mid \phi_P \in \mathcal{A}_i,\ \pi_i : \mathbb{P}^2(\mathbb{C}) \setminus H_i \to \mathbb{A}^2(\mathbb{C}) \text{ standard projection}\}$, then it is only a question of proving the compatibility between the charts.

Remark III.1.9. The projective smooth algebraic plane curves are compact since are closed sets in a compact.

III.2 Riemann Surface Maps

As $\mathbb{C}$ has holomorphic functions, we can define analogues for a generic Riemann surface X:

Definition III.2.1. Let $P \in X$ be a point. A function $f : X \mapsto \mathbb{C}$ is *holomorphic* (*meromorphic*) *at* P if there exists a chart $\phi : U \to V$, $P \in U$, such that $f \circ \phi^{-1} : V \to \mathbb{C}$ is holomorphic at $\phi(P)$. We say $f : X \to \mathbb{C}$ is *holomorphic* (*meromorphic*) if it is holomorphic (meromorphic) at every point of X.

The definition is well-posed since the transition maps are holomorphic, so that the property does not depend on the single chart chosen but only on the complex structure on X. In the same way, also the order of a pole at a point P does not depend on the choice of a particular chart, since the transition maps are biholomorphic and so a composition of $f \circ \phi^{-1}$ with a transition map $\phi \circ \psi^{-1}$ does not change the order of the pole in $\phi(P)$.

Remark III.2.2. As in the case of $X = \mathbb{C}$, the holomorphic functions $\mathcal{O}(X)$ form a ring with pointwise sum and multiplication, and the meromorphic functions $\mathcal{M}(X)$ form a field.

Example III.2.3. Let $V/\mathbb{C}$ be a smooth algebraic plane curve, with defining equation f, then any element h of the function field $\mathbb{C}(V)$ is a meromorphic function. In fact, $f \circ \phi^{-1}$, for a chart ϕ of the atlas defined before, is a rational expression of meromorphic functions, which is defined since $0 = f$ in $\mathbb{C}(V)$, so there is no possibility for a component of the denominator of h to vanish.

As for the case of smooth manifolds, we can define maps between Riemann surfaces that preserve the complex structure:

Definition III.2.4 (Holomorphic Map)**.** Let X, Y be Riemann surfaces, a map $\alpha : X \to Y$ is a *holomorphic map* if for every $P \in X$ there exists a chart $\phi_P : U_p \to \mathbb{C}$, $P \in U_p$, and a chart $\psi_P : V_P \to \mathbb{C}$, $\alpha(P) \in V_P$, such that the local map

$$\psi_P \circ \alpha \circ \phi_P^{-1} : W \subset \mathbb{C} \to \mathbb{C}$$

is holomorphic at P. The map α is an isomorphism of Riemann surfaces if there exists a holomorphic map $\alpha^{-1} : Y \to X$ such that $\alpha \circ \alpha^{-1} = id_Y$ and $\alpha^{-1} \circ \alpha = id_X$.

These holomorphic maps behave in the right way: the composition of holomorphic maps is a holomorphic map and the composition of a holomorphic (meromorphic) function with a holomorphic map is still a holomorphic (meromorphic) function.

Example III.2.5. We have already seen many holomorphic maps between elliptic curves. Consider an elliptic curve $E/\mathbb{C}$. As a smooth projective plane curve defined over $\mathbb{C}$ it is also a compact Riemann surface. Then any morphism of elliptic curves is a holomorphic map, in particular any isogeny and the addition by a point P map. This means that the group structure of the curve is compatible with the complex structure on it. As a result, $E/\mathbb{C}$ is a topological group.

As for isogenies, the surjectivity property holds.

Proposition III.2.6. *Let X, Y be compact Riemann surfaces and let $\alpha : X \to Y$ be a non-costant holomorphic map. Then the map α is surjective.*

Proof. Since X is compact, $\alpha(X) \subseteq Y$ is compact in a Hausdorff compact space and therefore is closed. Moreover, the local maps $\psi_i \circ \alpha \circ \phi_j : U_{ij} \subset \mathbb{C} \to V_{ij} \subset \mathbb{C}$ are non-constant holomorphic functions with an open domain, so that by the Open Mapping Theorem their image is open. Furthermore, because both ψ_i, ϕ_j are homeomorphisms, we also find that $\alpha\big|_{\phi_j^{-1}(U_{ij})}$ is open. Finally, recall that $X = \bigcup_{i,j} U_{ij}$, so $\alpha(X)$ is open but also closed, so that $\alpha(X) = Y$ since Y is connected. □

The following is another important result.

Proposition III.2.7. *Let X be a compact Riemann surface, and let $f : X \to \mathbb{C}$ be a non-constant meromorphic function. Then*

1. *the map f has a finite number of zeros,*

2. *the map f has a finite number of poles.*

Proof. 1. Assume by contradiction that f has an infinite number of zeros, since X is a second countable compact space there exists a zero $\bar{z}$ such that there exists an infinite sequence of distinct zeros $\{\bar{z}_n\}_{n\in\mathbb{N}}$ such that $\bar{z}_n \to \bar{z}$. Consider a chart $\phi : U \to V$, $\bar{z} \in U$, U a connected open set, then $f \circ \phi^{-1}$ has a zero of infinite order in $\phi(\bar{z})$, hence it is constant equal to zero since it is a meromorphic function. As a consequence, the map is constant on all connected domains of the charts that overlap with U. Then repeating the argument and considering that T is connected, we conclude that f is constant equal to zero.

2. The argument is similar since the poles of f are the zeros of $\frac{1}{f}$.

□

Remark III.2.8. Riemann surfaces seen as real manifolds are connected real 2-dimensional orientable manifolds, hence surfaces. In particular, as topological spaces, the connected real compact orientable surfaces are classified by the Euler characteristic $\chi = \#vertices - \#edges + \#faces = 2 - 2g$ of any proper triangulation of the surface, or equivalently by the genus g which counts the number of "holes" of the surface. In particular, all elliptic curves $E/\mathbb{C}$ have genus 1. In fact, suppose that we have a triangulation τ of the surface, then the multiplication-by-2 map $[2] : E \to E$ is a 2-covering, i.e. a local homeomorphism such that the cardinality of the fibers $[2]^{-1}(y)$ is constant, so $[2]^{-1}(\tau) = \tau_2$ is also a triangulation of E with twice the vertices, edges and faces, so $\chi(E) = 2\chi(E) \iff \chi(E) = 0 \iff g = 1$. This argument works for any surface that is a topological group with surjective covering maps with finite kernel, so that all these spaces are homeomorphic. This suggests a possible connection between the complex structure of elliptic curves and the one of another family of Riemann surfaces we are going to study in the next section.

III.3 Complex Tori

We have seen that elliptic curves are Riemann surfaces of genus 1 with a compatible group structure. These are not the only Riemann surfaces with this additional structure; in fact, consider a discrete lattice on $\mathbb{C}$:

Definition III.3.1 (Torus)**.** Let $\omega_1, \omega_2 \in \mathbb{C}$ be two $\mathbb{R}$-linearly independent complex numbers. Given the lattice $\Lambda = \Lambda_{\omega_1,\omega_2} = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$, a torus is the topological space

$$T_{w_1,w_2} = \mathbb{C}/\Lambda_{\omega_1,\omega_2}$$

endowed with the quotient topology.

We point out that, under the above hypothesis, the lattice $\Lambda_{\omega_1,\omega_2}$ is a discrete set.

Remark III.3.2. Sometimes it will be convenient to consider a torus T_{ω_1,ω_2} as the quotient space of a so-called *fundamental parallelogram* $P_{\omega_1,\omega_2}(z) \subset \mathbb{C} \simeq \mathbb{R}^2$ that is a parallelogram whose edges $\omega_1, \omega_2 \in \mathbb{C} \simeq \mathbb{R}^2$, which meet at the vertex $z \in \mathbb{C} \simeq \mathbb{R}^2$, generate the lattice. In fact the restriction of the projection $\pi\big|_{P_{\omega_1,\omega_2}} : P_{\omega_1,\omega_2} \to T_{\omega_1,\omega_2}$ is surjective. Moreover, the fundamental parallelogram is a connected compact set. This means that the torus is also a connected compact set. For brevity, we will denote $P_{\omega_1,\omega_2}(0) = P_{\omega_1,\omega_2}$.

As for an elliptic curve, one can give a torus a natural complex structure:

Proposition III.3.3 (Complex torus)**.** *T_{ω_1,ω_2} has a natural structure of a Riemann surface.*

Proof. We describe the inverse charts: let $z \in P_{\omega_1,\omega_2}$, $\bar{z} = \pi(z)$, and fix $\epsilon > 0$ such that

$$\min_{w \in \Lambda_{\omega_1,\omega_2} \setminus \{0\}} \|w\| > 2\epsilon > 0.$$

This is possible since $\Lambda_{\omega_1,\omega_2}$ is discrete. Then let $\phi_{\bar{z}}^{-1} : B_\epsilon(z) \to U_{\bar{z}}$ be an inverse chart equal to $\pi\big|_{B_\epsilon(z)}$. Since the projection is a continuous open map, we only have to verify the injectivity to prove that it is a homeomorphism.

$$\pi(z_1) = \pi(z_2) \iff z_1 - z_2 \in \Lambda_{w_1,w_2} \qquad \|w\| = \|z_1 - z_2\| \leq \|z_1 - z\| + \|z_2 - z\| \leq 2\epsilon$$

hence $w = 0$ and $z_1 = z_2$. Now, letting $\mathcal{A} = \{\phi_{\bar{z}} \mid \bar{z} \in T_{\omega_1,\omega_2}\}$ be our atlas, we have to prove that the charts are pairwise compatible. In particular, let $\phi_{\bar{z}_1}, \phi_{\bar{z}_2}$ be charts with overlapping domains, then $\phi_{\bar{z}_1} \circ \phi_{\bar{z}_2} = \phi_{\bar{z}_1} \circ \pi\big|_{B_\epsilon(z_2)} = h(z)$, moreover

$$\pi(h(z)) = \pi\big|_{B_\epsilon(z_2)}(z) = \pi(z).$$

As a result $z + w = h(z)$ locally, for a fixed $w \in \Lambda_{\omega_1,\omega_2}$, since h is continuous and $\Lambda_{\omega_1,\omega_2}$ is discrete. Then we conclude that the charts are compatible since $z + w$ is biholomorphic. □

A torus with a complex structure is called a *complex torus.*

Remark III.3.4. A complex torus has a group structure inherited by $\mathbb{C}$ since it is a quotient group.

III.3.1 Elliptic Functions

We would like to study and possibly characterize the field $\mathcal{M}(T)$ of meromorphic functions on a generic complex torus. Studying such functions directly is difficult, since topologically the torus is different from the complex plane, and even imagining nontrivial meromorphic functions can be challenging. That is the reason why we will find an equivalence between $\mathcal{M}(T)$ and a family of periodical meromorphic functions defined over $\mathbb{C}$.

Definition III.3.5 (Elliptic functions)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice. The *elliptic functions* over Λ are the Λ-periodic meromorphic functions:

$$\mathcal{E}_\Lambda = \{f : \mathbb{C} \to \mathbb{C} \text{ meromorphic } \mid f(z) = f(z + w)\ \forall w \in \Lambda\}$$

Proposition III.3.6. *Let $T = \mathbb{C}/\Lambda$ be a complex torus. Then $\mathcal{M}(T) \simeq \mathcal{E}_\Lambda$ as fields by the map $\Psi : \mathcal{M}(T) \to \mathcal{E}_\Lambda$, such that*

$$\Psi : f \mapsto f \circ \pi.$$

Proof. By the structure of the atlas we defined, we find that $f \circ \phi_{\bar{z}}^{-1} = f \circ \pi\big|_{B_\epsilon(z)}$ is a meromorphic function; hence $f \circ \pi$ is a meromorphic function and, by definition, is also Λ-periodic. Therefore, we proved $\Psi(\mathcal{M}(X)) \subseteq \mathcal{E}_\Lambda$. The fact that it is a field homomorphism is trivial. It remains to prove the surjectivity. Consider $g_\Lambda \in \mathcal{E}_\Lambda$ and let $g\big|_{U_{\bar{z}}} = g_\Lambda \circ \phi_{\bar{z}}$ be a map; we have to show that it is a well-defined meromorphic function independent of the chart. In fact

$$g_\Lambda \circ \phi_{\bar{z}'} = g_\Lambda \circ \phi_{\bar{z}'} \circ \phi_{\bar{z}}^{-1} \circ \phi_{\bar{z}} = g_\Lambda(z+w) \circ \phi_{\bar{z}} = g_\Lambda \circ \phi_{\bar{z}}$$

for some $w \in \Lambda$, from the structure of the transition maps of a torus and because g_Λ is Λ-periodic. Moreover $g : T \to \mathbb{C}$ is meromorphic since locally $g \circ \phi_{\bar{z}}^{-1} = g_\Lambda(z+w)$, meromorphic at $\phi(\bar{z})$, for some $w \in \Lambda$, again from the structure of the charts we defined. This last fact implies $\Psi(g) = g_\Lambda$ since g_Λ is Λ-periodic. □

Corollary III.3.7. *Let $T = \mathbb{C}/\Lambda$ be a complex torus. Then the function $f \in \mathcal{O}(T)$ if and only if $f = c \in \mathbb{C}$.*

Proof. Consider the corresponding elliptic function $f_\Lambda : \mathbb{C} \to \mathbb{C}$. Then $f_\Lambda(\mathbb{C}) = f(T)$ so that $f_\Lambda(\mathbb{C})$ is compact, hence limited. As a consequence of Liouville's Theorem $f_\Lambda = c \in \mathbb{C}$, a constant function, which means that $f = c \in \mathbb{C}$. □

Remark III.3.8. From the structure of the map $\Psi : \mathcal{M}(T) \to \mathcal{E}_\Lambda$ we know that given $f \in \mathcal{M}(T)$, with zeros $\bar{z}_i$ and poles $\bar{w}_j$, the corresponding function $f_\Lambda = \Psi(f)$ has zeros $z_i + \Lambda$ and poles $w_j + \Lambda$ of the same order of the corresponding point in T after the canonical projection.

The construction above suggests that to find a nontrivial meromorphic function of a complex torus $T = \mathbb{C}/\Lambda$ we must look for nontrivial elliptic functions over Λ.

Definition III.3.9. Let Λ be a lattice and let $T = \mathbb{C}/\Lambda$ be the corresponding complex torus. We define the Weierstrass $\wp$-function $\wp(z, \Lambda) : \mathbb{C} \to \mathbb{C}$

$$\wp_\Lambda(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

and its derivative

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

The corresponding meromorphic functions in $\mathcal{M}(T)$ are denoted by $\bar{X} : T \to \mathbb{C}$ and $\bar{Y} : T \to \mathbb{C}$.

It turns out that the series that defines $\wp_\Lambda$ converges uniformly and is equilimited on any compact of $\mathbb{C} \setminus \Lambda$, and moreover, $\wp'_\Lambda$ is Λ-periodic. As a consequence, the functions $\wp_\Lambda, \wp'_\Lambda \in \mathcal{E}_\Lambda$, see [Kob93, §I.4] for a proof.

Let's study some general properties of the meromorphic functions:

Proposition III.3.10. *Let $T = \mathbb{C}/\Lambda$ be a complex torus and let $f \in \mathcal{M}(T)$. Consider $f_\Lambda = \Psi(f) \in \mathcal{E}_\Lambda$ and denote by $\bar{z}_1, \ldots, \bar{z}_k$ the zeros of f of order $n_1, \ldots, n_i$, and denote by $\bar{w}_1, \ldots, \bar{w}_i$ the poles of f of order $m_1, \ldots, m_j$. Then the following properties hold.*

1. $\sum_i n_i - \sum{}_j m_j = 0$.

2. *$\sum_i n_i(\bar{z}_i) - \sum_j m_j(\bar{w}_j) = \bar{0}$ for the group law of T.*

Proof. 1. By the Remark III.3.8, it is enough to look at the restriction of f_Λ to a fundamental parallelogram $P_\Lambda(z_0)$, in particular we choose $z_0 \in \mathbb{C}$ such that $P_\Lambda(z_0)$ has no zeros or poles in the boundary, this is possible since there is only a finite number of such points in T. Then consider the complex integral

$$\frac{1}{2\pi i}\int_{\partial P_\Lambda(z_0)} \frac{f'_\Lambda}{f_\Lambda} dz = \sum_i n_i - \sum_j m_j$$

by Cauchy's argument principle and the injectivity of $\pi\big|_{int_{\mathbb{C}}(P_\Lambda(z_0))}$. By evaluating the integral we obtain the result:

$$\frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_1} \frac{f'_\Lambda}{f_\Lambda}(z) - \frac{f'_\Lambda}{f_\Lambda}(z+\omega_2)\, dz - \frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_2} \frac{f'_\Lambda}{f_\Lambda}(z) - \frac{f'_\Lambda}{f_\Lambda}(z+\omega_1)\, dz = 0$$

since f_Λ is Λ-periodic.

2. Consider the same fundamental parallelogram as above, the integral

$$\frac{1}{2\pi i}\int_{\partial P_\Lambda(z_0)} \frac{z f'_\Lambda}{f_\Lambda} dz = \sum_i n_i z_i - \sum_j m_j w_j$$

by Cauchy's argument principle and the residue theorem. The thesis is then equivalent to proving that the integral lies in Λ since

$$\pi\left(\sum_i n_i z_i - \sum_j m_j w_j\right) = \sum_i n_i(\bar{z}_i) - \sum_j m_j(\bar{w}_j).$$

So unwinding the line integral and rearranging the terms, we obtain

$$\begin{aligned}
&\frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_1} z\frac{f'_\Lambda}{f_\Lambda}(z) - (z+\omega_2)\frac{f'_\Lambda}{f_\Lambda}(z+\omega_2)\, dz = \\
-&\frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_2} z\frac{f'_\Lambda}{f_\Lambda}(z) - (z+\omega_1)\frac{f'_\Lambda}{f_\Lambda}(z+\omega_1)\, dz = \\
-&\frac{\omega_2}{2\pi i}\int_{z_0}^{z_0+\omega_1} \frac{f'_\Lambda}{f_\Lambda}(z)\, dz + \frac{\omega_1}{2\pi i}\int_{z_0}^{z_0+\omega_2} \frac{f'_\Lambda}{f_\Lambda}(z)\, dz = \\
-&\frac{\omega_2}{2\pi i}\oint_{C_1} \frac{1}{u}\, du + \frac{\omega_1}{2\pi i}\oint_{C_2} \frac{1}{u}\, du = a\omega_2 + b\omega_1 \in \Lambda
\end{aligned}$$

where we substituted $u = f(z)$ and we used the definition of the winding number to obtain $a, b \in \mathbb{Z}$.

□

Thanks to the special properties of the elliptic functions, we are ready to characterize the structure of $\mathcal{M}(T)$

Theorem III.3.11. *Let $T = \mathbb{C}/\Lambda$ be a complex torus. Then:*

$$\mathcal{M}(T) \simeq \frac{\mathbb{C}(\bar{X})[\bar{Y}]}{\left(\bar{Y}^2 - 4\bar{X}^3 + g_2(\Lambda)\bar{X} + g_3(\Lambda)\right)}$$

where $g_2(\Lambda) = 60\sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$ and $g_3(\Lambda) = 140\sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$.

Proof. First, we need to prove $\mathbb{C}(\bar{X})[\bar{Y}] = \mathcal{M}(T)$. It suffices to show that $\mathbb{C}(\bar{X})[\bar{Y}]$ generates all even meromorphic functions: each meromorphic function is the sum of an even and an odd meromorphic function, and an odd function f is the product of an even function and $\bar{Y}$ since $f = \frac{f}{\bar{Y}}\bar{Y} = g\bar{Y}$, where g is even since it is a product of two odd functions.

Lemma III.3.12. *$\mathbb{C}(\bar{X}) \subset \mathcal{M}(T)$ is the subfield of even meromorphic functions on the complex torus $T = \mathbb{C}/\Lambda$.*

Proof. We study the properties of $\bar{X}$. This even function has only one pole of order 2 in $\bar{0}$, so by III.3.10 it can have two distinct zeros P and $-P$ of order 1, or a single zero P of order 2. In the last case, necessarily $2P = \bar{0}$ and therefore P equals $\overline{\frac{\omega_1}{2}}$ or $\overline{\frac{\omega_2}{2}}$ or $\overline{\frac{\omega_1+\omega_2}{2}}$, the only 2-torsion points.

Next, consider a generic even meromorphic function $f : T \to \mathbb{C}$. If P is a zero, then also $-P$ is a zero. Moreover, in the case where the zero is a 2-torsion point, its order is even, since it is a zero of all its odd n^{th} derivatives and hence of all the derivatives of f of odd order. The same idea works for the poles of f, since they are the zeros of $\frac{1}{f}$. Now we build a rational function in $\mathbb{C}(X)$ that has the same zeros and poles of f with the same order

$$g = \frac{\prod_{z_i \in S}(\bar{X} - \bar{X}(z_i))^{n_i}}{\prod_{w_j \in V}(\bar{X} - \bar{X}(w_j)^{m_j}}.$$

Where S is a subset of the zeros of f such that $\bar{0} \notin S$ and for each zero $\bar{z}_i \neq \bar{0}$ one and only one of $\bar{z}_i, -\bar{z}_i$ is in S, with n_i the order of $\bar{z}_i$ if it is not a 2-torsion point and n_i half the order of $\bar{z}_i$ if it is a 2-torsion point. V is a subset of the poles that is defined in the same way as S. Now, consider a generic zero $\bar{z}_i$ of f. If it is a 2-torsion point, its order as a zero of g is $2n_i = ord_{\bar{z}_i}(\bar{X} - \bar{X}(\bar{z}_i))^{n_i}$, hence its order as a zero of f. If $\bar{z}_i$ is not a 2-rational point zero, then one of $\bar{z}_i, -\bar{z}_i$ is in S, hence its order as a zero of g is n_i. The same argument works for the poles of f. It remains to check that the order of $\bar{0}$ of f and g is equal, but this is a direct consequence of proposition III.3.10.1. So we see that $\frac{f}{g} \in \mathcal{O}(T)$ is a constant that we can obtain, for example, by evaluating the limit $\lim_{z\to 0} \Psi(\frac{f}{g}) = \lim_{z\to 0} \frac{\Psi(f)}{\Psi(g)}$. Then all the even functions belong to $\mathbb{C}(\bar{X})$, hence $\mathcal{M}(T) = \mathbb{C}(\bar{X})[\bar{Y}]$. □

Finally, $\bar{Y} \notin \mathbb{C}(\bar{X})$ since it is odd, but $\bar{Y}^2 \in \mathbb{C}(\bar{X})$ since it is even. $\bar{Y}$ has a pole of order 3 in $\bar{0}$, all the other 2-torsion points are zero. As a consequence, they are all the zeros and have order 1 by proposition III.3.10.1. So by the construction above

$$\bar{Y}^2 = c\left(\bar{X} - \bar{X}\left(\overline{\frac{\omega_1}{2}}\right)\right)\left(\bar{X} - \bar{X}\left(\overline{\frac{\omega_2}{2}}\right)\right)\left(\bar{X} - \bar{X}\left(\overline{\frac{\omega_1+\omega_2}{2}}\right)\right).$$

Finally if we compare $\Psi(\bar{Y}) = \wp'_\Lambda$ and $\Psi(\bar{X}) = \wp_\Lambda$ in a neighborhood of 0 , i.e. we compare the terms of negative degree of the Laurent series centered at $z = 0$, we find that the polynomial relation has the form

$$\bar{Y}^2 = 4\bar{X}^3 - g_2(\Lambda)\bar{X} - g_3(\Lambda).$$

See [Kob93, §I.6] for the details. □

Thus, given a complex torus $T = C/\Lambda$ and a cubic curve $E/\mathbb{C}$ of affine equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, the function $[\bar{X}(z) : \bar{Y}(z) : 1]$ maps the points of $T = \mathbb{C}/\Lambda$ to the points of E. Moreover E is an elliptic curve. In fact, $\bar{X}$ assumes different values for its 2-torsion points, which implies $\Delta(E) \neq 0$ since $4x^3 - g_2x - g_3$ has distinct zeros. This suggests the following important isomorphism.

Theorem III.3.13. *Let $T = \mathbb{C}/\Lambda$ be a complex torus; let $E/\mathbb{C}$ be the elliptic curve with affine equation $y^2 = 4x^3 - g_2x - g_3$. Then the map $\mathcal{F} : T \to E$ such that:*

$$\mathcal{F} : \bar{z} \mapsto [\bar{z}^3\bar{X}(\bar{z}) : \bar{z}^3\bar{Y}(\bar{z}) : \bar{z}^3]$$

is an isomorphism of Riemann surfaces and an isomorphism of groups.

Proof. First of all, we have to prove that $\mathcal{F}$ is a holomorphic map. For each $\bar{z} \in T$ we consider the natural chart $\phi_{\bar{z}}$ with inverse given by a restriction of $\pi : \mathbb{C} \to T$, the canonical projection. Therefore, we can reduce the statement to the fact that the map

$$\mathcal{F}_\Lambda = \mathcal{F} \circ \pi : z \mapsto [z^3\wp_\Lambda(z) : z^3\wp'_\Lambda(z) : z^3]$$

is a holomorphic map. We distinguish 3 cases.

1. Case $z_0 \in \Lambda$. Then $\mathcal{F}_\Lambda(z_0) = [0 : 1 : 0]$. We consider a chart $\psi : U \to \mathbb{C}$ of E, $[0 : 1 : 0] \in U$. Then $\psi : [X_0 : X_1 : X_2] \mapsto \frac{X_0}{X_1}$, so that

   $$\psi \circ \mathcal{F}_\Lambda : z \mapsto \frac{\wp_\Lambda(z)}{\wp'_\Lambda(z)}$$

   has zeros of order 1 for each $z_0 \in \Lambda$, hence it is holomorphic in a neighborhood of z_0.

2. Case $\pi(z_0)$ is not a 2-torsion point. Then the related charts $\psi_{z_0} : E \to \mathbb{C}$ have the form $\psi_{z_0} : [X_0 : X_1 : X_2] \to \frac{X_0}{X_2}$. As a result

   $$\psi_{z_0} \circ \mathcal{F}_\Lambda : z \mapsto \wp_\Lambda(z)$$

   is holomorphic in z_0 since $\wp_\Lambda$ is holomorphic in $\mathbb{C} \setminus \Lambda$. Moreover, its derivative never vanishes if $\pi(z)$ is not a 2-torsion point.

3. Case $\pi(z_0)$ is a nonzero 2-torsion point. Then the related charts $\psi_{z_0} : E \to \mathbb{C}$ have the form $\psi_{z_0} : [X_0 : X_1 : X_2] \mapsto \frac{X_1}{X_2}$. As a consequence

   $$\psi_{z_0} \circ \mathcal{F}_\Lambda : z \mapsto \wp'_\Lambda(z)$$

   is holomorphic in z_0 since $\wp'_\Lambda$ is holomorphic in $\mathbb{C} \setminus \Lambda$. Moreover, we remark z_0 is a simple zero.

Therefore, $\mathcal{F}$ is a holomorphic map. Next, we have to prove that $\mathcal{F}$ is bijective. It is surjective because it is a non-constant holomorphic map of compact Riemann surfaces. It is injective in the case $\mathcal{F}(\bar{z}) = O$ since $\mathcal{F}(\bar{z}) = O = [0 : 1 : 0]$ if and only if $\bar{z} = \bar{0}$, while for $\bar{z} \neq \bar{0}$ we can consider the affinization of the map with respect to H_2. Then it is enough to prove $\mathcal{F}^a : \bar{z} \mapsto (\bar{X}(\bar{z}), \bar{Y}(\bar{z}))$ is injective. Assume $\mathcal{F}^a(\bar{z}') = \mathcal{F}^a(\bar{z})$. Then, for the structure of $\bar{X}$, $\bar{z}' = \bar{z}$ or $\bar{z}' = -\bar{z}$. If $\bar{z}$ is a 2-torsion point necessarily $\bar{z} = \bar{z}'$. If $\bar{z}$ is not a 2-torsion point, we could suppose $\bar{z}' = -\bar{z}$, but then $\bar{Y}(\bar{z}') = -\bar{Y}(\bar{z}) \neq 0$, since $\bar{z}$ is a 2-torsion point, which is a contradiction. This proves $\bar{z} = \bar{z}'$ and the injectivity of $\mathcal{F}$. Further, we note that for all the local maps we studied, the derivatives in a neighborhood of $\pi(z_0)$ were never zero, so by a holomorphic version of the global inversion theorem since $\mathcal{F}$ is bijective we can say that it is an isomorphism.

Finally, the fact that it respects the group structure is simple to prove. We have shown before $\mathcal{F}(\bar{0}) = O$, $\mathcal{F}(-\bar{z}) = -\mathcal{F}(\bar{z})$, since $\bar{X}$ is even and $\bar{Y}$ is odd. Finally, consider the points $P_1, P_2 \in E^a$, $P_1 \neq -P_2$, in particular P_1, P_2 are not 2-torsion points, and let $\bar{z}_1, \bar{z}_2 \in T/\{\bar{0}\}$ be the corresponding points in the complex torus. Furthermore, considering $P = P_1 + P_2$, there exists a line described by the equation $y + bx + c = 0$ such that $P_1, P_2, -P$ are the only intersections of the line with the affine elliptic curve. So $\bar{Y} + b\bar{X} + c$ is an elliptic function with a pole in $\bar{0}$ of order 3, then it has 3 zeros that are necessarily $\bar{z}_1, \bar{z}_2, -(\bar{z}_1 + \bar{z}_2)$, since by Proposition III.3.10.2 their sum must be equal to $\bar{0}$. □

Remark III.3.14. So, the above result shows that all complex tori are elliptic curves; however,this does not show the opposite. In fact, the opposite is equivalent to proving that the j-invariant, seen as a rational map of $g_2(\Lambda)$ and $g_3(\Lambda)$, is surjective. This can be obtained by showing that the j-invariant is a non-constant holomorphic map between compact Riemann surfaces, see [Sil91, p. I.4.3] for a proof. As a consequence $\mathcal{F}$ is a category equivalence between the category of complex tori and that of elliptic curves seen as Riemann surfaces.

Remark III.3.15. If we consider the isomorphism of Riemann surfaces, from a complex torus to an elliptic curve:

$$\mathcal{F} : \bar{z} \mapsto \left[\bar{z}^3 \bar{X}(\bar{z}) : \bar{z}^3 \frac{\bar{Y}(\bar{z})}{2} : \bar{z}^3 \right]$$

the associated elliptic curve has equation $y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$, so it is in Weierstrass form. From now on, this will be the isomorphism that we will use to define the elliptic curve associated to a torus and vice versa.

In general, given an elliptic curve $E/\mathbb{C}$, the associated torus will be the torus associated with one of the Weierstrass forms of E. So, when we fix a torus we automatically fix a Weierstrass form of the curve.

III.3.2 Holomorphic Maps

After having characterized the meromorphic functions of T, the next step is studying its holomorphic maps. Surprisingly, they have a simple form.

Theorem III.3.16. *Let $T_1 = \mathbb{C}/\Lambda_1$ and $T_2 = \mathbb{C}/\Lambda_1$ be complex tori. Then all the holomorphic maps $\phi : T_1 \to T_2$ such that $\phi(\bar{0}) = \bar{0}$ have the following form:*

$$\phi : \bar{z} \mapsto \alpha\bar{z} \quad \text{for some } \alpha \in \mathbb{C} \text{ such that } \alpha\Lambda_1 \subseteq \Lambda_2.$$

Proof. The complex plane $\mathbb{C}$ is the universal cover of a torus, i.e. a simply connected covering space of the torus. So, by the monodromy theorems we have that the map

$\phi : T_1 \to T_2$ lifts to a continuous map from the universal covers $\bar{\phi} : \mathbb{C} \to \mathbb{C}$, which makes the following diagram commutative.

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\bar{\phi}"] \arrow[d, "\pi"] & \mathbb{C} \arrow[d, "\pi"] \\
T_1 \arrow[r, "\phi"] & T_2
\end{tikzcd}$$

As a result, the map $\bar{\phi}$ is locally equal, up to a costant, to the local maps $\psi_2 \circ \phi \circ \psi_1^{-1}$, so it is holomorphic. Now, for any $w \in \Lambda_1$, let $g_w(z) = \bar{\phi}(z+w) - \bar{\phi}(z)$ be holomorphic functions over $\mathbb{C}$. Then $\bar{\phi}(z+w) - \bar{\phi}(z) \in \Lambda_2$, so that g_w is constant, since it is continuous in a connected space and Λ_2 is discrete. Taking the derivative, we notice that $\bar{\phi}'(z+w) = \bar{\phi}'(z)$ for any $w \in \Lambda_1$, which means that $\bar{\phi}'(z) \in \mathcal{E}_{\Lambda_1}$ is holomorphic and hence constant equal to $\alpha \in \mathbb{C}$. So $\bar{\phi}(z) = \alpha z$ because $\phi(\bar{0}) = \bar{0}$ and this means that $\phi(\bar{z}) = \alpha \bar{z}$, such that $\alpha \Lambda_1 \subseteq \Lambda_2$. We conclude by noting that $\alpha : \bar{z} \to \alpha \bar{z}$ is well defined and holomorphic. □

Remark III.3.17. The general form of a holomorphic map of complex tori is also simple: $\phi : \bar{z} \mapsto \alpha \bar{z} + b$ for $\alpha \Lambda_1 \subseteq \Lambda_2$. In fact, $\phi - b$ is holomorphic and sends $\bar{0}$ to $\bar{0}$.

This result tells us that a sufficient condition for a holomorphic map of complex tori to respect the group structure is that it maps the origin to the origin. We call these maps *isogenies*. Regarding the isogenies of the elliptic curves, we can define the *(separable) degree* of an isogeny of complex tori as the order of its kernel. Here, we state a useful characterization.

Proposition III.3.18. *Let $T_1 = \mathbb{C}/\Lambda_1$ and $T_2 = \mathbb{C}/\Lambda_2$ be complex tori. Then the isogeny $\alpha : \bar{z} \mapsto \alpha \bar{z}$ with $\alpha \Lambda_1 \subseteq \Lambda_2$ has degree $\deg(\alpha) = [\Lambda_2 : \alpha \Lambda_1]$, that is, the index of the subgroup $\alpha \Lambda_1$.*

Proof. Consider the related map $\bar{\alpha} : \mathbb{C} \to \mathbb{C}$ such that $\bar{\alpha} : z \mapsto \alpha z$. Then the points of $\mathbb{C}$ that are sent to Λ_2 are simply $\frac{1}{\alpha}\Lambda_2$ and by the relation $\alpha \Lambda_1 \subseteq \Lambda_2$ we get $\Lambda_1 \subseteq \frac{1}{\alpha}\Lambda_2$. From the definition of torus, the order of the kernel of α is $[\frac{1}{\alpha}\Lambda_2 : \Lambda_1] = [\Lambda_2 : \alpha \Lambda_1]$. □

The results and observations that we have found so far can be summarized in this way.

Theorem III.3.19. *The following categories are equivalent:*

1. $\left\{ \begin{array}{c} \textbf{\textit{Objects}}\textit{: Elliptic curves } E/\mathbb{C} \textit{ in Weierstrass form} \\ \textbf{\textit{Maps}}\textit{: Isogenies} \end{array} \right\}$

2. $\left\{ \begin{array}{c} \textbf{\textit{Objects}}\textit{: Complex Tori } T = \mathbb{C}/\Lambda \\ \textbf{\textit{Maps}}\textit{: Isogenies, i.e. holomorphic maps which fix } \bar{0} \end{array} \right\}$

3. $\left\{ \begin{array}{c} \textbf{\textit{Objects}}\textit{: Lattices } \Lambda_{\omega_1,\omega_2} \subset \mathbb{C} \simeq \mathbb{R}^2 \\ \textbf{\textit{Maps}}\textit{: Linear maps } \alpha : z \to \alpha z\textit{, such that } \alpha \Lambda_1 \subseteq \Lambda_2 \end{array} \right\}$

Remark III.3.20 (Complex multiplication)**.** Let $E/\mathbb{C}$ be an elliptic curve and let $T = \mathbb{C}/\Lambda_{\omega_1,\omega_2}$ be the associated complex torus. Focusing on the endomorphisms $End(E)$ of the curve, we notice that the ring of multiplication-by-m maps is isomorphic to $\mathbb{Z}$, so that $\mathbb{Z} \subseteq End(E)$. However, some curves possess more endomorphisms, as we have seen in the example $II.2.6$. In particular, such special morphisms correspond to multiplication by $\alpha \in \mathbb{C} \setminus \mathbb{R}$ in the lattice $\Lambda_{\omega_1,\omega_2}$. In fact, suppose that $\alpha \in \mathbb{R}$ then $\alpha\omega_1 \in \Lambda \iff \alpha\omega_1 = m\omega_1 \iff \alpha = m$ for some $m \in \mathbb{Z}$, since ω_1, ω_2 are $\mathbb{R}$-linearly independent. So, the special endomorphism corresponds to a "complex multiplication", i.e. the multiplication by some non-real α. [ST15, §6.5] suggests that this is the origin of the appellation "complex multiplication" for elliptic curves. More generally, any elliptic curve defined over a field $K \subseteq \mathbb{C}$ with $End(E)$ larger than $\mathbb{Z}$ is called an *elliptic curve with complex multiplication*, or simply a *CM elliptic curve* for brevity.

III.4 Endomorphism Ring

In this section we focus on the structure of the endomorphism ring of the elliptic curves defined over $K \subset \mathbb{C}$, so that we can apply the analytic theory introduced so far. First, we introduce another characterization of the degree of isogenies.

Proposition III.4.1. *Let E/K be an elliptic curve, $T = \mathbb{C}/\Lambda$ the associated complex torus, and let $[\alpha] : E \to E$ be an endomorphism, $\alpha \in \mathbb{C}$, corresponding to the multiplication-by-α map on T. Then* $\deg(\alpha) = \|\alpha\|^2 = |Det(\tilde{\alpha})|$ *where $\tilde{\alpha} : \mathbb{R}^2 \to \mathbb{R}^2$ is the linear map corresponding to the multiplication by $\alpha \in \mathbb{C} \simeq \mathbb{R}^2$ and $\|\alpha\| = |\alpha|$ is the complex norm.*

Proof. Consider $\alpha : T \to T$. Since the map is a surjective homomorphism from T to T, we know that for each point $P \in T$ there are precisely $\deg(\alpha)$ distinct points that are sent to P by the map α. This translates to the fact that given the fundamental parallelogram P_Λ we have exactly $\deg(\alpha)$ numbers $z_j \in \alpha P_\Lambda$ such that $z_j \mod \Lambda = P$, except for the set of measure zero of the edges of the parallelogram. This means that αP_Λ covers P_Λ exactly $\deg(\alpha)$ times, except for that set of measure zero. Furthermore, we note that the projection $\tilde{\pi} : \mathbb{C} \to P_\Lambda$, where $\tilde{\pi}(x) = y$, such that $y \equiv x \mod \Lambda$, is defined except for a set of measure zero and moreover it is locally a translation, hence a measure-preserving map. As a result, we obtain $|\frac{Area(\alpha P_\Lambda)}{Area(P_\Lambda)}| = \deg(\alpha)$. Now, consider $\tilde{\alpha} : \mathbb{R}^2 \to \mathbb{R}^2$ with the basis $\mathcal{B} = \{\omega_1, \omega_2\}$, such that $\Lambda = \Lambda_{\omega_1,\omega_2}$. Then by the definition of the determinant $|Det(\tilde{\alpha})| = |\frac{Area(\tilde{\alpha}(P_\Lambda))}{Area(P_\Lambda)}|$. This settles the first equivalence. Finally, the fact that $\deg(\alpha) = \|\alpha\|^2$ is obtained considering the basis $\mathcal{B} = \{1, i\}$ for $\mathbb{R}^2$. In this case, if $\alpha = a + ib$ then

$$\tilde{\alpha} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

so that $|Det(\tilde{\alpha})| = |a^2 + b^2| = \|\alpha\|^2 = \deg(\alpha)$. □

Corollary III.4.2. *Let E/K be an elliptic curve $K \subseteq \mathbb{C}$. Then the multiplication-by-n endomorphism has degree n^2.*

Proof. $\|n\|^2 = n^2$. □

Remark III.4.3. As a consequence of the equivalence between endomorphisms and linear maps $\tilde{\alpha} : \mathbb{R}^2 \to \mathbb{R}^2$ with a basis $\mathcal{B} = \{\omega_1, \omega_2\}$, such that the corresponding torus is $T = \mathbb{C}/\Lambda_{\omega_1,\omega_2}$, we established an injective representation of rings:

$$\rho : End(E) \to M_2(\mathbb{Z}).$$

And in particular

$$\rho : End(E)^* \to GL_2(\mathbb{Q}) \cap M_2(\mathbb{Z})$$

as a semigroup, since the multiplication by $\alpha \neq 0$ is a base change of $\mathbb{R}^2$. Representations are crucial for the study of such rings since cast the structure of a less-known object into a more familiar context. As an example, we immediately find that for each endomorphism $[\alpha]$ there exists $[n], [m] \in \mathbb{Z} \subseteq End(E)$ such that

$$[\alpha]^2 + [n][\alpha] + [m] = 0,$$

since for each $\alpha \in M_2(\mathbb{Z})$ the following holds:

$$\alpha^2 - Tr(\alpha)\alpha + Det(\alpha) = 0$$

with $Tr(\alpha), Det(\alpha) \in \mathbb{Z}$. Later, we will meet an analogue but more intrinsic representation.

Before we present the main theorem of this section, let's characterize the structure of an endomorphism in standard form.

Proposition III.4.4 (Structure of the standard form)**.** *Let E/K be an elliptic curve $K \subset \mathbb{C}$ with equation in Weierstrass form with associated complex torus $T = \mathbb{C}/\Lambda$. Let $[\alpha] : E \to E$ be an endomorphism with standard form $\left(\frac{s(x)}{v(x)}, \frac{t(x)}{w(x)}y\right)$. Finally, let $\alpha : T \to T$ be the corresponding multiplication-by-α map, $\alpha \in \mathbb{C}$. Then*

$$s(x) = x^{\|\alpha\|^2} + \dots \quad v(x) = \alpha^2 x^{\|\alpha\|^2 - 1} + \dots$$
$$t(x) = x^n + \dots \quad w(x) = \alpha^3 x^n + \dots$$

where we omitted the lower-degree monomials.

Proof. We recall that $[\alpha]\left(\wp_\Lambda(z), \frac{\wp'_\Lambda(z)}{2}\right) = \left(\wp_\Lambda(\alpha z), \frac{\wp'_\Lambda(\alpha z)}{2}\right)$, which means, in particular, that $\frac{s(\wp_\Lambda(z))}{v(\wp_\Lambda(z))} = \wp_\Lambda(\alpha z)$. As a consequence, since both $\wp_\Lambda(z)$ and $\wp_\Lambda(\alpha z)$ have a pole of order 2 in $z = 0$, we have $\deg(s(x)) - \deg(t(x)) = 1$. Moreover $\deg(t(x)) < \deg(\alpha)$ since there is a zero of the endomorphism, $[0 : 1 : 0]$, which is not affine, and we conclude that $\|\alpha\|^2 = \deg(s(x))$ by the fact

$$\max\{\deg(s(x)), \deg(t(x))\} = \deg(s(x)) = \deg(\alpha) = \|\alpha\|^2.$$

The constant of $v(x)$ is obtained by comparing directly the Laurent series centered in $z = 0$ for $\frac{s(\wp_\Lambda)}{v(\wp_\Lambda)} = \frac{1}{cz^2} + o(z) = \wp_\Lambda(\alpha x) = \frac{1}{\alpha^2 z^2} + o(z)$, hence $c = \alpha^2$.
The structure of $t(x), w(x)$ is obtained by realizing that

$$\frac{t(\wp_\Lambda(z))}{w(\wp_\Lambda(z))}\frac{\wp'_\Lambda(z)}{2} = \frac{\wp'_\Lambda(\alpha z)}{2} = \frac{1}{2\alpha}\frac{d}{dz}\wp_\Lambda(\alpha z) =$$
$$\frac{1}{2\alpha}\frac{d}{dz}\left(\frac{s(\wp_\Lambda(z))}{v(\wp_\Lambda(z))}\right) = \frac{1}{\alpha}\left(\frac{d}{dx}\frac{s(x)}{v(x)}\right)\Bigg|_{x=\wp_\Lambda(z)} y\Big|_{y=\frac{\wp'_\Lambda}{2}}$$

which means that
$$\frac{t(x)}{w(x)} = \frac{1}{\alpha}\frac{d}{dx}\frac{s(x)}{v(x)}$$
and that $t(x), w(x)$ have the same degree. □

Remark III.4.5. This result tells us that, given $\phi \in End(E)$, in order to obtain $\alpha \in \mathbb{C}$ such that ϕ corresponds to the multiplication-by-α map in the associated complex torus, it is enough to divide the leading coefficient of $w(x)$ by the leading coefficient of $v(x)$

Now we are ready to characterize the structure of the endomorphism ring of an elliptic curve over a field $K \subset \mathbb{C}$.

Theorem III.4.6 (Structure Theorem)**.** *Let E/K be an elliptic curve with $K \subseteq \mathbb{C}$. Then $End(E)$ is a commutative domain isomorphic to:*

1. *$\mathbb{Z}$*
2. *An order $\mathbb{Z} \subsetneq R \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, d square-free negative integer, of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, the ring of integers of an imaginary quadratic extension of $\mathbb{Q}$.*

For each endomorphism $[\alpha] \in End(E)$ there is an endomorphism $\overline{[\alpha]} : E \to E$ called dual endomorphism *such that $[\alpha]\overline{[\alpha]} = [\deg(\alpha)] \in End(E)$. Moreover, let $y^2 = x^3 + Ax + B$ be the equation of E/K in Weierstrass form. Then the field of definition of $[\alpha] \in End(E)$ is:*

1. *$\mathbb{Z}[A, B]$ if $End(E) \simeq \mathbb{Z}$.*
2. *$\mathbb{Q}(\sqrt{d})[A, B]$ if $End(E)$ is an order in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.*

Proof. First, consider the associated complex torus $T = \mathbb{C}/\Lambda_1$. Then we find that the ring is commutative since the multiplication by a complex number is commutative and it is a domain since the degree of the product of two maps is the product of their degrees.

Now consider E' isomorphic to E with the property that the associated complex torus $T' = \mathbb{C}/\Lambda'$ has the associated lattice generated by 1 and $\omega' \in \mathbb{C}$, after the multiplication of the lattice Λ' by a constant $c \in \mathbb{C}$, where $\frac{1}{c}$ is one of the generators of Λ_1. This isomorphism induces an isomorphism of the endomorphism rings, where given $\alpha \in End(T)$ the corresponding endomorphism in $End(T')$ is $c\alpha c^{-1}$. So, to characterize the endomorphism ring of E, we can focus on the endomorphisms of E', hence the ones of T'. Now, we distinguish two cases.

1. If there is no special endomorphism, we have $End(E') \simeq \mathbb{Z}$.
2. If there exists $[\alpha] : E' \to E'$ such that $\alpha \in \mathbb{C}\backslash\mathbb{R}$ then we show that $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, d square-free, the ring of integers of a quadratic extension of $\mathbb{Q}$. In fact, there exists $n, m \in \mathbb{Z}$ such that $[\alpha]^2+[n][\alpha]+[m] = 0$ by the representation presented above, hence $\alpha^2 + n\alpha + m = 0$ and α lies in the ring of integers of a quadratic extension. Moreover, by the fact that $\alpha\Lambda' \subseteq \Lambda'$, then $\alpha \cdot 1 = a + b\omega'$, $a, b \in \mathbb{Z}$, hence $\omega' \in \mathbb{Q}(\sqrt{d})$. Then we conclude that given any other $[\beta] \in End(E')$ the associated complex number β lies in $\mathbb{Q}(\sqrt{d})$, since $\beta = a' + b'\omega'$. By the representation with integer coefficients we have that $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and this implies that $End(E) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

The dual endomorphism, when represented by a complex number, is necessarily the complex conjugate of α, in fact $[\alpha]\overline{[\alpha]} = [\deg(\alpha)] = [\|\alpha\|^2] = [\alpha\bar{\alpha}] = [\alpha][\bar{\alpha}]$. Now we prove that the complex conjugate $[\bar{\alpha}]$ is in $End(E)$. Consider the polynomial identity $(X - \alpha)(X - \bar{\alpha}) = X^2 + nX + m$, with $n, m \in \mathbb{Z}$, since α is in a ring of integers. As a result $\overline{[\alpha]} = -[\alpha] - [n] \in End(E)$.

Consider $K = \mathbb{Q}(A, B)$ the field of definition of the multiplication-by-n maps. We know this to be true, since we have already proved that the coefficients of such maps lie in $\mathbb{Z}[A, B]$. We notice that the endomorphisms in standard form have algebraic coefficients over K. In fact, the denominator of an isogeny $[\alpha]$ divides the denominator of the isogeny $[n] = [\alpha][\bar{\alpha}]$, $[n] \in \mathbb{Z} \subset End(E)$, while the numerator depends algebraically on the denominator of the isogenies. Let $K(\phi)$ be the field over K generated by the coefficients of the endomorphism when written in standard form. Consider $\sigma \in Gal(\overline{K(\phi)/K})$ in the Galois group of the Galois closure of the extension. Then the map

$$\phi^\sigma = \left(\frac{s^\sigma(x)}{v^\sigma(x)}, \frac{t^\sigma(x)}{w^\sigma(x)}y\right) \quad \sigma \text{ acts on the coefficients of the polynomials}$$

is still an endomorphism since σ is an automorphism of fields that fixes both the equation of the elliptic curve and the addition map. Thus, necessarily the endomorphism $[\beta] = \phi^\sigma$, for some $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. To determine β it is enough, by the remark above, to look at how the leading coefficients of $c_1 = v^\sigma$ and $c_2 = w^\sigma$ change.

$$\alpha' = \frac{\sigma(c_2)}{\sigma(c_1)} = \sigma\left(\frac{c_2}{c_1}\right) = \sigma(\alpha) = \alpha^\sigma \iff [\beta] = [\alpha^\sigma] \iff [\alpha]^\sigma = [\alpha^\sigma]$$

This interesting relation tells us that the only automorphisms that change the endomorphism, hence that change the coefficients, are in $Gal(K(\sqrt{d})/K)$. By Galois theory, this is equivalent to $K(\phi) = K(\sqrt{d})$. □

Chapter IV

Algebraic Structure

IV.1 Imaginary Quadratic Fields

On the following sections we will focus on the arithmetic of elliptic curves with complex multiplication by the full ring of integers of an imaginary quadratic extension of $\mathbb{Q}$. Since our main interest is the investigation of the rational points of such curves, it will be useful to restrict our attention to those whose equation in Weierstrass form is defined over $\mathbb{Q}$.

Consider an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and its associated complex torus $T = \mathbb{C}/\Lambda$. After a $\mathbb{C}$-isomorphism, we can make the associated torus equal to this one: $T_1 = \mathbb{C}/I$, where $I \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is an ideal. In fact, an isomorphism of elliptic curves corresponds to the multiplication by a complex number of the associated lattice, then by the proof of Theorem III.4.6 we know that there is a constant c' so that $c'\Lambda \subset \mathbb{Q}(\sqrt{d})$. This implies that there is a constant $c \in \mathbb{C}$ such that $c\Lambda \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and by the fact that $\alpha\Lambda \subset \Lambda$, for any $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, we see that $c\Lambda \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is an ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

On the other hand, any ideal $I \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a CM lattice since it is generated by two $\mathbb{R}$-linearly independent elements. Therefore, to classify and count all the $\mathbb{C}$ -isomorphism classes of the CM elliptic curves, that is, all the non-isomorphic CM lattices, it is natural to define the following equivalence relation on the ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

$$I_1 \simeq I_2 \iff \exists w \in Q(\sqrt{d}) \text{ such that } wI_1 = I_2$$

The number of classes is the *class number* h_K of the field $K = \mathbb{Q}(\sqrt{d})$ and $h_K = 1$ if and only if $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a principal ideal domain (PID). As a consequence of this construction and by the following theorem, we characterize all possible CM curves with a model over $\mathbb{Q}$.

Theorem IV.1.1. *Let E/L be an elliptic curve with CM by $\mathcal{O}_K$. Then:*

1. *$j(E)$ is an algebraic integer,*
2. *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$.*

Proof. (1). See [Sil91, §II.6]. (2) See [Sil91, Theorem II.4.3b]. □

Thus, since a CM elliptic curve that has coefficients in $\mathbb{Q}$ has rational j-invariant, in particular an integer according to the above theorem, it turns out that the only CM elliptic curves with a model over $\mathbb{Q}$ are those with complex multiplication by the ring of integers of an imaginary quadratic extension of class number one. Each class of such curves has at least a model defined over $\mathbb{Q}$ and by a famous theorem, proven by Heegner and Stark, $\mathbb{Q}(\sqrt{d})$ is an imaginary quadratic extension of class number one if and only if:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163. \tag{IV.1}$$

Example IV.1.2. Let E be an elliptic curve with equation in Weierstrass form $y^2 = x^3 + x$, this curve has a nontrivial endomorphism

$$\phi : (x, y) \mapsto \left(\frac{x}{-1}, \frac{1}{-i}y\right).$$

By the Theorem on the structure of endomorphisms in standard form, this corresponds to the multiplication-by-i map in the associated complex torus. Thus, this curve has complex multiplication by the ring of integers $\mathbb{Z}[i]$ and is defined over $\mathbb{Q}$, in fact $\mathbb{Q}(\sqrt{-1})$ is a class number one imaginary quadratic extension.

Example IV.1.3. Another example is the elliptic curve $y^2 = x^3 + 1$ which has the nontrivial endomorphism

$$\phi : (x, y) \mapsto \left(\frac{x}{\zeta_3^2}, y \right).$$

This corresponds to the multiplication-by-ζ_3 in the associated complex torus. As a consequence, the ring of integers is $\mathcal{O}_{\mathbb{Q}(\sqrt{3})}$, which is $\mathbb{Z}[\zeta_3]$ and its field of fractions is $\mathbb{Q}(\sqrt{-3})$, hence a class number one imaginary quadratic extension.

It is important to note that these curves have coefficients in $\mathbb{Q}$ but have their additional endomorphisms only over $K = \mathbb{Q}(\sqrt{d})$. So, to take advantage of the additional structure, we shall investigate the arithmetic of those fields, in particular the associated ring of integers. Since those rings are PID each number still has a unique decomposition, up to units, into irreducible elements, which are the primes of this ring. In particular, since $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, we can look at the behavior of the rational primes inside this larger ring.

Proposition IV.1.4. *Let $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be the ring of integers of an imaginary quadratic extension of class number one and let $p \in \mathbb{Z}$ be a rational prime. Then it has three possible behaviors.*

1. *(p) is still prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, we say that p is inert and $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(p)} \simeq \mathbb{F}_{p^2}$.*
2. *$(p) = (\pi_1)(\pi_2)$, $(\pi_1) \neq (\pi_2)$ primes, we say that p splits and the residue field is $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\pi_1)} \simeq \frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\pi_2)} \simeq \mathbb{F}_p$.*
3. *$(p) = (\pi)^2$ then we say p ramifies in K.*

Proof. We treat the different cases separately.

1. If (p) is still a prime, then $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(p)}$ is a finite domain, hence a field. Since $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is also a lattice in $\mathbb{C}$ and the multiplication-by-p is an endomorphism of this lattice, we can conclude $|\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(p)}| = [\mathcal{O}_{\mathbb{Q}(\sqrt{d})} : p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}] = \#\ker([p]) = \|p\|^2$.
2. If (p) is not a prime, then $p = \pi_1\pi_2$ with $(\pi_1), (\pi_2) \neq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Then necessarily $\|\pi_1\| = \sqrt{p} = \|\pi_2\|$ since these are not units and we obtain $\pi_1 = \bar{\pi}_2$. This proves that (π_1), (π_2) are irreducible, hence primes since $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID. Moreover $|\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\pi_1)}| = |\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\pi_1)}| = \ker([\pi_1]) = \|\pi_1\|^2 = p$.

□

As a result of the previous proposition, we can define the *degree* $d_\mathfrak{p} \in \mathbb{N}$ of a prime $\mathfrak{p} \in I_{\mathbb{Q}(\sqrt{d})}$, the set of the ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, with associated rational prime $(p) = \mathfrak{p} \cap \mathbb{Z}$, in the following way.

$$d_\mathfrak{p} = \left[\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{p}} : \frac{\mathbb{Z}}{(p)} \right]$$

which is equal to 1 if p splits and 2 if p is inert.

The following quantity is important to characterize the behavior of a rational prime in the ring of integers of a quadratic extension of $\mathbb{Q}$.

Definition IV.1.5. Let $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be the ring of integers of a quadratic extension $K/\mathbb{Q}$ then we define the discriminant D_K:

$$D_K : \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & d \equiv 2, 3 \mod 4 \end{cases}$$

Theorem IV.1.6. *Let p, $p \neq 2$, be a rational prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Then:*

1. *(p) ramifies if and only if $D_K \equiv 0 \mod p$*
2. *(p) splits if and only if $D_K \equiv a^2 \mod p$*
3. *(p) is inert if and only if $D_K \not\equiv a^2 \mod p$*

while if $p = 2$:

1. *(2) ramifies if and only if $D_K \equiv 0, 4 \mod 8$*
2. *(2) splits if and only if $D_K \equiv 1 \mod 8$*
3. *(2) is inert if and only if $D_K \equiv 5 \mod 8$*

Using quadratic reciprocity, the splitting pattern shows some regularity.

Theorem IV.1.7. *Let p be a rational prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $d \neq -2$. Then:*

1. *(p) ramifies if and only if $\left(\frac{p}{D_K}\right) = 0$*
2. *(p) splits if and only if $\left(\frac{p}{D_K}\right) = 1$*
3. *(p) is inert if and only if $\left(\frac{p}{D_K}\right) = -1$*

where $\left(\frac{p}{q}\right)$ is the quadratic residue symbol *or* Jacobi symbol *which is defined on rational primes p, q, $q \neq 2$, as the number $a \in \{1, -1, 0\}$ such that $p^{\frac{\mathbb{N}p-1}{2}} \equiv a \mod q$. This definition is extended to $q = 4$ in the same way and is extended by linearity in the numerator and denominator.*

IV.2 Reduction of CM Elliptic Curves

In the previous section, we saw that it is possible to reduce modulo a prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and obtain elements in a finite field. Therefore, a further step in the investigation of CM elliptic curves E/K, $\mathbb{Q}(\sqrt{d}) \subseteq K$, defined over $\mathbb{Z}$, i.e. with integer coefficients in Weierstrass form, is understanding how they behave when reduced modulo a prime.

Definition IV.2.1. Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, with equation $y^2 = x^3 + Ax + B$ in Weierstrass form defined over $\mathbb{Z}$. Let $(\pi) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be a prime, $q = \|\pi\|^2 = \mathbb{N}(\pi)$. Then we define the reduced curve $\tilde{E}_\pi/\mathbb{F}_q$ by the equation:

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

where $\tilde{A}, \tilde{B} \in \mathbb{F}_p$ are the reduction modulo π of A, B as elements of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Remark IV.2.2. In general, an elliptic curve E/K will always be reduced modulo a prime $\mathfrak{p} \leq \mathcal{O}_K$, the ring of integers of K.

The reduced curve is still a cubic curve, but defined over a finite field of characteristic $p > 0$. Obviously, not every reduction sends elliptic curves to elliptic curves.

Proposition IV.2.3. *Let E/K be a CM elliptic curve defined over $\mathbb{Z}$ and let $\tilde{E}_\pi$ be its reduction modulo π. Then $\tilde{E}_\pi$ is an elliptic curve if and only if $\pi \nmid \Delta(E)$.*

Proof. $\tilde{E}_\pi$ is an elliptic curve if and only if $\Delta(\tilde{E}_\pi) \neq 0 \iff \Delta(\tilde{E}_\pi) \not\equiv 0 \mod \pi$ and therefore if and only if $\pi \nmid \Delta(E)$. □

The primes π such that the reduced curve is still an elliptic curve are said to be *primes of good reduction*. The other primes are said to be *primes of bad reduction*. The structure of the reduced elliptic curve is similar to the original one by the following theorem.

Theorem IV.2.4. *Let E/K be an elliptic curve defined over $\mathbb{Z}$ in Weierstrass form, let π be a prime of good reduction and let $\tilde{E}_\pi$ be the reduced curve. Then there is a natural injective morphism of rings $\Phi : End(E) \to End(\tilde{E}_\pi)$ defined by*

$$\Phi : \phi \mapsto \tilde{\phi}$$

given by the reduction modulo π of the endomorphism in standard form. Moreover, the map Φ preserves the degree.

Proof. First of all, it is obvious that $\Phi([1]) = \widetilde{[1]}$, multiplication-by-1 morphism, i.e. the identity. Furthermore, the function respects the sum: $\Phi(\phi_1 + \phi_2) = \tilde{\phi_1} \tilde{+} \tilde{\phi_2}$, where $\tilde{+}$ is the standard sum of two points in the reduced elliptic curve. As a result we find $\Phi([n]) = \widetilde{[n]} \in End(\tilde{E}_\pi)$, the multiplication-by-$n$ morphism. Moreover, the map respects the product, i.e. the composition.

Now we prove that the multiplication-by-n maps have the same degree when reduced. First, let $\pi \nmid n$ and consider the x coordinate $\frac{s_n(x)}{v_n(x)}$ of $[n]$ in standard form, where $s_n(x) = x^{n^2} + \dots$ and $v_n(x) = n^2 x^{n^2-1}$. As a consequence, the reduced polynomials have the same degree of the original ones. It remains to prove that the reductions $\tilde{s_n}(x), \tilde{v_n}(x)$ are coprime. This follows by the identity $s_n = xv_n - h(x)g(x)$, where $h \mid v_{n+1}$ and $g \mid v_{n-1}$ in $\mathbb{Z}[A, B][X]$, see [Sut17b] for a proof. In fact, if the reduction of the numerator and of the denominator had a common zero, it would be both a n-torsion point and a $n+1$-torsion point or a $n-1$-torsion point, hence it would be the zero point which is not affine, and this proves, by contradiction, that the numerator and the denominator are coprime. We have shown that the degree of the reduced maps is $\deg(\widetilde{[n]}) = \max\{\tilde{s}_n(x), \tilde{v}_n(x)\} = n^2 = \deg([n])$. If the prime $\pi \mid n$ then we consider $\widetilde{[n]} = \Phi([n-1]) \tilde{+} \widetilde{[1]}$ which is defined and different from the zero isogeny since the two maps have different degrees. Furthermore, the degree of the numerator $\deg(\tilde{s}_n) = n^2$ so that the degree of the endomorphism is preserved. However, we stress that the degree of the reduced denominator in this case is necessarily lower than the original one, since $v_n = nx^{n^2-1} + \dots$ has the leading coefficient $\pi \mid n$. This means that the endomorphism is no longer separable.

Now, we consider a general endomorphism $\phi \in End(E)$.

Lemma IV.2.5. *Consider the equation $y^2 = x^3+Ax+B$ of E/K in the Weierstrass form, $A, B \in \mathbb{Z}$, and suppose that the curve has CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Then the coefficients of the endomorphism $\phi \in End(E)$ in standard form lie in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.*

Proof. First, recall that we already know that the coefficients lie in $\mathbb{Q}(\sqrt{d})[A, B]$. Moreover, the result obviously holds for $[m] \in \mathbb{Z} \subset End(E)$, then if we show that the same holds for an element $[\beta] \in End(E)$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}+\beta\mathbb{Z}$ we conclude, by the fact that the sum of two points is a rational map with coefficients in $\mathbb{Z}[A, B]$. Let $[\alpha] \in End(E)$ be an endomorphism such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\alpha]$. We choose β to be a number of the form $\alpha + n$, $n \in \mathbb{Z}$, such that $\gcd(\beta, \Delta(E)) = 1$, this is possible since $2\Delta(E)$ is finite. Then obviously β is still a generator of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Now, we prove that the result holds for $[\beta] \in End(E)$. Consider the x coordinate $\frac{v_1(x)}{s_1(x)}$ of such endomorphism in standard form and let $\frac{v(x)}{s(x)}$ be the x coordinate of the endomorphism $[\deg(\beta)] = [m] = [\beta][\bar{\beta}] \in \mathbb{Z}$. We notice that $\gcd(m, \Delta(E)) = 1$, since $\Delta(E) \in \mathbb{Z}$. Now, we know that $s_1(x) \mid s(x)$ in $\mathbb{Q}(\sqrt{d})$, so that if we prove that the content of $s(x)$, $cont(s)$, is (1), hence the polynomial is primitive, we conclude that $s_1(x) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}[X]$ by Gauss's Lemma. To do this, we show that there exists no prime $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ that divides $cont(s)$, hence such that $s(x) \equiv 0 \mod (\pi)$. First, if $\pi \mid \Delta(E)$, by the choice of β, the leading coefficient of $s(x)$, equal to m^2, is not divisible by π, therefore $s(x) \not\equiv 0 \mod (\pi)$, while if $p \nmid \Delta(E)$ we have just proven that the reduction of $[m]$ is well defined, only if $s(x) \not\equiv 0 \mod (\pi)$.

For the numerator, we know that $[\beta] \circ [\bar{\beta}] = [m]$ has integral coefficients. Then, if the numerator $v_1(x)$ had fractional coefficients, we would obtain as a consequence that the numerator of $[m]$ would also have rational coefficients, since $cont(s_1) = (1)$ and has integral coefficients. □

Now let $\phi \in End(E)$ and let $\bar{\phi} \in End(E)$ be its dual morphism, their coefficients are integral and in the same ring of integers of π, so we can reduce their equation in standard form and since $\Phi(\phi \circ \bar{\phi}) = \Phi(\phi) \circ \Phi(\bar{\phi}) = \tilde{[n]} \in \mathbb{Z}$ the reductions are well defined. Moreover we notice that the reduced morphisms are still morphisms of curves and respect also the group law, so are endomorphisms. Finally, the degree, being multiplicative, is necessarily preserved, if not, the degree of the multiplication-by-n maps will not be preserved. This last argument also settles the injectivity. □

A straightforward consequence is the characterization of the structure of the torsion points for the reduction $\tilde{E}_\pi$, over a prime (π) of good reduction, of the elliptic curves E/K defined over $\mathbb{Z}$.

Theorem IV.2.6 (Structure of the Torsion Points)**.** *Let $q \in \mathbb{N}$ be a rational prime. Then the group of the q^n-torsion points of the reduced elliptic curve $\tilde{E}_\pi$ is isomorphic to:*

1. *$\frac{\mathbb{Z}}{q^n\mathbb{Z}}$ or $\{0\}$ if $\pi \mid p$*

2. *$\frac{\mathbb{Z}}{q^n\mathbb{Z}} \times \frac{\mathbb{Z}}{q^n\mathbb{Z}}$ otherwise*

Proof. Case n=1. If $\pi \nmid q$ then $\#\tilde{E}_\pi[q] = q^2$, so the group of q-torsion points is commutative of order q and cardinality q^2 and therefore it is necessarily isomorphic to $\frac{\mathbb{Z}}{q\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$. Although if $\pi \mid q$ the kernel of the endomorphism is an abelian group of order q and with cardinality lower than q^2 by the proof of the above theorem, then its cardinality is q or 1.

General case. The result follows by induction. We have shown that the base case $n = 1$ holds. Moreover, if $\ker([q^k]) = \frac{\mathbb{Z}}{q^k\mathbb{Z}} \times \frac{\mathbb{Z}}{q^k\mathbb{Z}}$ for any $k \leq n$, then by multiplicativity of the separable degree we obtain that $|ker([q^{n+1}])| = q^{2n+2}$. Finally, by the structure theorem of finite abelian groups, we conclude since, for any $k \leq n$, the group $\ker([q^{n+1}])$ has exactly two cyclic subgroups of order q^k. □

Remark IV.2.7. As a consequence of the above result, there is a similarity between the endomorphism structure of E/K and the one of its reduction over a prime of good reduction. In particular, we found that the former injects into the latter and in many cases that is all we can say. For example, consider an elliptic curve E/K with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, fix an inert prime p with $p \nmid \Delta(E)$ and consider the associated reduced elliptic curve $\tilde{E}_p$. Since the reduced elliptic curve is defined over $\mathbb{F}_p$, we have the associated Frobenius endomorphism ϕ_p . Then $\deg(\phi_p) = p$ and there is no morphism $[\alpha] \in End(E)$ of degree p since if this was the case $[\alpha] \circ \overline{[\alpha]} = [p]$ but p is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, so there exists no $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ such that $\alpha\bar{\alpha} = p$. As a consequence, the endomorphism ring of E is strictly smaller than the one of its reduction.

IV.3 Isogeny Representation

When studying the endomorphism ring of the elliptic curves defined over $K \subseteq \mathbb{C}$ the representation $\rho : End(E) \to M_2(\mathbb{Z})$ was of great importance. However, this connection cannot work on the reduced curve $\tilde{E}_\pi/\mathbb{F}_p$ since there is no associated complex torus, so we need a more general construction.

Let E/K be an elliptic curve and fix a rational prime $\ell \nmid \mathrm{char}(K)$. The groups $E[\ell^n]$, $n > 0$, are linked by the surjective homomorphism $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$, the multiplication-by-$\ell$ endomorphism. As a result, these groups, together with the map $[\ell]$, form the inverse system

$$\begin{tikzcd} E[\ell] & E[\ell^2] \arrow[l, "{[\ell]}"'] & E[\ell^3] \arrow[l, "{[\ell]}"'] & \dots . \arrow[l, "{[\ell]}"'] \end{tikzcd}$$

Next, recall that the group of the ℓ^n-torsion points is

$$E[\ell^n] \simeq \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}},$$

we have proved this result only in some cases, which are the ones we are interested in, but we can assume that this holds in general. Then the above inverse system is equivalent to the following:

$$\begin{tikzcd} \frac{\mathbb{Z}}{\ell\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}} & \frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \arrow[l, "{[\ell]}"'] & \frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \arrow[l, "{[\ell]}"'] & \dots . \arrow[l, "{[\ell]}"'] \end{tikzcd}$$

Now choose an ordered basis $\mathcal{B}_n = (P_1^n, P_2^n)$ of the points of $E[\ell^n]$, $n > 0$, such that $[\ell](P_i^{n+1}) = P_i^n$. By the fact $\langle P_i^n \rangle \simeq \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$ the above inverse system breaks into two equal inverse systems isomorphic to:

$$\begin{tikzcd} \frac{\mathbb{Z}}{\ell\mathbb{Z}} & \frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \arrow[l, "\ell"'] & \frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \arrow[l, "\ell"'] & \dots , \arrow[l, "\ell"'] \end{tikzcd}$$

where ℓ is the standard projection of $\frac{\mathbb{Z}}{\ell^{n+1}\mathbb{Z}} \to \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$, that is, the multiplication by ℓ. Further, to any inverse system we can associate an inverse limit, in particular the last one is very interesting since

$$\mathbb{Z}_\ell = \varprojlim_{n\in\mathbb{N}^*} \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} = \frac{\mathbb{Z}}{\ell\mathbb{Z}} \xleftarrow[\ell]{} \frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \xleftarrow[\ell]{} \frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \xleftarrow[\ell]{} \dots$$

is the ring of the ℓ-adic integers. Hence we obtain the following definition.

Definition IV.3.1 (ℓ-adic Tate module)**.** Let $\ell \in \mathbb{Z}$ be a prime as before then the inverse limit

$$T_\ell[E] = \varprojlim_{n\in\mathbb{N}^*} E[\ell^n] \simeq \varprojlim_{n\in\mathbb{N}^*} \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \simeq \left(\varprojlim_{n\in\mathbb{N}^*} \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}\right) \times \left(\varprojlim_{n\in\mathbb{N}^*} \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}\right) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

is the *ℓ-adic Tate module* associated to the elliptic curve E.

Therefore, the Tate module is a $\mathbb{Z}_\ell$-module and comes equipped with the ring of the endomorphisms $End(T_\ell(E)) \simeq M_2(\mathbb{Z}_\ell)$, where any sequence of endomorphisms ϕ_n of $E[\ell^n]$, which respects the transition maps, that is, that makes the following diagram commutative

$$\begin{tikzcd}
E[\ell] \arrow[d, "\phi_1"] & E[\ell^2] \arrow[l, "{[\ell]}"'] \arrow[d, "\phi_2"] & E[\ell^3] \arrow[l, "{[\ell]}"'] \arrow[d, "\phi_3"] & \dots \arrow[l, "{[\ell]}"'] \\
E[\ell] & E[\ell^2] \arrow[l, "{[\ell]}"'] & E[\ell^3] \arrow[l, "{[\ell]}"'] & \dots \arrow[l, "{[\ell]}"']
\end{tikzcd}$$

is an endomorphism of the Tate module. This happens if and only if the maps respect $[\ell](\phi_{n+1}(P_i^{n+1})) = \phi_n([\ell](P_i^{n+1}))$, for any $n \geq 0$ and any $1 \leq i \leq 2$. So, if we prove that any $\phi \in End(E)$ respects this hypothesis, we will construct a ring representation:

$$\rho : End(E) \to M_2(\mathbb{Z}_\ell) \simeq End(T_\ell(E)).$$

But this is true since $[\ell] \in \mathbb{Z} \subset End(E)$, commuting with any endomorphism, fixes $E[\ell^n]$ and can be seen as a sequence of homomorphisms ϕ_n of $E[\ell^n]$. Moreover

$$[\ell](\phi_{n+1}(P_i^{n+1})) = [\ell](\phi(P_i^{n+1})) = \phi([\ell](P_i^{n+1})) = \phi_n([\ell](P_i^{n+1}).$$

Proposition IV.3.2. *The ℓ-adic representation is injective.*

Proof. Consider $\phi \in End(E)$ such that $\rho(\phi) = 0 \in M_2(\mathbb{Z}_l)$. Then the associated homomorphisms $\phi_n = 0 \in M_2(\frac{\mathbb{Z}}{q^n\mathbb{Z}})$ for any $n > 0$. Hence, ϕ has an infinite kernel, so $\phi = 0$. □

However, instead of simple injectivity, a much stronger result holds.

Theorem IV.3.3. *Let E/K be an elliptic curve and fix a rational prime $q \in \mathbb{Z}$, $q \nmid \mathrm{char}(K)$. Recall that $End(E)$ is a $\mathbb{Z}$-module and, for the curves we have studied, it is torsion-free. Then the natural extension by linearity of the q-adic representation with $\mathbb{Z}_q$ coefficients*

$$\rho_q : End(E) \otimes \mathbb{Z}_q \to End(T_q(E))$$

is injective.

We stress the importance of this result, as it means that if two endomorphisms $\phi, \psi \in End(E)$ are independent over $\mathbb{Z}$, then their representations are independent over $\mathbb{Z}_q$, or as a contrapositive statement, if the representations are dependent over $\mathbb{Z}_q$ the endomorphisms are dependent over $\mathbb{Z}$. See [Sil09, Theorem III.7.4] for a proof.

The injectivity has many consequences; in particular, it is very helpful for the following result.

Proposition IV.3.4. *Let E/K be an elliptic curve defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and suppose that it has good reduction $\tilde{E}_\pi$ over a prime π. Denote by $End_\pi(E) \simeq \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subseteq End(\tilde{E}_\pi)$ the reduction of $End(E)$. Then:*

$$\phi \in End_\pi(E) \iff \phi \text{ commutes with any } \psi \in End_\pi(E).$$

Proof. The first direction is obvious since $End(E)$ is a commutative ring. Consider $\phi_q = \rho_q(\phi)$ and let $[\alpha]_q = \rho_q([\alpha])$ with $[\alpha] \in End_\pi(E)$ such that $End_\pi(E) = \mathbb{Z}[[\alpha]]$. Then if ϕ_q commutes with $[\alpha]_q$ and is not in $\mathbb{Q}_q[[\alpha_q]]$ we would have a subspace of $M_2(\mathbb{Q}_q)$ of dimension 3 that is commutative, a contradiction. Then $\phi_q \in \mathbb{Q}_q[\alpha_q]$ and it has a minimal polynomial $\phi_q^2+\beta\phi_q+\gamma = 0$ and $\gamma, \beta \in \mathbb{Z}_q$. Now we apply Theorem IV.3.3 to conclude that $\phi^2+a\phi+b = 0$ with $a, b \in \mathbb{Z}$ which means that ϕ and $[\alpha]$ are in the ring of integers of the same extension and by the fact that $\mathbb{Z}[[\alpha]] \simeq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is the full ring of integers, we conclude $\phi \in \mathbb{Z}[[\alpha]] = End(E)$. □

This results in the following.

Corollary IV.3.5. *Let E/K be an elliptic curve defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, let $\tilde{E}_\pi$ be its reduction over a good prime π and let $p \in \mathbb{Z}$ be a rational prime such that $(p) = \mathbb{Z} \cap (\pi)$. Denote by ϕ_p the Frobenius endomorphism. Then:*

1. *If p splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ then $\phi_p \in End_\pi(E)$, in particular $\phi_p = [\alpha\pi] \in End_\pi(E)$ with α of degree 1. In this case $ker([p]) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ and the reduced curve is called* ordinary*.*

2. *If p is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, then $\phi_p \notin End_\pi(E)$ and $\phi^2 = -[p] \in End_\pi(E)$. In this case $ker([p]) = \{0\}$ and the reduced curve is called* supersingular*.*

Proof. Recall that the Frobenius automorphism of fields has the property that $\phi_p^n(x) = x \iff x \in F_{p^n}$. Then, if p splits, all the coefficients of the endomorphisms $\psi \in End_\pi(E)$ lie in $\mathbb{F}_p$, so that $\phi_p \circ \psi = \psi^{\phi_p} \circ \phi_p = \psi \circ \phi_p$, hence ϕ_p commutes with $End_\pi(E)$. As a result of the above theorem $\phi_p \in End_\pi(E)$. Now, recall that by the structure theorem of the endomorphisms in standard form and the structure of the reduction mapping also $\pi \in End_\pi(E)$ is inseparable since the degree of the denominator of its x coordinate in standard form is lower than $p-1$. This means that $\pi = \beta\phi_p$ and by a degree argument β is invertible. Moreover, $\bar{\pi}$ is still separable after the reduction, since $\pi \nmid \bar{\pi}$. This means that $\deg_{sep}(\widetilde{[p]}) = p$.

If p is inert, the coefficients of the endomorphism $\psi \in End_\pi(E)$ lie in $\mathbb{F}_{p^2}$. Therefore, by the fact that ϕ_p is induced by the complex conjugation on $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, we obtain that $\phi_p \circ \psi = \psi^{\phi_p} \circ \phi_p = \bar{\psi} \circ \phi_p$ and ϕ_p does not commute with $End_\pi(E)$. However, ϕ_p^2 fixes $\mathbb{F}_{p^2}$, which means that ϕ_p^2 necessarily commutes with $End_\pi(E)$, so that $\phi_p^2 \in End_\pi(E)$. By the fact p is inert $\phi_p^2 = \beta \circ [p]$, where $[\beta]$ is invertible, since

ϕ_p^2 has degree p^2, so we get its dual endomorphism $\bar{\phi_p} = \alpha\phi_p$. But $\phi_p^2 = \beta \circ [p]$ has to commute with ϕ_p, hence $\beta \in \mathbb{Z}$, which means $\beta = [1]$ or $\beta = [-1]$. Then ϕ_p is a root of $X^2 - [p] = 0$ or $X^2 + [p] = 0$, suppose the first one. If this is true $\mathbb{Z}[\phi_p] \simeq \mathbb{Z}[\sqrt{p}]$ and we will prove $\mathbb{Z}[\sqrt{p}]$ has an infinite number of units; hence $\mathbb{Z}[\phi] \subseteq End(E)$ has an infinite number of units, which is a contradiction since $|Aut(E)|$ is a finite group. First, we have to show that $\mathbb{Z}[\sqrt{p}]$ has a nontrivial unit of the form $a + b\sqrt{p}$ for $a, b \neq 0 \in \mathbb{Z}$ and a, b coprime. This is equivalent to

$$(a + b\sqrt{p})(a - b\sqrt{p}) = 1 \iff a^2 - pb^2 = 1$$

because the inverse of $a + b\sqrt{d}$ has the form $\frac{a-b\sqrt{p}}{a^2-bp^2}$ and this representation is unique inside $\mathbb{Q}(\sqrt{p})$. The equation $a^2 - pb^2 = 1$ is the Pell's equation and it can be shown quite easily that it has a nontrivial solution, see [IR90, §17.5] for a proof. So, we have a nontrivial unit $u = a + b\sqrt{d}$ and then u^n are the other infinite units, since if $u^n = 1$ for $n > 2$ then u would be a n^{th} root of unity that lies in $\mathbb{R} \setminus \mathbb{C}$, but this is impossible since $\mathbb{Q}(\sqrt{p})$ is a totally real field.

As a result, we conclude that $\phi^2 = -[p]$ and that $[p]$ is purely inseparable. □

Remark IV.3.6. We characterized the structure of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ for the split and inert primes $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, however, we have not treated the case in which π ramifies. These cases are finite, in particular for our choice of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ there is only one prime $p \mid D_K$ that ramifies, where D_K is the discriminant of $K = \mathbb{Q}(\sqrt{d})$.

IV.4 Galois Representation

Consider an elliptic curve E/K, $K \subset \mathbb{C}$. Let $\sigma \in Gal(\bar{K}/K)$ be an element of the absolute Galois group. For each point $P \in E_{Tor}$, then σ acts on the coordinates of P. In particular, the group $E[n]$ is stable under the action of σ since:

$$0 = \sigma([n](P)) = [n]^\sigma(P^\sigma) = [n](P^\sigma) = 0 \iff P^\sigma \in E[n]$$

where we used the fact that σ commutes with the maps $[n] \in \mathbb{Z} \subset End(E)$, since they are defined over K. Moreover, like the endomorphisms, σ respects the addition law

$$\sigma(P_1 + P_2) = \sigma(P_1) + \sigma(P_2)$$

since $+ : E \to E$ is a rational map with coefficients in K, fixed by the automorphism. Then σ induces automorphisms of $E[m]$ and hence

$$\rho_m : Gal(\bar{K}/K) \to GL_2\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) \simeq Aut(E[m]).$$

As a result of what we have shown in the previous section, there exists a well-defined representation of groups from $Gal(\bar{K}/K)$ to $Aut(T_q(E))$, for any rational prime $q \in \mathbb{Z}$.

Definition IV.4.1. Let E/K, $K \subset \mathbb{C}$ be an elliptic curve and let $\sigma \in Gal(\bar{K}/K)$. Fix a rational prime q. Then the q-adic Galois representation is

$$\rho(\sigma) : Gal(\bar{K}/K) \to Aut(T_q(E)) \simeq GL_2(\mathbb{Z}_q).$$

Among all the finite extensions there are ones for which the representation ρ_m is more meaningful.

Proposition IV.4.2. *Let $L_m = K(E[m])$ be the field given by adjoining the coordinates of the m-torsion points for some $m \in \mathbb{N}$ and let $L_m^x = K(E[m]_x)$ and $L_m^y = K(E[m]_y)$ be the fields given by adjoining, respectively, only the x coordinate and the y coordinates of the m-torsion points:*

1. *L_m/K, L_m^x/K and L_m^y/K are Galois extensions*
2. *$Gal(L_m/K)$ is isomorphic to a subgroup of $GL_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$*

Proof.

1. Any $\sigma \in Gal(\bar{K}/K)$ fixes L_m, L_m^x, L_m^y since the action of σ on $E[m]$ sends m-torsion points to m-torsion points. This immediately implies that those extensions are Galois.
2. There is a representation $\rho_m : Gal(L_m/K) \to GL_2\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)$ and it is injective since $\rho_m(\sigma) = 1 \iff P^\sigma = P\ \forall P \in E[m] \iff \sigma$ fixes $L_m \iff \sigma = id$. □

However, a much stronger result holds for curves with complex multiplication by the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Theorem IV.4.3. *Let E/K be an elliptic curve defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and let $K = \mathbb{Q}(\sqrt{d})$. Consider $[\alpha] \in End(E)$, $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, and let $L_\alpha = K(E[\alpha])$ be the field obtained by adjoining the coordinates of the points in $E[\alpha] = \ker([\alpha])$. Then $Gal(L/K)$ is abelian and isomorphic to a subgroup of $\left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\alpha)}\right)^\times$.*

Proof. After an isomorphism, the complex torus associated with E is $T = \mathbb{C}/\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ since this has complex multiplication by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and all these tori are $\mathbb{C}$-isomorphic. This means that an endomorphism $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ of the associated lattice, such that $\ker(\beta) \supseteq \ker(\alpha)$, sends $\frac{\beta}{\alpha} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. This happens if and only if $\beta = \alpha b$ if and only if $\alpha \mid \beta$ by unique factorization. From this we obtain

$$End(E)\big|_{\ker(\alpha)} \simeq \frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\alpha)} \qquad |End(E)\big|_{\ker(\alpha)}| = |\ker(\alpha)|.$$

Then consider P_α the point corresponding to $\frac{1}{\alpha}$ in T. The elements of $End(E)\big|_{\ker(\alpha)}$ act freely on this point of $\ker(\alpha)$, which means that the orbit of $\frac{1}{\alpha}$ under the action of $End(E)\big|_{\ker(\alpha)}$ is $\ker(\alpha)$, hence the orbit of P_α under the action of $End(E)\big|_{\ker(\alpha)}$ is $E[\alpha]$. Now consider any $\sigma \in Gal(L_\alpha/K)$. Since it commutes with $End(E)$, due to the fact that it fixes K, it is completely determined by its action on the α-torsion point P_α. Thus, σ acts on $\ker(\alpha) \subset \Lambda$ as the multiplication by a complex number in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ hence $Gal(L_\alpha/K) \hookrightarrow (\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\alpha)})^\times$. In particular, $Gal(L_\alpha/K)$ is abelian. □

Remark IV.4.4. Since $Gal(L_\alpha/K)$ is abelian, the same holds for $Gal(L_\alpha^x/K)$ and $Gal(L_\alpha^y/K)$ and, moreover, they inject into $\left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\alpha)}\right)^\times$.

IV.5 Class Field Theory

Consider an elliptic curve E/K defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, with Weierstrass form $y^2 = f_1(x)$, and its reduction $\tilde{E}_\pi$, for a good prime π. It seems reasonable that there is a connection between the Galois group $Gal(L_\alpha/K)$ and the one of the reduction $Gal(L_{\tilde{\alpha}}/F_p^{d(\pi)})$ for $\pi \nmid \alpha$. In fact, both act as endomorphisms in $\ker(\alpha)$ so that they can be represented as a subgroup of $(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(\alpha)})^\times$. However, there is a remarkable difference. In a finite field the Frobenius endomorphism ϕ_π or its square ϕ_π^2, which generates the finite Galois group, lies in $End_\pi(E)$ and its action on the torsion points has been characterized, while in the characteristic zero case the endomorphisms and the elements of $Gal(L_\alpha/K)$ look different. However, there is a well-defined relationship.

Theorem IV.5.1. *Let E/K be an elliptic curve defined over $\mathbb{Z}$ with CM by $\mathcal{O}_K$ and fix an endomorphism $[\alpha] \in End(E)$. Consider the extension L_α/K given by adjoining the coordinates of the α-torsion points. Let $\mathfrak{p} \in I_K$, $\mathfrak{p} \nmid (\alpha\Delta(E))$, be a prime, let $(p) = \mathbb{Z} \cap \mathfrak{p}$ and let $\mathfrak{P}$ be a prime of $\mathcal{O}_{L_\alpha}$, the ring of integers of the extension, such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then there is an element $\sigma_\mathfrak{p} \in Gal(L_\alpha/K)$ such that the following diagram commutes.*

$$\begin{tikzcd}
E[\alpha] \arrow[r, "\sigma_\mathfrak{p}"] \arrow[d] & E[\alpha] \arrow[d] \\
\tilde{E}[\alpha] \arrow[r, "\phi_\mathfrak{p}"] & \tilde{E}[\alpha]
\end{tikzcd}$$

where $\phi_\mathfrak{p} = \phi_p^{d_\mathfrak{p}}$ is a power of the Frobenius automorphism and where the vertical lines are the reduction modulo $\mathfrak{P}$. Such an element $\sigma_\mathfrak{p}$ is called the Frobenius element.

See [Lan94, Chapter I] for a treatment of the algebraic prerequisites and the existence of the Frobenius element, see [Sil91, §II.3] for another overview of the theory of this section.

For any extension L_α/K we can construct a function defined on the primes $\mathfrak{p}$, coprime to $(\alpha\Delta(E))$, as

$$(\mathfrak{p}, L_\alpha/K) = \sigma_\mathfrak{p}.$$

Then, extending the map by linearity, we obtain a map of $I(\alpha\Delta(E))$, the ideals coprime to $(\alpha\Delta(E))$:

$$(\cdot, L_\alpha/K) : I(\alpha\Delta(E)) \to Gal(L_{\alpha/K}),$$

$$(\mathfrak{a}, L_\alpha/K) = \left(\prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}, L/K\right) = \prod_\mathfrak{p} \sigma_\mathfrak{p}^{n_\mathfrak{p}}.$$

This is the *Artin Map* of L_α/K. Then the following theorem on the behavior of this map, which we will state for the abelian extensions L_α/K but holds in a more general form for any finite abelian extension M/N, provides important global information.

Theorem IV.5.2 (Artin reciprocity). *Fix $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Then there exists an ideal $\mathfrak{c} \in I_K$, divisible exactly by the primes that divide $(\alpha\Delta(E))$, such that:*

$$((a), L_\alpha/K) = 1 \qquad \textit{for all } a \equiv 1 \mod \mathfrak{c}.$$

The largest ideal $\mathfrak{c}$ for which the law holds is called the conductor of the extension L_α/K.

We can restate the law in an equivalent way

$$((a), L_\alpha/K) = ((b), L_\alpha/K) \qquad \text{for all } a \equiv b \mod \mathfrak{c}.$$

These results will be crucial to establish the regularity of a map we will meet in the following section, naturally associated to a CM elliptic curve.

Chapter V

Local Results and the Local Zeta Function

V.1 Weil Conjectures

Consider an elliptic curve $E/\mathbb{Q}$ with a Weierstrass equation with coefficients in $\mathbb{Z}$ and fix a prime $p \in \mathbb{N}$. Then the reduction $\tilde{E}_p$ is a cubic curve, not necessarily an elliptic curve, and we can count the number of $\mathbb{F}_{p^n}$-rational points it has. Before doing that, we shall deal with the problem of choosing the right model for $E/\mathbb{Q}$, i.e. the right Weierstrass equation. In fact, there could be a $\mathbb{Q}$-isomorphism that sends our curve to $E'/\mathbb{Q}$ in Weierstrass form with coefficients in $\mathbb{Z}$ with good reduction over the prime q, where $E/\mathbb{Q}$ had bad reduction. To account for this possibility, we require $p^{12} \nmid \Delta(E)$, for any prime $p \neq 2, 3$, while for the primes $p = 2, 3$ we require $p^4 \nmid A$ and $p^6 \nmid B$. We show now that for our curves that's not a restriction.

Proposition V.1.1. *Let E/K be a CM curve with Weierstrass equation given by $y^2 = x^3 + Ax + B$, defined over $\mathbb{Z}$. If $p \neq 2, 3$ is a prime such that $p^{12} \mid \Delta(E)$ then there exists a curve E'/K which is $\mathbb{Q}$-isomorphic to E which has integral Weierstrass equation and such that $\frac{\Delta(E)}{\Delta(E')} = p^{12}$.*

Proof. We recall that for a CM curve, the j-invariant is integral. As a consequence, if $p \neq 2, 3$ and $p \mid \Delta(E)$ then the relation

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)}$$

implies $p^4 \mid A$. Therefore, since $\Delta(E) = -16(4A^3 + 27B^2)$, we necessarily have $p^6 \mid B$. As a result, the $\mathbb{Q}$-isomorphism of elliptic curves $\phi : E \to E'$ is the following:

$$\phi : (x, y) \to \left(\frac{x}{p^2}, \frac{y}{p^3}\right)$$

and the equation of E' is $y^2 = x^3 + \frac{A}{p^4}x + \frac{B}{p^6}$. □

Remark V.1.2. The model of E/K such that $p^{12} \nmid \Delta(E)$, $p \neq 2, 3$, is a minimal Weierstrass model in the sense that we cannot find a $\mathbb{Q}$-isomorphic elliptic curve E'/K with coefficients in $\mathbb{Z}$, even not in Weierstrass form, such that if $p \mid \Delta(E)$, $p \neq 2, 3$, then E' has good reduction over p. In general, there exists a *minimal model* E^m/K in generalized Weierstrass form which has minimal discriminant, in the sense that for any prime p and any other model E''/K with equation defined over $\mathbb{Z}$ if E^m/K has bad reduction over p then the same holds for E''/K.

Now, we introduce the following formal series.

Definition V.1.3 (Local Zeta Function)**.** Let $E/\mathbb{Z}$ be an elliptic curve with coefficients in $\mathbb{Z}$. Then the local zeta function $Z(E, p) \in \mathbb{Q}[[T]]$ is

$$Z(E, p) = \exp\left(\frac{\#\tilde{E}_p[\mathbb{F}_p]}{1}T + \frac{\#\tilde{E}_p[\mathbb{F}_{p^2}]}{2}T^2 + \dots\right) = \exp\left(\sum_{n=1}^{\infty} \frac{\#\tilde{E}_p[\mathbb{F}_{p^n}]}{n}T^n\right)$$

where $\exp(T) = \sum_{n=0}^{\infty} \frac{T^n}{n!} \in \mathbb{Q}[[T]]$.

Although using the exponential in the generating function may seem unnatural, the Weil conjectures for elliptic curves, proven by Hasse in 1934, show that this is the correct way to represent local information.

Theorem V.1.4 (Weil Conjectures for Elliptic Curves)**.** *Let $p \in \mathbb{N}$ be a prime of good reduction. Then:*

1. $Z(E,p) = \frac{P(T)}{(1-T)(1-pT)}$ *with* $P(T) \in \mathbb{Z}[T]$ *a polynomial of degree 2.*
2. $P(T) = (1-\alpha T)(1-\bar{\alpha}T)$ *with* $\|\alpha\|^2 = p$.

We will reduce our arguments to the CM curves we studied since, with the theory we have developed, the proof is easier and the results are stronger. We will treat separately the case in which p ramifies, since we do not know yet whether it is a prime of good reduction or not.

Proof. Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and defined over $\mathbb{Z}$. Essentially, we will determine $\#\tilde{E}_p[\mathbb{F}_{p^n}]$ for any $n \geq 1$. First, consider the way p splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. If $(p) = (\pi)(\bar{\pi})$ splits, where $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a prime, then canonically $\tilde{E}_\pi \simeq \tilde{E}_p$. On the contrary, if p is inert, then the reductions of E/K, $K = \mathbb{Q}(\sqrt{d})$, and of $E/\mathbb{Q}$ are naturally isomorphic over $\mathbb{F}_{p^2}$. Moreover, since the equation of the reduced curve is in both cases in $\mathbb{F}_p$ those reductions are also isomorphic over $\mathbb{F}_p$. Therefore, it is enough to count the $\mathbb{F}_{p^n}$-rational points of a good reduction of E/K over a prime $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

In these cases, considering the Frobenius automorphism ϕ_p, we notice

$$x \in \mathbb{F}_p^n \iff \phi_p^n(x) = x \iff (\phi_p^n - 1)(x) = 0.$$

So that the associated Frobenius endomorphism $\phi_p \in End(\tilde{E}_\pi)$ respects the following:

$$P \in \tilde{E}_\pi[\mathbb{F}_{p^n}] \iff (\phi_p^n - id)(P) = 0 \iff P \in \ker(\phi_p^n - [1]).$$

So, first of all, we have to evaluate $\deg(\phi_p^n - id)$.

1. Case p splits. We know that $\phi_p \in End_\pi(E)$ corresponds to $[\alpha\pi] \in End_\pi(E)$ for some invertible $[\alpha] \in End_\pi(E)$, $\alpha \in (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$. First, we prove that $\phi_p^n - 1$ is separable. In fact $(\alpha\pi)^n - 1 \equiv -1 \mod \pi$ and by unique factorization of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ this means $\alpha\pi \nmid (\alpha\pi)^n - 1$. As a consequence $[\alpha\pi] = \phi_p \nmid \phi_p^n - 1$. Now, the order of $\tilde{E}_\pi[\mathbb{F}_{p^n}]$ is:

$$\#\ker(\phi_p^n - 1) = \deg(\phi_p^n - 1) = \|(\alpha\pi)^n - 1\|^2 = p^n + 1 - (\alpha\pi)^n - (\bar{\alpha}\bar{\pi})^n.$$

2. Case p is inert. For the $\mathbb{F}_{p^{2n}}$ rational points $\phi_p^{2n} - 1 = (-[p])^n - [1]$. Therefore, $\deg((-[p])^n - [1]) = ((-p)^n - 1)^2$ and since $p \nmid \deg(\phi_p^{2n} - 1)$ we deduce that $\phi_p^{2n} - 1$ is separable and that

$$\#\ker(\phi_p^{2n} - 1) = \deg(\phi_p^{2n} - 1) = ((-p)^n - 1)^2.$$

   To obtain $\deg(\phi_p^{2n+1} - 1)$ we consider the endomorphism $[\sqrt{d}]$. Then we recall $[\sqrt{d}]\phi_p = -\phi_p[\sqrt{d}]$, since the frobenius automorphism acts as the reduction of the complex conjugation $\sigma \in Gal(K/\mathbb{Q})$ on the coefficients of $[\sqrt{d}]$. As a result:

$$(\phi_p^{2n+1} - [1])[\sqrt{d}] = [\sqrt{d}](-\phi_p^{2n+1} - [1]).$$

Considering the degrees, this implies

$$\deg(\phi_p^{2n+1}-[1])\deg([\sqrt{d}]) = \deg([\sqrt{d}])\deg(-\phi_p^{2n+1}-[1])$$

and simplifying by the degree of $[\sqrt{d}]$

$$\deg(\phi_p^{2n+1}-[1]) = \deg(\phi_p^{2n+1}+[1]).$$

As a consequence, we obtain the degree of $\phi_p^{2n+1}-[1]$:

$$\begin{aligned}(\deg(\phi_p^{2n+1}-[1]))^2 &= \deg((\phi_p^{2n+1}-[1])(\phi_p^{2n+1}+[1]))\\ &= \deg([-p^{2n+1}]-[1])\\ &= (p^{2n+1}+1)^2.\end{aligned}$$

From this we conclude that

$$\deg(\phi_p^{2n+1}-1) = p^{2n+1}+1.$$

As a result $\#\tilde{E}_p[\mathbb{F}_{p^n}] = 1+p^n-(i\sqrt{p})^n-(-i\sqrt{p})^n$.

Now, we shall use some properties of the formal series; in particular, if we define $\ln(1-aT) = -\sum_{n=1}^{\infty}\frac{a^nT^n}{n}$, we have the following formal properties:

1. $\exp(bT+cT) = \exp(bT)\exp(cT)$
2. $\exp(-T) = (\exp(T))^{-1}$
3. $\exp(\ln(1-aT)) = 1-aT$.

Now, consider $a = \alpha\pi$ in the split case and $a = i\sqrt{p}$ in the inert case, then

$$Z(E,p) = \exp\left(\sum_{n=1}^{\infty}\frac{1^n-a^n-\bar{a}^n+p^n}{n}T^n\right) =$$

$$= \exp(-\ln(1-T)-\ln(1-pT)+\ln(1-aT)+\ln(1-\bar{a}T)) = \frac{(1-aT)(1-\bar{a}T)}{(1-T)(1-pT)}$$

□

To be sure that we have treated all the cases of good reduction, we shall deal with the reduction by the ramified prime.

Proposition V.1.5. *Let E/K, $K=\mathbb{Q}(\sqrt{d})$ be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ defined over $\mathbb{Z}$, for a prime d, hence $d \neq -1$. Recall that (d) is the ramified prime. Then $d \mid \Delta(E)$, in particular $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta(E)})$.*

Proof. We consider the curve in Weierstrass form $y^2 = x^3+Ax+B$, $A, B \in \mathbb{Z}$. We recall that $\Delta(E) = 16\Delta(x^3+Ax+B)$. Let L be the field generated by the roots of the polynomial x^3+Ax+B and consider the Galois group

$$Gal(L_2/K) = Gal(K(E[2])/K) = Gal(L_2^x/K) = Gal(L/K) \hookrightarrow \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{(2)}\right)^{\times}.$$

Then, if 2 splits, $Gal(L_2/K)$ is necessarily trivial, while if 2 is inert it is isomorphic to C_3, the cyclic group with three elements, or it is trivial. In both cases $Gal(L/K)$, as a subgroup of S_3, the group of the permutations of the three roots of the polynomial, is contained in A_3 and by Galois theory this happens if and only if the number $\sqrt{\Delta(x^3+Ax+B)} \in K$. Thus, if we show that $\Delta(x^3+Ax+B)$ is not a perfect square in $\mathbb{Q}$, then $[\mathbb{Q}(\sqrt{\Delta(E)}) : \mathbb{Q}] = 2$ and $\mathbb{Q}(\sqrt{\Delta(E)}) \subseteq K$, which means that the field $\mathbb{Q}(\sqrt{\Delta(E)}) = K$ and that $\Delta(E) = 16\Delta(x^3+Ax+B) = dn^2$ for some $n \in \mathbb{Z}$. To do this, we need to find the right primes and, to ensure that they exist, we need the following lemma.

Lemma V.1.6. *There exist infinite rational primes $p \in \mathbb{N}$ such that $p \equiv 1 \mod 4$ and (p) is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, where $d \neq -1$.*

Proof. This is a quick corollary of the infinitude of primes in arithmetic progressions. But we can prove the result in a more elementary way. By Theorem IV.1.7 p splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$ and $\left(\frac{p}{D_K}\right) = -1$, since it is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Therefore, we have to prove that there are infinite primes of the form x^2+y^2 such that $\left(\frac{x^2+y^2}{D_K}\right) = -1$. Equivalently, we can prove that there exist infinite coprime numbers of the form $n = x^2+y^2$ such that $\left(\frac{x^2+y^2}{D_K}\right) = -1$. In fact, any such number can be written as

$$n = \prod_{q\equiv 3 \mod 4} q^{2n_q} \prod_{p\equiv 1 \mod 4} p^{n_p},$$

which means there exists a prime $p|n$, $p \equiv 1 \mod 4$, such that $\left(\frac{p}{D_K}\right) = -1$. It is not difficult to show that there exists a solution $n_1 = a^2+b^2$ such that $\left(\frac{x^2+y^2}{D_K}\right) = -1$, $D_K \neq 4$. From this solution, we can build an infinite sequence of numbers

$$n_{i+1} = n_i^2 a_i^2 + b_i^2$$

such that $n_i a_i \equiv a \mod D_K$, while $b_i \equiv b \mod D_K$ is coprime to $n_i a_i$. Then the number $n_j = x^2+y^2$, furthermore $n_j \equiv n \mod D_K$ so that $\left(\frac{n_j}{D_K}\right) = -1$ and finally $gcd(n_j, n_k) = 1$ for any $j > k > 0$. □

Now consider an inert prime $p \nmid \Delta(E)$, $p \neq 2, 3$, and require $p \equiv 1 \mod 4$. If $\Delta(E)$ were a perfect square, then its reduction modulo π would also be a perfect square in $\mathbb{F}_p \subset \mathbb{F}_{p^2}$, this implies

$$Gal(\mathbb{F}_p(\tilde{E}_\pi[2])/\mathbb{F}_p) \hookrightarrow A_3 \simeq C_3$$

for the same argument as above. Next, consider the action of the Frobenius endomorphism ϕ_p on $E[2]$: we know that ϕ_p fixes $\deg(\phi_p - 1) = p+1$ points. By the restrictions on p we obtain $p+1 \equiv 2 \mod 4$ hence $4 \nmid p+1$ but $2 \mid p+1$ which means that ϕ_p fixes a proper 2-torsion point, while it necessarily permutes the other 2. Therefore, the order of $\phi_p \in Gal(\mathbb{F}_p(\tilde{E}_\pi[2])/\mathbb{F}_p)$ is 2 but C_3 has no elements of such an order. This is a contradiction. As a result, $\Delta(E)$ is not a square, hence $\mathbb{Q}(\Delta(E)) = K$, which implies $d \mid \Delta(E)$ and $\Delta(E) = dn^2$. □

Remark V.1.7. As for the elliptic curves with CM by $\mathbb{Z}[i]$ and defined over $\mathbb{Z}$ we already know that the prime $2 \mid \Delta(E)$, hence the ramified prime is of bad reduction.

Thus, given a CM elliptic curve $Z(E,p)$ has an additional structure that can be summarized by the following result.

Corollary V.1.8. *Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ defined over $\mathbb{Z}$ and let $\mathfrak{p} = (\pi)$, $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, be a prime of good reduction. Define the function $\alpha : I_K(\Delta(E)) \to K^\times$ as*

$$\alpha_{(\pi)} = \chi_\pi \pi \qquad \textit{such that } [\chi_\pi \pi] = \phi_{\mathfrak{p}} \in End_\pi(E)$$

and extended by linearity to the other ideals. Then the function is well defined and $\chi_\pi \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$. Furthermore, the local zeta function has the form:

$$Z(E,p) = \frac{\prod_{\mathfrak{p}|(p)}(1-\alpha_{\mathfrak{p}} T^{d_{\mathfrak{p}}})}{(1-T)(1-pT)}.$$

Proof. The well definition relies on the fact that given any generator π_1, π_2 of the ideal $\mathfrak{p}$, the reduced curves $\tilde{E}_{\pi_1} \simeq \tilde{E}_{\pi_2}$ are obviously the same curve, since the reduction is made over the same prime ideal $(\pi_1) = (\pi_2)$. This means that $\phi_{\mathfrak{p}}$ does not depend on the generator of the prime ideal.

For the second part, we consider two cases. If p splits, considering the $\mathbb{F}_{p^n}$-rational points, we have $\deg(\phi_p^n - 1) = p^n + 1 + a^n + \bar{a}^n$, where the endomorphism $[a] = [\chi_\pi \pi] = \phi_{\mathfrak{p}} \in End_\pi(E)$, $\chi_\pi \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$. Then $\frac{(1-aT)(1-\bar{a}T)}{(1-T)(1-pT)}$. Conversely, if p is inert, $a = (i\sqrt{p})$ which implies that $\frac{(1-aT)(1-\bar{a}T)}{(1-T)(1-pT)} = \frac{(1+pT^2)}{(1-T)(1-pT)}$ and we conclude since $\phi_{\mathfrak{p}} = \phi_p^2 = [-p]$ and $d_{\mathfrak{p}} = 2$. □

V.2 Bad Reduction

We have treated all the cases where the reduction is well defined; however, a priori, information about the curve is given also by the reduced curves over the primes of bad reduction. We distinguish three behaviors, considering $p \neq 2, 3$ and $p|\Delta(E)$

1. Additive reduction: $\tilde{E}_p$ has a cusp. This happens if and only if $\tilde{c_4} = 0$. Then the equation of the curve is $y^2 = x^3$.

2. Split multiplicative reduction: $\tilde{E}_p$ has a node, with the tangents to the singular point defined in $\mathbb{P}^2(\mathbb{F}_p)$.

3. Non-Split multiplicative reduction: $\tilde{E}_p$ has a node, with the tangents to the singular point not defined in $\mathbb{P}^2(\mathbb{F}_p)$.

In our case, we are interested in the first one: we calculate $\#\tilde{E}_p[\mathbb{F}_p^n]$. The curve $X_2 X_1^2 = X_0^3$ is parametrized by

$$\bar{\phi} : [\alpha : \beta] \mapsto [\alpha^2\beta : \alpha^3 : \beta^3],$$

which induces the affine parametrization

$$\phi : t \mapsto (t^2, t^3).$$

In any case the parametrization is injective and surjective, which means that over $\mathbb{F}_{p^n}$ there are p^n affine points in our curve plus the point $[0:1:0]$. As a consequence

$$\#\tilde{E}_p[\mathbb{F}_{p^n}] = p^n + 1,$$

hence we have proved the following.

Proposition V.2.1. *If E has additive reduction over $p \mid \Delta(E)$, $p \neq 2,3$, then*

$$Z(E,p) = \frac{1}{(1-T)(1-pT)}$$

Proof. Simply, $\#\tilde{E}_p[\mathbb{F}_{p^n}] = p^n + 1 = p^n + a^n + \bar{a}^n + 1$, with $a = 0$. Hence, the local zeta function is $Z(E,p) = \frac{(1-aT)(1-\bar{a}T)}{(1-T)(1-pT)} = \frac{1}{(1-T)(1-pT)}$. □

Remark V.2.2. The numerator of the local zeta function is called the *local factor*. For the three cases of poor reduction, the local factor is equal to:

$$\text{Local Factor} \begin{cases} 1 & \text{additive reduction} \\ 1-T & \text{split multiplicative reduction} \\ 1+T & \text{non-split multiplicative reduction} \end{cases}$$

Returning to the elliptic curves E/K with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ defined over $\mathbb{Z}$ we find the following remarkable property.

Theorem V.2.3. *Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ defined over $\mathbb{Z}$ and let $p \mid \Delta(E)$, be a prime different from $2,3$. Then E has additive reduction at p.*

Proof. Here we use the fact that $j(E)$ is an algebraic integer. In our special case, we know $j(E) \in \mathbb{Q}$ therefore $j(E)$ is an integer, so consider a prime p as in the hypothesis and recall the relation

$$j(E) = -12^3 \frac{(4A)^3}{\Delta(E)}.$$

Since $p \nmid 2,3$ and $j(E)$ is an integer, then necessarily $p|A$, therefore the reduction modulo p has $\tilde{c_4} = 0$, which means that the reduction is additive. □

Corollary V.2.4. *The local zeta function of the reduced curve $\tilde{E}_p$ over primes of bad reduction, different from $2,3$, of an elliptic curve E/K, defined over $\mathbb{Z}$, with complex multiplication by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is*

$$Z(E,p) = \frac{1}{(1-T)(1-qT)}.$$

Remark V.2.5. From these considerations, it seems reasonable to extend the function $\alpha : \mathcal{I}_K(\Delta(E)) \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ by requiring that

$$\alpha_{(\pi)} = 0,$$

for any $(\pi) \mid (\Delta(E))$. In particular $\chi_{\pi'} = 0$ for any generator π' of (π). Thanks to this argument, we can extend $\alpha : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Thus, we still have the relation

$$Z(E,p) = \frac{\prod_{(\pi)|(p)}(1 - \alpha_{(\pi)} T^{d_{(\pi)}})}{(1-T)(1-pT)}$$

for any prime $p \neq 2,3$.

After having treated the bad reduction case, we can state another important result that will be useful later.

Theorem V.2.6 (Hasse bound)**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ over $K = \mathbb{Q}(\sqrt{d})$ and let $p \neq 2, 3$ be a prime, $q = p^n$. Then:*

$$|\#\tilde{E}_p[\mathbb{F}_q] - q - 1| \leq 2\sqrt{q}.$$

Proof. $\#\tilde{E}_p[\mathbb{F}_q] = q + 1 + a^n + \bar{a}^n$ with $\|a\|^n = (\sqrt{p})^n = \sqrt{q}$ then

$$|\#\tilde{E}_p[\mathbb{F}_q] - q - 1| = |a^n + \bar{a}^n| \leq \|a\|^n + \|\bar{a}\|^n = 2\sqrt{q}$$

by triangle inequality. □

Remark V.2.7. For the primes 2 and 3, we define $\alpha_{(2)} = 0$ and if $3 \mid \Delta(E)$ we define $\alpha_{(3)} = 0$. This is an artificial correction of our function and we will see later how another definition will actually arise naturally in the last chapter.

V.3 Complex Multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

In order to make concrete examples of the theory we have developed so far we are going to obtain the local zeta functions for the elliptic curve $E/\mathbb{Q}$ defined over $\mathbb{Z}$ with CM by $Z[i]$ and $Z[\omega] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, $\omega = \frac{-1+\sqrt{-3}}{2}$.

Proposition V.3.1. *All elliptic curves E/K defined over $\mathbb{Z}$ with CM by $Z[i]$ have the following Weierstrass form*

$$G^n : \ y^2 = x^3 - nx^2 \quad n \in \mathbb{Z}^*,$$

while the ones with CM by $\mathbb{Z}[\omega]$ have the following Weierstrass form

$$E^n : \ y^2 = x^3 + n \quad n \in \mathbb{Z}^*.$$

Proof. All the curves of the first form are the only curves with j-invariant $j(G^n) = 0$ and Weierstrass equation defined over $\mathbb{Z}$, while the curves of the second form are the only ones with j-invariant $j(E^n) = 1728$ and with Weierstrass equation defined over $\mathbb{Z}$. In particular E^n are all isomorphic over $\bar{\mathbb{Q}}$ and the same holds for the curves G^n. So, if we show that even one curve of the first form has CM by $Z[i]$ and one of the second form has CM by $Z[\omega]$, we obtain the result, but recall that we have already shown such examples at the beginning of Chapter IV. □

Remark V.3.2. The condition $n^{12} \nmid \Delta(E)$ we imposed in the previous section is equivalent to the following restriction on $n \in \mathbb{Z}$:

1. G^n with $b^4 \nmid n$ for any prime $b \in \mathbb{Z}$,

2. E^n with $b^6 \nmid n$ for any prime $b \in \mathbb{Z}$.

First, we express G^n in a more convenient way.

Proposition V.3.3. *Consider the smooth curves $F^n : \ u^2 = v^4 + 4n$ and let $p \nmid 2n$. Then:*

$$\#\tilde{G}^n_p[\mathbb{F}_{p^m}] = \#\tilde{F}^n_p[\mathbb{F}_{p^m}] + 2.$$

Proof. We can write the maps $(u,v) \mapsto (\frac{1}{2}(u+v^2), \frac{1}{2}v(u+v^2))$ and its inverse $(x,y) \mapsto (2x - \frac{y^2}{x^2}, \frac{y}{x})$ from $\tilde{G}_p^n \setminus \{(0,0)\}$ to $\tilde{F}_p^n$. Finally, since there are no points at infinity in F^n, we also have to add the point at infinity of G^n. From this we conclude. □

We have reduced the problem to counting the $\mathbb{F}_p$-rational points of a *diagonal hypersurface*, hence a hypersurface in which any variable appears alone and in at most one monomial in the equation that defines the variety. For such curves the theory of Gauss and Jacobi sums reveals to be a useful tool.

Definition V.3.4. Let $\mathbb{F}_q$ be a finite field. Consider a nontrivial additive character $\psi : \mathbb{F}_q \to \mathbb{C}^*$ and let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^*$ be a a multiplicative character. Then the *Gauss sum* is defined as follows:

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x),$$

where $\chi(0) = 0$ by convention. The *Jacobi sum* is the following:

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

From now on we will fix $\psi(x) = \xi^{\mathrm{Tr}(x)}$ where $\xi = e^{\frac{2\pi i}{p}}$ and $\mathrm{Tr}(x)$ is the trace of the field extension $\mathbb{F}_q/\mathbb{F}_p$.

These sums share notable identities:

Proposition V.3.5. *Let χ, χ_1, χ_2 be nontrivial multiplicative characters. Then:*

1. $g(\chi_{triv}) = -1$; $\quad J(\chi_{triv}, \chi_{triv}) = q-2$; $\quad J(\chi_{triv}, \chi) = -1$;
   $J(\chi, \bar{\chi}) = -\chi(-1)$; $\quad J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$
2. $g(\chi)g(\bar{\chi}) = \chi(-1)q$; $\quad |g(\chi)| = \sqrt{q}$
3. $J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$ *if* $\chi_2 \neq \bar{\chi}_1$

Proof. We omit the proof of the first identities since they follow by a simple application of the definition. We prove the second and third ones:

$$\begin{aligned} g(\chi)g(\bar{\chi}) &= \sum_{x,y \in \mathbb{F}_q} \chi(x)\bar{\chi}(y)\psi(x+y) = \sum_{x,u \in \mathbb{F}_q} \chi(x)\bar{\chi}(u-x)\psi(u) = \\ &= \left(\sum_{x \in \mathbb{F}_q^*} \bar{\chi}(-1)\right) + \left(\sum_{x \in \mathbb{F}_q, u \in \mathbb{F}_q^*} \chi(x)\bar{\chi}(u-x)\psi(u)\right) = \\ &= (q-1)\bar{\chi}(-1) + \sum_{v \in \mathbb{F}_q, u \in \mathbb{F}_q^*} \chi(vu)\bar{\chi}(u-vu)\psi(u) = \\ &= (q-1)\chi(-1) + J(\chi, \bar{\chi}) \left(\sum_{u \in \mathbb{F}_q^*} \psi(u)\right) = q\chi(-1) \end{aligned}$$

and since $\overline{g(\chi)} = \bar{\chi}(-1)g(\bar{\chi})$ we conclude. As for the third identity:

$$\begin{aligned} g(\chi_1)g(\chi_2) &= \sum_{x,y\in\mathbb{F}_q} \chi_1(x)\chi_2(y)\psi(x+y) = \sum_{x,u\in\mathbb{F}_q} \chi_1(x)\chi_2(u-x)\psi(u) = \\ &= \sum_{x\in\mathbb{F}_q, u\in\mathbb{F}_q^*} \chi_1(x)\chi_2(u-x)\psi(u) = \sum_{v\in\mathbb{F}_q, u\in\mathbb{F}_q^*} \chi_1(uv)\chi_2(u-uv)\psi(u) = \\ &= \left(\sum_{u\in\mathbb{F}_q} \chi_1(u)\chi_2(u)\psi(u)\right)\left(\sum_{v\in\mathbb{F}_q} \chi_1(v)\chi_2(1-v)\right) = g(\chi_1\chi_2)J(\chi_1,\chi_2). \end{aligned}$$

□

The link between multiplicative characters and the number of $\mathbb{F}_q$-rational points of a diagonal hypersurface is given by the following result.

Theorem V.3.6. *Let $a \in \mathbb{F}_q^\times$ and consider $m \in \mathbb{N}$ such that $m \mid |F_q^\times| = q-1$. Then:*

$$\#\{x^m = a\} = \sum_{\chi^m=1} \chi(a).$$

Proof. Since x^m is a homomorphism, if a is a m^{th} power, then the number of solutions of $\#\{x^m = a\} = \frac{q-1}{m}$ while if a is not a m^{th} power, $\#\{x^m = a\} = 0$. First, we will prove that the group $\widehat{\mathbb{F}_q^\times}$ of multiplicative characters of $\mathbb{F}_q^\times$ is itself cyclic of order $q-1$. Fixing a generator g of $\mathbb{F}_q^\times$, any character $\chi \in \widehat{\mathbb{F}_q^\times}$ will be completely defined by its action on g. Now, let $\zeta_{q-1} \in \mathbb{C}$ be a primitive $(q-1)^{th}$ root of unity and consider the multiplicative character $\chi : g \mapsto \zeta_{q-1}$. We show that $\widehat{\mathbb{F}_q^\times} = \langle\chi\rangle$. Obviously $\langle\chi\rangle \subset \widehat{\mathbb{F}_q^\times}$, while the other inclusion follows by the first isomorphism theorem: we know that the image of a multiplicative character has order that divides $q-1$, so it maps g to a $(q-1)^{th}$ root of unity ζ_{q-1}^n for some $n \in \mathbb{Z}$. As a result, the order of the subgroup of the characters of order m is $\frac{q-1}{m}$. As a consequence, if $a \in \mathbb{F}_q$ is a m^{th} power, then $\sum_{\chi^m=1} \chi(a) = \sum_{\chi^m=1} 1 = \frac{q-1}{m}$.

For the second part, consider the group of the characters $\widehat{\widehat{\mathbb{F}_q^\times}}$ of $\widehat{\mathbb{F}_q^\times}$. We have a canonical isomorphism with $\mathbb{F}_q^\times$:

$$a \mapsto ev_a : \chi \mapsto \chi(a).$$

This means that if $\{\chi^m = 1\} \subseteq ker(ev_a)$ then ev_a is an m^{th} power and also a is an m^{th} power. Thanks to this argument, we conclude that if a is not a m^{th} power, there exists $\chi_1 \in \widehat{\mathbb{F}_q^\times}$ such that $\chi_1^m = 1$ and $\chi_1(a) \neq 1$, which implies that:

$$\sum_{\chi^m=1} \chi(a) = \sum_{\chi'^m=1} (\chi'\chi_1)(a) = \chi_1(a) \sum_{\chi'^m=1} \chi'(a) \iff \sum_{\chi^m=1} \chi(a) = 0$$

since $\{\chi^m = 1\}$ is a subgroup of $\widehat{\mathbb{F}_q^\times}$. □

Next, we proceed to the computation of the number of the $\mathbb{F}_p$ rational points.

Theorem V.3.7. *Let (π) be a prime of $\mathbb{Z}[i]$ and $(\pi) \nmid 2n$, consider $q = \left|\frac{\mathbb{Z}[i]}{(\pi)}\right| = \mathbb{N}(\pi)$ and let $(p) = \mathbb{Z} \cap (\pi)$ be a rational prime:*

$$\#\tilde{G}^n_\pi[\mathbb{F}_q] = q + 1 - \overline{\left(\frac{n}{\pi}\right)_4} \pi - \left(\frac{n}{\pi}\right)_4 \bar{\pi} \qquad \pi \equiv 1 \mod (1+i)^3$$

where $\left(\frac{n}{\pi}\right)_4 = i^j \in \mathbb{Z}[i]$ such that $n^{\frac{q-1}{4}} \equiv i^j \mod \pi$.
Let (π) be a prime of $\mathbb{Z}[\omega]$ and $(\pi) \nmid 6n$, consider $q = |\frac{\mathbb{Z}[\omega]}{(\pi)}|$ and let $(p) = \mathbb{Z} \cap (\pi)$ be a rational prime:

$$\#\tilde{E}^n_\pi[\mathbb{F}_p] = q + 1 - \overline{\left(\frac{4n}{\pi}\right)_6} \pi - \left(\frac{4n}{\pi}\right)_6 \bar{\pi} \qquad \pi \equiv 2 \mod 3$$

where $\left(\frac{n}{\pi}\right)_6 = (-\omega)^j \in \mathbb{Z}[\omega]$ such that $n^{\frac{q-1}{6}} \equiv (-\omega)^j \mod \pi$.

Remark V.3.8. We notice that if (π) is a prime of $\mathbb{Z}[i]$ then necessarily $q \equiv 1 \mod 4$. Conversely, if (π) is a prime of $\mathbb{Z}[\omega]$ then necessarily $q \equiv 1 \mod 6$.

Remark V.3.9. The condition $\pi \equiv 1 \mod (1+i)^3$ uniquely determines the generator of (π), in fact $\left(\frac{\mathbb{Z}[i]}{(1+i)^3}\right)^\times$ has $8 - 4 = 4$ elements. Then, since the units of $\mathbb{Z}[i]$ are i^j, hence four, and are not equivalent modulo $(1+i)^3$, we conclude $i^j\pi$, which are the four different generators of (π), are neither equivalent modulo $(1+i)^3$ nor congruent to 0. Thus, the condition uniquely determines the generator. The same holds for the condition $\pi \equiv 1 \mod 3$ that uniquely determines the generator of (π), in fact $\left(\frac{\mathbb{Z}[\omega]}{(\sqrt{3})^2}\right)^\times$ has only $9 - 3 = 6$ elements. Then, since the units of $\mathbb{Z}[\omega]$ are $(-\omega)^j$, hence six, and are not equivalent modulo 3, we conclude that the numbers $(-\omega)^j\pi$, which are the six different generators of (π), are neither equivalent modulo 3 nor congruent to 0. We call such generators *primary*.

Proof. First of all let's consider the following multiplicative characters.

1. If $q \equiv 1 \mod 4$ then $\chi_4(x) = \left(\frac{x}{\pi}\right)_4$ is a generator of the characters of order 4 of $\frac{\mathbb{Z}[i]}{(\pi)} \simeq \mathbb{F}_q$.
2. If $q \equiv 1 \mod 3$ then $\chi_6(x) = \left(\frac{x}{\pi}\right)_6$ is a generator of the characters of order 6 of $\frac{\mathbb{Z}[\omega]}{(\pi)} \simeq \mathbb{F}_q$.

Let's start with G^n. We know that it is a question of computing $N' = \#\tilde{F}^n_\pi[\mathbb{F}_q]$:

$$\begin{aligned} N' = \#\{u \in \mathbb{F}_q \mid u^2 = 4n\} + \#\{v \in \mathbb{F}_q \mid v^4 = -4n\} \\ + \#\{u, v \in \mathbb{F}_q^* \mid u^2 = v^4 + 4n\} \end{aligned} \tag{V.1}$$

The first term is equal to :

$$\#\{u \in \mathbb{F}_q \mid u^2 = 4n\} = 1 + \chi_4^2(4n) \tag{V.2}$$

since χ_4^2 is of order 2. The second term is equal to:

$$\#\{v \in \mathbb{F}_q \mid v^4 = -4n\} = \sum_{i=0}^{3} \chi_4^i(-4n). \tag{V.3}$$

Now let's work on the third term.

$$\#\{u, v \in \mathbb{F}_q^* \mid u^2 = v^4 + 4n\} = \sum_{a,b\in\mathbb{F}_q^*,\ a=b+4n} \#\{u^2 = a\} \cdot \#\{v^4 = b\} =$$

$$\sum_{\substack{a\in\mathbb{F}_q^* \\ a-4n\neq 0}} \sum_{\substack{j=0,\,1,\,2,\,3 \\ k=0,\,2}} \chi_4^k(a)\chi_4^j(a-4n) = \sum_{x\in\mathbb{F}_q^*,} \sum_{\substack{j=0,\,1,\,2,\,3 \\ k=0,\,2}} \chi_4^{j+k}(-4n)J(\chi_4^k, \chi_4^j) =$$

$$q-2-\left(\sum_{j=1}^{3}\chi_4^j(-4n)\right)-\chi_4^2(-4n)-\chi_4^2(-1)+\chi_4(-4n)^3J(\chi_4^2,\chi_4)+\chi_4(-4n)J(\chi_4^2,\chi_4^3)$$

$$= q-3+\left(\sum_{j=1}^{3}\chi_4^j(-4n)\right)-\chi_4^2(-4n)-a-\bar{a} \qquad a = -\chi_4(-4n)^3J(\chi_4^2,\chi_4) \quad \text{(V.4)}$$

Here, we simplified the expression using the Jacobi sum identities and using the fact $\chi_4^2(-1) = 1$. Now, putting together the three expressions and simplifying, we end up with:

$$N' = q-3+\chi_4^0(-4n)+1+\chi_4^2(4n)-\chi_4^2(-4n)-a-\bar{a} = q-1-a-\bar{a}. \quad \text{(V.5)}$$

Which means:

$$\#\tilde{E}_\pi[\mathbb{F}_q] = N'+2 = q+1-a-\bar{a} \qquad a \in \mathbb{Z}[i], \quad \text{(V.6)}$$

$$|a| = |-\chi_4(-4n)^3J(\chi_4^2,\chi_4)| = \frac{|g(\chi_2)||g(\chi_4^3)|}{|g(\chi)|} = \sqrt{q}. \quad \text{(V.7)}$$

Next, we have to characterize the behavior of $J(\chi_4^2, \chi_4)$.

Lemma V.3.10. *Consider* $\chi_4(x) = \left(\frac{x}{\pi}\right)_4$ *as a character of* $\frac{\mathbb{Z}[i]}{(\pi)} \simeq \mathbb{F}_q$*. Then:*

1. $1 + J(\chi_4^2, \chi_4) \equiv 0 \mod 2+2i$
2. $(J(\chi_4^2, \chi_4)) = (\pi)$ *as ideals of* $\mathbb{Z}[i]$.

Proof. (1). First, we relate $J(\chi_4^2, \chi_4)$ to $J(\chi_4, \chi_4)$ using the following identity, whose proof can be found in [IR90, Lemma §17.3].

$$J(\chi_2, \chi) = \chi(4)J(\chi, \chi)$$

where $\chi_2 = \chi_4^2$ is the only nontrivial character of order 2. If we apply the identity to our case, we notice that $-4 = (1+i)^4$ is a 4^{th} power in $\frac{\mathbb{Z}[i]}{(\pi)}$ then we obtain $J(\chi_2, \chi_4) = \chi_4(-1)J(\chi_4, \chi_4)$. Next we write:

$$J(\chi_4, \chi_4) = \sum_{x\in\mathbb{F}_q} \chi_4(x)\chi_4(1-x) = \chi_4^2\left(\frac{q+1}{2}\right) + 2\sum_{S\subset\mathbb{F}_q} \chi_4(x)\chi_4(1-x)$$

where the second sum is over $\frac{q-3}{2}$ elements, one for each pair $(x, 1-x)$ except for the pair $(\frac{q+1}{2}, \frac{q+1}{2})$. Now, since $\chi_4(x) = i^j \in \mathbb{Z}[i]$ we have that $\chi_4(x) \equiv 1 \mod 1+i$, hence $2\chi(x)\chi(1-x) \equiv 2 \mod 2+2i$. This means that reducing modulo $2+2i$

$$J(\chi_4, \chi_4) \equiv q-3+\chi_4^2\left(\frac{q+1}{2}\right) \equiv 2+\chi_4^2(2) \equiv 2+\chi_4(4) \equiv 2+\chi_4(-1) \mod 2+2i$$

since $q-1 \equiv 1 \mod 4$. Then we conclude that

$$1 + J(\chi_2, \chi_4) = 1 + \chi_4(-1)J(\chi_4, \chi_4) \equiv 2 + 2\chi_4(-1) \equiv 0 \mod 2+2i$$

since $2(1+\chi_4(-1)) = 0$ or 4.

(2). We simply use the definition of $\chi_4(x) = \left(\frac{x}{\pi}\right)$ and we prove the relation $J(\chi_4^2, \chi_4) \equiv 0 \mod \pi$.

$$\begin{aligned} J(\chi_4^2, \chi_4) &\equiv \sum_{x\in\mathbb{F}_q} x^{\frac{q-1}{4}}(1-x)^{\frac{q-1}{4}} \equiv \sum_{x\in\mathbb{F}_q}\sum_{j=0}^{\frac{q-1}{4}} \binom{\frac{q-1}{4}}{j} x^{\frac{q-1}{4}}(-x)^j \equiv \\ &\equiv \sum_{j=0}^{\frac{q-1}{4}} (-1)^j \sum_{x\in\mathbb{F}_q} x^{\frac{q-1}{2}+j} \equiv \sum_{j=0}^{\frac{q-1}{4}} (-1)^j \cdot 0 \mod \pi \end{aligned}$$

since $1 \le \frac{q-1}{4} + j \le q-1$, hence the map $\phi_j : x \mapsto x^{\frac{q-1}{2}+j}$ is multiplicative and nontrivial which means:

$$\sum_{x\in\mathbb{F}_q} \phi_j(x) = \phi_j(a) \sum_{y\in\mathbb{F}_q} \phi_j(y) \quad y = \frac{x}{a} \quad \phi_j(a) \neq 0, 1.$$

If the sum were nonzero, then we could cancel both terms and end up with:

$$\phi_j(a) = 1.$$

A contradiction. □

The lemma proves that

$$a = \chi_4(-4n)^3(-J(\chi_4^2, \chi_4)) = \overline{\chi_4(n)}\pi = \overline{\left(\frac{n}{\pi}\right)_4}\pi \qquad \pi \equiv 1 \mod 2+2i.$$

This settles the first part of Theorem 5.2.7.

The proof of the second part is similar to the first one. To ease the notation, let $1 + N' = \tilde{E}_\pi^n[\mathbb{F}_q]$. Then

$$\begin{gathered} N' = \#\{y \in \mathbb{F}_q \mid y^2 = n\} + \#\{x \in \mathbb{F}_q \mid x^3 = -n\} \\ + \#\{x, y \in \mathbb{F}_q^* \mid y^2 = x^3 + n\}. \end{gathered} \tag{V.8}$$

Now, by defining $\chi_2 = \chi_6^3$ and $\chi_3 = \chi_6^2$ as multiplicative characters of exact order, respectively, 2 and 3. The first term is equal to

$$\#\{y \in \mathbb{F}_q \mid y^2 = n\} = 1 + \chi_2(n). \tag{V.9}$$

The second term is equal to

$$\#\{x \in \mathbb{F}_q \mid x^3 = -n\} = 1 + \chi_3(-n) + \chi_3^2(-n). \tag{V.10}$$

The third term then is equal to

$$\#\{x,y\in\mathbb{F}_q^*\mid y^2=x^3+n\}=\sum_{a,b\in\mathbb{F}_q^*,\ b=a-n}\#\{x\in\mathbb{F}_q^*\mid x^2=a\}\cdot\#\{y\in\mathbb{F}_q^*\mid y^3=b\}=$$

$$=\sum_{a\in\mathbb{F}_q^*,\ a-n\neq0}\ \sum_{\substack{i=0,1\\ j=0,1,2}}\chi_2^i(a)\chi_3^j(a-n)=\sum_{\substack{i=0,1\\ j=0,1,2}}\chi_2^i(n)\chi_3^j(-n)J(\chi_2,\chi_3)=$$

$$q-2-\left(\sum_{j=1,2}\chi_3^j(-n)\right)-\chi_2(n)+\chi_2(n)\chi_3(-n)J(\chi_2,\chi_3)+\chi_2(n)\chi_3^2(-n)J(\chi_2,\chi_3^2)=$$

$$=q-2-\left(\sum_{j=1,2}\chi_3^j(-n)\right)-\chi_2(n)-a-\bar{a}\qquad a=-\chi_2(n)\chi_3(n)J(\chi_2,\chi_3)\quad\text{(V.11)}$$

Again, we simplified the equation using the Jacobi sum identities. Summing the three terms and simplifying, we obtain the following:

$$\#\tilde{E}_\pi[\mathbb{F}_q]=N'+1=q-2+1+1-a-\bar{a}+1=q+1-a-\bar{a}\quad\text{(V.12)}$$

$$a=-\chi_2(n)\chi_3(n)J(\chi_2,\chi_3)\qquad |a|=\frac{|g(\chi_2)||g(\chi_3)|}{|g(\chi_2\chi_3)|}=\sqrt{q}.\quad\text{(V.13)}$$

Here we used the fact that $\chi_3(-1)=1$ since $\bar{\chi_3}(-1)=\chi_3^2(-1)=\chi_3((-1)^2)=1$.

Finally, we characterize the structure of $J(\chi_2,\chi_3)$. However, it turns out that $J(\chi_3,\chi_3)$ is simpler to study, where the link between the two Jacobi sums is given by the previous identity $J(\chi_3,\chi_3)=\chi_3(4)J(\chi_2,\chi_3)$.

Lemma V.3.11. *Consider* $\chi_6(x)=\left(\frac{x}{\pi}\right)_6$ *as a character of* $\frac{\mathbb{Z}[i]}{(\pi)}\simeq\mathbb{F}_q$. *Then:*

1. $J(\chi_3,\chi_3)\equiv 2\mod 3$,

2. $(J(\chi_3,\chi_3))=(\pi)$ *as ideals of* $\mathbb{Z}[\omega]$.

Proof. (1). By unwinding the definition of Jacobi sum, we obtain the following.

$$J(\chi_3,\chi_3)=\frac{g(\chi_3)^2}{g(\bar{\chi}_3)}=\frac{g(\chi_3)^3}{\chi_3(-1)q}\equiv g(\chi_3)^3\mod 3\equiv\sum_{x\in\mathbb{F}_q}\chi_3(x)^3\psi(3x)\mod 3$$

$$\equiv\sum_{y\in\mathbb{F}_q^*}\psi(y)\mod 3\equiv g(\chi_{triv})\mod 3\equiv -1\mod 3.$$

Here we used the fact that $q\equiv 1\mod 3$ and the Gauss and Jacobi sum identities.

(2). For G^n we have to use the definition of χ_3 to prove $J(\chi_3,\chi_3)\equiv 0\mod\pi$:

$$J(\chi_3,\chi_3)\equiv\sum_{x\in\mathbb{F}_q}x^{\frac{q-1}{3}}(1-x)^{\frac{q-1}{3}}\mod\pi\equiv\sum_{x\in\mathbb{F}_q}\sum_{j=0}^{\frac{q-1}{3}}\binom{\frac{q-1}{3}}{j}x^{\frac{q-1}{3}}(-x)^j\mod\pi$$

$$\equiv\sum_{j=0}^{\frac{q-1}{3}}(-1)^j\binom{\frac{q-1}{3}}{j}\sum_{x\in\mathbb{F}_q}x^{\frac{q-1}{3}+j}\mod\pi\equiv\sum_{j=0}^{\frac{q-1}{3}}(-1)^j\cdot 0\mod\pi\equiv 0\mod\pi$$

Where we used the fact that $\phi_j : x \mapsto x^{\frac{q-1}{3}+j}$ is multiplicative and nontrivial since $1 < \frac{q-1}{3} + j < q - 1$ which means

$$\sum_{x \in \mathbb{F}_q} \phi_j(x) = \phi_j(a) \sum_{y \in \mathbb{F}_q} \phi_j(y) \quad y = \frac{x}{a} \quad \phi_j(a) \neq 0, 1.$$

Then if the sum were nonzero we could cancel both terms and end up with

$$\phi_j(a) = 1,$$

a contradiction. □

Thanks to this lemma we proved:

$$a = -\chi_2(n)\chi_3(n)J(\chi_2, \chi_3) = -\chi_6^5(n)\chi_3(4)J(\chi_3, \chi_3) =$$
$$-\bar{\chi}_6(4n)\bar{\chi}_2(4)\pi = -\bar{\chi}_6(4n)\pi = -\overline{\left(\frac{4n}{\pi}\right)_6}\pi.$$

Where $\pi \equiv 2 \mod 3$ is our primary generator of (π). □

Remark V.3.12. Recalling the definition of $\alpha_{(\pi)}$ we have that for G^n:

$$\alpha_{(\pi)} = \overline{\left(\frac{n}{\pi}\right)_4}\pi \qquad \pi \equiv 1 \mod 2 + 2i.$$

Moreover for E^n:

$$\alpha_{(\pi)} = -\overline{\left(\frac{4n}{\pi}\right)_6}\pi \qquad \pi \equiv 2 \mod 3.$$

In fact, let $q = \mathbb{N}(\pi)$. Then, unwinding the definition, $\alpha_{(\pi)} = a$, such that the number of $\mathbb{F}_q$-rational points $\#\tilde{E}^n_\pi[\mathbb{F}_q] = q + 1 - a - \bar{a}$ and $(a) = (\pi)$.

Remark V.3.13. The choice of the condition that defines the primary primes is not random and is determined by the existence of reciprocities, similar to the quadratic one, for $\left(\frac{n}{\pi}\right)_4$ and $\left(\frac{4n}{\pi}\right)_6$ that have a simpler structure if π is primary.

Chapter VI

Global Results and the Hasse-Weil L-function

VI.1 Global Zeta Function

So far we have studied the elliptic curves E/K defined over $\mathbb{Z}$ with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, the ring of integers of an imaginary quadratic extension of class number one. In the third and fourth chapters we studied the ring of the endomorphisms of those curves and those of their good reduction. This led us in the previous chapter to the proof of the Weil conjectures for such elliptic curves and the determination of the local Zeta functions and of the local factors. We now combine these local functions to construct a global complex-valued zeta function.

Definition VI.1.1 (Hasse-Weil L-function - First definition)**.** Let E/K be a CM elliptic curve defined over $\mathbb{Z}$ and recall that the local zeta function is:

$$Z(E,p)(T) = \frac{(1-a_pT)(1-\bar{a}_pT)}{(1-T)(1-pT)}.$$

Then consider a complex variable s and define

$$\begin{aligned} L(E,s) &= \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E,p)(p^{-s})} \\ &= \prod_p \frac{1}{(1-a_pp^{-s})(1-\bar{a}_pp^{-s})} \qquad\qquad \text{(VI.1)} \\ &= \prod_{\mathfrak{p}} \frac{1}{1-\alpha_{\mathfrak{p}}(\mathbb{N}\mathfrak{p})^{-s}} \qquad \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \end{aligned}$$

the *Hasse-Weil L-function* of E/K.

Remark VI.1.2. The reason why we multiply by $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ is to clear the denominator of the local zeta functions, which is independent of the curve and therefore does not carry additional information.

The function $L(E,s)$ is defined on the complex values of the variable s for which the infinite product converges. In particular, for the standard criterion for the absolute convergence of an infinite product, we have to evaluate the convergence of

$$\sum_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|(\mathbb{N}\mathfrak{p})^{-\mathfrak{Re}(s)} = \sum_{\mathfrak{p}} (\mathbb{N}\mathfrak{p})^{-\mathfrak{Re}(s)+\frac{1}{2}} \leq 2\sum_{p\in\mathbb{N}} p^{-\mathfrak{Re}(s)+\frac{1}{2}} \qquad \text{(VI.2)}$$

where we used the Hasse bound. Then VI.2 converges if and only if $\mathfrak{Re}(s) > \frac{3}{2}$. Thus, $L(E,s)$ is defined on the half-plane $\mathfrak{Re}(s) > \frac{3}{2}$.

Once we have established its domain of definition, we may consider an equivalent form, using the identity:

$$\frac{1}{1-\alpha_{\mathfrak{p}}(\mathbb{N}\mathfrak{p})^{-s}} = \sum_{n\in\mathbb{N}} \alpha_{\mathfrak{p}}^n(\mathbb{N}\mathfrak{p})^{-ns} = \sum_{n\in\mathbb{N}} \alpha_{\mathfrak{p}^n}(\mathbb{N}\mathfrak{p}^n)^{-s}$$

where we used the fact $\mathbb{N}I$ and $\alpha : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ are multiplicative. Now recall that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD, so any element $a \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is uniquely factorized by primes up to units. As a result, any ideal can be written as $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ with only finitely many nonzero exponents, and this expression is unique. From this argument and by the absolute convergence of both the sums and the product we conclude that

$$\prod_{\mathfrak{p}} \frac{1}{1-\alpha_{\mathfrak{p}}(\mathbb{N}\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \sum_{n\in\mathbb{N}} \alpha_{\mathfrak{p}^n}(\mathbb{N}\mathfrak{p}^n)^{-s} = \sum_{I} \alpha_I(\mathbb{N}I)^{-s} \qquad \mathfrak{Re}(s) > \frac{3}{2}$$

where the last sum is over all ideals $I \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Thus we showed

$$L(E,s) = \sum_{I} \alpha_I(\mathbb{N}I)^{-s} \qquad \mathfrak{Re}(s) > \frac{3}{2}.$$

We will call this expression the additive form of our L-function.

VI.2 Hecke Character

The additive form of our L-function seems at a first glance far from regular: even though the coefficients α_I are necessarily generators of the principal ideal $I = (\beta)$, so up to a unit $u_\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ we have $\alpha_{(\beta)} = u_\beta\beta$, we don't know if such units share some regularity themselves. However we know that by definition

$$\alpha_{\mathfrak{p}} = \chi_\pi\pi \qquad \text{such that } [\chi_\pi\pi] = \phi_{\mathfrak{p}} = \phi_p^{d_{\mathfrak{p}}} \in End_\pi(E)$$

for a prime $\mathfrak{p} = (\pi)$ coprime to $\Delta(E)$. Now fix some integer $m \geq 3$, $m \nmid \Delta(E)$ and consider the field extension $L_m/K = L(E[m]/K)$. We know by the theory of Section §IV.5 that there exists a Frobenius element $\sigma_{\mathfrak{p}} \in Gal(L(E[m]/K)$ such that $\widetilde{\sigma_{\mathfrak{p}}(P)} = \phi_{\mathfrak{p}}(\tilde{P})$ for any $P \in E[m]$ and for any $\mathfrak{p}$ coprime to $(m\Delta(E))$.

Proposition VI.2.1. *Let* $\mathfrak{p}$ *be coprime with* $(m\Delta(E))$*, then the Frobenius element* $\sigma_{\mathfrak{p}}$ *acts as* $[\alpha_{\mathfrak{p}}] \in End(E)$ *on the group* $E[m]$*.*

Proof. Consider the inverse $\sigma_{\mathfrak{p}}^{-1}$. Then for any $P \in E[m]$:

$$\sigma_{\mathfrak{p}}^{-1}\widetilde{([\alpha_{\mathfrak{p}}](P))} = \phi_{\mathfrak{p}}\big|_{L_{\tilde{m}}}^{-1}(\phi_{\mathfrak{p}}(\tilde{P})) = \tilde{P}$$

where $L_{\tilde{m}}$ is the extension of $\mathbb{F}_{p^{d_{\mathfrak{p}}}}$ obtained by adjoining the coordinates of the points of $\tilde{E}_{\mathfrak{p}}[\tilde{m}]$. Hence, necessarily $\sigma_{\mathfrak{p}}$ acts as $[\alpha_\pi]$ on $E[m]$. □

Then by Artin reciprocity:

$$a \equiv b \mod \mathfrak{c}_m \Rightarrow ((a), L_m/K) = ((b), L_m/K)$$

where $\mathfrak{c}_m$ is the conductor of the extension. The immediate consequence is that if $a, b \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and $a \equiv b \mod \mathfrak{c}_m$ then:

$$\alpha_{(a)} \equiv \alpha_{(b)} \mod \mathfrak{c}_m \iff \chi_a a \equiv \chi_b b \mod \mathfrak{c}_m \iff \chi_a \equiv \chi_b \mod \mathfrak{c}_m.$$

From this we conclude:

$$a \equiv b \mod \mathfrak{c}_m \Rightarrow \chi_a = \chi_b$$

since in $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_m}$ the units, which are at most six, are not equivalent because $\mathbb{N}\mathfrak{c}_m > 6$.

Next, changing the integer $m' \nmid \Delta(E)$ such that m and m' are coprime, we get another conductor $\mathfrak{c}_\alpha = \mathfrak{c}_{m'} + \mathfrak{c}_m$ divisible only by the primes that divide $\Delta(E)$. A function of I_K with this regularity is called *algebraic Hecke character.*

Definition VI.2.2. Let $K/\mathbb{Q}$ be an imaginary quadratic extension of class number one. Then a map $\psi_{\mathfrak{c}} : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ of modulus $\mathfrak{m} \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is an *algebraic Hecke character* if:

1. $\psi(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = 1$

2. $\psi(I) \neq 0$ if and only if I and $\mathfrak{m}$ are coprimes

3. $\psi(IJ) = \psi(I)\psi(J)$ for any $I, J \in \mathcal{I}_K$

4. for any $\sigma \in Gal(K/\mathbb{Q})$ there exists a number $n(\sigma) \in \mathbb{N}$ such that if the algebraic integer $\alpha \equiv 1 \mod \mathfrak{m}$ then $\psi((a)) = \prod_{\sigma \in Gal(K/\mathbb{Q})} a^{n(\sigma)}$

Then ψ is said to be primitive if there is no other smaller modulus $\mathfrak{m}'|\mathfrak{m}$ for which property (4) holds.

As a consequence of the Artin reciprocity, we derive the following crucial result.

Theorem VI.2.3. *The function $\alpha : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is an algebraic Hecke character of modulus $\mathfrak{c}_\alpha$, which is divisible by the primes that divide $\Delta(E)$.*

Proof. Simply, if $a \equiv 1 \mod \mathfrak{c}_\alpha$ then $\alpha_{(a)} = a$, so property (1) is valid. By definition, also property (2) and (3) hold. Property (4) holds if we consider $n(\sigma) = 0$, σ the restriction of the complex conjugation to K, while $n(id) = 1$. Finally, if a prime $\mathfrak{p} \mid \Delta(E)$ then the curve E/K in Weierstrass form has bad reduction, then the reduction is additive, which means $\alpha_{\mathfrak{p}} = 0$ so that $\mathfrak{p} \mid \mathfrak{c}_\alpha$. □

However, α with conductor $\mathfrak{c}_\alpha$ could be non-primitive, in particular the primes in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ that divide 2 and 3 can appear in $\Delta(E)$ in a fictitious way: there can be a $\mathbb{Q}$-isomorphism of elliptic curves that sends E/K to another elliptic curve with an equation with coefficients in $\mathbb{Z}$, not necessarily in Weierstrass form, such that it has good reduction over 2 or 3. To account for this possibility, we proceed in the following way.

1. We define $\mathfrak{c}_\psi \mid \mathfrak{c}_\alpha$ as the maximal integral ideal such that if $(x) \in I(\mathfrak{c}_\alpha)$, the ideals coprime to $\mathfrak{c}_\alpha$, and $x \equiv 1 \mod \mathfrak{c}_\psi$ then $\alpha_{(x)} = x$.

2. We extend our algebraic Hecke character by requiring some "continuity". This means that if $n \equiv m \mod \mathfrak{c}_\psi$ and $\alpha_{(m)} = 0$ while $\alpha_{(n)} = \chi_n n \neq 0$ then $\alpha_{(m)} = \chi_n m$.

3. Finally, by doing so, we can extend $\alpha : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ to a primitive Hecke character $\psi : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ of all the ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ with modulus $\mathfrak{c}_\psi$.

The following result tells us that it is the right way to extend α:

Theorem VI.2.4. *Let $\mathfrak{p}$ be the prime of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Then $\mathfrak{p} \mid \mathfrak{c}_\psi$ if and only if $\mathfrak{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a prime of bad reduction, in the sense that it is a prime of bad reduction for any $\mathbb{Q}$ isomorphic curve with an equation with integer coefficients. Moreover, for any prime $\mathfrak{p}$ of good reduction, $\mathbb{N}\mathfrak{p} = q$, we have $\#\tilde{E}_{\mathfrak{p}}[\mathbb{F}_{q^n}] = q + 1 - \bar{\psi}^n(\mathfrak{p}) - \psi^n(\mathfrak{p})$, where the reduction is done over a $\mathbb{Q}$-isomorphic curve with good reduction at $\mathfrak{p}$.*

Proof. For the first part see [Sil91, Theorem II.9.2b]. We just stress that we already know that if $\mathfrak{p} \mid \mathfrak{c}_\psi$ then necessarily $\mathfrak{p} \mid (\Delta(E))$.

For the second part we just notice that if $\mathfrak{p} \nmid (\Delta(E))$ then $\psi(\mathfrak{p}) = \alpha_\mathfrak{p}$. For the case $p = 2, 3$ see [Sil91, §II.10.1]. Moreover, the number of the reduced points do not depend on the choice of the $\mathbb{Q}$-isomorphic curve if it has good reduction over that prime. □

Remark VI.2.5. By the definition of α we notice $\overline{\psi((a))} = \psi((\bar{a}))$ which means $\mathfrak{c}_\psi = (c) = (\bar{c})$.

Then ψ is the factor such that:

$$Z(E,p) = \prod_{\mathfrak{p}|(p)} \frac{(1 - \psi(\mathfrak{p})T^{d_\mathfrak{p}})}{(1-T)(1-pT)}$$

for every prime $p \in \mathbb{N}$ for the minimal model of E/K.

The above proposition suggests that the right and more meaningful definition of our L-function is:

Definition VI.2.6 (Hasse Weil L-Function - Second definition)**.**

$$L(E,s) = \prod_{\mathfrak{p}} \frac{1}{(1 - \psi(\mathfrak{p})(\mathbb{N}\mathfrak{p})^{-s})} = \sum_{I \in \mathcal{I}_K} \psi(I)(\mathbb{N}I)^{-s}$$

We will call $\mathfrak{c}_\psi$ the *conductor* of $L(E,s)$.

All the properties of the first one transfer to the second one since they differ by a finite product of local zeta functions.

Example VI.2.7. Consider the elliptic curve E^{16} with CM by $\mathbb{Z}[\omega]$ and equation $y^2 = x^3 + 16$ in Weierstrass form. Then we know that in this case $\Delta(E) = -16^3 \cdot 27$, so the primes of bad reduction for this curve are 2 and 3. Furthermore, we know that

$$\alpha_{(\pi)} = -\left(\frac{4^3}{\pi}\right)_6 \pi \qquad \pi \equiv 2 \mod 3.$$

As a consequence, necessarily the conductor $\mathfrak{c}_\alpha$ is divided by 2 and 3. Now, let's define the multiplicative function $\chi_6 : \mathbb{Z}[\omega] \to \mathbb{C}$ such that:

$$\chi_6(\pi) = (-\omega)^j \qquad \text{such that } \pi \equiv (-\omega)^j \mod 3.$$

Then we can rewrite

$$\alpha_{(m)} = \left(\frac{4^3}{m}\right)_6 \bar{\chi}_6(m)m$$

for $(m) \in \mathcal{I}_K(6)$. We notice, moreover, that since $4^3 = 2^6$ is a 6^{th} power, then $\left(\frac{4^3}{m}\right)_6 = 1$, hence $\alpha_{(\pi)}$ is a non-primitive Hecke character of modulus $\mathfrak{c}_\alpha = (6)$. Then we can complete it to a primitive Hecke character $\psi : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ of modulus $\mathfrak{c}_\psi = (3)$ simply by defining

$$\psi((m)) = \bar{\chi}_6(m)m \qquad \chi_\psi = \bar{\chi}_6.$$

By the theorem above, there exists another curve which is $\mathbb{Q}$-isomorphic to E^{16} with an equation defined over $\mathbb{Z}$ such that it has good reduction over 2. In fact, consider the elliptic curve

$$E' : y^2 + y = x^3.$$

It is $\mathbb{Q}$-isomorphic to the curve E^{16} by the $\mathbb{Q}$-isomorphism

$$\phi : (x, y) \mapsto (2^2 x, 2^3 y + 2^2).$$

Next, reducing E'/K modulo the inert prime (2) and counting the number of $\mathbb{F}_q$ points, we obtain:

$$\#\tilde{E}_2'[\mathbb{F}_q] = \#\{y \in \mathbb{F}_q \mid y^2 + y = 0\} + \#\{x, y \in \mathbb{F}_q^* \mid y^2 + y = x^3\} + 1.$$

The first term is obviously equal to 2 while the second term can be evaluated with the theory of characters and is equal to:

$$\sum_{\substack{y \in \mathbb{F}_q \\ y^2+y \neq 0}} 1 + \chi_3(y^2 + y) + \bar{\chi}_3(y^2 + y) = q - 2 + \sum_{y \in \mathbb{F}_q} \chi_3(y)\chi_3(1 - y) + \bar{\chi}_3(y)\bar{\chi}_3(1 - y)$$

since $y^2 = -y^2$ if $char(F) = 2$. As before $\chi_3(\tilde{x}) = \left(\frac{x}{2}\right)_3$ where $x \equiv \tilde{x} \mod 2$. If we sum all the terms we get:

$$\begin{gathered}\#\tilde{E}_2'[\mathbb{F}_q] = q + 1 + \sum_{y \in \mathbb{F}_q} \chi_3(y)\chi_3(1 - y) + \bar{\chi}_3(y)\bar{\chi}_3(1 - y) = \\ q + 1 + J(\chi_3, \chi_3) + J(\bar{\chi}_3, \bar{\chi}_3) = q + 1 - (-\pi) - (-\bar{\pi})\end{gathered} \tag{VI.3}$$

where π is the unique generator of (2) such that $\pi \equiv 2 \mod 3$. Hence

$$\psi((2)) = -2 = \bar{\chi}_6(2)2.$$

Finally recall that the rings of integers we are considering are PID and have only a finite number of units, hence a finite number of distinct generators. Then we could transform the algebraic Hecke character into a multiplicative function of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $\chi_\psi : \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \to (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$, which is equal to:

$$\chi_\psi(a) = \begin{cases} \frac{a}{\psi_{(a)}} & \psi_{(a)} \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

such that $\psi_{(a)} = \chi_\psi(a)a$. This finally leads to the identity:

$$L(E, s) = \sum_{\mathcal{I}} \psi(I)(\mathbb{N}I)^{-s} = \frac{1}{w} \sum_{z \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}} \psi(z)(\mathbb{N}(z))^{-s} = \frac{1}{w} \sum_{z \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}} \chi_\psi(z) \frac{z}{\|z\|^{2s}}$$

where $w = |(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times|$ is the number of distinct generators of an ideal. We will use the last expression of $L(E, s)$ to derive its main analytical properties. However, before doing that, we shall study the function $\chi_\psi(z)$ more accurately.

Proposition VI.2.8. *The multiplicative function χ_ψ induces a primitive multiplicative character $\tilde{\chi}_\psi : \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_\psi}\right)^\times \to (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$ defined by*

$$\tilde{\chi}_\psi(x) = \chi_\psi(\bar{x}) \qquad \bar{x}\mathfrak{c}_\psi = x$$

Proof. Since χ_ψ is multiplicative, it is enough to show that the function is well defined. By definition, if $\bar{y} \equiv \bar{x} \mod \mathfrak{c}_\psi$ then $\chi_\psi(\bar{x}) = \chi_\psi(\bar{y})$, moreover $\chi_\psi(\bar{x}) = 0$ if and only if $\bar{x} \equiv 0 \mod \mathfrak{c}_\psi$. This shows that $\tilde{\chi}_\psi(x)$ is a multiplicative character of $\left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_\psi}\right)^\times$.

The fact that χ_ψ is primitive implies that $\tilde{\chi}_\psi$ is primitive. □

In the previous chapter we already met the multiplicative characters associated to the units of a quotient ring and it turned out that the theory of Gauss sums gave interesting insights. Here, we develop a similar theory which will help us later.

Definition VI.2.9 (Generalized Gauss Sum)**.** Let R be a number ring and consider an ideal I then define $\mathbb{N}I = \#(\frac{R}{I}) < \infty$. Let $\psi : \frac{R}{I} \to \mathbb{C}^*$ be an additive character nontrivial on any additive subgroup of the form $\frac{J}{I}$, for an ideal $J \supsetneq I$, and let $\chi : \left(\frac{R}{I}\right)^\times \to \mathbb{C}^*$ be a multiplicative character. Then we define the Gauss sum $g(\chi, \psi)$ in the following way.

$$g(\chi) = g(\chi, \psi) = \sum_{x \in \frac{R}{I}} \chi(x)\psi(x)$$

where $\chi(x) = 0$ if x is not invertible in $\frac{R}{I}$.

Proposition VI.2.10. *Consider R, ψ, I as before and let $\chi : \left(\frac{R}{I}\right)^\times \to \mathbb{C}^*$ be a primitive character. Then:*

1. *$\sum \chi(x)\psi(ax) = \bar{\chi}(a)g(\chi, \psi)$ for any $a \in \frac{R}{I}$,*
2. *$g(\chi)g(\bar{\chi}) = \chi(-1)\mathbb{N}I$ and $|g(\chi)| = \sqrt{\mathbb{N}I}$.*

Proof. (1). If $a \in \left(\frac{R}{I}\right)$, then the change of variables $y = ax$ proves the identity. On the contrary, if a is not a unit, we have to prove $g(\chi, \psi) = 0$. Consider the kernel $\ker(a)$ of the homomorphism of rings that maps $x \mapsto ax$, since a is not invertible and $\mathbb{N}I < \infty$ we conclude $\{0\} < ker(a) = \frac{J}{I} \leq \frac{R}{I}$. Then consider the subgroup J_1 of the elements of $\left(\frac{R}{I}\right)^\times$ congruent to 1 modulo $\frac{J}{I}$, hence, such that $ay = a$. By definition of primitive character, we see that χ is nontrivial over J_1. So, setting $n = \#J_1$ the sum is given by:

$$n \sum_{x \in \left(\frac{R}{I}\right)^\times} \chi(x)\psi(ax) = \sum_{x \in \left(\frac{R}{I}\right)^\times,\, u \in J_1} \chi(x)\psi(axu) = \sum_{u \in J_1} \bar{\chi}(u)g(\chi, \psi) = g(\chi, \psi) \cdot 0 = 0$$

since our character is nontrivial over J_1 and any u is invertible.

(2) Unwinding the definition we get

$$g(\chi)g(\bar{\chi}) = \sum_{x,y \in \frac{R}{I}} \chi(x)\bar{\chi}(y)\psi(x+y) = \sum_{x \in \left(\frac{R}{I}\right)^\times, u \in \frac{R}{I}} \chi(x)\bar{\chi}(ux)\psi(x(u+1)) =$$
$$= \sum_{x \in \left(\frac{R}{I}\right)^\times, u \in \frac{R}{I}} \bar{\chi}(u)\psi(x(u+1)).$$

If x is not invertible, we notice

$$\sum_{u \in \frac{R}{I}} \bar{\chi}(u)\psi(x(u+1)) = \psi(x) \sum_{u \in \frac{R}{I}} \bar{\chi}(u)\psi(xu) = \psi(x)\chi(x)g(\bar{\chi}, \psi) = 0.$$

Hence we can extend the previous sum to non-invertible x:

$$g(\chi)g(\bar{\chi}) = \sum_{x\in\frac{R}{I}, u\in\frac{R}{I}} \bar{\chi}(u)\psi(x(u+1)) = \sum_{u\in\frac{R}{I}} \bar{\chi}(u) \sum_{x\in\frac{R}{I}} \psi(x(u+1)) =$$

$$= \chi(-1)\mathbb{N}I + \sum_{u+1\in\left(\frac{R}{I}\right)^*} \bar{\chi}(u) \sum_{x\in\frac{R}{I}} \psi(x(u+1)) = \chi(-1)\mathbb{N}I + 0.$$

Here we used the fact that $\psi(x)$ is an additive character nontrivial in any $\frac{J}{I}$, with $J \supsetneq I$, hence $\psi(x(u+1))$ is a nontrivial additive character if $u \neq -1$. Moreover, we recall $\chi(-1) = \bar{\chi}(-1)$.

Finally, for any Gauss sum the following holds:

$$\overline{g(\chi, \psi)} = \bar{\chi}(-1)g(\bar{\chi}, \psi)$$

since we have that:

$$\sum_{x\in\frac{R}{I}} \bar{\chi}(x)\bar{\psi}(x) = \sum_{x\in\frac{R}{I}} \bar{\chi}(x)\psi(-x) = -\bar{\chi}(-1)g(\bar{\chi}, \psi).$$

Then

$$|g(\chi)|^2 = g(\chi)\overline{g(\chi)} = \bar{\chi}(-1)g(\chi)g(\bar{\chi}) = \mathbb{N}I.$$

□

VI.3 Determination of the Hecke Character

In this section we determine the Hecke characters for the elliptic curves we studied. We distinguish three cases.

Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. If $K = \mathbb{Q}(\sqrt{d})$ has class number one and $d \neq -1, -3$, then we know that $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times = \{1, -1\}$, by the theory of the automorphisms of the associated CM elliptic curves. Furthermore, let $\mathfrak{c}_\psi$ be the conductor of $L(E, s)$. The Hecke character $\psi : \mathcal{I}_K \to \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is completely determined by the associated multiplicative function $\chi_\psi : \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \to (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$. This function, in turn, is completely determined by the primitive multiplicative character $\tilde{\chi}_\psi : \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_\psi}\right)^\times \to (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$. Since $\left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_\psi}\right)^\times$ is a finite abelian group, that is, a finite product of cylic groups, the group of its multiplicative characters is isomorphic to the product of the groups of the multiplicative characters of the cyclic groups. Hence, there is only one primitive character of order 2, which is equal to 1 if $x \in \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{\mathfrak{c}_\psi}\right)^\times$ is a square.

As for the curves with CM by $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ the more concrete biquadratic and sextic reciprocity are the analog of Artin reciprocity for generic curves.

In the case of the elliptic curves defined over $\mathbb{Z}$ with CM by $\mathbb{Z}[i]$, which we called G^n/K in the previous section, the Hecke character $\alpha : I_K \to \mathbb{Z}[i]$ was defined in the following way:

$$\alpha_{(\pi)} = \overline{\left(\frac{n}{\pi}\right)_4}\pi \qquad \pi \equiv 1 \mod (1+i)^3.$$

Moreover, since $q^4 \nmid n$ for any prime q, we conclude that it is a primitive Hecke character, hence $\psi = \alpha$. We now state the biquadratic reciprocity to express the Hecke character in an alternative way.

Theorem VI.3.1 (Biquadratic reciprocity)**.** *Let $\pi = a + ib \in \mathbb{Z}[i]$ and the number $\ell = c + id \in \mathbb{Z}[i]$ be coprime primary elements. Then*

$$\begin{aligned}\left(\frac{\pi}{\ell}\right)_4 &= \left(\frac{\ell}{\pi}\right)_4 (-1)^{(\frac{\mathbb{N}\pi-1}{4})(\frac{\mathbb{N}\ell-1}{4})} \\ &= \left(\frac{\ell}{\pi}\right)_4 (-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}.\end{aligned} \tag{VI.4}$$

Moreover the following supplementary laws hold:

$$\left(\frac{i}{\pi}\right)_4 = i^{\frac{\mathbb{N}\pi-1}{4}} \tag{VI.5}$$

$$\left(\frac{i+1}{\pi}\right)_4 = i^{\frac{a-b-b^2-1}{4}}. \tag{VI.6}$$

Corollary VI.3.2. *Let $\pi = a + ib \in \mathbb{Z}[i]$ be a primary element. Then the following holds:*

$$\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{\mathbb{N}\pi-1}{4}} \tag{VI.7}$$

$$\left(\frac{2}{\pi}\right)_4 = i^{-\frac{b}{2}}. \tag{VI.8}$$

Moreover, they are characters of conductor, respectively, (4) *and* (8)*.*

See [IR90, §10.9] and [Lem00, Theorem 6.9] for a proof using Jacobi and Gauss sums.

Remark VI.3.3. If $\ell \in \mathbb{Z}$ is an odd primary integer, then necessarily $\ell \equiv 1 \mod 4$, hence $\mathbb{N}\ell - 1 = \ell^2 - 1 = (\ell-1)(\ell+1) \equiv 0 \mod 8$. As a consequence, the biquadratic reciprocity law becomes:

$$\left(\frac{\pi}{\ell}\right)_4 = \left(\frac{\ell}{\pi}\right)_4.$$

Now, consider the curve G^n/K, then $n = (-1)^e 2^t N$, where $0 \leq e \leq 1$ and $0 \leq t \leq 3$, such that N is odd and primary. As a consequence, we can rewrite ψ as:

$$\begin{aligned}\psi((\pi)) &= \overline{\left(\frac{n}{\pi}\right)_4}\pi \\ &= \overline{\left(\frac{-1}{\pi}\right)_4}^{e} \overline{\left(\frac{2}{\pi}\right)_4}^{t} \overline{\left(\frac{N}{\pi}\right)_4}\pi \\ &= (-1)^{e\frac{\mathbb{N}\pi-1}{4}}(-i)^{-t\frac{b}{2}}\overline{\left(\frac{\pi}{N}\right)_4}\pi.\end{aligned} \tag{VI.9}$$

This means that the conductor $\mathfrak{c}_\psi$ divides $(8N')$, where $(N') = \prod_{\mathfrak{p} \mid (N)} \mathfrak{p}$.

In the case of the elliptic curves E^n/K defined over $\mathbb{Z}$ with CM by $\mathbb{Z}[\omega]$, with $\omega = \frac{-1+\sqrt{-3}}{2}$, the Hecke character $\alpha : I_K \to \mathbb{Z}[i]$ was defined in the following way:

$$\alpha_{(\pi)} = -\overline{\left(\frac{4n}{\pi}\right)_6}\pi \qquad \pi \equiv 2 \mod 3.$$

Since $q^6 \nmid n$ for any prime q, we conclude that it is a primitive Hecke character if and only if $n \neq 16n'$, where n' is odd. Therefore, for a primary prime:

$$\psi((\pi)) = \begin{cases} -\overline{\left(\dfrac{4n}{\pi}\right)_6}\pi & n \neq 16n' \\ -\overline{\left(\dfrac{n'}{\pi}\right)_6}\pi & n = 16n'. \end{cases}$$

The cubic reciprocity plays the same role as the biquadratic reciprocity for the curves G^n. So we state it.

Theorem VI.3.4 (Cubic reciprocity)**.** *Let $\pi = a + ib \in \mathbb{Z}[\omega]$ and $\ell = c + id \in \mathbb{Z}[\omega]$ be coprime primary elements. Then*

$$\left(\frac{\pi}{\ell}\right)_3 = \left(\frac{\ell}{\pi}\right)_3. \tag{VI.10}$$

Moreover the following supplementary laws hold:

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{1+a+b}{3}} \tag{VI.11}$$

$$\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{\frac{-1-a}{3}}. \tag{VI.12}$$

Corollary VI.3.5. *Let $\pi = a + ib \in \mathbb{Z}[\omega]$ be a primary element. Then the following holds:*

$$\left(\frac{-1}{\pi}\right)_3 = 1 \tag{VI.13}$$

$$\left(\frac{3}{\pi}\right)_3 = \omega^{-\frac{b}{3}}. \tag{VI.14}$$

Moreover, the last one is a character of conductor (9).

The proofs of such results can be found in [IR90, §9.4, §18.7] .

Now let's rewrite the function $\overline{\left(\frac{x}{\pi}\right)_6}$ as $\left(\frac{x}{\pi}\right)_3 \left(\frac{x}{\pi}\right)_2$. We have already studied the first term of the product; now we will find a more familiar expression for the second term.

Lemma VI.3.6. *Suppose $\alpha \in \mathbb{Z}[\omega]$, $A \in \mathbb{Z}$, and $gcd(\alpha, 2A) = 1$. Then the character $\left(\frac{A}{\alpha}\right)_2 = \left(\frac{A}{\mathbb{N}\alpha}\right)$, the Jacobi symbol.*

Proof. See [IR90, Lemma 2, §18.7]. □

Remark VI.3.7. If $q \in \mathbb{Z}$ is a primary prime, then $\left(\frac{A}{q}\right)_2 = \left(\frac{A}{q^2}\right) = 1$.

As a result, we can use quadratic reciprocity.

Now, consider the curve E^n/K, then $n = (-1)^e 2^t 3^s N$, where $0 \leq e \leq 1$ and $0 \leq t, s \leq 5$, such that N is odd and primary. We treat the case $n \neq 16n'$, the other one is similar. As a consequence, we can rewrite ψ as:

$$\begin{aligned}\psi((\pi)) &= -\left(\frac{4n}{\pi}\right)_3\left(\frac{4n}{\pi}\right)_2\pi\\ &= -\left(\frac{\pi}{N}\right)_3\left(\frac{\pi}{2}\right)_3^{t+2}\left(\frac{3}{\pi}\right)_3^{s}\left(\frac{2}{\mathbb{N}\pi}\right)^{t}\left(\frac{-1}{\mathbb{N}\pi}\right)^{e}\left(\frac{\mathbb{N}\pi}{3^sN}\right)(-1)^{(\frac{\mathbb{N}\pi-1}{2})(\frac{3^sN-1}{2})}\pi\\ &= -\left(\frac{\pi}{2^{t+2}N}\right)_3\left(\frac{\mathbb{N}\pi}{3^sN}\right)\omega^{-s\frac{b}{3}}(-1)^{(\frac{\mathbb{N}\pi-1}{2})(\frac{3^sN-1+2e}{2})}(-1)^{t\frac{\mathbb{N}\pi^2-1}{8}}\pi.\end{aligned} \tag{VI.15}$$

Hence the conductor $\mathfrak{c}_\psi$ divides $(9\cdot 8N')$, where $(N')=\prod_{\mathfrak{p}\mid(N)}\mathfrak{p}$.

VI.4 Theta Series

Recall that the additive form of the L-function is

$$L(E,s)=\sum_{I\in\mathcal{I}_{\mathcal{K}}}\psi(I)(\mathbb{N}I)^{-s}=\sum_{z\in\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}\chi_\psi(z)\frac{z}{\|z\|^{2s}}.$$

We know that this expression converges only for $D=\mathfrak{Re}(z)>\frac{3}{2}$, moreover in this half-plane our function is holomorphic. It happens that if we find another holomorphic or meromorphic function $f(z)$, defined over a connected open set V, such that $f\big|_U=L(E,s)\big|_U$, for an open set $U\subseteq D\cap V$, then automatically we find that the function $f(z)$ is the only possible holomorphic (meromorphic) extension of $L(E,s)$ to V. This is the technique of analytic continuation. We will use this idea to extend the L-function to the whole complex plane. But first of all we shall find an alternative representation for the additive form of $L(E,s)$, and it turns out that the theory of integral transforms is the natural setting for such expressions.

Definition VI.4.1 (Mellin Transform)**.** Let $f(z):\mathbb{R}_{>0}\to\mathbb{C}$ be a continuous function. The *Mellin transform* $\mathcal{M}\{f\}$ is defined by

$$\mathcal{M}\{f\}(s)=\int_0^\infty f(t)t^s\frac{dt}{t}$$

for the values of s for which the above integral converges.

Example VI.4.2. Let $f(z)=e^{-z}$. Then its Mellin transform is

$$\Gamma(s)=\int_0^\infty e^{-t}t^s\frac{dt}{t} \tag{VI.16}$$

the Gamma function for $\mathfrak{Re}(s)>0$. From this definition it's not difficult to derive some properties. First

$$\Gamma(s+1)=s\Gamma(s). \tag{VI.17}$$

This functional equation provides a way to continue $\Gamma(s)$ analytically to a meromorphic function defined in the entire complex plane, except for simple poles on $s=0,\ -1,\ -2,\ -3,\ \ldots$. The second identity

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin(\pi s)} \tag{VI.18}$$

tells us with VI.17 that the reciprocal of the Gamma function is an entire function, hence holomorphic on the whole complex plane. For a proof of such identities, see [WW13].

Let's prove a simple property of the Mellin transform.

Proposition VI.4.3. *Let $f(z) : U \to \mathbb{C}$ be a continuous function, such that the mellin transform is defined for some $s \in \mathbb{C}$ and consider $a \in \mathbb{R}_{>0}$:*

$$\{f(az)\}(s) = a^{-s}\{f(z)\}(s)$$

Proof.

$$\int_0^\infty f(at)t^s \frac{dt}{t} = \int_0^\infty f(u)\frac{u}{a^s}\frac{du}{u} = a^{-s}\{f(z)\}(s)$$

□

Now the idea is to find a function whose Mellin transform is equal, up to an entire function, to the additive form of $L(E, s)$ for $\mathfrak{Re}(s) > \frac{3}{2}$ but which also converges in other regions of the complex plane. In order to find the right candidate, we also need some theory of Fourier transforms.

Definition VI.4.4 (Fourier Transform)**.** Let $\mathcal{S}$ be the space of rapidly decreasing C^∞ functions $f : \mathbb{R}^n \to \mathbb{C}$, such that $\lim_{|x|\to\infty} |x|^n f(x) = 0$ for any $n \in \mathbb{N}$. Then the Fourier transform of $f \in \mathcal{S}$ is the function $\hat{f}(y) : \mathbb{R}^n \to \mathbb{C}$ defined by

$$\mathcal{F}\{f\}(y) = \hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi x\cdot y} f(x)dx.$$

We notice that the above integral converges for any $y \in \mathbb{R}^n$ and $f \in \mathcal{S}$, hence the Fourier transform is well defined on all $\mathbb{R}^n$. Now, we list some basic properties of the Fourier transform, whose proof can be found in [WW13].

Proposition VI.4.5. *Let $f : \mathbb{R}^n \to \mathbb{C}$ and $g : \mathbb{R}^n \to \mathbb{C}$ be functions in $\mathcal{S}$ then:*

1. *If $a \in \mathbb{R}^n$ and $g(x) = f(x + a)$, then $\hat{g}(y) = e^{2\pi i a\cdot y}\hat{f}(y)$*
2. *If $a \in \mathbb{R}^n$ and $g(x) = e^{2\pi i a\cdot x} f(x)$, then $\hat{g}(y) = \hat{f}(y - a)$*
3. *If $b \in \mathbb{R}_{>0}$ and $g(x) = f(bx)$, then $\hat{g}(y) = b^{-n}\hat{f}(\frac{y}{b})$*
4. *Fix $w \in \mathbb{R}^n$ and let $w\cdot\frac{\partial}{\partial x} f = w_1\frac{\partial f}{\partial x_1} + \cdots + w_n\frac{\partial f}{\partial x_n}$. Then $\mathcal{F}(w\cdot\frac{\partial}{\partial x} f) = 2\pi i w\cdot x\hat{f}$.*

Now, we prove the following important identity.

Proposition VI.4.6. *If $f(x) = e^{-\pi x\cdot x}$, then $\hat{f} = f$.*

Proof. (1) Case n=1. Then we have the following.

$$\begin{aligned}\hat{f} &= \int_{\mathbb{R}} e^{-2\pi ixy-\pi x^2}dx = e^{i^2\pi y^2}\int_{\mathbb{R}} e^{-i^2\pi y^2-2\pi ixy-\pi x^2}dx \\ &= e^{-\pi y^2}\int_{\mathbb{R}} e^{-\pi(x+yi)^2}dx = e^{-\pi y^2}\int_{iy-\infty}^{iy+\infty} e^{-\pi u^2}du \\ &= e^{-\pi y^2}\int_{-\infty}^{+\infty} e^{-\pi u^2}du = e^{-\pi y^2}.\end{aligned}$$

In the last expression, we used the fact that the function $f(z)$ is holomorphic and that $f(x+a) \in \mathcal{S}$ for any $a \in \mathbb{C}$. Then the result follows by complex integration.

(2) General case.

$$\hat{f} = \int_{\mathbb{R}^n} e^{\sum_{i=1}^n -2\pi i x_i y_i - \pi x_i^2} dx = \prod_{i=1}^n \int_{\mathbb{R}} e^{-2\pi i x_i y_i - \pi x_i^2} dx_i = \prod_{i=0}^n e^{-\pi y_i^2} = e^{-\pi y \cdot y}.$$

□

For us, the crucial property of the Fourier transform is the following.

Proposition VI.4.7 (Poisson Summation Formula). *If $g \in \mathcal{S}$, then*

$$\sum_{m \in \mathbb{Z}^n} g(m) = \sum_{m \in \mathbb{Z}^n} \hat{g}(m)$$

Proof. (1) Case n=1. Consider the function $h(x) = \sum_{m \in \mathbb{Z}} g(m+x)$, it is periodic of period 1 and obviously belongs to $L^2[0,1]$ since $g \in \mathcal{S}$. As a consequence, we can write it as $h(z) = \sum_{n \in \mathbb{Z}} c_n e^{2\pi i n z}$, its Fourier series. The coefficients are given by the formula:

$$\begin{aligned} c_n &= \int_0^1 \sum_{m=-\infty}^{+\infty} g(x+m) e^{-2\pi i n} dx = \sum_{m=-\infty}^{+\infty} \int_0^1 g(x+m) e^{-2\pi i n} dx \\ &= \int_{-\infty}^{+\infty} g(x) e^{-2\pi i n} dx = \hat{g}(n). \end{aligned}$$

Where we used the fact that $g(x) \in \mathcal{S}$ to exchange the sum and the integral. Then we can rewrite our function as $h(x) = \sum_{m \in \mathbb{Z}} \hat{g}(m) e^{2\pi i m}$, as a result

$$g(0) = \sum_{m \in \mathbb{Z}} g(m) = \sum_{m \in \mathbb{Z}} \hat{g}(m).$$

(2) It's enough to repeat the first case one variable at a time until we end up with the result. □

Corollary VI.4.8. *Let $f : R^n \to \mathbb{C}$, $f \in \mathcal{S}$ and consider a lattice $\Lambda = M\mathbb{Z}^n$ with $M \in GL_n(\mathbb{R})$. Then:*

$$\sum_{m \in \Lambda} g(m) = \frac{1}{|\det M|} \sum_{m \in \Lambda'} \hat{g}(m)$$

where Λ' is the dual lattice given by the elements $x \in \mathbb{R}^n$ such that $x\Lambda \subseteq \mathbb{Z}^n$. The lattice satisfies the identity $\Lambda' = (M^{-1})^t \mathbb{Z}^n$.

Proof. Let $h(x) = f(Mx)$. Then:

$$\begin{aligned} \sum_{m \in \Lambda} f(m) &= \sum_{m \in \mathbb{Z}^n} h(m) = \sum_{m \in \mathbb{Z}^n} \hat{h}(m) \\ &= \sum_{m \in \mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi x \cdot m} f(Mx) dx \\ &= \sum_{m \in \mathbb{Z}^n} \frac{1}{|M|} \int_{\mathbb{R}^n} e^{-2\pi M^{-1} u \cdot m} f(u) du \\ &= \frac{1}{|M|} \sum_{m \in \mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi u \cdot (M^{-1})^t m} f(u) du \\ &= \frac{1}{|M|} \sum_{m \in (M^{-1})^t \mathbb{Z}^n} \hat{f}(m). \end{aligned}$$

Finally, we notice that if $x \cdot y = w \in \mathbb{Z}^n$, for any $x \in \Lambda$, then $Me_i \cdot y \in \mathbb{Z}$, for any element e_i of the standard base of $\mathbb{Z}^n$. As a consequence $y = M'v$, where $M'e_i = e_i^*$ is the orthogonal or dual basis of Me_i and $v \in \mathbb{Z}^n$. We know from theory that $M' = (M^{-1})^t$. As a consequence $\Lambda' = (M^{-1})^t\mathbb{Z}^n$. □

Now, we are ready to define the main objects of this chapter.

Definition VI.4.9 (Theta Series)**.** Fix $u \in \mathbb{R}^2$ such that $u \notin \mathbb{Z}^2$ and consider the fixed vector $w = (1, i) \in \mathbb{C}^2$. Then we define the theta series:

$$\theta_u(t) = \sum_{m\in\mathbb{Z}^2} (m+u) \cdot we^{-\pi t|m+u|^2} \tag{VI.19}$$

$$\theta^u(t) = \sum_{m\in\mathbb{Z}^2} m \cdot we^{2\pi i m\cdot u}e^{-\pi t|m+u|^2} \tag{VI.20}$$

for $t > 0$.

Proposition VI.4.10. *The theta series respect the following identity:*

$$\theta_u(t) = \frac{-i}{t^2}\theta^u\left(\frac{1}{t}\right).$$

Proof.

$$\sum_{m\in\mathbb{Z}^2} (m+u) \cdot we^{-\pi t|m+u|^2} = \sum_{m\in\mathbb{Z}^2} \mathcal{F}\{(y+u) \cdot we^{-\pi t|y+u|^2}\}(m) =$$

$$\sum_{m\in\mathbb{Z}^2} e^{2\pi i m\cdot u}\mathcal{F}\{y \cdot we^{-\pi t|y|^2}\}(m) = \sum_{m\in\mathbb{Z}^2} \frac{-1}{2\pi t}e^{2\pi i m\cdot u}\mathcal{F}\{w \cdot \frac{\partial e^{-\pi t|y|^2}}{\partial y}\}(m) =$$

$$\sum_{m\in\mathbb{Z}^2} \frac{-2\pi i}{2\pi t}e^{2\pi i m\cdot u}m \cdot w\mathcal{F}\{e^{-\pi t|y|^2}\}(m) = \sum_{m\in\mathbb{Z}^2} \frac{-i}{t^2}e^{2\pi i m\cdot u}m \cdot we^{-\pi\frac{|m|^2}{t}} = \frac{-i}{t^2}\theta^u\left(\frac{1}{t}\right)$$

□

Corollary VI.4.11. *There exist constants $C_1, C_2 > 0$ such that:*

1. $|\theta_u(t)| < e^{-C_1 t}$ *for $t \to +\infty$*
2. $|\theta_u(t)| < e^{-\frac{C_2}{t}}$ *for $t \to 0$.*

Proof. (1). Let $c = \min_{m\in\mathbb{Z}^2} |m+u|^2 > 0$ since $u \notin \mathbb{Z}^2$, $(0,0) \in \mathbb{Z}^2$ and the lattice $\mathbb{Z}^2$ is discrete. Then

$$|\theta_u(t)| \leq \sum_{m\in\mathbb{Z}^2} |(m+u) \cdot \omega|e^{-\pi t|m+u|^2} = e^{-\pi tc}\sum_{m\in\mathbb{Z}^2} |(m+u) \cdot \omega|e^{-\pi t(|m+u|^2-c)}.$$

The last sum obviously converges and is decreasing with respect to t, which means $|\theta_u(t)| \leq e^{-\pi ct}A$, for a positive constant A. So, taking, for example, $C_1 = \frac{c}{2}$ we obtain the result.

(2) We use the identity proved before to rewrite $\theta_u(t) = \frac{-i}{t^2}\theta^u\left(\frac{1}{t}\right)$. Consider $\epsilon = \min_{w\in\mathbb{Z}^2\setminus\{(0,0)\}} |w|^2 > 0$, since the lattice $\mathbb{Z}^2$ is discrete.

$$|\theta^u(t)| \leq \frac{1}{t^2}\sum_{m\in\mathbb{Z}^2} |m \cdot w|e^{-\frac{\pi}{t}|m|^2} = \frac{1}{t^2}e^{-\frac{\epsilon\pi}{t}}\sum_{m\in\mathbb{Z}^2} |m \cdot w|e^{-\frac{\pi}{t}(|m|^2-\epsilon)} < \frac{1}{t^2}e^{-\frac{\epsilon\pi}{t}}|\theta^u(1)|e^{\pi\epsilon}$$

for $t < 1$. Here we used the fact that the last sum is a strictly increasing function because the only term $m \in \mathbb{Z}^2$ such that $|m|^2 < \epsilon$ is $m = (0,0)$ and it vanishes since in the sum $m \cdot w = 0$. Therefore, we conclude by setting, for example, $C_2 = \frac{\epsilon\pi}{2}$. □

A straightforward consequence of these results is that the Mellin transform $\mathcal{M}\{\theta_u\}(s)$ converges for any $s \in \mathbb{C}$. Moreover, for $\mathfrak{Re}(s) > \frac{3}{2}$ we can evaluate the transform term by term:

$$\mathcal{M}\{\theta_u\}(s) = \sum_{m \in \mathbb{Z}^2} (m+u) \cdot w \int_0^\infty t^s e^{\pi t|m+u|^2} \frac{dt}{t} = \pi^{-s}\Gamma(s) \sum_{m \in \mathbb{Z}^2} \frac{(m+u) \cdot w}{|m+u|^{2s}}$$

There is an evident similarity with the additive form of the L function; in fact, we will express it as a weighted sum of slightly modified theta series.

VI.5 Generalized Theta Series

Consider a quadratic imaginary extension $K/\mathbb{Q}$ of class number one. Then we define the generalized theta series in the following way.

Definition VI.5.1. Let $(\alpha) = \alpha\mathcal{O}_K \subset \mathbb{C}$, $\alpha \in K^*$, be a fractional ideal and fix $u \in \mathbb{C}$ such that $u \notin (\alpha)$. Then:

$$\theta_u(t,(\alpha)) = \sum_{z \in (\alpha)} (z+u) e^{-\pi t|z+u|^2} \tag{VI.21}$$

$$\theta^u(t,(\alpha)) = \sum_{z \in (\alpha)} z e^{2\pi i Re(\bar{z}u)} e^{-\pi t|z|^2}. \tag{VI.22}$$

Remark VI.5.2. If we consider $\mathbb{C} \simeq \mathbb{R}^2$ and under this identification, we let M be the matrix of the lattice associated with (α), $M\mathbb{Z}^2 = \alpha\mathcal{O}_\mathcal{K} \subset \mathbb{R}^2 \simeq \mathbb{C}$, where R^2 has basis $\{e_1 = 1, e_2 = i\}$. We retrieve the original definition:

$$\theta_u(t,(\alpha)) = \sum_{m \in M} (m+u) \cdot w e^{-\pi t|m+u|^2} \tag{VI.23}$$

$$\theta_u(t,(\alpha)) = \sum_{m \in M} m \cdot w e^{2\pi i m \cdot u} e^{-\pi t|m|^2}, \tag{VI.24}$$

where $w = (1, i)$ is a fixed vector. Then a consequence of Corollary VI.4.8 is that

$$\theta_u(t,\alpha) = \frac{1}{|M|} \frac{-i}{t^2} \theta^u\left(\frac{1}{t}, 2(\bar{\alpha})^\vee\right),$$

where $(\alpha)^\vee$ is the fractional ideal of the elements $y \in \mathbb{C}$ such that

$$Tr(xy) = 2Re(xy) \in \mathbb{Z}$$

for any $x \in (\alpha)$.

As a result of the above remark, we find that $\theta_u(t,\alpha)$ satisfies the following proposition, equivalent to Corollary VI.4.11, in fact (α) is a discrete lattice and we can repeat the proof in a similar way.

Proposition VI.5.3. *There exist constants $C_1, C_2 > 0$ such that:*

1. $|\theta_u(t,(\alpha))| < e^{-C_1 t}$ *for* $t \to +\infty$

2. $|\theta_u(t,(\alpha))| < e^{-\frac{C_2}{t}}$ *for* $t \to 0$.

Proof. (1). Consider the equivalent form (VI.23) of $\theta_u(t,(\alpha))$. Next, consider the constant $c = \min_{z\in(\alpha)} |z+u|^2 > 0$, since $u \notin (\alpha)$, $0 \in (\alpha)$ and the lattice $(\alpha) \subset \mathbb{C}$ is discrete. Then

$$|\theta_u(t,(\alpha))| \leq \sum_{z\in(\alpha)} |z+u|e^{-\pi t|z+u|^2} = e^{-\pi tc} \sum_{z\in(\alpha)} |z+u|e^{-\pi t(|z+u|^2-c)}.$$

The last sum obviously converges and is decreasing with respect to t, which means $|\theta_u(t,(\alpha))| \leq e^{-\pi ct}A$, for a positive constant A. So, taking, for example, $C_1 = \frac{c}{2}$ we obtain the result.

(2) We use the identity showed before to rewrite $\theta_u(t,(\alpha)) = \frac{-i}{|M|t^2}\theta^u\left(\frac{1}{t}, 2(\bar{\alpha})^\vee\right)$, where M is the matrix associated to (α). Consider $\epsilon = \min_{z\in 2(\bar{\alpha})^\vee\setminus\{0\}} |z|^2 > 0$, since the lattice $2(\bar{\alpha})^\vee$ is discrete.

$$\begin{aligned}|\theta^u(t,(\alpha))| &\leq \frac{1}{|M|t^2} \sum_{z\in 2(\bar{\alpha})^\vee} |z|e^{-\frac{\pi}{t}|z|^2} = \frac{1}{|M|t^2}e^{-\frac{\epsilon\pi}{t}} \sum_{z\in 2(\bar{\alpha})^\vee} |z|e^{-\frac{\pi}{t}(|z|^2-\epsilon)} \\ &< \frac{1}{|M|t^2}e^{-\frac{\epsilon\pi}{t}}|\theta^u(1)|e^{\pi\epsilon}\end{aligned}$$

for $t < 1$. Here we used the fact that the last sum is a strictly increasing function because the only term $z \in 2(\bar{\alpha})^\vee$ such that $|z|^2 < \epsilon$ is $z = 0$ and it vanishes since in the sum $z = 0$. Therefore, we conclude by setting, for example, $C_2 = \frac{\epsilon\pi}{2}$. □

This result tells us that the Mellin transform of the generalized theta series is entire. Furthermore, for $\mathfrak{Re}(s) > \frac{3}{2}$ we can evaluate the series term by term to obtain the following:

$$\begin{aligned}\mathcal{M}\{(z+u)e^{\pi t|z+u|^2}\} &= \pi^{-s}\Gamma(s)\frac{z+u}{|z+u|^{2s}}, \\ \mathcal{M}\{\theta_u(t,(\alpha))\}(s) &= \sum_{z\in(\alpha)} \pi^{-s}\Gamma(s)\frac{z+u}{|z+u|^{2s}}.\end{aligned}$$

Finally a technical result that will be useful later.

Definition VI.5.4. Let $K = \mathbb{Q}(\sqrt{d})$ and consider the fractional ideal (α). Then the different $\mathfrak{D}_\alpha$ is the only fractional ideal (b), $b \in K^*$, such that $(\alpha)^\vee\mathfrak{D}_\alpha = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Proposition VI.5.5. *Let* $K = \mathbb{Q}(\sqrt{d})$ *and consider the fractional ideal* (α)*. Then the following holds.*

1. $\mathfrak{D}_K = \mathfrak{D}_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}} = \begin{cases} (2\sqrt{d}) & d \not\equiv 1 \mod 4 \\ (\sqrt{d}) & d \equiv 1 \mod 4 \end{cases}$

2. $\mathfrak{D}_\alpha = \alpha\mathfrak{D}_K = (\alpha)\mathfrak{D}_K$

Proof. (1). See [Lan94, Prop. II.2].

(2). Simply by the definition of $(\alpha)^\vee$ its elements are $\frac{1}{\alpha}(\mathcal{O}_K)^\vee$. As a result, we obtain $\mathfrak{D}_\alpha = \alpha\mathfrak{D}_K = (\alpha)\mathfrak{D}_K$.

□

VI.6 Analytic Continuation and Functional Equation

Now we are ready to prove the main result.

Theorem VI.6.1. *Let E/K be an elliptic curve with CM by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathcal{O}_K$ and with equation in Weierstrass form defined over $\mathbb{Z}$. Let $\psi : \mathcal{I}_K \to \mathcal{O}_K$ be the associated Hecke character.*

1. *$L(E,s) = \sum_{I\in\mathcal{I}_K} \psi(I)(\mathbb{N}I)^{-s}$ admits a holomorphic analytic continuation to the entire complex plane.*

2. *Let*
$$\Lambda(E,s) = (\mathbb{N}(\mathfrak{D}_K\mathfrak{c}_\psi))^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s)$$
where $\mathfrak{D}_K = (s)$ is the different and $\mathfrak{c}_\psi = (c)$ is the conductor of $L(E,s)$. Then $\Lambda(E,s)$ satisfies the functional equation:
$$\Lambda(E,s) = \epsilon\Lambda(E,2-s)$$
where $\epsilon = \pm 1$ is the root number*.*

Proof. First recall
$$L(E,s) = \frac{1}{w}\sum_{z\in\mathcal{O}_K}\chi_\psi(z)\frac{z}{|z|^{2s}}$$
where w is the number of units in $\mathcal{O}_K$ and $\chi_\psi : \mathcal{O}_K \to (\mathcal{O}_K)^\times$ is the associated multiplicative function. Choosing representatives $u \in \mathcal{O}_K$ for the elements of $\frac{\mathcal{O}_K}{\mathfrak{c}_\psi}$, we can then rewrite the sum as follows.
$$\frac{1}{w}\sum_{z\in\mathcal{O}_K}\chi_\psi(z)\frac{z}{|z|^{2s}} = \frac{1}{w}\sum_{z\in(c),\,u}\chi_\psi(u+z)\frac{z+u}{|z+u|^{2s}} =$$
$$\frac{1}{w}\sum_{u}\sum_{z\in\mathcal{O}_K}\chi_\psi(u)\frac{cz+u}{|cz+u|^{2s}} = \frac{1}{w}\sum_{u}\chi_\psi(u)\sum_{z\in\mathcal{O}_K}\frac{c}{|c|^{2s}}\frac{z+\frac{u}{c}}{|z+\frac{u}{c}|^{2s}},$$
where we used the fact that $\chi_\psi(x) = \chi_\psi(y)$ if $x \equiv y \mod \mathfrak{c}_\psi$. Now, using the theta series $\theta_{\frac{u}{c}}(t,\mathcal{O}_K)$, we rewrite the expression as:
$$\begin{aligned}\frac{1}{w}\sum_{u}\chi_\psi(u)\sum_{z\in\mathcal{O}_K}\frac{c}{|c|^{2s}}\frac{z+\frac{u}{c}}{|z+\frac{u}{c}|^{2s}} &= \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\sum_{u}\chi_\psi(u)\mathcal{M}\{\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s)\\ &= \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\mathcal{M}\{\sum_{u}\chi_\psi(u)\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s).\end{aligned}$$
Here we stress that $\frac{u}{c} \in \mathcal{O}_K \iff u \equiv 0 \mod \mathfrak{c}_\psi \iff \chi_\psi(u) = 0$, so the above equality holds even in this case. Now we know that
$$\mathcal{M}\{\sum_{u}\chi_\psi(u)\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s) = \sum_{u}\chi_\psi(u)\mathcal{M}\{\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s)$$

is an entire function since each term in the sum is an entire function. In addition, the function $\frac{\pi^s}{\Gamma(s)}$ is an entire function since $\frac{1}{\Gamma(s)}$ is an entire function. This proves that

$$\frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\sum_u \chi_\psi(u)\mathcal{M}\{\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s) = \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\mathcal{M}\{\sum_u \chi_\psi(u)\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s)$$

is the analytical continuation of $L(E,s)$ to the whole complex plane. In fact we have proved for $\mathfrak{Re}(s) > \frac{3}{2}$ that the two functions are equal and the other one is entire.

To derive the functional equation we use the identity

$$\theta_{\frac{u}{c}}(t,\mathcal{O}_K) = \frac{1}{|M|}\frac{-i}{t^2}\theta^{\frac{u}{c}}\left(\frac{1}{t}, 2\left(\frac{1}{s}\right)\right)$$

where we recall that $(s) = \mathfrak{D}_K$, that $M\mathbb{Z}^2 = \mathcal{O}_K$ and that $(s) = (\bar{s})$ by Proposition VI.5.5. Then:

$$\begin{aligned}
L(E,s) &= \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\mathcal{M}\{\sum_u \chi_\psi(u)\theta_{\frac{u}{c}}(t,\mathcal{O}_K)\}(s) = \\
&= \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\mathcal{M}\{\sum_u \chi_\psi(u)\frac{1}{|M|}\frac{-i}{t^2}\theta^{\frac{u}{c}}\left(\frac{1}{t}, 2\left(\frac{1}{s}\right)\right)\}(s) = \\
&= \frac{\pi^s}{\Gamma(s)}\frac{1}{w}\frac{c}{|c|^{2s}}\int_0^{+\infty}\sum_u \chi_\psi(u)\frac{1}{|M|}\frac{-i}{t^2}\sum_{z\in\frac{2}{s}\mathcal{O}_K} z e^{2\pi i Re(\frac{\bar{z}u}{c})}e^{\pi\frac{1}{t}|z|^2}t^s\frac{dt}{t} = \\
&= \frac{\pi^s}{\Gamma(s)}\pi^{s-2}\Gamma(2-s)\frac{1}{w}\frac{c}{|c|^{2s}}\frac{-i}{|M|}\sum_{z\in\frac{2}{s}\mathcal{O}_K}\sum_u \chi_\psi(u)e^{2\pi i Re(\frac{\bar{z}u}{c})}\frac{z}{|z|^{2(2-s)}} = \\
&= \frac{\pi^s}{\Gamma(s)}\pi^{s-2}\Gamma(2-s)\frac{1}{w}\frac{c}{|c|^{2s}}\frac{-i}{|M|}\sum_{z\in\mathcal{O}_K}\sum_u \chi_\psi(u)e^{2\pi i Re(\frac{2\bar{z}u}{\bar{s}c})}\frac{\frac{2}{s}z}{|\frac{2}{s}z|^{2(2-s)}} = \\
&= \frac{\pi^s}{\Gamma(s)}\pi^{s-2}\Gamma(2-s)\frac{1}{w}\frac{c}{|c|^{2s}}\frac{2^{2(s-2)}2}{s|s|^{2(s-2)}}\frac{-i}{|M|}\sum_{z\in\mathcal{O}_K}\sum_u \chi_\psi(u)e^{2\pi i \mathrm{Tr}(\frac{\bar{z}u}{\bar{s}c})}\frac{z}{|z|^{2(2-s)}}.
\end{aligned}$$

For $\mathfrak{Re}(2(2-s)) > 3$. Now we evaluate $|M|$:

$$M = \begin{cases} \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|d|}}{2} \end{bmatrix} & d \equiv 1 \mod 4 \\ \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{|d|} \end{bmatrix} & d \equiv 2,3 \mod 4 \end{cases}.$$

Hence we obtain that

$$i|M| = \begin{cases} \frac{\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2,3 \mod 4 \end{cases} = -\frac{s}{2}$$

Choosing the right generator $s = -2i|M|$ for $\mathfrak{D}_K$. So that the above expression becomes:

$$L(E,s) = \frac{\pi^s}{\Gamma(s)}\pi^{s-2}\Gamma(2-s)\frac{1}{w}\frac{1}{\bar{c}|c|^{2s-2}}\frac{2^{2(s-2)}4}{|s||s|^{2(s-2)}}\sum_u \chi_\psi(u)e^{2\pi i \mathrm{Tr}(\frac{\bar{z}u}{\bar{s}c})}\frac{z}{|z|^{2(2-s)}}.$$

As a result we obtain that

$$|cd|^s\Gamma(s)(2\pi)^{-s}L(E,s) = |cd|^{2-s}\Gamma(2-s)(2\pi)^{-(2-s)}\frac{\sum_u \chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{\bar z u}{\bar s c})}}{\bar c}\sum_{z\in\mathcal{O}_K}\frac{z}{|z|^{2(2-s)}}.$$

Next, we analyze $\sum_u \chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{\bar z u}{\bar s c})}$. Let $\tilde\chi_\psi : \frac{\mathcal{O}_K}{\mathfrak{c}_\psi} \to (\mathcal{O}_K)^\times$ be the primitive multiplicative character associated with χ_ψ. We can rewrite

$$\sum_u \chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{\bar z u}{\bar s c})} = \sum_{u\in\frac{\mathcal{O}_K}{\mathfrak{c}_\psi}} \tilde\chi_\psi(u)\phi(\bar z u)$$

where $\phi : x \to e^{2\pi i\mathrm{Tr}(\frac{x}{\bar s c})}$ is an additive character of $\frac{\mathcal{O}_K}{\mathfrak{c}_\psi}$. In fact, if $x \equiv 0 \mod \mathfrak{c}_\psi$, then $x = ac$ and $\phi(ac) = e^{2\pi i\mathrm{Tr}(\frac{a}{\bar s})}$. Therefore, by the definition of $(\frac{1}{\bar s}) = (\frac{1}{s}) = (\mathcal{O}_K)^\vee$ we conclude $\mathrm{Tr}(\frac{a}{\bar s}) \in \mathbb{Z}$, hence $\phi(ac) = 1$. Moreover, $\phi(x)$ is nontrivial on any $J \supsetneq \mathfrak{c}_\psi$, in fact $\psi(x)$ is trivial if and only if $\mathrm{Tr}(\frac{x}{\bar s c}) \in \mathbb{Z} \iff x \in (\frac{1}{\bar s c})^\vee = (\frac{1}{s})(sc) = (c) = \mathfrak{c}_\psi$. This means that by the proposition VI.2.10.1:

$$\sum_{u\in\frac{\mathcal{O}_K}{\mathfrak{c}_\psi}} \tilde\chi_\psi(u)\phi(\bar z u) = \bar\chi_\psi(\bar z)g(\tilde\chi_\psi,\phi).$$

Then we recall that $\bar\chi_\psi(\bar x) = \chi_\psi(x)$, from this we obtain:

$$\begin{aligned}(\mathbb{N}\mathfrak{D}_K\mathfrak{c}_\psi)^{\frac{s}{2}}\Gamma(s)(2\pi)^{-s}L(E,s) &= \\ &= (\mathbb{N}\mathfrak{D}_K\mathfrak{c}_\psi)^{\frac{2-s}{2}}\Gamma(2-s)(2\pi)^{-(2-s)}\frac{g(\tilde\chi_\psi,\phi)}{\bar c}\sum_{z\in\mathcal{O}_K}\chi_\psi(z)\frac{z}{|z|^{2(2-s)}}.\end{aligned}$$

Therefore, we conclude that

$$\Lambda(E,s) = \frac{g(\tilde\chi_\psi,\phi)}{\bar c}\Lambda(E,2-s).$$

It remains to prove that $\frac{g(\chi_\psi,\phi)}{\bar c} = \pm 1$. First, by Proposition VI.2.10.2 we know $\frac{|g(\chi_\psi,\phi)|}{|\bar c|} = 1$. Furthermore, we recall that $(c) = (\bar c)$ since $\chi_\psi(\bar z) = \bar\chi_\psi(z)$, which means that we could choose $\bar c$ as a generator of $\mathfrak{c}_\psi$ and $\bar u$ as representatives of the equivalence classes. Then repeating the arguments presented so far we end up with

$$\Lambda(E,s) = \frac{\sum_u \chi_\psi(\bar u)e^{2\pi i\mathrm{Tr}(\frac{\bar u}{\bar s\bar c})}}{c}\Lambda(E,2-s).$$

Then comparing the two functional equations we obtain the following equality:

$$\frac{\sum_u \chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{u}{\bar s c})}}{\bar c} = \frac{\sum_u \chi_\psi(\bar u)e^{2\pi i\mathrm{Tr}(\frac{\bar u}{\bar s\bar c})}}{c}.$$

In particular the second numerator is equivalent to

$$\sum_u \bar\chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{u}{sc})} = \sum_u \bar\chi_\psi(u)e^{-2\pi i\mathrm{Tr}(\frac{u}{\bar s c})} = \overline{\sum_u \chi_\psi(u)e^{2\pi i\mathrm{Tr}(\frac{u}{\bar s c})}}.$$

Where we used the fact that $\mathrm{Tr}(y) = \mathrm{Tr}(\bar{y})$ and that $\bar{s} = -s$. This means

$$\frac{g(\tilde{\chi}_\psi, \phi)}{\bar{c}} = \frac{\overline{g(\tilde{\chi}_\psi, \phi)}}{c}$$

hence $\frac{g(\chi\psi,\phi)}{\bar{c}} \in \mathbb{R}$ and has norm 1. This proves that $\epsilon = \frac{g(\tilde{\chi}_\psi,\phi)}{\bar{c}} = \pm 1$.

Therefore, we have proved the functional equation for $|\mathfrak{Re}(s) - 1| > \frac{1}{2}$, so that

$$\frac{\Lambda(E, s)}{\Lambda(E, 2 - s)} = \epsilon$$

in this domain. But we notice that both the right-hand side and the left-hand side are meromorphic equations defined on $\mathbb{C}$, hence the functional equation holds for every $s \in \mathbb{C}$.

□

VI.7 Analytic Rank and Weak BSD Conjecture

Now that we know that the Hasse-Weil L function of our CM curves has an analytic continuation, we can introduce the following definition.

Definition VI.7.1 (Analytic Rank)**.** Let E/K be an elliptic curve defined over $\mathbb{Z}$ such that the Hasse-Weil L-function $L(E, s)$ has an analytic continuation to the whole complex plane. Then

$$\mathrm{rank}(L(E, s)) = \mathrm{ord}_{s=1} L(E, s).$$

As the terminology suggests, the analytic rank and the rank of E are conjecturally related by the following.

Conjecture VI.7.2 (Weak Birch-Swinnerton-Dyer, 1965)**.** *Let E/K be an elliptic curve defined over $\mathbb{Q}$, and let $L(E, s)$ be its Hasse-Weil L-function. Then*

$$\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}(L(E, s)) = \mathrm{rank}(E[Q]).$$

Remark VI.7.3. We notice that if the root number $\epsilon = -1$ necessarily the order $\mathrm{rank}(L(E, s)) \geq 1$ by the functional equation and by the fact that $\Gamma(s) = 1$ for $s = 1$. Hence, by the conjecture, we shall have infinite rational points on that elliptic curve. However, if the root number is equal to 1, we cannot say anything a priori about the analytic rank of the L-function.

Furthermore, there are rapidly converging series for $L(E, 1)$, like the one presented in [Kob93, Prop. II.6.12].

The confidence in this hypothesis increased not only because of numerical evidence but also because of striking partial results, such as the following.

Theorem VI.7.4 (Coates-Wiles, 1977)**.** *Let E/K be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by the ring of integers of an imaginary quadratic extension of class number 1. If E has infinitely many $\mathbb{Q}$-rational points, then $L(E, 1) = 0$.*

This theorem already gives a really useful criterion to show that a CM elliptic curve has a finite number of rational points: it is enough to look at the value of $L(E, 1)$ and see if it is different from zero!

Appendix A

Minimal Models of CM Elliptic Curves defined over $\mathbb{Z}$

In this work we treated the elliptic curves defined over $\mathbb{Z}$ with complex multiplication by a full ring of integers of an imaginary quadratic extension of class number one. In the case of CM by $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ we have already described all the $\mathbb{Q}$-isomorphism classes of such curves. In this table we give a representative elliptic curve E with CM by the ring of integers of K in generalized Weierstrass form with minimal discriminant Δ_E. Then the other curves are simple twists of these ones.

D_K	Minimal Weierstrass equation over $\mathbb{Z}$	Δ_E
-3	$y^2 + y = x^3$	-3^3
-4	$y^2 = x^3 + x$	-2^6
-7	$y^2 + xy = x^3 - x^2 - 2x - 1$	-7^3
-8	$y^2 = x^3 + 4x^2 + 2x$	-2^9
-11	$y^2 + y = x^3 - x^2 - 7x + 10$	-11^3
-19	$y^2 + y = x^3 - 38x + 90$	-19^3
-43	$y^2 + y = x^3 - 860x + 9707$	-43^3
-67	$y^2 + y = x^3 - 7370x + 243528$	-67^3
-163	$y^2 + y = x^3 - 2174420x + 1234136692$	-163^3

Bibliography

[GH94] Phillip Griffiths and Joseph Harris. *Principles of Algebraic Geometry.* Wiley Classics Library. John Wiley and sons, Inc., 1994.

[IR90] Kenneth Ireland and Micheal Rosen. *A Classical Introduction to Modern Number Theory.* volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New-York, 1990.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Second Edition. volume 97 of Graduate Texts in Mathematics. Springer-Verlag, New-York, 1993.

[Lan94] Serge Lang. *Algebraic Number Theory.* Second Edition. volume 110 of Graduate Texts in Mathematics. Springer-Verlag, New-York, 1994.

[Lem00] Franz Lemmermeyer. *Reciprocity Laws.* Springer Monographs in Mathematics. Springer-Verlag, Berlin Heidelberg, 2000.

[Mir95] Rick Miranda. *Algebraic Curves and Riemann Surfaces.* volume 5 of Graduate Studies in Mathematics. American Mathematical Society, 1995.

[Sil91] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New-York, 1991.

[Sil09] Joseph H. Silverman. *Arithmetic of Elliptic Curves.* Second Edition. volume 106 of Graduate Texts in Mathematics. Springer-Verlag New-York, 2009.

[ST15] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves.* Second Edition. Undergraduate Texts in Mathematics. Springer-Verlag, New-York, 2015.

[Sut17a] Andrew Sutherland. *MIT Course on Elliptic Curves, Lecture 5, Isogenies.* 2017. URL: `https://math.mit.edu/classes/18.783/2017/LectureNotes5.pdf`.

[Sut17b] Andrew Sutherland. *MIT Course on Elliptic Curves, Lecture 6, Isogeny Kernels and division polynomials.* 2017. URL: `https://math.mit.edu/classes/18.783/2017/LectureNotes6.pdf`.

[Wal00] R. J. Walker. *Algebraic Curves.* Springer-Verlag, New York, 2000.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Second Edition. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2008.

[WW13] E. T. Whittaker and G. N. Watson. *A Course of Modern Analysis*. Fourth Edition. Cambridge Mathematical Library. Cambridge University Press, 2013.