Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Magistrale in Matematica

Elliptic curves with complex multiplication and applications to class field theory

Candidato:
Ersilia Silvestri
Matricola 1176523

Relatore:
Prof. Matteo Longo

21 Febbraio 2020

Contents

Introduction

One of the aims of algebraic number theory is to describe the field of algebraic numbers $\bar{\mathbb{Q}}$, i.e., to describe the group theoretic structure of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of $\bar{\mathbb{Q}}/\mathbb{Q}$. The simplest Galois extensions $K \subset \mathbb{Q}$ of $\mathbb{Q}$ are those such that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, called *abelian extensions*; for instance, they arise from maps

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^{\times}$$

because any continuous homomorphism $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^{\times}$ factors through a finite abelian extension. For example, any quadratic extension of the field $\mathbb{Q}$, obtained by adjoining the roots of a quadratic polynomial, is abelian; another example of abelian extension of $\mathbb{Q}$ is the so called *cyclotomic field*, obtained by adjoining the n^{th}-root of unity. Gauss proved that any quadratic field is contained in a cyclotomic field. Moreover, the *Kronecker-Weber theorem* states that any finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension. This means that, il K is an abelian extension of $\mathbb{Q}$, then there exists some integer $n \geq 1$ such that

$$K \subset \mathbb{Q}(\zeta_n)$$

where ζ_n is a n^{th}-root of unity.

For a general number field K it is an open question to describe all the abelian extensions of K. This problem appears as the 12^{th} problem in the complete list of *Hilbert's problems*. Hilbert presented, at the Paris Conference of International Congress of Mathematicans in 1900, a list of ten unsolved (at the time) problems about various branches of mathematics, from geometry to calculus, from physics to algebra and number theory. The complete list of 23 Hilbert's problems, which contains the problem of the field extension, was published later, in 1902. Some of these problems had a great impact on the development of mathematical research of the *XX* century. Up to now, ten of these problems have been completely resolved, seven have a solution not universally accepted by the community of mathematicians, or a partial solution, four of them have a too vague formulation to have a

solution. The last two problems are the 8^{th}, the *Riemann hypothesis*, and the 12^{th}, the explicit description of the abelian extensions of a number field (by *explicit* we mean $F = K(a_i)$ for some a_i): they are unsolved, up to now.

Even if the 12^{th} Hilbert's problem is unsolved, the case of quadratic imaginary fields is completely understood, thanks to the *theory of elliptic curves with complex multiplication*. An elliptic curve $E/\mathbb{C}$ is a complex torus. We say that $E/\mathbb{C}$ has complex multiplication if the endomorphism ring $\mathrm{End}(E)$ is isomorphic to an order in a quadratic imaginary field K, for example the ring of integers R_K of K.

Then, using the theory of complex multiplication of the elliptic curves we will show the following theorem:

Theorem. *Let K be an imaginary quadratic field, namely, $K = \mathbb{Q}(\tau)$, with τ a quadratic imaginary irrational, let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring of integers R_K of K. Then, the maximal abelian extension of K can be obtained as*

$$K^{ab} = K(j(E), h(E_{tors}))$$

namely, by adjoining some algebraic numbers related to an elliptic curve E.

More precisely, $j(E)$ is the *singular j-invariant of the curve* that depends on the coefficients of the equation that defines the curve, a priori it is an element of $\mathbb{C}$ but in the case of a curve with complex multiplication it is an algebraic integer. E_{tors} denotes the *torsion subgroup of E*, namely the set of the points of finite order of the curve E, and the function $h : E \longrightarrow \mathbb{P}^1$, called the *Weber function*, sends any point P of E to a function of its x-coordinate (up to a suitable change of variables in the equation of the curve, it is simply the x-coordinate of the point, for almost all the curves E). Thus, $h(E_{tors})$ is the set of the x-coordinate of the torsion points of the curve E.

From this description of the maximal abelian extension, we will able to characterize any abelian extension of K.

We remark that the case of non-abelian extensions of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ is much more difficult to study. For instance, some GL_2-type extensions, i.e., such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{GL}_2(K)$ for some field K, can be described by the theory of modular forms, and a much more general perspective is given by the *Langlands program*.

The purpose of this dissertation is to introduce some definitions and properties of the elliptic curves (in Chapter 1), of the complex multiplication on them (in Chapter 2), of the class field theory (in Chapter 3) and then to prove the result about the maximal abelian extension of quadratic imaginary fields, with some other interesting properties about the elliptic curves with complex multiplication (in Chapter 4).

Chapter 1

Elliptic curves

1.1 Geometry of elliptic curves

Elliptic curves are curves of genus one with a specified base point. We start the study of elliptic curves given by explicit polynomial equations called *Weierstrass equations*.

1.1.1 Weierstrass equation

Every elliptic curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only the base point on the line at infinity.

Definition 1.1 (Weierstrass equation)**.** After X and Y are scaled appropriately, an elliptic curve has equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6$$

called *Weierstrass equation*, with $a_1, \ldots, a_6 \in \bar{K}$ algebraically closed field. Here, the base point is $O = [0, 1, 0]$.

To ease notation, we generally write the Weierstrass equation using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$, so in the form

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

with the base point $O = [0, 1, 0]$ at infinity. If the coefficients $a_1, \ldots, a_6$ are in K, we say that E is *defined over* K. Moreover, if $\mathrm{char}(\bar{K}) \neq 2$ we can complete the

square and simplify the equation, thus the substitution

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

gives

$$\begin{aligned}(y - a_1x - a_3)^2 + 2a_1x(y - a_1x - a_3) + 2a_3(y - a_1x - a_3) &= 4x^3 + 4a_2x^2 + 4a_4x + 4a_6\\ \Leftrightarrow \quad y^2 - a_1^2x^2 - a_3^2 - 2a_1a_3x &= 4x^3 + 4a_2x^2 + 4a_4x + 4a_6\\ \Leftrightarrow \quad y^2 &= 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + (a_3^2 + 4a_6).\end{aligned}$$

So, if we define the coefficients

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

the equation takes the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Moreover, with the assumption that $\mathrm{char}(\bar{K}) \neq 2, 3$, with the substitution

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

we get

$$\begin{aligned}\frac{y^2}{108^2} = 4\frac{(x - 3b_2)^3}{36^3} + b_2\frac{(x - 3b_2)^2}{36^2} + 2b_4\frac{x - 3b_2}{36} + b_6\\ \Leftrightarrow \quad y^2 = x^3 - 27(b_2^2 - 24b_4)x - 54(-b_2^3 + 36b_2b_4 - 216b_6).\end{aligned}$$

Then we define the quantities

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

and the equations gets the form

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Moreover, we can define the quantities, depending on the coefficients a_i, b_j, c_k previously determined,

$$\begin{aligned}b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4\\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\\ j &= \frac{c_4^3}{\Delta}\\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}\end{aligned}$$

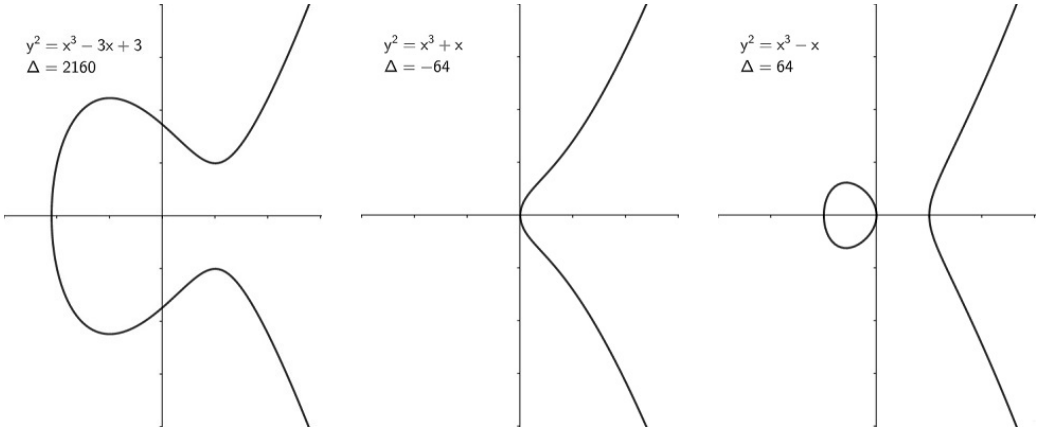


Figure 1.1: Three examples of elliptic curves.

and it is easy to prove that

$$4b_8 = b_2b_6 - b_4^2, \qquad 1728\Delta = c_4^3 - c_6^2.$$

Definition 1.2 (Discriminant, j-invariant, invariant differential)**.** The quantity Δ is called *discriminant of the Weierstrass equation*, while j is the *j-invariant of the Weiestrass equation* and ω is the *invariant differential associated to the Weierstrass equation*.

Definition 1.3 (Singular point of a curve)**.** Let C be a curve given by the non-constant polynomial $f(X, Y) = 0$, then $P \in C$ is a *singular point* if and only if

$$\frac{\partial f}{\partial X}(P) = 0 = \frac{\partial f}{\partial Y}(P).$$

In general, let $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation

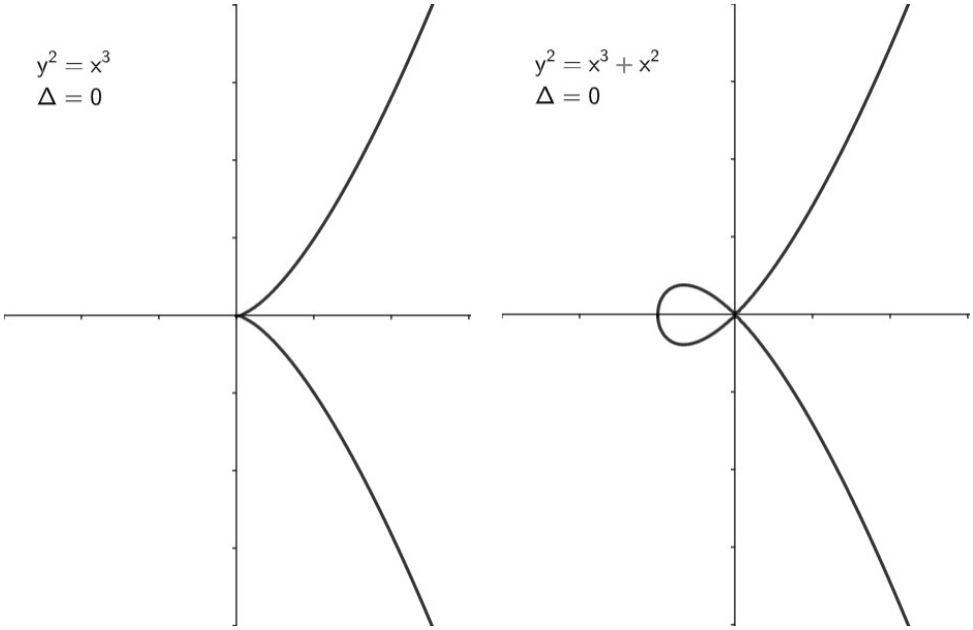
$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Assume that P is a singular point of the curve $f(x, y) = 0$, then we have

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

It follows that there are $\alpha, \beta \in \bar{K}$ such that the Taylor series expansion of $f(x, y)$ at P has the form

$$\begin{aligned} &f(x, y) - f(x_0, y_0) \\ &\qquad = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3. \end{aligned}$$



(a) *Cusp: one tangent direction.* (b) *Node: two distinct tangent directions.*

Figure 1.2: Two singular cubic curves.

Definition 1.4 (Node, cusp, tangent lines)**.** With notation as above, the singular point P is:

- a *node* if $\alpha \neq \beta$. In this case, the two distinct lines
$$y - y_0 = \alpha(x - x_0), \qquad y - y_0 = \beta(x - x_0)$$
are the *tangent lines at* P.
- a *cusp* if $\alpha = \beta$. In this case, the only *tangent line at* P is
$$y - y_0 = \alpha(x - x_0).$$

To what extend is the Weierstrass equation for an elliptic curve E unique? Assuming that the line at infinity $Z = 0$ in $\mathbb{P}^2$ intersects E only at the base point $[0, 1, 0]$, the only change of variables fixing the point and preserving the Weierstrass form of the equation is

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

where $u, r, s, t \in \bar{K}$ and $u \neq 0$. In fact, if we substitute into the equation we get

$$\begin{aligned}(u^3y' + u^2sx' + t)^2 + a_1(u^2x' + r)(u^3y' + u^2sx' + t) + a_3(u^3y' + u^2sx' + t)\\ = (u^2x' + r)^3 + a_2(u^2x' + r)^2 + a_4(u^2x' + r) + a_6\end{aligned}$$

$$\begin{aligned}\Leftrightarrow y'^2 + \frac{a_1 + 2s}{u}x'y' + \frac{a_3 + ra_1 + 2t}{u^3}y' = x'^3 + \frac{a_2 - sa_1 + 3r - s^2}{u^2}x'^2 \\ + \frac{a_4 - sa_3 + 2ra_2 - (t - rs)a_1 + 3r^2 - 2st}{u^4}x' \\ + \frac{a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1}{u^6}\end{aligned}$$

and, if we define new coefficients $a'_1, \ldots, a'_6$ such that

$$\begin{aligned}ua'_1 &= a_1 + 2s \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t - rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1\end{aligned}$$

the equation has the form

$$y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6$$

so this shows that the substitution preserves the form of the equation.

Under this transformation, similarly we can show the following relations hold:

$$\begin{aligned}u^2b'_2 &= b_2 + 12r \\ u^4b'_4 &= b_4 + rb_2 + 6r^2 \\ u^6b'_6 &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b'_8 &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\ u^4c'_4 &= c_4 \\ u^6c'_6 &= c_6\end{aligned}$$

and using these results we see that, under the substitution, the quantities associated to the equation change as

$$u^{12}\Delta' = \Delta, \qquad j' = j, \qquad u^{-1}\omega' = \omega.$$

This is now clear why the j-invariants have been so named: it is an invariant of the isomorphism class of the curve, and it does not depend on the particular

equation choosen. As we will see in the next paragraph, precisely in (1.5.b), for algebraically closed fields also the converse is true.

If we consider the simplest form for the Weierstrass equation, $y^2 = x^3 + Ax + B$, we can easily compute the quantities associate to it:

$$\Delta = -16(4A^3 + 27B^2)$$
$$j = -1728\frac{(4A)^3}{\Delta}$$

and, as in the general case, we can see that the only change of variables preserving this form of the equation is

$$x = u^2 x' \qquad\qquad y = u^3 y'$$

for some element of the multiplicative group of the closed field $u \in \bar{K}^\times$. Again, we can compute the new coefficients for the equation, after the substitution:

$$u^4 A' = A, \qquad\qquad u^6 B' = B$$

and see also that

$$u^{12}\Delta' = \Delta.$$

After this results, we can show how to use the coefficients and the quantities defined above in order to have informations about the curve.

Proposition 1.5. [6, III.1.4, p. 45].

(a) *The curve given by a Weierstrass equation satisfies the following statements:*

(i) *it is non-singular if and only if* $\Delta \neq 0$*;*
(ii) *it has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$*;*
(iii) *it has a cusp if and only if* $\Delta = 0$ *and* $c_4 = 0$*.*

In the singular case, there can be only one singular point.

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

(c) *Let* $j_0 \in \bar{K}$*. There exists an elliptic curve defined over* $K(j_0)$ *whose j-invariant is equal to* j_0*.*

Proof. (a) Let E be an elliptic curve given by the Weierstrass equation

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

We can easily prove that the point at infinity of the curve is never singular: we can look at the curve in $\mathbb{P}^2$ with homogeneous equation

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - A_6Z^3 = 0$$

at the point $O = [0,1,0]$: since $\frac{\partial F}{\partial Z}(O) = 1 \neq 0$, the point is not singular. Then, suppose E is singular: let $P_0 = (x_0, y_0)$ be a singular point. From what we have computed above, the substitution $x = x' + x_0, y = y' + y_0$ leaves Δ and c_4 invariant, so we may assume that E is singular at $(0,0)$. We can easily compute some coefficients:

$$a_6 = f(0,0) = 0, \qquad a_4 = \frac{\partial f}{\partial x}(0,0) = 0, \qquad a_3 = \frac{\partial f}{\partial y}(0,0) = 0$$

and simplify the equation for the curve:

$$E\colon f(x,y) = y^2 + a_1xy - x^3 - a_2x^2 = 0.$$

The quantities associated to the equation are $c_4 = (a_1 + 4a_2)^2$ and $\Delta = 0$. By definition, the curve E has a node in $(0,0)$ if and only if the quadratic form $y^2 + a_1xy + a_2x^2$ has two distinct factors: this happens if and only if its discriminant satisfies

$$a_1 + 4a_2 \neq 0$$

but it follows immediately that $c_4 \neq 0$. Similarly, the point $(0,0)$ is a cusp for E if and only if the quadratic form has two equal factors, if and only if its discriminant is zero, so $c_4 = 0$. To complete the proof we need to show that, if E is non-singular, then $\Delta \neq 0$. To simplify the computation we can assume that $\mathrm{char}(K) \neq 2$ and that the Weierstrass equation for E is of the form

$$E\colon f(x,y) = y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6 = 0.$$

Then E is singular if and only if there exists a point (x_0, y_0) of E such that

$$\frac{\partial f}{\partial x}(x_0,y_0) = -12x_0^2 - 2b_2x_0 - 2b_4 = 0, \qquad \frac{\partial f}{\partial y}(x_0,y_0) = 2y_0 = 0.$$

This tells us that the singular points of E are exactly the points $(x_0, 0)$ of E such that x_0 is a double root of the polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. This polynomial has double roots if and only if its discriminant vanishes: it is equal to 16Δ, so it follows that $\Delta = 0$. Finally, any cubic polynomial cannot have two double roots, so the curve E has at most one singular point.

(b) If two elliptic curves are isomorphic then by the transformation formulas we can easily see that they have the same j-invariant. Conversely, let E, E' be two elliptic curves with Weierstrass equations

$$E\colon y^2 = x^3 + Ax + B$$
$$E'\colon y'^2 = x'^3 + A'x' + B'.$$

Then we suppose that $j(E) = j(E')$: by definition it means that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2} \quad \Longrightarrow \quad A^3B'^2 = A'^3B^2.$$

We look for an isomorphism of the form $(x, y) = (u^2x', u^3y')$, so we need to find u. We have to consider three cases:

- $A = 0$ (so $j = 0$): then $B' = 0$ since $\Delta \neq 0$, so also $A' = 0$. Using $u = \left(\frac{B}{B'}\right)^{1/6}$ we get the isomorphism we were looking for.
- $B = 0$ (so $j = 1728$): then $A' \neq 0$ so $B' = 0$. Using $u = \left(\frac{A}{A'}\right)^{1/4}$ we get the isomorphism we were looking for.
- $AB \neq 0$ (so $j \neq 0, 1728$): then $A'B' \neq 0$ (since if one of them were 0, then both of them would be 0, contradicting $\Delta \neq 0$). Using $u = \left(\frac{A}{A'}\right)^{1/4} = \left(\frac{B}{B'}\right)^{1/6}$ we get the isomorphism we were looking for.

(c) Assume that $j_0 \neq 0, 1728$, consider the elliptic curve of Weierstrass equation

$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

A simple calculation yields to

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3}, \qquad j = j_0.$$

This gives the elliptic curve we were looking for if $j_0 \neq 0, 1728$. In the other two cases:

$$\begin{aligned} &E\colon y^2 = x^3 + Ax + B && \Delta = -27 && \text{if } j = 0 \\ &E'\colon y'^2 = x'^3 + A'x' + B' && \Delta = -64 && \text{if } j = 1728. \end{aligned}$$

We observe that, if $\mathrm{char}(K) = 2, 3$ it holds $0 \equiv 1728$, so even in these cases one of the two curves will be non-singular and fill in the missing value of j. □

We state here a useful proposition, whose proof is omitted.

Proposition 1.6. [6, III.1.5, p. 48]. *Let E be an elliptic curve. Then the invariant differential ω associated to a Weierstrass equation for E is holomorphic and non-vanishing.*

Proof. See [6, III.1.5, p. 48]. □

Next, we look at what happens when a Weierstrass equation is singular.

Proposition 1.7. [6, III.1.6, p. 48]. *If a curve E given by a Weierstrass equation is singular, then there exists a rational map $\phi\colon E \longrightarrow \mathbb{P}^1$ of degree one, i.e., the curve E is birational to $\mathbb{P}^1$.*

Proof. Given a Weierstrass equation for the curve

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

we know that making a linear change of variables we may assume that the singular point of E is $(0, 0)$. So, checking the value of the function and of the partial derivatives

$$f(0,0) = a_6 = 0, \qquad \frac{\partial f}{\partial x}(0,0) = -a_4 = 0, \qquad \frac{\partial f}{\partial y}(0,0) = a_3 = 0$$

we may simplify the equation to

$$E\colon y^2 + a_1xy = x^3 + a_2x^2.$$

Then, the rational map $E \longrightarrow \mathbb{P}^1, (x, y) \mapsto [x, y]$ has degree 1, since it has an inverse given by $\mathbb{P}^1 \longrightarrow E, [1, t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$. To derive this formula, let $t = y/x$ and note that $f(x, y)/x^2$ yields to $t^2 + a_1t = x + a_2$, so both x and $y = xt$ are in $\bar{K}(t)$. □

1.1.2 Reduction types

Let K be a field with the ring of integers R_K and let $\mathfrak{P}$ be a prime ideal of K, namely a prime ideal in R_K. Let $F_\mathfrak{P} = R_K/\mathfrak{P}$ be the *residue field of K modulo* $\mathfrak{P}$.

Definition 1.8 (Reduction of E modulo $\mathfrak{P}$)**.** Given a *minimal Weierstrass equation* for the elliptic curve E/K (see [6, VII.1, p. 186] for details) of the form

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

we can reduce its coefficients modulo $\mathfrak{P}$ to obtain a curve over the residue field $F_\mathfrak{P}$, namely

$$\tilde{E}\colon y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}.$$

The curve $\tilde{E}/F_\mathfrak{P}$ is called the *reduction of E modulo* $\mathfrak{P}$.

We started from a minimal equation for E (the proposition [6, VII.1.3.a, p. 186] ensures the existence of such equation) so the equation for $\tilde{E}$ is unique up to the standard change of coordinates (1.18.b) for Weierstrass equations over the residue field (from [6, VII.1.3b, p. 186]).

Then we give some useful definitions about $\tilde{E}$, in order to get informations about E. From the proposition (1.5), the reduced curve is one of three types: we can classify E according to these possibilities.

Definition 1.9 (Reduction types)**.** Let E/K be an elliptic curve.

(a) E has *good reduction* or *stable reduction* if $\tilde{E}$ is non-singular (otherwise, we say that E has *bad reduction* and distinguish the types of singularity).

(b) E has *multiplicative reduction* or *semistable reduction* if $\tilde{E}$ has a node. The reduction is said to be *split* if the slopes of the tangent lines at the node are in the residue field $F_\mathfrak{P}$, otherwise it is said to be *non-split*.

(c) E has *additive reduction* or *unstable reduction* if $\tilde{E}$ has a cusp.

It is quite easy to read off the reduction type of an elliptic curve from a minimal Weierstrass equation:

Proposition 1.10. [6, VII.5.1, p. 196]. *Let E/K be an elliptic curve given by a minimal Weierstrass equation*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation and let c_4 be the usual expression involving the coefficients of the equation. Recall that $R_K^\times$ denotes the unit group of R_K.

(a) *E has good reduction if and only if* $\Delta \in R_K^\times$.
(b) *E has multiplicative reduction if and only if* $\Delta \in \mathfrak{P}$ *and* $c_4 \in R_K^\times$.
(c) *E has additive reduction if and only if* $\Delta \in \mathfrak{P}$ *and* $c_4 \in \mathfrak{P}$.

Proof. It follows immediately from the proposition (1.5) applied to the reduced Weierstrass equation over the field $F_\mathfrak{P}$. □

When an elliptic curve E/K has bad reduction, it is often useful to know whether it attains good reduction over some extension of K.

Definition 1.11 (Potential good reduction)**.** Let E/K be an elliptic curve. We say that E/K has *potential good reduction* if there is a finite extension K'/K such that E/K' has good reduction.

Then we want to know how reduction type behaves under field extension, so we state the next proposition. Finally, the proposition immediately following provides a useful characterization of when an elliptic curve has potential good reduction.

Proposition 1.12. [6, VII.5.4, p. 197]. *Let E/K be an elliptic curve.*

(a) *Let K'/K be an unramified extension. Then the reduction type of E over K is the same as the reduction type of E over the extension K'.*

(b) *Let K'/K be a finite extension. If E has good or multiplicative reduction over K, it has the same reduction type over the extension K'.*

(c) *There exists a finite extension K'/K such that E has good or (split) multiplicative reduction over K'.*

Proof. See [6, VII.5.4, p. 197]. □

Proposition 1.13. [6, VII.5.4, p. 197]. *Let E/K be an elliptic curve. E has potential good reduction if and only if its j-invariant is integral, namely $j(E) \in R_K$.*

Proof. See [6, VII.5.5, p. 199]. □

1.1.3 Group law

Let E be an elliptic curve given by a Weierstrass equation. Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the equation and the point at infinity $O = [0, 1, 0]$. Let $L \subset \mathbb{P}^2$ be a line: since the equation of the curve has degree three, $L \cap E$ contains exactly three points, say P, Q, R, that could be not distinct (if L is tangent to E). Using this fact, we may define a composition law $\oplus$ on E as follows:

Definition 1.14 (Composition law)**.** Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$ then L is tangent to E at P) and let R be the third intersection point of L with E. Let L' be the line through R and the point at infinity O. Then L' intersect E at R, O and a third point. We denote this third point by $P \oplus Q$.

This composition law has the following properties:

Proposition 1.15. [6, III.2.2, p. 51]. *The composition law makes E into an abelian group with identity element O. In particular*

(a) *If a line L intersects E at the points P, Q, R (not necessarily distinct), then $(P \oplus Q) \oplus R = O$;*

(b) *$P \oplus O = P$ for all $P \in E$, it means that O is the identity for the composition law;*

(c) *$P \oplus Q = Q \oplus P$, so the composition law is abelian;*

(d) *Let $P \in E$, there is a point of E, denoted by $\ominus P$, that satisfies $P \oplus (\ominus P) = O$, so for every element there is an inverse;*

(e) *Let $P, Q, R \in E$, then $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, so the composition law is associative.*

(f) *Suppose that E is defined over K. Then*

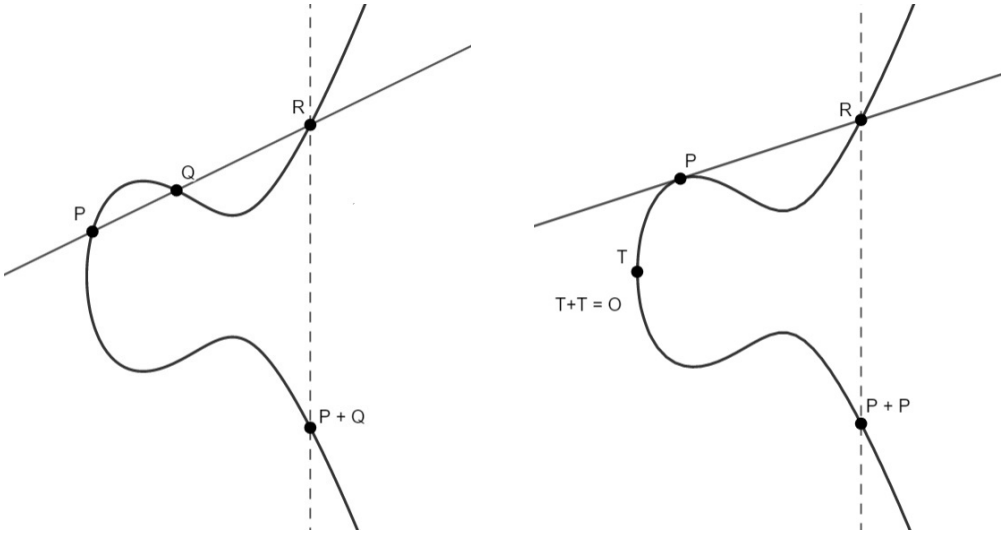
$$E(K) = \{(x, y) \in K^2 \colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of E.

Proof. (a) It follows directly from the definition. It is easy to see it graphically in the figure (1.4).

(b) Taking $Q = O$ in the composition law (1.14), we see that the lines L and L' coincide. The former intersects E at P, O, R and the latter in $R, O, P \oplus O$, so necessarily $P \oplus O = P$. See the figure (1.4) for a graphic representation.

(c) It follows from the symmetry of the construction of $P \oplus Q$ in the composition law: the line through P and Q is clearly the same line through Q and P.



(a) *Addition of distinct points:* $P \oplus Q$ (b) *Adding a point to itself:* $P \oplus P$

Figure 1.3: Group law over an elliptic curve.

(d) Let the line through P and O also intersect E at R. Using (a) and (b) we find that

$$O = (P \oplus O) \oplus R = P \oplus R$$

so $\ominus P = R$ is the desired point.

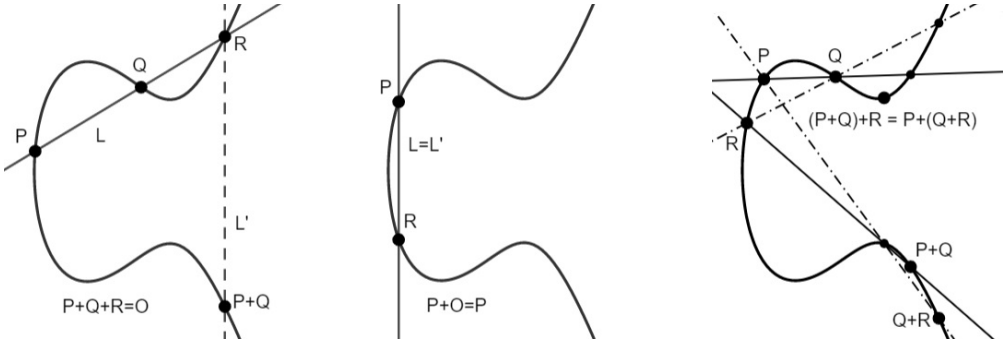
(e) To prove the associativity we could use the *Riemann-Roch theorem*, as in [6, III.3.4.e, p. 61], or a geometric argument. A third, laborious, way to check this property uses the explicit formulas given later in this section. Again in the figure (1.4) there is a graphical example that shows this property holds.

(f) If P and Q have coordinates in K, then the equation of the line connecting them has coefficients in K. If, further, E is defined over K, then the third point of intersection has coordinates given by a rational combination of the coordinates of coefficients of the line and of E, so will be in K.

□

From now on, we simply write the symbols + and − for the group operations $\oplus$ and $\ominus$.

For $m \in \mathbb{Z}$ and $P \in E$, we can add the point to itself m times and get another



(a) *Sum of three aligned points.* (b) *Existence of the identity.* (c) *Associativity.*

Figure 1.4: Some graphic proofs of the proposition (1.15).

point of the curve, simply as follows:

$$[m]P = \begin{cases} \overbrace{P + \cdots + P}^{m \text{ terms}} & \text{if } m > 0 \\ \underbrace{-P - \cdots - P}_{m \text{ terms}} & \text{if } m < 0 \end{cases}$$
$$[0]P = O.$$

A nice application of this simple definition is the *elliptic curve cryptography* (ECC): given an elliptic curve E defined by the Weierstrass equation $y^2 = x^3 + ax + b$ on some finite field, when we sum two points of E (or sum a point to itself) we obtain a new point of E whose location is not immediate from the location of the initial summands. If we repeat the process a large number of times we obtain a point that may be essentially everywhere on the curve. Reverting this process, i.e., given the points P and $Q = nP$ on the curve with n unknown integer, determining n can only be done by trying all the possible integers n. If this number is sufficiently large this process is computationally intractable. The security of modern ECC depends exactly on the intractability of determining the integer n from $Q = nP$ given known values of Q and P. This is known as the *elliptic curve discrete logarithm problem*, by analogy to other cryptographic systems.

To go deep to the heart of this subject, see "*Guide to elliptic curve cryptography*", Hankerson, Menezes, Vanstone.

Now we want to derive explicit formulas for the group law on E: given the coordinates of two points of E we want to find a way to express their sum point in

terms of their coordinates. We state the following *group law algorithm*.

Theorem 1.16 (Group law algorithm)**.** [6, III.2.3, p. 53]. *Let E be an elliptic curve given by the Weierstrass equation*

$$E\colon F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

(a) *Let $P_0 = (x_0, y_0) \in E$, then the opposite point has coordinates*

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3) \quad \textit{(negation formula).}$$

(b) *Let $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$, such that $P_1 + P_2 = P_3$. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = O$. Otherwise, we define λ and ν by the following formulas:*

	λ	ν
if $x_1 \neq x_2$:	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
if $x_1 = x_2$:	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Then $y = \lambda x + \nu$ is the equation of the line through P_1 and P_2 (or the equation of the tangent line to E if $P_1 = P_2$). The point $P_1 + P_2 = P_3$ has coordinates

$$x_3 = \lambda^2 + a_1\lambda - a_2x_1 - x_2, \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Proof. (a) Let $P_0 = (x_0, y_0) \in E$, in order to compute $-P_0$ we follow the proof of proposition (1.15.d): we take the line L through P_0 and O and find the third point of intersection with E. Namely, the equation of the line L is $x - x_0 = 0$, we substitute it into the Weierstrass equation of the curve and get

$$F(x_0, y) = y^2 + a_1x_0y + a_3y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0$$

whose roots are y_0, already known, and y_0', which is the value we are looking for, so we can write also as

$$\begin{aligned} F(x_0, y) &= c(y - y_0)(y - y_0') \\ &= cy^2 - c(y_0 + y_0')y + cy_0y_0' \end{aligned}$$

and equating the coefficients of the two expressions we deduce that $c = 1$ from the coefficient of y^2, and $y_0' = -y_0 - a_1x_0 - a_3$ from the coefficient of y. So $-P_0 = (x_0, y_0') = (x_0, -y_0 - a_1x_0 - a_3)$ and this proves the statement.

(b) Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points of E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then by the previous computation $P_1 + P_2 = O$. Otherwise the line through P_1 and P_2, or the tangent line if the two points coincide, has equation of the form $L\colon\ y = \lambda x + \nu$, where the values of λ and ν are exactly as in the statement. Then, substituting the equation into the Weierstrass equation of E gives

$$\begin{aligned} F(x,\lambda x+\nu) &= (\lambda x+\nu)^2 + a_1x(\lambda x+\nu) + a_3(\lambda x+\nu) - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0 \\ &\Leftrightarrow -x^3 + (\lambda^2+a_1\lambda-a_2)x^2 + (2\lambda\nu+a_1\nu+a_3\lambda-a_4)x + \nu^2 + a_3\nu - a_6 = 0. \end{aligned}$$

On the other hand, this polynomial has roots x_1, x_2, x_3, where $P'_3 = (x_3, y'_3)$ is the third point of intersection of L and E. So again, we can write also

$$\begin{aligned} F(x, \lambda x + \nu) &= c(x - x_1)(x - x_2)(x - x_3) \\ &= cx^3 - c(x_1 + x_2 + x_3)x^2 + c(x_1x_2 + x_2x_3 + x_1x_3)x - cx_1x_2x_3 \end{aligned}$$

and equating the coefficients of the two expressions we obtain $c = -1$ from the coefficient of x^3 and $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ from the coefficient of x^2. We substitute the value of x_3 into the equation of the line L and get the second coordinate of the point P'_3, $y'_3 = \lambda x_3 + \nu$. Finally, since P'_3 is the third point of intersection of the line with E, after P_1 and P_2, then (1.15.a) tells us that $P_1 + P_2 + P'_3 = O$, so $P_1 + P_2 = -P'_3$. Thus, to compute $P_3 = P_1 + P_2$ we need to apply the negation formula to $P'_3 = (x_3, \lambda x_3 + \nu)$, namely

$$P_3 = P_1 + P_2 = -P'_3 = (x_3, -y'_3 - a_1x_3 - a_3) = (x_3, -(\lambda + a_1)x_3 - \nu - a_3)$$

and we obtain the desired result.

□

Using the explicit formulas, as we already noticed above, it is possible to prove directly (1.15.e), namely the associativity of the composition law over E.

1.1.4 Elliptic curves as abelian groups

Let E be a smooth curve of genus one, for example we may consider the curves defined by the non-singular Weierstrass equations described above. We have also seen that such curves can be given the structure of abelian group. In order to make a set into a group we need to choose the identity element: this leads to the following definition.

Definition 1.17 (Elliptic curve)**.** An *elliptic curve* is a pair (E, O) where E is a non-singular curve of genus one and $O \in E$. The elliptic curve E is *defined over* K if E is defined over K as a curve and $O \in E(K)$, we write it as E/K.

We generally denote the elliptic curve by E, the point O is usually understood.

In order to connect this definition with the material in the previous sections, we need to show that every elliptic curve can be written as a plane cubic, and conversely every smooth Weierstrass plane cubic curve is an elliptic curve. The key tool that allows us to prove this facts is the *Riemann-Roch theorem*.

Proposition 1.18. [6, III.3.1, p. 59]. *Let E be an elliptic curve defined over K. We denote by $K(E)$ be the* function field of E over K*, namely, the field of the rational functions on E (ratio of polynomials).*

(a) *There exist functions $x, y \in K(E)$ such that the map $\phi\colon E \longrightarrow \mathbb{P}^2$, $\phi = [x, y, 1]$ gives an isomorphism of E/K onto a curve given by a Weierstrass equation*

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

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

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

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

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

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

Proof. See [6, III.3.1, p. 59]. □

From these facts we can deduce the following

Remark 1.19. Let E/K be an elliptic curve with Weierstrass coordinate functions x and y, then $K(E) = K(x, y)$ and $[K(E)\colon K(x)] = 2$.

Remark 1.20. [6, III.3.2, p. 61]. We note that (1.18.b) does not imply that, if two Weierstrass equations have coefficients in a given field K, then every change of variables mapping one to the other has coefficients in K. For instance, the

Weierstrass equation $y^2 = x^3 - x$ has coefficients in $K = \mathbb{Q}$, but it is mapped to itself by the substitution

$$x = -x', \qquad y = \sqrt{-1}y'$$

which has not coefficients in $\mathbb{Q}$.

Finally one can prove a fundamental fact about the addition law on an elliptic curve: it is a morphism.

Theorem 1.21. [6, III.3.6, p. 64]. *Let E/K be an elliptic curve. Then the equations giving the explicit form of the composition law on E define morphisms*

$$\begin{aligned} +\colon E \times E &\longrightarrow E, \\ (P_1, P_2) &\longmapsto P_1 + P_2 \end{aligned} \qquad \textit{and} \qquad \begin{aligned} -\colon E &\longrightarrow E \\ P &\longmapsto -P \end{aligned}$$

Proof. See [6, III.3.6, p. 64]. □

1.1.5 Isogenies

After the geometry of an elliptic curve, we need to study the maps between curves. Since an elliptic curve has a distinguished zero point, it is natural to single out the maps that respect this property.

Let K be a field, give a curve E/K we denoted by $K(E)$ be the *function field of E over K*, namely, the field of the rational functions on E (ratio of polynomials).

Definition 1.22 (Isogeny)**.** Let E_1 and E_2 be two elliptic curves. An *isogeny from E_1 to E_2* is a morphism

$$\phi : E_1 \longrightarrow E_2 \quad \text{satisfying } \phi(O) = O$$

Two elliptic curves E_1 and E_2 are said to be *isogenous* if there exists an isogeny from E_1 to E_2 with $\phi E_1 \neq \{O\}$.

We recall that the theorem [6, II.2.3, p. 20] tells us that a morphism of curves is either constant or surjective. From this fact, it follows that an isogeny satisfies either $\phi(E_1) = \{O\}$ or $\phi(E_1) = E_2$. Thus, except for the zero isogeny defined by $[0](P) = O$ for all $P \in E_1$, every other isogeny is a finite map of curves. Hence we obtain the injection of function fields

$$\phi^*\colon \bar{K}(E_2) \longrightarrow \bar{K}(E_1), \qquad f \mapsto \phi^*(f) = f \circ \phi.$$

Moreover, the theorem [6, II.2.4.a, p. 20] tells us that $\bar{K}(C_1)$ is a finite extension of the field $\phi^*(\bar{K}(C_2))$. The *degree of* ϕ, denoted by $\deg\phi$, is the degree of the finite extension of fields $\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$, namely

$$\deg(\phi) = [\bar{K}(C_1)\colon \phi^*(\bar{K}(E_2))]$$

and similarly we define the *separable degree* of ϕ, $\deg_s\phi$, and *inseparable degree* of ϕ, $\deg_i\phi$, as the separable and inseparable degree of the field extension, respectively. We also refer to the map ϕ as being *separable, inseparable, purely inseparable* according to the corresponding property of the field extension. Further, by convention we set $\deg[0] = 0$, so for all chains of isogenies $E_1 \overset{\phi}{\to} E_2 \overset{\psi}{\to} E_3$

$$\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi).$$

Elliptic curves are abelian groups, so the maps between them form groups: we denote the set of isogenies from E_1 to E_2 by

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \longrightarrow E_2\}$$

and define the sum of two isogenies $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ is defined pointwise as

$$(\phi + \psi)(P) = \phi(P)\,\psi(P) \qquad \text{for all } P \in E_1$$

and the theorem (1.21) says that $\phi + \psi$ is a morphism, so it is an isogeny. This proves that $\mathrm{Hom}(E_1, E_2)$ is a group.

If $E_1 = E_2 = E$ we can also compose isogenies, so $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is the *endomorphism ring of* E, a ring whose addition law is as given above and whose multiplication is the composition of isogenies, namely for all $\phi, \psi \in \mathrm{End}(E)$

$$(\phi\psi)(P) = \phi(\psi(P)) \qquad \text{for all } P \in E.$$

$\mathrm{End}(E)$ is an important invariant of the elliptic curve E. The invertible elements of the endomorphism ring form the *automorphism group of* E, denoted by $\mathrm{Aut}(E)$.

If the curves E_1, E_2, E are defined over a field K, we can restrict attention to those isogenies that are defined over K, so the corresponding groups of isogenies are denoted by

$$\mathrm{Hom}_K(E_1, E_2), \qquad \mathrm{End}_K(E), \qquad \mathrm{Aut}_K(E).$$

In particular, the remark (1.20) shows that $\mathrm{Aut}(E)$ may be strictly larger than $\mathrm{Aut}_K(E)$.

An isogeny is a map between elliptic curve that sends O to O. Since an elliptic curve is a group, it might seem more natural to focus on those isogenies that are group homomorphisms. However it turns out that every isogeny is automatically a homomorphism.

Theorem 1.23. [6, III.4.8, p. 71]. *Let $\phi\colon E_1 \longrightarrow E_2$ be an isogeny, then*

$$\phi(P+Q) = \phi(P) + \phi(Q) \qquad \text{for all } P, Q \in E_1.$$

Proof. See [6, III.4.8, p. 71]. □

Corollary 1.24. [6, III.4.9, p. 72]. *Let $\phi\colon E_1 \longrightarrow E_2$ be a non-zero isogeny, then* $\ker(\phi) = \phi^{-1}(O)$ *is a finite group.*

Proof. See [6, III.4.9, p. 72]. □

Example 1.25. [6, III.4.7, p. 71]. We can easily show that any morphism between elliptic curves is the composition of an isogeny and a translation. Let E/K be an elliptic curve and let $Q \in E$. Then we can define a *translation-by-Q map*

$$\tau_Q\colon E \longrightarrow E, \qquad P \mapsto P + Q$$

that is clearly an isomorphism, with inverse the translation τ_{-Q}, but if $Q \neq O$ it is not an isogeny. Let E_1, E_2 be two elliptic curves and consider an arbitrary morphism $F\colon E_1 \longrightarrow E_2$ between them. The composition

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

sends O into O by construction, so it is an isogeny. This proves that any morphism F between elliptic curves can be written as the composition of an isogeny and a translation, namely $F = \tau_{F(O)} \circ \phi$.

Definition 1.26 (Multiplication-by-m isogeny)**.** For each $m \in \mathbb{Z}$ we define the *multiplication-by-m isogeny* $[m]\colon E \longrightarrow E$ in the natural way: for each $P \in E$

$$\begin{aligned} [m](P) &= \underbrace{P + \cdots + P}_{m \text{ terms}} && \text{if } m > 0 \\ [m](P) &= [-m](-P) && \text{if } m < 0 \\ [0](P) &= O \end{aligned}$$

Using the theorem (1.21), an easy induction shows that $[m]$ is a morphism and since clearly it sends O to O so it is an isogeny. Moreover, if E is defined over K then also $[m]$ is defined over K. We start the study of the group of isogenies by showing that, if $m \neq 0$, then the multiplication-by-m map is non-constant, and then we deduce some characteristics of the endomorphism ring of E.

Proposition 1.27. [6, III.4.2, p. 68].

(a) *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$, then the multiplication-by-m map $[m]\colon E \longrightarrow E$ is non-constant.*

(b) *Let E_1 and E_2 be elliptic curves, then the group of isogenies $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.*

(c) *Let E be an elliptic curve, then the endomorphism ring $\mathrm{End}(E)$ is a ring of characteristic 0 with no zero divisors, not necessarily commutative.*

Proof. (a) We start by showing that $[2] \neq [0]$. The *duplication formula* (proved in [6, III.2.3.d, p. 54]) says that if a point $P = (x, y) \in E$ has order 2, then it must satisfy

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

where the coefficients are defined in the first section. If $\mathrm{char(K)} \neq 2$, this shows immediately that there are only finitely many such points; if $\mathrm{char(K)} = 2$ the only way to have $[2] = [0]$ is for the cubic polynomial to be identically zero, which means $b_2 = 0 = b_6$, that implies that $\Delta = 0$. Hence in all cases we have $[2] \neq [0]$. Now, using the fact that $[mn] = [m] \circ [n]$, we are reduced to study only the case with m odd.

Assume that $\mathrm{char(K)} \neq 2$, then one can check that the polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$ does not divide the polynomial $x^3 - b_2x^2 - 2b_6x - b_8$ (otherwise we get again $\Delta = 0$). Hence we can find an $x_0 \in \bar{K}$ such that the former polynomial vanishes to higher order at x_0 than the latter. Choosing $y_0 \in \bar{K}$ so that $P_0 = (x_0, y_0)$ is a point of the curve E, the duplication formula says that $[2]P_0 = O$, in other words, E has a non-trivial point P_0 of order 2. Then for odd integers m we necessarily have $[m]P_0 = P_0 \neq O$, so clearly $[m] \neq [0]$. If $\mathrm{char(K)} = 2$ we can proceed as above, using a *triplication formula* (see [6, III.Exercise 3.2, p. 104]) to produce a point of order 3.

(b) Suppose that $\phi \in \mathrm{Hom}(E_1, E_2)$ and $m \in \mathbb{Z}$ satisfy $[m] \circ \phi = [0]$, so their degrees satisfy $\deg([m])\deg(\phi) = 0$. So either $m = 0$, or else (a) implies that $\deg([m]) \geq 1$, in which case we must have $\phi = [0]$.

(c) From (b), it follows that the endomorphism ring $\mathrm{End}(E)$ has characteristic 0. Suppose that $\phi, \psi \in \mathrm{End}(E)$ satisfy $\phi \circ \psi = [0]$, then their degree satisfy

$$\deg(\phi)\deg(\psi) = \deg(\phi \circ \psi) = 0$$

so either $\phi = [0]$ or $\psi = [0]$. Therefore $\mathrm{End}(E)$ is an integral domain.

□

Definition 1.28 (m-torsion subgroup, torsion subgroup of E)**.** Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The *m-torsion subgroup of E* is the set of points of E of order m, namely

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

The *torsion subgroup of E* is the set of points of E of finite order,

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

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

The most important fact about the multiplication-by-m map is that it has degree $\deg[m] = m^2$, it will be proven later. From this property one can deduce the structure of the finite subgroup of m-torsion $E[m]$.

1.1.6 The invariant differential

We first recall some definitions and properties of the vector space of differential forms of a curve C, then we consider in particular the invariant differential of an elliptic curve E.

Definition 1.29 (Space of differential forms on a curve)**.** Let C be a curve, the *space of (meromorphic) differential forms on C*, denoted by Ω_C, is the $\bar{K}$-vector space generated by symbols of the form dx for $x \in \bar{K}(C)$ that satisfy the following relations: for all $x, y \in \bar{K}(C)$, for all $a \in \bar{K}$

(a) $d(x + y) = dx + dy$;
(b) $d(xy) = xdy + ydx$;
(c) $da = 0$.

Let $\phi\colon C_1 \longrightarrow C_2$ be a non-constant map of curves, the associated function field map $\phi^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ induces a map on differentials, that we denote again as

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}, \qquad \sum f_i\, dx_i \mapsto \phi^*\Big(\sum f_i\, dx_i\Big) = \sum (\phi^* f_i)\, d(\phi^* x_i)$$

and call it the *pull-back of omega via ϕ*. This map provides a useful criterion for determining when the map ϕ is separable: in fact proposition [6, II.4.2, p. 30] tells us that

(a) Ω_C is a 1-dimensional $\bar{K}$-vector space;
(b) if $x \in \bar{K}(C)$, then dx is a $\bar{K}(C)$-basis for Ω_C if and only if $\bar{K}(C)/\bar{K}(x)$ is a finite separable extension;
(c) given ϕ as above, then it is separable if and only if $\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$ is injective (equivalently, non-zero).

Let E/K be an elliptic curve given by the usual Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We have seen in proposition (1.6) that the invariant differential

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

has neither zeros nor poles. The following proposition tells us that it is also invariant under translation.

Proposition 1.30. [6, III.5.1, p. 76]. *Let E and ω be as above, let $Q \in E$ and let $\tau_Q\colon E \longrightarrow E$ be the translation-by-Q. Then*

$$\tau_Q^*\omega = \omega.$$

Proof. See [6, III.5.1, p. 76]. □

We know that differential calculus is a linearization tool: the invariant differential is useful to linearize the, otherwise quite complicate, addition law on the elliptic curve.

Theorem 1.31. [6, III.5.2, p. 77]. *Let E, E' be elliptic curves, let ω be an invariant differential on E and let $\phi, \psi\colon E' \longrightarrow E$ be isogenies. Then the pull-back is compatible with the sum of isogenies:*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

Proof. See [6, III.5.2, p. 77] □

Corollary 1.32. [6, III.5.3, p. 79]. *Let ω be an invariant differential on an elliptic curve E, Let $m \in \mathbb{Z}$. Then the pull-back of omega via the multiplication-by-m isogeny is simply the multiplication-by-m of the differential:*

$$[m]^*\omega = m\omega.$$

Proof. We prove it by induction over m.

The assertion is true for $m = 0$, since [0] is the constant map; it is also true for $m = 1$, since [1] is the identity map.

Using the theorem (1.31) with $\phi = [m]$ and $\psi = [1]$ and applying induction we obtain

$$[m+1]^*\omega = [m]^*\omega + \omega = m\omega + \omega = (m+1)\omega.$$ □

As an example of the utility of the invariant differential, we can give a less computational proof of proposition (1.27.a).

Corollary 1.33. [6, III.5.4, p. 79]. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$. Assume that $m \neq 0$ in K, then the multiplication-by-m map on E is a finite separable endomorphism.*

Proof. Let ω be an invariant differential on E. Then corollary (1.32) and the assumption on m imply that $[m]^*\omega = m\omega \neq 0$, so certainly $[m] \neq 0$. Hence $[m]$ is finite, so by proposition [6, II.4.2, p. 30], already seen at the beginning of this section, $[m]$ is separable. □

As a second application of the theorem (1.31) and the corollary (1.32), we examine when a linear combination involving the Frobenius morphism is separable. In order to do this, we first recall the definition of Frobenius map and some of its basic properties.

Assume that k is a field of $\mathrm{char}(k) = p > 0$, let $q = p^r$ for some r natural. For any polynomial f with coefficients in k, let $f^{(q)}$ be the polynomial obtained by raising each coefficient of f to its q^{th}- power. The, for any curve C/k defined by a polynomial f we can define the curve $C^{(q)}/k$, given by the polynomial $f^{(q)}$.

Definition 1.34 (Frobenius morphism)**.** We define the *q^{th}-power Frobenius morphism* the natural map

$$\phi\colon C \longrightarrow C^{(q)}, \qquad P \mapsto P^q$$

namely, ϕ sends any point P of C to the point of $C^{(q)}$ whose coordinates are the q^{th}-power of the coordinates of P.

The next proposition shows the basic properties of the *Frobenius* map:

Proposition 1.35. [6, II.2.11, p. 25]. *With notations as above:*
(a) ϕ *is purely inseparable;*
(b) $\deg\phi = q$.

Proof. See [6, II.2.11, p. 25]. □

Finally, an important consequence of those basic properties of ϕ, which will be useful later, is the following:

Corollary 1.36. [6, II.2.12, p. 26]. *Every map* $\psi\colon C_1 \longrightarrow C_2$ *of curves over a field* k *of* $\mathrm{char}(k) = p > 0$ *factors as*

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

where $q = \deg_i\psi$ *is the inseparable degree of* ψ, ϕ *is the* q^{th}*-power Frobenius morphism and* λ *is a separable map.*

Proof. See [6, II.2.12, p. 26]. □

Now, we can go back to the second application of theorem (1.31) and corollary (1.32) we were talking about.

Corollary 1.37. [6, III.5.5, p. 79]. *Let* E *be an elliptic curve defined over a finite field* $\mathbb{F}_q$ *of characteristic* p*, let* $\phi\colon E \longrightarrow E$ *be the* q^{th}*-power Frobenius morphism and let* $m, n \in \mathbb{Z}$*. Then the map*

$$m + n\phi\colon E \longrightarrow E$$

is separable if and only if $p \nmid m$*. In particular, the map* $1 - \phi$ *is separable.*

Proof. See [6, III.5.5, p. 79]. □

Corollary 1.38. [6, III.5.6, p. 80]. *Let* E/K *be an elliptic curve and let* ω *be a non-zero invariant differential on* E*. We define a map*

$$\mathrm{End}(E) \longrightarrow \bar{K}, \qquad \phi \mapsto a_\phi \quad \text{such that } \phi^*\omega = a_\phi\omega.$$

Then:
(a) The map $\phi \mapsto a_\phi$ *is a ring homomorphism;*
(b) The kernel of $\phi \mapsto a_\phi$ *is the set of inseparable endomorphisms of* E*;*
(c) If $\mathrm{char}(K) = 0$ *then* $\mathrm{End}(E)$ *is a commutative ring.*

Proof. See [6, III.5.6, p. 80]. □

1.1.7 The endomorphism ring

Let E be an elliptic curve. In this section we characterize which rings may occur as the endomorphism ring of E.

Definition 1.39 (Order of a $\mathbb{Q}$-algebra)**.** Let $\mathcal{K}$ be a (non-necessarily commutative) $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An *order $\mathcal{R}$ of $\mathcal{K}$* is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Definition 1.40 (Quaternion algebra)**.** A *quaternion algebra* is an algebra of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \beta\alpha = -\alpha\beta.$$

Theorem 1.41. [6, III.9.3, p. 100]. *Let $\mathcal{R}$ be a ring of characteristic* 0 *having no zero divisors, and the following properties:*

i. *$\mathcal{R}$ has rank at most four as a $\mathbb{Z}$-module;*
ii. *$\mathcal{R}$ has an anti-involution satisfying*

$$\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}, \qquad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \qquad \hat{\hat{\alpha}} = \alpha, \qquad \hat{a} = a \ \text{ for } a \in \mathbb{Z} \subset \mathcal{R}.$$

iii. *For $\alpha \in \mathcal{R}$, the product $\alpha\hat{\alpha}$ is non-negative integer, and $\alpha\hat{\alpha} = 0$ if and only if $\alpha = 0$.*

Then $\mathcal{R}$ is one of the following types of rings:

a. *$\mathcal{R} \cong \mathbb{Z}$;*
b. *$\mathcal{R}$ is an order in an imaginary quadratic extension of $\mathbb{Q}$;*
c. *$\mathcal{R}$ is an order in a quaternion algebra over $\mathbb{Q}$.*

Proof. See [6, III.9.3, p. 100]. □

Corollary 1.42. [6, III.9.4, p. 102]. *The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If* $\operatorname{char}(K) = 0$ *then only the first two are possible.*

Proof. From some properties of the isogenies (see [6, III.6.2, p. 83] and [6, III.6.3, p. 85]) and from (1.27.b) we know that the ring $\operatorname{End}(E)$ satisfies all the conditions needed to apply theorem (1.41). This proves the first part of the corollary. If $\operatorname{char}(K) = 0$, then the corollary (1.38.c) says that $\operatorname{End}(E)$ is commutative, so it cannot be an order in a quaternion algebra. □

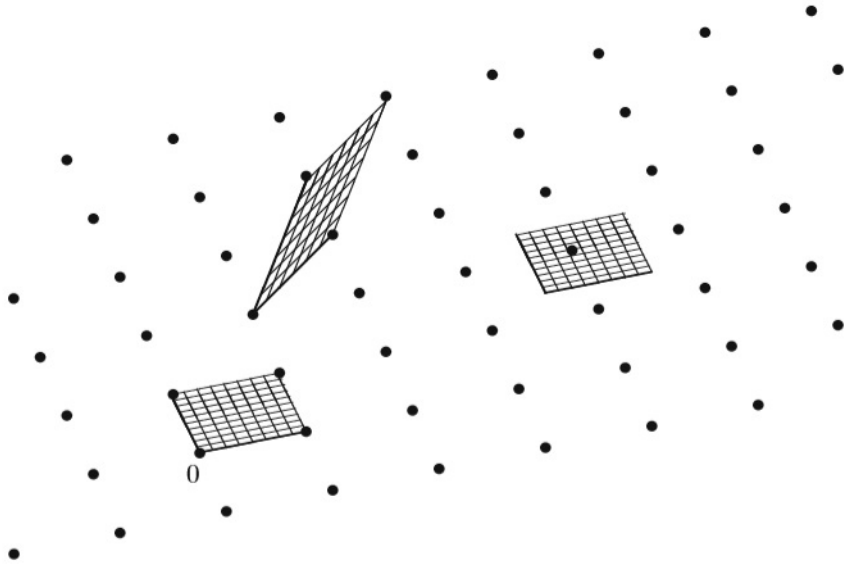


Figure 1.5: A lattice and three fundamental parallelograms.

1.2 Elliptic curves over $\mathbb{C}$

Our goal in this section is to study the space $\mathbb{C}/\Lambda$ for a given lattice Λ, known as the *complex torus induced by* Λ. We will show that it is isomorphic to $E_\Lambda(\mathbb{C})$ for a certain elliptic curve $E_\Lambda/\mathbb{C}$, then we will introduce the *uniformization theorem*, which says that every elliptic curve $E/\mathbb{C}$ is isomorphic to some E_Λ.

1.2.1 Elliptic functions over $\mathbb{C}$

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

Definition 1.43 (Elliptic function)**.** An *elliptic function relative to the lattice* Λ is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies

$$f(z+\omega) = f(z) \qquad \text{for all } z \in \mathbb{C} \text{ and all } \omega \in \Lambda.$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, and it is clearly a field.

In order to prove the next proposition we need the following

Definition 1.44 (Fundamental parallelogram)**.** A *fundamental parallelogram for* Λ is a set of the form

$$D = \{\, a + t_1\omega_1 + t_2\omega_2 \colon 0 \le t_1, t_2 < 1 \,\}$$

where $a \in \mathbb{C}$ and $\{\, \omega_1, \omega_2 \,\}$ is a basis for Λ.

Note that the definition of D implies that the natural map $D \to \mathbb{C}/\Lambda$ is bijective.

Proposition 1.45. [6, VI.2.1, p. 161]. *A holomorphic elliptic function, i.e. an elliptic function with no poles, is constant. Similarly, an elliptic function with no zeros is constant.*

Proof. Suppose that $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Let D be a fundamental parallelogram for Λ. The periodicity of f implies that

$$\sup_{z\in\mathbb{C}}|f(z)| = \sup_{z\in\bar{D}}|f(z)|$$

where $\bar{D}$ denotes the closure of D in $\mathbb{C}$. Since f is a continuous function and $\bar{D}$ is compact, then $|f(z)|$ is bounded on $\bar{D}$. Hence f is bounded on all of $\mathbb{C}$, so *Liouville's theorem* tells us that f is constant. This proves the first statement. Finally, if f has no zeros, then $1/f$ is holomorphic, hence constant. □

Let f be an elliptic function and let $\omega \in \mathbb{C}$. Then we can look at

$$\begin{aligned} \operatorname{ord}_\omega(f) &= \text{order of vanishing of } f \text{ at } \omega \\ \operatorname{res}_\omega(f) &= \text{residue of } f \text{ at } \omega. \end{aligned}$$

We can define those two quantities for any meromorphic function, the fact that f is elliptic implies that the order and the residue of f do not change if we replace ω with $\omega + \omega$ for any $\omega \in \Lambda$

Notation 1.46. We denote by $\sum_{\omega\in\mathbb{C}/\Lambda}$ a sum over $\omega \in D$. The value of the sum is actually independent on the choice of the fundamental parallelogram and only finitely many terms of the sum are non-zero.

With this notation it is easier to state the following theorem:

Theorem 1.47. [6, VI.2.2, p. 162]. *Le* $f \in \mathbb{C}(\Lambda)$ *be an elliptic function relative to the lattice* Λ*. Then*

$$\sum_{\omega\in\mathbb{C}/\Lambda} res_\omega(f) = 0, \qquad \sum_{\omega\in\mathbb{C}/\Lambda} ord_\omega(f) = 0, \qquad \sum_{\omega\in\mathbb{C}/\Lambda} ord_\omega(f)\omega \in \Lambda.$$

Proof. See [6, VI.2.2, p. 162]. □

Definition 1.48 (Order of an elliptic function)**.** The *order of an elliptic function* is its number of poles, counted with multiplicity, in a fundamental parallelogram. Equivalently, by the second relation in (1.47), the order can be defined as its number of zeros.

It is immediate to prove the following

Corollary 1.49. [6, VI.2.3, p. 164]. *A non-constant elliptic function has order at least* 2*.*

Proof. Suppose that $f(z)$ has order 1, i.e., it has a single pole. Then by the first relation in (1.47) the residue at the pole is necessarily 0, so $f(z)$ is actually holomorphic. Then we can conclude by applying the theorem (1.45) that $f(z)$ is constant. □

Now we want to construct some useful non-constant elliptic functions. From the previous corollary (1.49), we know that any such function has order at least 2, so we look for a function with a pole of order 2 at $z = 0$.

Definition 1.50 (Weierstrass $\wp$-function)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function relative to* Λ is defined by the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big).$$

For notational convenience, if the lattice Λ has been fixed we write only $\wp(z)$. One can prove the following results, given in [6, VI.3.1, p. 165]: the series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$; moreover, the series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles, and lastly the $\wp$-function is an even elliptic function.

Next, one can show that every elliptic function is a rational function on the Weierstrass $\wp$-function and its derivative.

Theorem 1.51. [6, VI.3.2, p. 166]. *Let $\Lambda \subset \mathbb{C}$ be a lattice, then*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$$

i.e., every elliptic function is a rational combination of $\wp$ and $\wp'$.

Proof. See [6, VI.3.2, p. 166]. □

We next derive the Laurent series expansion for $\wp(z)$ around $z = 0$, from which we will deduce the fundamental algebraic relation satisfied by $\wp(z)$ and $\wp'(z)$.

Theorem 1.52. [6, VI.3.5, p. 169].

(a) *The Laurent series for $\wp(z)$ around $z = 0$ is given by*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}$$

where $G_{2n} = G_{2n}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2n}$ is the Eisenstein series of weight $2n$ for Λ.

(b) *For all $z \in \mathbb{C} \setminus \Lambda$, the Weierstrass $\wp(z)$-function and its derivative satisfy the relation*

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

Proof. (a) For all z with $|z| < |\omega|$ we have

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}}.$$

Substituting this formula into the series for $\wp(z)$ and reversing the order of summation gives

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}} \right) \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-(n+2)} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n G_{n+2} \qquad \text{and necessarily } n \text{ must be even} \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) z^{2k} G_{2k+2}
\end{aligned}$$

so we obtain the desired result.

(b) We write out the first few terms of various Laurent expansions:

$$\begin{aligned}\wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + \dots\\ \wp(z)^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + \dots\\ \wp(z) &= z^{-2} + 3G_4z^2 + \dots\end{aligned}$$

and comparing these expansions we see that the function

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

is holomorphic at $z = 0$ and satisfies $f(0) = 0$. But $f(z)$ is an elliptic function relative to the lattice Λ and from the properties of the $\wp(z)$-function it follows that it is holomorphic away from Λ. So $f(z)$ is a holomorphic elliptic function. Then the proposition (1.45) says that $f(z)$ is constant, and the fact that $f(0) = 0$ tells us that it is identically zero.

□

Notation 1.53. It is standard notation to set

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

Then the algebraic relation satisfied by $\wp(z)$ and $\wp'(z)$ is

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Let $E/\mathbb{C}$ be an elliptic curve. The group law $E \times E \longrightarrow E$ is given by everywhere locally defined rational functions, by (1.21), so we see in particular that $E = E(\mathbb{C})$ is a *complex Lie group*, i.e., it is a complex manifold with a group law given locally by complex analytic functions. Similarly, if $\Lambda \subset \mathbb{C}$ is a lattice, then $\mathbb{C}/\Lambda$ with its natural addition is a complex Lie group.

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

Proposition 1.54. [6, VI.3.6, p. 170]. *Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to the lattice $\Lambda \subset \mathbb{C}$.*

(a) *The polynomial $f(x) = 4x^3 - g_2x - g_3$ has distinct roots, so its discriminant $\Delta(\Lambda) = 16(g_2^3 - 27g_3^2)$ is non-zero;*

(b) *Let $E/\mathbb{C}$ be the elliptic curve $E\colon y^2 = 4x^3 - g_2x - g_3$. Then the map*

$$\phi\colon \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \qquad z \mapsto [\wp(z), \wp'(z), 1]$$

is a complex analytic isomorphism of complex Lie groups, i.e., it is an isomorphism of Riemann surfaces that is also a group homomorphism.

Proof. See [6, VI.3.6, p. 170]. □

Then we need to investigate complex analytic maps between complex tori. It turns out that they all have a particular simple form and that the maps they induce on the corresponding elliptic curves are isogenies, i.e., they are given by rational functions.

Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$, and suppose that $\alpha \in \mathbb{C}$ has the property that $\alpha\Lambda_1 \subset \Lambda_2$. Then the scalar multiplication by α induces a well-defined holomorphic homomorphism

$$\phi_\alpha\colon \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad z \mapsto \phi_\alpha(z) = \alpha z \pmod{\Lambda_2}.$$

The next result tells us that these are essentially the only holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$.

Theorem 1.55. [6, VI.4.1, p. 171].

(a) *With notation as above, the association*

$$\begin{array}{ccc} \{\alpha \in \mathbb{C}\colon \alpha\Lambda_1 \subset \Lambda_2\} & \to & \left\{ \begin{array}{c} \textit{holomorphic maps} \\ \phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \phi(0) = 0 \end{array} \right\} \\ \alpha & \mapsto & \phi_\alpha \end{array}$$

is a bijection.

(b) *Let E_1 and E_2 be elliptic curves corresponding to lattices Λ_1 and Λ_2 respectively. Then the natural inclusion*

$$\{\textit{isogenies } \phi\colon E_1 \longrightarrow E_2\} \to \left\{ \begin{array}{c} \textit{holomorphic maps} \\ \phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \phi(0) = 0 \end{array} \right\}$$

is a bijection.

Proof. (a) We first prove that the association is *injective*: if $\phi_\alpha = \phi_\beta$ then

$$\alpha z = \beta z \pmod{\Lambda_2} \quad \text{for all } z \in \mathbb{C}.$$

Hence, the map $z \mapsto (\alpha - \beta)z$ sends $\mathbb{C}$ to Λ_2, which is discrete, so the map must be constant. Necessarily $\alpha = \beta$ and this shows the injectivity.

Next, we prove the *surjectivity*: let $\phi\colon \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ be a holomorphic map with $\phi(0) = 0$. Then, since $\mathbb{C}$ is simply connected, then we can lift ϕ to a holomorphic map $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ with $f(0) = 0$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\ f\ } & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\ \phi\ } & \mathbb{C}/\Lambda_2 \end{array}$$

Thus $f(z + \omega) \equiv f(z) \pmod{\Lambda_2}$ for all $\omega \in \Lambda_1$ and for all $z \in \mathbb{C}$. Since Λ_2 is discrete, the difference $f(z + \omega) - f(z)$ must be independent from z, so differentiating we obtain

$$f'(z + \omega) = f'(z) \qquad \text{for all } \omega \in \Lambda_1 \text{ and for all } z \in \mathbb{C}$$

and this means that $f'(z)$ is a holomorphic elliptic function. But then proposition (1.45) tells us that $f'(z)$ is constant, so $f(z) = \alpha z + \gamma$ for some $\alpha, \gamma \in \mathbb{C}$. The assumption $f(0) = 0$ implies that $\gamma = 0$ and so $f(z) = \alpha z$, while the fact that $f(\Lambda_1) \subset \Lambda_2$ means that $\alpha\Lambda_1 \subset \Lambda_2$, hence $\phi = \phi_\alpha$. This completes the proof of the surjectivity of the correspondence.

(b) First we note that, since an isogeny is given locally by everywhere defined rational functions, i.e., an isogeny is a morphism, then the map induced between the corresponding complex tori is holomorphic. Thus, the association

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \text{Holomorphic maps}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$

is well defined and *injective*.

To prove the *surjectivity*: from (a), it suffices to consider a map of the form ϕ_α where $\alpha \in \mathbb{C}^\times$ satisfies $\alpha\Lambda_1 \subset \Lambda_2$. The induced map on Weierstrass equations is given by

$$E_1 \to E_2, \qquad [\wp(z;\Lambda_1), \wp'(z;\Lambda_1), 1] \mapsto [\wp(\alpha z;\Lambda_2), \wp'(\alpha z;\Lambda_2), 1]$$

so we must show that $\wp(\alpha z; \Lambda_2)$ and $\wp'(\alpha z; \Lambda_2)$ can be expressed as rational expressions in $\wp(z; \Lambda_1)$ and $\wp'(z; \Lambda_1)$. Using the fact that $\alpha\Lambda_1 \subset \Lambda_2$ we see that, for any $\omega \in \Lambda_1$

$$\wp(\alpha(z + \omega); \Lambda_2) = \wp(\alpha z + \alpha\omega; \Lambda_2) = \wp(\alpha z; \Lambda_2)$$

and similarly for $\wp'(\alpha z; \Lambda_2)$. Thus $\wp(\alpha z; \Lambda_2)$ and $\wp'(\alpha z; \Lambda_2)$ are in the field $\mathbb{C}(\Lambda_1)$ and the result follows from Theorem (1.51), which tells us that $\mathbb{C}(\Lambda_1) = \mathbb{C}(\wp(\alpha z; \Lambda_2), \wp'(\alpha z; \Lambda_2))$.

□

From this theorem, we can deduce a useful consequence.

Corollary 1.56. [6, VI.4.1.1, p. 173]. *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be elliptic curve corresponding to lattices Λ_1 and Λ_2 respectively. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are* homothetic*, i.e., there exists some $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$.*

Remark 1.57. Since the maps ϕ_α are homomorphisms, the previous corollary ensures that every complex analytic map from $E_1(\mathbb{C})$ to $E_2(\mathbb{C})$ taking O to O is necessarily a homomorphism. This is the analytic analogue of the theorem (1.23), which says that every isogeny of elliptic curves is a homomorphism.

1.2.2 Uniformization

The *uniformization theorem for elliptic curves* says that every elliptic curve over $\mathbb{C}$ is parametrized by elliptic functions. The most natural proof of this fact uses the theory of modular functions, that is, functions whose domain is the set of lattices in $\mathbb{C}$, for example the functions $g_2(\Lambda)$ and $g_3(\Lambda)$. In this section we only state the result and use it to make some useful deductions.

Theorem 1.58 (Uniformization Theorem)**.** [6, VI.5.1, p. 173]. *Let $A, B \in \mathbb{C}$ be complex numbers satisfying the condition $4A^3 - 27B^2 \neq 0$, then there exists a unique lattice $\Lambda \subset \mathbb{C}$ satisfying*

$$g_2(\Lambda) = A, \qquad g_3(\Lambda) = B.$$

Proof. See [7, I.4.3, p. 35]. □

Corollary 1.59. [6, VI.5.1.1, p. 173]. *Let $E/\mathbb{C}$ be an elliptic curve. There exist a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism*

$$\phi\colon \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad \phi(z) = [\wp(z;\Lambda), \wp'(z;\Lambda), 1]$$

of complex Lie groups.

Proof. The existence follows from the theorems (1.54.b) and (1.58), while the uniqueness is immediate from the corollary (1.56). □

We may observe, after these results, a useful category equivalence:

Theorem 1.60. [6, VI.5.3, p. 175]. *The following categories are equivalent:*

(a) $\left\{ \begin{array}{c} \textit{Objects: Elliptic curves over } \mathbb{C} \\ \textit{Maps: Isogenies} \end{array} \right\}$

(b) $\left\{ \begin{array}{c} \textit{Objects: Elliptic curves over } \mathbb{C} \\ \textit{Maps: Complex analytic maps taking } O \textit{ to } O \end{array} \right\}$

(c) $\left\{ \begin{array}{c} \textit{Objects: Lattices } \Lambda \subset \mathbb{C}\textit{, up to homothety} \\ \textit{Maps: } \mathrm{Maps}(\Lambda_1, \Lambda_2) = \{\, \alpha \in \mathbb{C} \colon \alpha\Lambda_1 \subset \Lambda_2 \,\} \end{array} \right\}$

Proof. The one-to-one correspondence between elliptic curves over $\mathbb{C}$ and lattices $\Lambda \subset \mathbb{C}$, up to homothety follows from the proposition (1.54.b), the corollary (1.59) and the proposition [6, VI.5.2, p. 174]. The matchup of the maps in the three categories is precisely the theorem (1.55). □

We now use the uniformization theorem, in particular the corollary (1.59), to make some general deductions about elliptic curves over $\mathbb{C}$: actually, everything that we are about to prove would at least apply to those elliptic curves that occur in the theorem (1.54.b), the uniformization theorem merely says that this class of curves includes every elliptic curve over $\mathbb{C}$.

Proposition 1.61. [6, VI.5.4, p. 175]. *Let $E/\mathbb{C}$ be an elliptic curve and let $m \geq 1$ be an integer.*

(a) *There is an isomorphism of abstract groups*

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

(b) *The multiplication-by-m map $[m]\colon E \longrightarrow E$ has degree m^2.*

Proof. (a) From the corollary (1.59), we know that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Hence

$$E[m] \cong \left(\frac{\mathbb{C}}{\Lambda}\right)[m] \cong \frac{\frac{1}{m}\Lambda}{\Lambda} \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^2.$$

(b) Since $\mathrm{char}(\mathbb{C}) = 0$ and the map $[m]$ is unramified, the degree of $[m]$ is equal to the number of points in $E[m] \cong [m]^{-1}\{O\}$.

□

Let $E/\mathbb{C}$ be an elliptic curve. Note that the theorem (1.55) allows us to identify $\mathrm{End}(E)$ with a certain subring of $\mathbb{C}$. Thus if $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then

$$\mathrm{End}(E) \cong \{\, \alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda \,\}.$$

Since Λ is unique up to homothety, this ring is independent of the choice of Λ. We use this description of $\mathrm{End}(E)$ to completely characterize the endomorphism rings that may occur.

Definition 1.62 (Order in a field)**.** Let $\mathcal{K}$ be a number field. An *order $\mathcal{R}$ in $\mathcal{K}$* is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Example 1.63. Let K be an imaginary quadratic field and let R_K be its ring of integers. Then, for each integer $c \geq 1$ the ring $\mathbb{Z} + cR_K$ is an order of K. In fact, we will see in the next chapter that these are all of the orders of K.

Theorem 1.64. [6, VI.5.5, p. 176]. *Let $E/\mathbb{C}$ be an elliptic curve, let ω_1 and ω_2 be generators for the lattice Λ associated to E. Then one of the following is true:*

(a) $\mathrm{End}(E) = \mathbb{Z}$*;*

(b) *The field $\mathbb{Q}(\omega_1/\omega_2)$ is an imaginary quadratic extension of $\mathbb{Q}$ and* $\mathrm{End}(E)$ *is isomorphic to an order in $\mathbb{Q}(\omega_1/\omega_2)$.*

Proof. Multiplying Λ by $\tau = \omega_1/\omega_2$ shows that Λ is homothetic to $\mathbb{Z} + \tau\mathbb{Z}$, so we may replace Λ by $\mathbb{Z} + \tau\mathbb{Z}$. Let

$$\mathcal{R} = \{\, \alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda \,\}$$

so $\mathcal{R} \cong \mathrm{End}(E)$, from (1.55). Then, for any $\alpha \in \mathcal{R}$, there are integers a, b, c, d such that

$$\alpha = a + b\tau, \qquad\qquad \alpha\tau = c + d\tau.$$

From these relations we can eliminate τ: using the latter we get $\tau = \frac{c}{\alpha - d}$ and substituting it into the former yields

$$\begin{aligned} \alpha = a + \frac{bc}{\alpha - d} &\Rightarrow \alpha(\alpha - d) = a(\alpha - d) + bc \\ &\Rightarrow \alpha^2 - (a + d)\alpha + ad - bc = 0 \end{aligned}$$

and this proves that $\mathcal{R}$ is an integral extension of $\mathbb{Z}$.

Now suppose that $\mathcal{R} \neq \mathbb{Z}$ and choose some $\alpha \in \mathcal{R} \setminus \mathbb{Z}$. Then, with notation as above, we have that $b \neq 0$, so substituting $\alpha = a + b\tau$ into the equation gives a non-trivial equation:

$$\begin{aligned}(a+b\tau)^2 - (a+d)(a+b\tau) + ad - bc = 0 &\Rightarrow\ b^2\tau^2 + (a-d)b\tau - bc = 0\\ &\Rightarrow\ b\tau^2 + (a-d)\tau - c = 0.\end{aligned}$$

It follows that $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ (in particular we note that $\tau \notin \mathbb{R}$). Finally, since $\mathcal{R} \subset \mathbb{Q}(\tau)$ and $\mathcal{R}$ is integral over $\mathbb{Z}$, it follows that $\mathcal{R}$ is an order in $\mathbb{Q}(\tau)$. □

Chapter 2

Complex multiplication

Most elliptic curves over $\mathbb{C}$ have only the multiplication-by-m endomorphisms. Suppose that $\operatorname{char}(K) = 0$, then the map $[\,\cdot\,]\colon \mathbb{Z} \longrightarrow \operatorname{End}(E)$ usually makes $\operatorname{End}(E) \cong \mathbb{Z}$, in other words the only endomorphisms of E are multiplication-by-m, for $m \in \mathbb{Z}$, but in some cases there may be extra endomorphisms. On the other hand, if K is a finite field, then $\operatorname{End}(E)$ is always larger than $\mathbb{Z}$, so there are always other endomorphisms.

2.1 Definition and basic properties

Definition 2.1 (Elliptic curve with CM)**.** An elliptic curve that possesses extra endomorphisms, i.e., such that $\operatorname{End}(E)$ is strictly larger than $\mathbb{Z}$, is said to have *complex multiplication*.

Elliptic curves with complex multiplication have many special properties, some of which we are going to discuss in the following chapters.

Example 2.2. Assume that $\operatorname{char}(K) \neq 2$ and let $\imath \in \bar{K}$ be a primitive fourth root of unity, i.e., $\imath^2 = -1$. Then, as we observed in the remark (1.20), the elliptic curve E/K given by the equation

$$E\colon y^2 = x^3 - x$$

has endomorphism ring $\operatorname{End}(E)$ strictly larger than $\mathbb{Z}$, since it contains a map given by

$$[\imath]\colon E \longrightarrow E, \qquad (x, y) \mapsto (-x, \imath y).$$

Thus E has complex multiplication.

Clearly, $[\imath]$ is defined over K if and only if $\imath \in K$. Hence even if E is defined over K, it may happen that $\mathrm{End}_K(E)$ is strictly smaller than $\mathrm{End}(E)$.

Continuing with the same example, we observe that

$$[\imath] \circ [\imath](x, y) = [\imath](-x, \imath y) = (x, -y) = -(x, y)$$

so $[\imath] \circ [\imath] = [-1]$. There is thus a ring homomorphism

$$\mathbb{Z}[\imath] \longrightarrow \mathrm{End}(E), \qquad m + n\imath \mapsto [m] + [n] \circ [\imath]$$

If $\mathrm{char}(K) = 0$ this map is an isomorphism, so the ring of endomorphism of the curve E is (isomorphic to) the ring of Gaussian integers $\mathbb{Z}[\imath]$.

Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. We know, from the theorem (1.64), that $\mathrm{End}(E) \otimes \mathbb{Q}$ is isomorphic to a quadratic imaginary field K and that $\mathrm{End}(E)$ is an order in that field. In view of this, we may give the following definition.

Definition 2.3 (Complex multiplication by R or K)**.** If $\mathrm{End}(E) \cong R \subset \mathbb{C}$, then we say that E has *complex multiplication by R* or *by K*.

We denote by R_K the ring of integers of K and put our attention to elliptic curves with complex multiplication by R_K, in order to get a much easier theory.

If E has complex multiplication, there are two ways to embed the order $\mathrm{End}(E)$ into $\mathbb{C}$. One of these embeddings is described in the following proposition. We can easily observe that the corollary(1.32) is the particular case with $\alpha \in \mathbb{Z}$.

Proposition 2.4. [7, II.1.1, p. 97]. *let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring $R \subset \mathbb{C}$. There is a unique isomorphism*

$$[\,\cdot\,]\colon R \xrightarrow{\sim} \mathrm{End}(E), \qquad \alpha \mapsto [\alpha]\colon E \longrightarrow E$$

such that, for any invariant differential $\omega \in \Omega_E$ on E it holds

$$[\alpha]^*\omega = \alpha\omega.$$

Proof. Choosing a lattice $\Lambda \subset \mathbb{C}$ and an isomorphism $E \cong E_\Lambda$, it suffices to show the proposition for E_Λ.

We need to recall that, by the computations in the first chapter, an isomorphism has the effect of multiplying an invariant differential by a constant. Moreover we recall that, by the theorem (1.60), the endomorphism ring of E_Λ is isomorphic to

$\{\, \alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda \,\} = R \subset \mathbb{C}$. Each $\alpha \in R$ gives an isomorphism $[\alpha] \colon E_\Lambda \longrightarrow E_\Lambda$ determined by the commutativity of the following diagram:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\phi_\alpha} & \mathbb{C}/\Lambda \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ E_\Lambda & \longrightarrow & E_\Lambda \end{array}$$

We *claim* that the map $[\,\cdot\,] \colon R \xrightarrow{\sim} \mathrm{End}(E_\Lambda)$ satisfies $[\alpha]^*\omega = \alpha\omega$. To verify the claim, we observe that, given any two non-zero invariant differential on E_Λ, their quotient would be a translation invariant function, hence it would be constant, so those invariant differential are scalar multiples of one another. So, if we take any invariant differential $\omega \in \Omega_{E_\Lambda}$ and pull back via the isomorphism $f \colon \mathbb{C}/\Lambda \longrightarrow E_\Lambda$, we obtain a multiple of the invariant differential dz on $\mathbb{C}/\Lambda$, say $f^*\omega = c\,dz$. The commutativity of the diagram given above shows the desired result:

$$\begin{aligned} [\alpha]^*\omega &= (f^{-1})^* \circ \phi_\alpha^* \circ f^*(\omega) = (f^{-1})^* \circ \phi_\alpha^*(c\,dz) \\ &= (f^{-1})^*(c\alpha\,dz) = \alpha\omega. \end{aligned}$$ □

If the curve E with the isomorphism $[\,\cdot\,]$ satisfy the previous proposition, we say that the pair $(E, [\,\cdot\,])$ is *normalized*.

Corollary 2.5. [7, II.1.1.1, p. 98]. *Let $(E_1, [\,\cdot\,]_1)$ and $(E_2, [\,\cdot\,]_2)$ be two normalized elliptic curves with complex multiplication by R. Let $\phi \colon E_1 \to E_2$ be an isogeny. Then*

$$\phi \circ [\alpha]_1 = [\alpha]_2 \circ \phi \qquad \textit{for all } \alpha \in R.$$

Proof. Let $0 \neq \omega \in \Omega_{E_2}$ be an invariant differential. Then

$$\begin{aligned} (\phi \colon [\alpha]_{E_1})^*\omega &= [\alpha]_{E_1}^*(\phi^*\omega) \\ &= \alpha\phi^*\omega \quad \text{since } \phi^*\omega \text{ is an invariant differential on } E_1 \\ &= \phi^*(\alpha\omega) \\ &= \phi^*([\alpha]_{E_2}^*\omega) \\ &= ([\alpha]_{E_2} \circ \phi)^*\omega. \end{aligned}$$

Since we work in characteristic 0, every non-zero isogeny isogeny $E_1 \longrightarrow E_2$ is separable, so by the proposition [6, II.4.2.c, p. 30], already cited in the subsection (1.1.6), the map

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(\Omega_{E_1}, \Omega_{E_2}), \quad \psi \mapsto \psi^*$$

is injective. Therefore $\phi \colon [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi$. □

Theorem 2.6. [5, 3.2, p. 297]. *Let $E_1 = \mathbb{C}/\Lambda_1$, $E_2 = \mathbb{C}/\Lambda_2$ be two elliptic curves and suppose there exists a complex analytic homomorphism $f\colon E_1 \longrightarrow E_2$. Then there exists $\beta \in \mathbb{C}$ with $\beta\Lambda_1 \subset \Lambda_2$ such that f is induced by the map $z \mapsto \beta z$ on $\mathbb{C}$.*

Proof. This theorem states exactly the surjectivity of the one-to-one corrispondence

$$\begin{array}{ccc} \{\beta \in \mathbb{C}\colon \beta\Lambda_1 \subset \Lambda_2\} & \to & \left\{ \begin{array}{c} \text{holomorphic maps} \\ \phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \text{with } \phi(0) = 0 \end{array} \right\} \\ \beta & \mapsto & \phi_\beta \end{array}$$

where $\phi_\beta\colon \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$, $\phi_\beta(z) = \beta z \pmod{\Lambda_2}$, proved in the theorem (1.55.a). □

We fix K an imaginary quadratic field and denote by R_K its ring of integers. By the definition (1.62) it is easy to see that R_K is an order in K and contains any other order R, so it is the maximal order of K. Moreover we recall that R_K can be expressed as

$$R_K = [1, \tau] \quad \text{where } \tau = \omega_K = \frac{d_K + \sqrt{d_K}}{2}$$

with d_K the discriminant of K. We observed, in the example (1.63) that for each integer $c \geq 1$ the ring $\mathbb{Z} + cR_K$ is an order of K. We can show that these are all of the orders of K.

Theorem 2.7. [5, 3.3, p. 297]. *Let R be an order in the imaginary quadratic field K. Then there exists a unique positive integer c such that $R = \mathbb{Z} + cR_K = [1, c\tau]$. In particular, the integer c is the index of R in R_K as an abelian group.*

Proof. [3, 8.1, Theorem 6, p. 91]. We first note that R is a sublattice of $R_K = [1, \tau]$, so it has a finite index. Let $c > 0$ be the unique positive integer such that $R \cap \mathbb{Z}\tau = \mathbb{Z}c\tau$. We need to show that this integer satisfies the statement. Let $\lambda \in R$, then surely there exist some integers m, n such that $\lambda = m + n\tau$, but it means that $n\tau = \lambda - m$ and since $n\tau \in \mathbb{Z}\tau$, $\lambda - m \in R$, then this quantity belongs to their intersection, but by construction $R \cap \mathbb{Z}\tau = \mathbb{Z}c\tau$. Thus $c \mid n$ and then $\lambda \in \mathbb{Z} + \mathbb{Z}c\tau$. □

Definition 2.8 (Conductor of R)**.** The integer c in the theorem (2.7) is called the *conductor of R* and we write $R = R_c$.

We recall that, if $\Lambda \subset K$ is a lattice, in particular it is a subgroup isomorphic as a group to $\mathbb{Z}^2$ and $\Lambda \otimes \mathbb{Q} = K$.

Definition 2.9 (Conductor of Λ)**.** Let $\Lambda \subset K$ be a lattice, let R denote the largest order in K such that $\alpha\Lambda \subset \Lambda$ for $\alpha \in R$. By the theorem (2.7) $R = R_c$ for some positive integer c, that we call *conductor of* Λ.

The following theorem tells us that, given an elliptic curve $E = \mathbb{C}/\Lambda$ over $\mathbb{C}$ with complex multiplication, we can always attribute to the case in which the lattice is in some imaginary quadratic field. Thus we do not lose generality when we fix a imaginary quadratic field K.

Theorem 2.10. [5, 3.5, p. 298]. *Suppose that $E = \mathbb{C}/\Lambda$ an elliptic curve over $\mathbb{C}$ with complex multiplication. Then there exists $\beta \in \mathbb{C}$ such that $\beta\Lambda$ is a lattice in some imaginary quadratic field K.*

Proof. [3, 1.5, pp. 19-20]. Consider the theorem (1.55.a) with $\Lambda_1 = \Lambda_2 = \Lambda$: it tells us that $\mathrm{End}(E)$ is in bijective correspondence with the set $S = \{\, \alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda \,\}$. Since E has complex multiplication, we know that $\mathrm{End}(E)$ is strictly larger that $\mathbb{Z}$, so it contains also non-trivial endomorphisms (we say that an endomorphism is *trivial* when it is induced by ordinary integers in S): so S contains also elements of $\mathbb{C} \setminus \mathbb{Z}$. In general, let $\Lambda = \omega_1\mathbb{Z} + \omega_1\mathbb{Z}$ and let $\alpha \in S$, so $\alpha\Lambda \subset \Lambda$. Then there exist some integers a, b, c, d such that

$$\begin{cases} \alpha\omega_1 = a\omega_1 + b\omega_2 \\ \alpha\omega_2 = c\omega_1 + d\omega_2 \end{cases}$$

so α is a root of the polynomial

$$\det \begin{pmatrix} x-a & -b \\ -c & x-d \end{pmatrix} = 0 \quad \Leftrightarrow \quad (x-a)(x-d) - bc = 0$$

so α is a quadratic irrational over $\mathbb{Q}$ and integral over $\mathbb{Z}$. Dividing $\alpha\omega_2$ by ω_2 yields to

$$\alpha = c\frac{\omega_1}{\omega_2} + d\frac{\omega_2}{\omega_2} = c\tau + d \qquad \text{where } \tau = \frac{\omega_1}{\omega_2}.$$

Since ω_1, ω_2 span a lattice, their ratio cannot be real, so $\tau \notin \mathbb{R}$.

Moreover, suppose that α induces a non-trivial endomorphism, i.e., $\alpha \notin \mathbb{Z}$. This implies that $c \neq 0$ (otherwise $\alpha = d \in \mathbb{Z}$), and then $\mathbb{Q}(\tau) = \mathbb{Q}(\alpha)$ so $\alpha \notin \mathbb{R}$, i.e., α is quadratic imaginary.

Thus the ring R of elements $\alpha \in \mathbb{Q}(\tau)$ such that $\alpha\Lambda \subset \Lambda$ is a subring of the quadratic field $K = \mathbb{Q}(\tau)$ and, in fact, a subring of R_K. □

Then, without loss of generality, by replacing $\mathbb{C}/\Lambda$ by the isomorphic curve $\beta\mathbb{C}/\beta\Lambda = \mathbb{C}/\beta\Lambda$ we may assume that Λ is a lattice in an imaginary quadratic field.

Remark 2.11. [5, 3.6, p. 298]. Let E be an elliptic curve which admits an abstract embedding $i\colon R \longrightarrow \mathrm{End}(E)$ for an order R in K. Then each $\alpha \in R$ induces an endomorphism $[\alpha]$ by the given embedding. On the other hand, if ω is an invariant differential on E, then $[\alpha]^*\omega = \mu(\alpha)\omega$ for a complex number $\mu(\alpha)$. Clearly, $\mu\colon R \longrightarrow \mathbb{C}$ is a homomorphism, so we may view R as a subring of $\mathbb{C}$ by the *I^{st} theorem of isomorphism*.

2.2 Classification of the CM elliptic curves

Our task here is to classify the elliptic curves with complex multiplication up to isomorphism, at least over $\mathbb{C}$, by the conductors. Let c denote a positive integer and consider the set of isomorphism classes of complex elliptic curves $\mathbb{C}/\Lambda$, where Λ is a lattice with associated order $R = R_c \subset R_K$.

Definition 2.12 (R-lattice, principal R-lattice)**.** We say that a lattice Λ in K is an *R-lattice* if it is stable under multiplication by R. It is *principal* if there exists some $\alpha \in K$ such that $\Lambda = \alpha R$.

We note that a principal R-lattice has conductor c.

Definition 2.13 (Invertible R-lattice, proper R-lattice)**.** Since the product of R-lattices is again an R-lattice, we can say that a lattice Λ in K is an *invertible R-lattice* if there exists another R-lattice Λ' such that $\Lambda\Lambda'$ is a principal R-lattice. Moreover, we note that any ideal $\mathfrak{a}$ in the ring R is automatically a R-lattice, so if $\mathfrak{a}$ has conductor c we call it a *proper R-ideal*.

Theorem 2.14. [5, 3.8, p. 298]. *Let Λ denote a lattice of K of conductor c. Then Λ is invertible as a lattice over $R = R_c$. Conversely, any invertible R-lattice has conductor c. The set of lattices of conductor c form a multiplicative group.*

Proof. It follows from [3, 8.1, Theorem 2, p. 90]. □

Definition 2.15 (Ideal prime to c)**.** Let $\mathfrak{a}$ denote an ideal in R. We say that $\mathfrak{a}$ is *prime to c* if

$$\mathfrak{a} + cR = R \qquad \text{or} \qquad \mathfrak{a} + cR_K = R.$$

Remark 2.16. [3, 8.1, pp. 91-92]. The two conditions in the definition of ideal prime to c are actually equivalent. In fact:

- Suppose that $\mathfrak{a} + cR = R$, but $\mathfrak{a} + cR_K \neq R$. Then $\mathfrak{a} + cR_K$ is contained in a maximal ideal $\mathfrak{p}$, which also contains $\mathfrak{a} + cR = R$: this gives a contradiction.

- Suppose that $\mathfrak{a} + cR_K = R$, but $\mathfrak{a} + cR \neq R$. Then $\mathfrak{a} + cR$ is contained in a maximal ideal $\mathfrak{p}$ and since R_K is integral over R, there is a maximal ideal of R_K lying above $\mathfrak{p}$: this gives a contradiction with the assumption.

We denote by $I_{K,c}$ the monoid of ideals of R_K that are prime to the ideal cR_K and by $I_{R,c}$ the monoid of ideals of R that are prime to c.

Theorem 2.17. [5, 3.10, p. 299]. *There is a multiplicative bijection between $I_{K,c}$ and $I_{R,c}$ given by $\mathfrak{a} \mapsto \mathfrak{a} \cap R$, whose inverse is given by $\mathfrak{a} \mapsto \mathfrak{a}R_K$. Moreover, any ideal of R that is prime to c has conductor c and so is a proper R-ideal.*

Proof. [3, 8.1, Theorem 4, p. 92]. To show that the two sets are in bijection we show that the composition of the given maps is the identity. We first denote them as follows:

$$\begin{aligned} \phi\colon I_{K,c} &\longrightarrow I_{R,c} & \qquad \psi\colon I_{R,c} &\longrightarrow I_{K,c} \\ \mathfrak{a} &\longmapsto \phi(\mathfrak{a}) = \mathfrak{a} \cap R & \qquad \mathfrak{a} &\longmapsto \psi(\mathfrak{a}) = \mathfrak{a}R_K. \end{aligned}$$

Let $\mathfrak{a} \in I_{K,c}$ be an ideal of R_K prime to cR_K, so $\mathfrak{a} + cR_K = R_K$. We *claim* that $\mathfrak{a} = \psi \circ \phi(\mathfrak{a}) = (\mathfrak{a} \cap R)R_K$. The direct inclusion is obvious; to show the converse we see that

$$R = R_K \cap R = (\mathfrak{a} \cap cR_K) \cap R \subset (\mathfrak{a} \cap R) + cR_K \subset R.$$

so the inclusions are actually equalities. In particular $(\mathfrak{a} \cap R) + cR_K = R$, that means that $\mathfrak{a} \cap R$ is prime to c. Next, we observe that $\mathfrak{a}c \subset \mathfrak{a} \cap R$, so

$$\mathfrak{a} = \mathfrak{a}R = \mathfrak{a}((\mathfrak{a} \cap R) + cR_K) \subset R_K(\mathfrak{a} \cap R) + cR_K \subset (\mathfrak{a} \cap R)R_K.$$

This shows the claim, $\psi \circ \phi = id_{I_{K,c}}$.

On the other hand, let $\mathfrak{a} \in I_{R,c}$, i.e., it is an R-ideal which is prime to c: $\mathfrak{a} + cR_K = R$. We *claim* that $\mathfrak{a} = \phi \circ \psi(\mathfrak{a}) = \mathfrak{a}R_K \cap R$. The direct inclusion is clearly true; also the converse is quite immediate:

$$\mathfrak{a}R_K \cap R = (\mathfrak{a}R_K \cap R)R = (\mathfrak{a}R_K \cap R)(\mathfrak{a} + cR_K) \subset \mathfrak{a} + \mathfrak{a}cR_K \subset \mathfrak{a} + \mathfrak{a}R \subset \mathfrak{a}.$$

This shows that $\phi \circ \psi = id_{I_{R,c}}$.

Now we need to show that those bijections preserve the multiplication: using the surjectivity of ϕ, for any $\mathfrak{a}_0, \mathfrak{b}_0 \in I_{R,c}$ there exist some $\mathfrak{a}, \mathfrak{b} \in I_{K,c}$ such that $\mathfrak{a}_0 = \mathfrak{a} \cap R$ and $\mathfrak{b}_0 = \mathfrak{b} \cap R$. Then $\mathfrak{a}_0\mathfrak{b}_0 \in I_{R,c}$ and

$$\begin{aligned}\phi(\mathfrak{a})\phi(\mathfrak{b}) &= (\mathfrak{a} \cap R)(\mathfrak{b} \cap R) = \mathfrak{a}_0\mathfrak{b}_0 = (\mathfrak{a}_0\mathfrak{b}_0 R_K) \cap R \quad \text{(using the second } \textit{claim}\text{)} \\ &= ((\mathfrak{a} \cap R)(\mathfrak{b} \cap R)R_K) \cap R = (\mathfrak{a}\mathfrak{b}) \cap R \quad \text{(using the first } \textit{claim}\text{)} \\ &= \phi(\mathfrak{a}\mathfrak{b}).\end{aligned}$$

Finally, in order to show that an R-ideal $\mathfrak{a}$ prime to c is proper, let $\lambda \in K$ and suppose that $\lambda\mathfrak{a} \subset \mathfrak{a}$. Then

$$\lambda R = \lambda(\mathfrak{a} + cR_K) = \lambda\mathfrak{a} + \lambda cR_K \subset \mathfrak{a} + cR_K = R$$

and since $1 \in R$ we conclude that $\lambda \in R$. □

Theorem 2.18. [5, 3.11, p. 299]. *Let Λ be an R-lattice of conductor c and let m be a positive integer. Then there exist an ideal $\mathfrak{a} \subset R$ such that $\mathfrak{a} = \alpha\Lambda$ and $\mathfrak{a}$ is prime to m.*

Proof. See [3, 8.1, Theorem 5, p. 93]. □

Let I_c denote the monoid of R-lattices of conductor c and P_c denote the submonoid of principal R-lattices (which are automatically of conductor c, so $P_c \subset I_c$).

Definition 2.19 (Group of ideal classes of R)**.** We define the *group of ideal classes of R* as the quotient $G_c = I_c/P_c$.

Remark 2.20. In view of the theorem (2.18), that tells us that in the equivalence class of Λ there exists a lattice that is prime to m and is integral, we see that every element of G_c has a representative that is prime to the conductor c. Thus we may replace I_c and P_c in the definition by the corresponding sets of ideals prime to c.

In particular, using this observation, we can express G_c as a factor group of a generalized ideal class group of the full ring of integers in K. Let $P_{\mathbb{Z}}(c)$ be the monoid of principal ideals of R_K of the form $\mathfrak{a} = \alpha R_K$ such that $\alpha \equiv a \pmod{cR_K}$ for some $a \in \mathbb{Z}$ and such that a is prime to c. Let $I(c)$ denote the monoid of ideals of R_K prime to c (previously called $I_{K,c}$) Then, as previously observed, we can prove the following statement:

Theorem 2.21. [5, 3.14, p. 299]. *There exists an isomorphism $I(c)/P_{\mathbb{Z}}(c) \cong G_c$ given by $\mathfrak{a} \mapsto \mathfrak{a} \cap R$.*

Proof. [3, 8.1, p. 94]. We start by proving the following lemma:

Lemma 2.22. *Let $\alpha \in P_{\mathbb{Z}}(c)$ be as above, then $\mathfrak{a} \cap R = \alpha R$.*

Proof. Let $x \in R_K$ and suppose that $x\alpha \in R$: we can write

$$\begin{cases} x = m + n\tau \\ \alpha = a + bc\tau \end{cases} \qquad \text{with } m, n, a, b \in \mathbb{Z} \text{ such that } (a, c) = 1$$

then

$$\begin{aligned} x\alpha &= (m + n\tau)(a + bc\tau) = ma + mcb\tau + an\tau + ncb\tau^2 \\ &\equiv ma + an\tau \pmod{cR_K}. \end{aligned}$$

Since $x\alpha \in R = \mathbb{Z} + cR_K$, it follows that $c \mid na$; by assumption $(a, c) = 1$ so necessarily $c \mid n$. It means that $n = cn'$ for some $n' \in \mathbb{Z}$, so $x = m + cn'\tau \in R$ and then $x\alpha \in \alpha R$. This shows that $\mathfrak{a} \cap R \subset \alpha R$.

To show the converse it suffices to note that, since $\alpha \in R$ then $\alpha R \subset \mathfrak{a} \cap R$. □

Next we recall that, by theorem (2.17) and with the new definitions for the monoids, there is a multiplicative bijection between $I(c)$ and I_c given by $\mathfrak{a} \mapsto \mathfrak{a} \cap R$.

We need to show that the inverse image of P_c is $P_{\mathbb{Z}}(c)$. To show the first inclusion we suppose that $\mathfrak{a}$ is an element of the inverse image of P_c: it means that $\mathfrak{a} \cap R = \alpha R$ with $\alpha \equiv a \pmod{cR_K}$ and $a \in \mathbb{Z}$. Then necessarily $\mathfrak{a} = \alpha R_K$, so $\mathfrak{a} \in P_{\mathbb{Z}}(c)$. The other inclusion follows from the lemma (2.22).

Thus we can conclude that $G_c = I_c/P_c \cong I(c)/P_{\mathbb{Z}}(c)$. □

We easily observe that the ring of integers R_K is an order of conductor $c = 1$ of K. We introduce a particular notation for its ideal class group: we set

$$C\mathcal{L}(R_K) = \frac{\{ \text{ non-zero fractional ideals of } K \}}{\{ \text{ non-zero principal ideals of } K \}}$$

in order to point out the ring R_K. Moreover, we define the *class number of K*, denoted by h_K, as the order of the ideal class group $C\mathcal{L}(R_K)$.

Finally, we can use these properties in order to classify the CM elliptic curves up to isomorphism (over $\mathbb{C}$) with respect to the conductor. The basic case is that of the maximal order, namely, curves of conductor 1.

Theorem 2.23. [5, 3.7, p. 298]. *The elliptic curves of conductor* 1 *with complex multiplication are in bijective correspondence with the elements of the ideal class group of R_K, denoted by $C\mathcal{L}(R_K)$:*

$$\left\{ \begin{array}{l} \textit{CM elliptic curves} \\ \textit{of conductor } c = 1 \end{array} \right\} \quad \overset{1:1}{\longleftrightarrow} \quad C\mathcal{L}(R_K).$$

In particular, there are exactly h_K non-isomorphic curves of conductor 1 *with complex multiplication, where h_K is the* class number of K.

Proof. Let $E = \mathbb{C}/\Lambda$ denote a CM elliptic curve of conductor 1. By definition, Λ is a lattice in K which is stable under multiplication by R_K. Thus Λ defines a fractional ideal of K. Moreover, the class of Λ modulo principal ideals depends only on the isomorphism class of E and every ideal class of R_K is obtained in this way from some E. It remains only to show that if E and E' give the same class, then they are isomorphic. But this follows from the theorem (2.6). □

Theorem 2.24. [5, 3.16, p. 299]. *The elliptic curves of conductor $c > 1$ with complex multiplication are in bijective correspondence with elements of the group G_c:*

$$\left\{ \begin{array}{l} \textit{CM elliptic curves} \\ \textit{of conductor } c > 1 \end{array} \right\} \quad \overset{1:1}{\longleftrightarrow} \quad G_c$$

Namely, the bijection is induced by sending an R-ideal $\mathfrak{a}$ of conductor c to the elliptic curve $\mathbb{C}/\mathfrak{a}$. In particular, there are exactly h_c non-isomorphic CM curves of conductor c, where h_c is the order of the group G_c.

Proof. It is similar to the case with $c = 1$. □

2.3 Complex multiplication over $\mathbb{C}$

In order to study elliptic curves with complex multiplication, it is useful to study the set of isomorphism classes of elliptic curves with the same endomorphism ring, namely we define

$$\begin{aligned} \mathcal{ELL}(R) &= \frac{\{ \text{ elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong R \}}{\text{isomorphism over } \mathbb{C}} \\ &= \frac{\{ \text{ lattices } \Lambda \text{ with } \mathrm{End}(E_\Lambda) \cong R \}}{\text{homothety}}. \end{aligned}$$

Given a quadratic imaginary field K, we can build an elliptic curve with complex multiplication by R_K in several ways. For example, if $\mathfrak{a}$ is a non-zero fractional ideal of K (or integer ideal of R_K), then using the embeddings $\mathfrak{a} \subset K \subset \mathbb{C}$ we see that $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Hence we can define an elliptic curve $E_{\mathfrak{a}}$ whose endomorphism ring is

$$\begin{aligned}\mathrm{End}(E_{\mathfrak{a}}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} \quad \text{since } \mathfrak{a} \subset K \\ &= R_K \quad \text{since } \mathfrak{a} \text{ is a fractional ideal}\end{aligned}$$

Thus each non-zero fractional ideal of K will define an elliptic curve with complex multiplication by R_K. On the other hand, since homothetic lattices give isomorphic elliptic curves, then the ideals $\mathfrak{a}$ and $\alpha\mathfrak{a}$ give the same element of $\mathcal{ELL}(R_K)$: so we look at the group of fractional ideals modulo principal ideals. We recall the definition of *ideal class group of* R_K, given in the previous section:

Definition 2.25 (Ideal class group of R_K)**.**

$$C\mathcal{L}(R_K) = \frac{\{\text{ non-zero fractional ideals of } K\ \}}{\{\text{ non-zero principal ideals of } K\ \}}$$

the *ideal class group of* R_K. If $\mathfrak{a}$ is a fractional ideal of K, we denote by $\bar{\mathfrak{a}}$ its class in the quotient, called *ideal class of* $\mathfrak{a}$ *in* $C\mathcal{L}(R_K)$.

By the previous argument, then, we can define a map

$$C\mathcal{L}(R_K) \longrightarrow \mathcal{ELL}(R_K), \qquad \bar{\mathfrak{a}} \mapsto E_{\mathfrak{a}}$$

namely, we can associate to each ideal class an elliptic curve.

More generally, if Λ is any lattice with $E_\Lambda \in \mathcal{ELL}(R_K)$ we can define the product

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

and we will show that this induces a simply transitive action of the ideal class group on the set of elliptic curves.

Proposition 2.26. [7, II.1.2, p. 99].

(a) *Let* Λ *be a lattice with* $E_\Lambda \in \mathcal{ELL}(R_K)$*, let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be two non-zero fractional ideals of* K*. Then:*

i. $\mathfrak{a}\Lambda$ *is a lattice in* $\mathbb{C}$*.*

ii. *The elliptic curve* $E_{\mathfrak{a}\Lambda}$ *satisfies* $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong R_K$.
iii. $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ *if and only if* $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ *in* $C\mathcal{L}(R_K)$.

Hence, there is a well-defined action of $C\mathcal{L}(R_K)$ *on* $\mathcal{ELL}(R_K)$ *given by*

$$* : C\mathcal{L}(R_K) \times \mathcal{ELL}(R_K) \to \mathcal{ELL}(R_K), \qquad (\bar{\mathfrak{a}}, E_\Lambda) \mapsto \bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

(b) *The action is simply transitive. In particular* $|C\mathcal{L}(R_K)| = |\mathcal{ELL}(R_K)|$.

Proof. (a) (i) By assumption $\mathrm{End}(E_\Lambda) = R_K$, so $R_K\Lambda = \Lambda$. By definition of fractional ideal, we can choose a non-zero integer $d \in \mathbb{Z}$ such that $d\mathfrak{a} \subset R_K$. Then $\mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$, which means that $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$. Similarly we can choose a non-zero integer $d \in \mathbb{Z}$ such that $dR_K \subset \mathfrak{a}$, so we find that $d\Lambda \subset \mathfrak{a}\Lambda$. Using both of these relations we have $d\Lambda \subset \mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$, so $\mathfrak{a}\Lambda$ spans $\mathbb{C}$: this proves that $\mathfrak{a}\Lambda$ is a lattice.

(ii) For any $\alpha \in \mathbb{C}$ and any non-zero fractional ideal $\mathfrak{a}$ we have that

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \quad \Longleftrightarrow \quad \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \quad \Longleftrightarrow \quad \alpha\Lambda \subset \Lambda.$$

Hence

$$\begin{aligned} \mathrm{End}(E_{\mathfrak{a}\Lambda}) &= \{\alpha \in \mathbb{C} : \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} \\ &= \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} \\ &= \mathrm{End}(E_\Lambda) = R_K. \end{aligned}$$

(iii) From the corollary (1.56) we know that the isomorphism class of the curve $E_{\mathfrak{a}\Lambda}$ into the quotient $\mathcal{ELL}(R_K)$ is univocally determined by the homothety class of the lattice $\mathfrak{a}\Lambda$, namely $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if there exists $c \in \mathbb{C}^\times$ such that $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$, but then by multiplying by $\mathfrak{a}^{-1}$ and using the fact that $R_K\Lambda = \Lambda$ we get

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \quad \Longleftrightarrow \quad \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Similarly, multiplying by $c^{-1}\mathfrak{b}^{-1}$ gives

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \quad \Longleftrightarrow \quad \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda.$$

Using both these results, we deduce that if $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ then both $c\mathfrak{a}^{-1}\mathfrak{b}$ and $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ take Λ to itself, so they are both contained in R_K:

$$\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda \subset R_K\Lambda = \Lambda, \qquad \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda \subset R_K\Lambda = \Lambda$$

and so they are both equal to R_K. Therefore $\mathfrak{a} = c\mathfrak{b}$, from which it follows that $c \in K$ and $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ in $C\mathcal{L}(R_K)$.

Then we need to show that $*$, defined into the proposition, is an action of $C\mathcal{L}(R_K)$ on $\mathcal{ELL}(R_K)$:

$$(\bar{1}) * E_\Lambda = E_{R_K^{-1}\Lambda} = E_{R_K\Lambda} = E_\Lambda$$
$$\bar{\mathfrak{a}} * (\bar{\mathfrak{b}} * E_\Lambda) = \bar{\mathfrak{a}} * E_{\mathfrak{b}^{-1}\Lambda} = E_{\mathfrak{a}^{-1}(\mathfrak{b}^{-1}\Lambda)} = E_{(\mathfrak{a}\mathfrak{b})^{-1}\Lambda} = \overline{\mathfrak{a}\mathfrak{b}} * E_\Lambda$$

where the first relation holds since $(\bar{1})$ is the class of R_K into $C\mathcal{L}(R_K)$. Recall that R_K is the ring of integers of a field, so $C\mathcal{L}(R_K)$ is an abelian group, then $\mathfrak{a}^{-1}\mathfrak{b}^{-1} = (\mathfrak{a}\mathfrak{b})^{-1}$.

(b) Given two elliptic curves in $\mathcal{ELL}(R_K)$, namely E_{Λ_1} and E_{Λ_2}, we choose any non-zero element $\lambda_1 \in \Lambda_1$ (respectively $\lambda_2 \in \Lambda_2$), and consider the lattice $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$ (resp. $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$). From theorem (1.64) it follows that $\mathfrak{a}_1 \subset K$ and by assumption it is a finitely generated R_K-module, hence a fractional ideal of K (analogous for $\mathfrak{a}_2$). Then we see that

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2$$

and, if we denote $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$, then

$$\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}$$

where the last isomorphism is given by the fact that homothetic lattices give isomorphic elliptic curves. This shows the transitivity of the action. From part (ii) in (a) we deduce that, if $\mathfrak{a} * E_\Lambda = \mathfrak{b} * E_\Lambda$ then $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$, and it means that the action is simply transitive.

□

Example 2.27. [7, II.1.3.1, p. 101]. In the example (2.2) we have seen an elliptic curve with complex multiplication by the ring $\mathbb{Z}[\imath]$. Now we look at this curve from a complex point of view.

Let $\Lambda = \mathbb{Z}[\imath]$ be the lattice of Gaussian integers, let E_Λ be the curve associate to it, so the endomorphism ring of the curve E_Λ is $\mathbb{Z}[\imath]$. The curve is given by a Weierstrass equation of the form

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

where $g_2(\Lambda) = 140 \sum_\omega \omega^{-6}$, $g_3(\Lambda) = 60 \sum_\omega \omega^{-4}$. We can easily get some informations about the functions g_2, g_3, in particular we see know that $\iota\Lambda = \Lambda$, so

$$g_3(\Lambda) = g_3(\iota\Lambda) = 140 \sum_\omega (\iota\omega)^{-6} = 140\iota^{-6} \sum_\omega \omega^{-6} = -140 \sum_\omega \omega^{-6} = -g_3(\Lambda)$$

so necessarily $g_3(\Lambda) = 0$. Moreover, after a suitable isomorphism, we can delete the coefficient of the x^3 term, thus the equation of the curve simplifies as

$$y^2 = x^3 - g_2(\Lambda)x.$$

By applying the definition, we can easily compute the discriminant and then the j-invariant of the curve:

$$\Delta = -16(-4g_2(\Lambda)^3 + 27g_3(\Lambda)^2) = 4^3 g_2(\Lambda)^3$$
$$j(E_\Lambda) = -1728\frac{(4g_2(\Lambda))^3}{\Delta} = 1728.$$

Since $j(E_\Lambda)$ is rational, we know that E_Λ is isomorphic to an elliptic curve defined over $\mathbb{Q}$ (for example the curve in (2.2) of equation $y^2 = x^3 - x$), but it does not imply that that $g_2(\Lambda)$ itself is an element of $\mathbb{Q}$: indeed a theorem by *Hurewitz* says that

$$g_2(\mathbb{Z}[\iota]) = 64\Big(\int_0^1 \frac{dt}{\sqrt{1-t^4}}\Big)^4.$$

If E has complex multiplication we will use torsion points of E to generate abelian extensions of K. We could restrict the study to the points of order m for various integers m, but since E has complex multiplication, there are also other natural finite subgroups to look at.

Definition 2.28 (Group of $\mathfrak{a}$-torsion points of E)**.** If $\mathfrak{a}$ is any integral ideal of R_K we define

$$E[\mathfrak{a}] = \{\, P \in E \colon [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a} \,\}$$

and call it the *group of* $\mathfrak{a}$*-torsion points of* E.

Remark 2.29. The previous definition depends on the choice of a particular isomorphism $[\,\cdot\,] : R_K \to \mathrm{End}(E)$. We always choose the normalized isomorphism defined in (2.4).

Example 2.30. If we consider a principal integral ideal $\mathfrak{a} = mR_K$ for some $m \in R_K$, then $E[\mathfrak{a}] = E[m]$, defined in (1.28). So the definition of $E[\mathfrak{a}]$ extends the m-torsion subgroup to a generic ideal $\mathfrak{a}$.

If $\mathfrak{a}$ is an integral ideal of R_K, then $\Lambda \subset \mathfrak{a}^{-1}\Lambda$ and it induces a natural homomorphism between the corresponding elliptic curves

$$\mathbb{C} \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}\Lambda, \qquad\qquad z \longmapsto z$$

which induces a natural isogeny

$$E_\Lambda \longrightarrow \bar{\mathfrak{a}} * E_\Lambda.$$

To describe this isogeny and the group $E[\mathfrak{a}]$ we consider the following

Proposition 2.31. [7, II.1.4, p. 102]. *Let $E \in \mathcal{ELL}(R_K)$ and let $\mathfrak{a}$ be an integral ideal of R_K.*

(a) *$E[\mathfrak{a}]$ is the kernel of the natural map $E \longrightarrow \bar{\mathfrak{a}} * E$.*
(b) *$E[\mathfrak{a}]$ is a free $R_K/\mathfrak{a}$-module of rank* 1.

Proof. Let E be an elliptic curve, let Λ be the lattice associate to it: we can fix an analytic isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. The we find that

$$\begin{aligned} E[\mathfrak{a}] &\cong \{\, z \in \mathbb{C}/\Lambda \colon \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a} \,\} \\ &= \{\, z \in \mathbb{C} \colon \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a} \,\}/\Lambda \\ &= \{\, z \in \mathbb{C} \colon z\mathfrak{a} \subset \Lambda \,\}/\Lambda \\ &= \mathfrak{a}^{-1}\Lambda/\Lambda \\ &= \ker\left(\mathbb{C}/\Lambda \xrightarrow{z\mapsto z} \mathbb{C}/\mathfrak{a}^{-1}\Lambda\right) \\ &= \ker\left(E \to \bar{\mathfrak{a}} * E\right). \end{aligned}$$

This shows (a).

To show (b) we choose a non-zero $\lambda \in \Lambda$, then by the theorem (1.64) we know that the lattice $\frac{1}{\lambda}\Lambda \in K$ and is a finitely generated R_K-module, so is a fractional ideal of K. Since homothetic lattices give isomorphic elliptic curves, we may assume that Λ is a fractional ideal of K. From (a) it follows that $E[\mathfrak{a}] \cong \mathfrak{a}^{-1}\Lambda/\Lambda$ as $R_K/\mathfrak{a}$-module. Note that, if $\mathfrak{q}$ is any integral ideal dividing $\mathfrak{a}$, the fact that $R_K\Lambda = \Lambda$ implies that

$$(\mathfrak{a}^{-1}\Lambda/\Lambda) \otimes_{R_K} (R_K/\mathfrak{q}) \cong \mathfrak{a}^{-1}\Lambda/(\Lambda + \mathfrak{q}\mathfrak{a}^{-1}\Lambda) = \mathfrak{a}^{-1}\Lambda/\mathfrak{q}\mathfrak{a}^{-1}\Lambda.$$

Hence, by the *Chinese Remainder Theorem*, we write

$$R_K/\mathfrak{a} \cong \prod_{\mathfrak{p}\ prime} R_K/\mathfrak{p}^{e(\mathfrak{p})}$$

then

$$E[\mathfrak{a}] \cong \prod_{\mathfrak{p}\ prime} \mathfrak{a}^{-1}\Lambda/\mathfrak{p}^{e(\mathfrak{p})}\mathfrak{a}^{-1}\Lambda.$$

It suffices to show that if $\mathfrak{b}$ is a fractional ideal of R_K, such as $\mathfrak{b} = \mathfrak{a}^{-1}\Lambda$ and $\mathfrak{p}^e$ is a power of a prime ideal, then $\mathfrak{b}/\mathfrak{p}^e\mathfrak{b}$ is a free $R_K/\mathfrak{p}^e$- module of rank one. In order to ease notation, let

$$R' := R_K/\mathfrak{p}^e, \qquad \mathfrak{p}' := \mathfrak{p}/\mathfrak{p}^e, \qquad \mathfrak{b}' := \mathfrak{b}/\mathfrak{p}^e\mathfrak{b}$$

and observe that R' is a local ring whose ideals are exactly $\{(0), \mathfrak{p}'^{e-1}, ..., \mathfrak{p}', (1)\}$, so its maximal ideal is $\mathfrak{p}'$. Finally we *claim* that the vector space over the field $R'/\mathfrak{p}' \cong R_K/\mathfrak{p}$

$$\mathfrak{b}'/\mathfrak{p}'\mathfrak{b}' \cong \mathfrak{b}/\mathfrak{p}\mathfrak{b}$$

is a 1-dimensional vector space. We first observe that any two elements of $\mathfrak{b}$ are R_K-linearly dependent, so the dimension of $\mathfrak{b}/\mathfrak{p}\mathfrak{b}$ over $R_K/\mathfrak{p}$ is at most one. If, by contraddiction, this dimension was zero, then we would have that $\mathfrak{b} = \mathfrak{p}\mathfrak{b}$ but this gives a contraddiction. Applying *Nakayama's Lemma* to the local ring R' and the R'-module $\mathfrak{b}'$, it follows that $\mathfrak{b}'$ is a free R'-module of rank one, and this gives the proof of (b). □

Finally, we can deduce from the previous proposition how to compute the degree of the isogeny $E \to \bar{\mathfrak{a}} * E$, as well as the degree of the endomorphism $[\alpha]\colon E \to E$.

Corollary 2.32. [7, II.1.5, p. 103]. *Let $E \in \mathcal{ELL}(R)$.*

(a) *For all integral ideals $\mathfrak{a} \subset R_K$, the natural map $E \to \bar{\mathfrak{a}} * E$ has degree $N_{\mathbb{Q}}^K\mathfrak{a}$.*

(b) *For all $\alpha \in R_K$, the endomorphism $[\alpha]\colon E \to E$ has degree $\left|N_{\mathbb{Q}}^K\alpha\right|$.*

Proof. It follows immediately from (2.31): namely

$$\begin{aligned} \deg(E \to \bar{\mathfrak{a}} * E) &= |E[\mathfrak{a}]| && \text{from (2.31.a)} \\ &= N_{\mathbb{Q}}^K\mathfrak{a} && \text{from (2.31.b)} \end{aligned}$$

and similarly

$$\deg[\alpha] = |\ker[a]| = |E[\alpha R_K]| = N_{\mathbb{Q}}^K(\alpha R_K) = \left|N_{\mathbb{Q}}^K\alpha\right|.$$ □

Definition 2.33 (Singular j-invariant)**.** The j-invariant of an elliptic curve with CM is called *singular j-invariant*.

Into the following chapters we will study some properties of the singular j-invariant of an elliptic curve.

Chapter 3

Class field theory

Class field theory describes the abelian extensions of a number field K in terms of the arithmetic of K. The theory of complex multiplication provides an analytic realization of class field theory for quadratic imaginary fields.

3.1 A brief review

As in the previous chapter, we restrict attention to totally imaginary fields, that is, fields with no real embeddings.

Let K be a totally imaginary number field and let L be a finite abelian extension of K, i.e., L/K is Galois with abelian Galois group $\mathrm{Gal}(L/K) = G$. As usual, we write R_K and R_L for the rings of integers of K and L respectively. In order to ease the notation, we say that $\mathfrak{p}$ is a *prime (ideal) of a field* if it is a prime (ideal) in its ring of integers.

Definition 3.1 (Ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$)**.** Let $\mathfrak{p}$ be a prime of K and suppose that if factorizes as product of powers of prime ideals of L, i.e.,

$$\mathfrak{p}R_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_n^{e_n}, \quad \text{for some naturals } e_1, \dots, e_n$$

such that $\mathfrak{P}_1 \cap R_K = \mathfrak{p}$ for each $i = 1, \dots, n$. The natural value e_i is called *ramification index of* $\mathfrak{P}_i$ *over* $\mathfrak{p}$.

Since the extension L/K is Galois, it is possible to prove that $e_i = e_j$ for all i, j.

We define the *residue fields* $F_\mathfrak{p} = R_K/\mathfrak{p}$ and its extensions $F_{\mathfrak{P}_i} = R_L/\mathfrak{P}_i$ for each $i = 1, \dots, n$, that are in particular finite fields. Moreover, the extension is Galois and we denote by $\bar{G} = \mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{p})$ its Galois group.

Definition 3.2 (Inertia index of $\mathfrak{P}_i$ over $\mathfrak{p}$)**.** The degree of the extension $[F_{\mathfrak{P}_i} : F_{\mathfrak{p}}] = f_i$ is called the *inertia index of* $\mathfrak{P}_i$ *over* $\mathfrak{p}$.

If L/K is an extension of degree n, the indeces e_i, f_i for $i = 1, \dots, n$ and n are related by the formula

$$n = \sum_i^n e_i f_i.$$

Moreover, we suppose that $\mathfrak{p}$ does not ramify in L, it means that it factorizes as product of distinct prime ideals of L, so $e_i = 1$ for all $i = 1, \dots, n$, and the previous formula simplifies to $n = \sum_i^n f_i$.

G acts transitively over the prime factors of $\mathfrak{p}R_L$, i.e., for each pair $\mathfrak{P}_i, \mathfrak{P}_j$ there exists an automorphism $\sigma \in G$ such that $\mathfrak{P}_j = \mathfrak{P}_i^{\sigma}$.

Definition 3.3 (Decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$)**.** Fix $\mathfrak{P}$ as one of the primes of L that lie over $\mathfrak{p}$, i.e., $\mathfrak{P}$ is one of the $\mathfrak{P}_i$'s. Then we define the *decomposition group of* $\mathfrak{P}$ *over* $\mathfrak{p}$ as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\, \sigma \in G \colon \mathfrak{P}^{\sigma} = \mathfrak{P} \,\}$$

namely, the subgroup of G of the automorphisms that fix the prime ideal $\mathfrak{P}$.

Each $\sigma \in G = \mathrm{Gal}(L/K)$ induces an isomorphism between residue fields, namely if $\sigma \colon L \longrightarrow L$ fixes the subfield K, then if we restrict it to the ring of integers we get $\sigma|_{R_L} \colon R_L \longrightarrow R_L$ such that $\sigma(R_K) = R_K$ and sends $\mathfrak{P}$ to one of the other prime factors of $\mathfrak{p}$, and we get an isomorphism $\bar{\sigma} \colon F_{\mathfrak{P}} \longrightarrow F_{\mathfrak{P}^{\sigma}}$. If we consider the same argument with $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, then $\mathfrak{P}^{\sigma} = \mathfrak{P}$, so we obtain an automorphism $\bar{\sigma} \colon F_{\mathfrak{P}} \longrightarrow F_{\mathfrak{P}}$. This automorphism also fixes the subfield $F_{\mathfrak{p}}$, because σ fixes both $R_K = R_L \cap K$ and $\mathfrak{p} = \mathfrak{P} \cap K$, thus $\bar{\sigma} \in \mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$.

This actually means that we can define a homomorphism from the decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$ to the Galois group of the extension of the residue fields

$$\pi_{\mathfrak{P}} \colon D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \bar{G}, \qquad \sigma \mapsto \bar{\sigma}$$

where we denoted by $\bar{G}$ the Galois group $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$.

Definition 3.4 (Inertia group of $\mathfrak{P}$ over $\mathfrak{p}$)**.** The group

$$\ker(\pi_{\mathfrak{P}}) = E(\mathfrak{P}/\mathfrak{p}) = \{\, \sigma \in \mathrm{G} \colon \sigma(\alpha) \equiv \alpha \,(\mathrm{mod}\ \mathfrak{P}) \text{ for all } \alpha \in R_L \,\}$$

is called the *inertia group of* $\mathfrak{P}$ *over* $\mathfrak{p}$.

Since $E(\mathfrak{P}/\mathfrak{p})$ is a subgroup of $D(\mathfrak{P}/\mathfrak{p})$ and is the kernel of a homomorphism, then it is normal in the decomposition group, and by the *I^{st} isomorphism theorem* it follows that

$$D(\mathfrak{P}/\mathfrak{p})/E(\mathfrak{P}/\mathfrak{p}) \hookrightarrow \bar{G}$$

but one can prove that this morphism is also surjective, so it is an isomorphism. So the situation is the following: $E(\mathfrak{P}/\mathfrak{p}) \triangleleft D(\mathfrak{P}/\mathfrak{p}) < G$ and this tells that we can construct an exact sequence

$$1 \longrightarrow E(\mathfrak{P}/\mathfrak{p}) \longrightarrow D(\mathfrak{P}/\mathfrak{p}) \xrightarrow{\pi_{\mathfrak{P}}} \bar{G} \longrightarrow 1.$$

Since we are assuming that $\mathfrak{p}$ is unramified, then the order of the inertia subgroup of $\mathfrak{P}$ (that is the ramification index e of $\mathfrak{P}$ over $\mathfrak{p}$) is equal to 1, so $E(\mathfrak{P}/\mathfrak{p})$ is the trivial group and actually $D(\mathfrak{P}/\mathfrak{p}) \cong \bar{G}$.

Next, since $F_{\mathfrak{P}}/F_{\mathfrak{p}}$ is an extension of finite fields, it follows that $D(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ is a cyclic group generated by the Frobenius automorphism

$$x \mapsto x^{N_{\mathbb{Q}}^K(\mathfrak{p})}$$

where $N_{\mathbb{Q}}^K(\mathfrak{p}) = p^{f'}$ with $f' = \dim_{\mathbb{F}_p}(F_{\mathfrak{p}})$, and the order of this cyclic group is equal to the inertia index of $\mathfrak{P}$ over $\mathfrak{p}$, namely, $|\bar{G}| = [F_{\mathfrak{P}} : F_{\mathfrak{p}}] = f$.

Definition 3.5 (Frobenius element)**.** Since $\mathfrak{p}$ is unramified, there is a unique element $\sigma_{\mathfrak{p}} \in D(\mathfrak{P}/\mathfrak{p}) \subset \mathrm{Gal}(L/K)$ which is mapped by $\pi_{\mathfrak{P}}$ to Frobenius, and we call it the *Frobenius element* or the *Frobenius substitution of* $\mathfrak{P}$ *over* $\mathfrak{p}$.

Note that in our situation it is completely determined by the prime ideal $\mathfrak{p}$ of K (for a general Galois extension L/K, $\mathfrak{p}$ will only determine the conjugacy class of $\sigma_{\mathfrak{p}}$ and making a new choice for the prime $\mathfrak{P}$ over $\mathfrak{p}$ will change $\sigma_{\mathfrak{p}}$ by conjugation; but we are assuming that the extension L/K is abelian, so $\sigma_{\mathfrak{p}}$ will not change). Thus, $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ is uniquely determined by the condition

$$\sigma_{\mathfrak{p}}(x) \equiv x^{N_{\mathbb{Q}}^K(\mathfrak{p})} \pmod{\mathfrak{P}} \qquad \text{for all } x \in R_L.$$

Let $\mathfrak{c}$ be an integral ideal of K that is divisible by all primes that ramify in the extension L/K, and let $I(\mathfrak{c})$ be the group of fractional ideals of K which are prime to $\mathfrak{c}$. It means that $\mathfrak{a} = \prod_{\mathfrak{p} prime} \mathfrak{p}^{n_{\mathfrak{p}}}$ where $n_{\mathfrak{p}} \in \mathbb{N}$ and each prime ideal $\mathfrak{p}$ of K is unramified in L (otherwise the ramified $\mathfrak{p}$'s would be divisors of $\mathfrak{c}$ by construction).

Definition 3.6 (Artin symbol)**.** For each prime ideal $\mathfrak{p}$ of K we define the *Artin symbol for unramified prime ideals of K* as

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma_{\mathfrak{p}}$$

i.e., we associate to each prime ideal $\mathfrak{p}$ of K the unique Frobenius element of $\mathfrak{p}$ in $G = \mathrm{Gal}(L/K)$.

Then we observe that, if we factorize $\mathfrak{p}$ as product of prime ideals of L, $\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_m$, we can define the Artin symbol for each factor $\mathfrak{P}_i$, but since L/K is an abelian extension, the Frobenius elements depend only on $\mathfrak{p}$, so the symbol takes the same value for each factor:

$$\left(\frac{L/K}{\mathfrak{P}_i}\right) = \sigma_{\mathfrak{P}_i} = \sigma_{\mathfrak{P}_j} = \left(\frac{L/K}{\mathfrak{P}_j}\right) \quad \text{for every } i = 1, \dots, m$$

so we denote it simply as the Artin symbol of $\mathfrak{p}$.

Up to now, we use the Artin symbol as a function mapping unramified prime ideals $\mathfrak{p}$ of K to Frobenius elements $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$. We wish to extend this map to a multiplicative homomorphism from the ideal group $I(\mathfrak{c})$ to $\mathrm{Gal}(L/K)$. We observe that, since any prime factor $\mathfrak{p}$ of any element $\mathfrak{a}$ of $I(\mathfrak{c})$ is unramified, the homomorphism $\pi_{\mathfrak{p}} \colon D(\mathfrak{p}/\mathfrak{a}) \longrightarrow \mathrm{Gal}(F_{\mathfrak{p}}/F_{\mathfrak{a}})$ is a bijection, so the construction is actually well defined.

Definition 3.7 (Artin map)**.** The *Artin map* is defined using the Frobenius maps $\sigma_{\mathfrak{p}}$'s and linearity as follows:

$$\left(\frac{L/K}{\cdot}\right) \colon I(\mathfrak{c}) \longrightarrow \mathrm{Gal}(L/K), \qquad \mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}}\right) = \left(\frac{L/K}{\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}}\right) := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

Note that the Artin map is defined by piecing together local information, one prime at a time.

One of the main result of class field theory is that the Artin map is surjective (this is part of what is known as *Artin's reciprocity law*).

Theorem 3.8. [2, X.1, Theorem 1, p. 199]. *Let L/K be an abelian extension. Then the Artin map is surjective as a map from $I(\mathfrak{c})$ to $\mathrm{Gal}(L/K)$, for any ideal $\mathfrak{c}$ divisible by all the ramified primes.*

Proof. Let $\mathfrak{c}$ be a fixed ideal of K, divisible by all the ramified primes. Let H be the subgroup of $\mathrm{Gal}(L/K)$ given by the image of the Artin map. Let F be the field fixed by H. We *claim* that $F = K$.

We first observe that, for any unramified prime $\mathfrak{p}$ in $I(\mathfrak{c})$, $\mathfrak{p}$ splits completely if and only if the Artin symbol of $\mathfrak{q}$ is equal to 1 for every prime $\mathfrak{q}$ that lies above $\mathfrak{p}$ (in fact, $\mathfrak{p}$ is unramified so $e_{\mathfrak{p}} = 1$, it splits if and only if the extension of residue fields has degree 1, i.e., $f_{\mathfrak{p}} = [F_{\mathfrak{q}} \colon F_{\mathfrak{p}}] = 1$. But then, the two conditions are equivalent to $e_{\mathfrak{p}} f_{\mathfrak{p}} = 1$, if and only if $D(\mathfrak{q}/\mathfrak{p}) = \langle \sigma_{\mathfrak{q}} \rangle = 1$).

So, using this observation, we deduce that any $\mathfrak{p} \in I(\mathfrak{c})$ must split completely in F (otherwise $\left(\frac{F/K}{\mathfrak{p}}\right) \neq 1$ and since $\left(\frac{F/K}{\mathfrak{p}}\right)$ is the restriction of $\left(\frac{L/K}{\mathfrak{p}}\right)$, this contradicts the fact that F is fixed by H). Thus, all but finitely many primes of K split completely in F. If we suppose, by contradiction, that $F \neq K$ then F contains a subfield F_0 which is cyclic over K, of degree > 1 and all but finitely many primes of K split completely in F_0. This contradicts a corollary of the *global norm index equality* (see [2, IX.5, p. 194]), namely, if the extension F_0/K is cyclic of degree > 1, then infinitely many primes of K do not split completely in F_0. This proves the theorem. □

The following proposition, which is a weak version of the *Artin's reciprocity law*, provides important global informations.

Proposition 3.9 (Artin Reciprocity)**.** [7, II.3.1, p. 117]. *Let L/K be a finite abelian extension of number fields. Then there exists an integral ideal $\mathfrak{c} \subset R_K$, divisible by precisely the primes of K that ramify in L, such that*

$$\left(\frac{L/K}{(\alpha)}\right) = 1 \qquad \text{for all } \alpha \in K^{\times} \text{ satisfying } \alpha \equiv 1 \pmod{\mathfrak{c}}.$$

Proof. See [2, X.2, p. 200]. □

Proposition (3.9) ensures the existence of the ideal, it can be not unique: if it is true for two ideals $\mathfrak{c}_1$ and $\mathfrak{c}_2$, then it is also true for $\mathfrak{c}_1 + \mathfrak{c}_2$.

Definition 3.10 (Conductor of the extension L/K)**.** We call the largest ideal for which Artin reciprocity is true the *conductor of the extension L/K* and denote it by $\mathfrak{c}_{L/K}$.

In view of (3.9), it is natural to define the group of principal ideals congruent to 1 modulo $\mathfrak{c}$:

$$P(\mathfrak{c}) = \{\, (\alpha) \colon \alpha \in K^{\times}, \alpha \equiv 1 \pmod{\mathfrak{c}} \,\}.$$

Artin reciprocity says that the kernel of the Artin map contains $P(\mathfrak{c})$ for an appropriate choice of $\mathfrak{c}$, more precisely if we take the conductor of the extension:

$$\mathfrak{a} \in P(\mathfrak{c}_{L/K}) \quad \Rightarrow \quad \left(\frac{L/K}{\mathfrak{a}}\right) = 1 \quad \Rightarrow \quad P(\mathfrak{c}_{L/K}) \subset \ker\left(\frac{L/K}{\cdot}\right).$$

It is important to observe that a principal ideal (α) may be in $P(\mathfrak{c})$ even if the generator $\alpha \not\equiv 1 \pmod{\mathfrak{c}}$: it suffices the existence of a unit $\varepsilon \in R_K^\times$ such that $\varepsilon\alpha \equiv 1 \pmod{\mathfrak{c}}$.

During the proof of theorem (3.8), we observed that a prime $\mathfrak{p}$ of K, unramified in L, splits completely in L if and only if the extension of residue fields has degree 1, or equivalently, if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. Thus, the unramified prime ideals in the kernel of the Artin map are precisely the primes of K that split completely in L.

Let K be a number field, let $\mathfrak{c}$ be an integral ideal of K and let $I(\mathfrak{c})$ be as above. Let $P_{\mathbb{Z}}(\mathfrak{c})$ denote the group of principal ideals of K which have a generator congruent to an integer modulo $\mathfrak{c}$. Let $G_{\mathfrak{c}} = I(\mathfrak{c})/P_{\mathbb{Z}}(\mathfrak{c})$ be the ideal class group of modulo $\mathfrak{c}$. let H be a subgroup of $G_{\mathfrak{c}}$ and let $\tilde{H}$ be its inverse image in $I(\mathfrak{c})$. An abelian extension L of K is said to be a *class field for* H if the prime ideals of K not dividing $\mathfrak{c}$ that split in L are exactly those in $\tilde{H}$.

In particular, a class field exists for each subgroup of a class group $G_{\mathfrak{c}}$, it is unique and every finite abelian extension of K arises as the class field of some subgroup of a class group.

If L is the class field of $H \subset G_{\mathfrak{c}}$ then

$$\mathrm{Gal}(L/K) \cong G_{\mathfrak{c}}/H$$

and the prime ideals $\mathfrak{p}$ of K not dividing $\mathfrak{c}$ are unramified in L and for every prime ideal $\mathfrak{q}$ of L that lies above $\mathfrak{p}$ the inertia index $f(\mathfrak{q}/\mathfrak{p})$ is equal to the order of the image of $\mathfrak{p}$ in the quotient group $G_{\mathfrak{c}}/H$.

More precisely, if $\mathfrak{c}' \mid \mathfrak{c}$ then $I(\mathfrak{c}) \subset I(\mathfrak{c}')$ defines a surjective homomorphism

$$G_{\mathfrak{c}} \longrightarrow G_{\mathfrak{c}'}.$$

If $H \subset G_{\mathfrak{c}}$ is the inverse image of $H' \subset G_{\mathfrak{c}'}$, then every class field for H' will also be a class field for H. If L is a class field for $H \subset G_{\mathfrak{c}}$ and H does not arise in this way from a prime ideal properly dividing $\mathfrak{c}$, then the set of prime ideals that divide $\mathfrak{c}$ consists exactly of the prime ideals ramifying in L.

Definition 3.11 (Ray class field)**.** Let $\mathfrak{c}$ be an integral ideal of K. A *ray class field of K (modulo $\mathfrak{c}$)* is a finite abelian extension $K_\mathfrak{c}/K$ such that for every finite abelian extension L/K

$$\mathfrak{c}_{L/K} \mid \mathfrak{c} \quad \Rightarrow \quad L \subset K_\mathfrak{c}$$

namely, if the conductor of the extension L/K divides the ideal $\mathfrak{c}$ then the field L is a subfield of $K_\mathfrak{c}$.

Ray class field of K is the class field corresponding to the subgroup $H' = P(\mathfrak{c})$ of the ideal class group $G_\mathfrak{c} = I(\mathfrak{c})/P(\mathfrak{c})$ and is characterized by the property that primes splitting completely are the principal ones and have a generator congruent to 1 modulo $\mathfrak{c}$. Intuitively, $K_\mathfrak{c}$ is the largest field with a given conductor (that need not actual to be equal to $\mathfrak{c}$). Moreover, if we apply the Artin map to the extension $K_\mathfrak{c}/K$ we see that it induces an isomorphism

$$G_\mathfrak{c} = I(\mathfrak{c})/P(\mathfrak{c}) \longrightarrow \mathrm{Gal}(K_\mathfrak{c}/K).$$

We conclude this section with the following proposition, that shows some results of class field theory. In order to understand what we are going to prove, we start with a definition.

Definition 3.12 (Norm ideal)**.** Given an extension L/K of number fields and a prime fractional ideal $\mathfrak{q}$ of L we define the fractional ideal $N_K^L(\mathfrak{q})$ of K as follows:

$$N_K^L(\mathfrak{q}) = \mathfrak{p}^f$$

where $\mathfrak{p} = \mathfrak{q} \cap R_K$ is a prime of K lying below $\mathfrak{q}$. The norm is multiplicative, so we can extend the definition to any fractional ideal $\mathfrak{a}$ of L.

Then we denote by $N_K^L(I_L)$ the group of norms from L to K of the fractional ideals of L, namely the group whose elements are of the form $N_K^L(\mathfrak{a})$ where $\mathfrak{a}$ ranges over the fractional ideals of L prime to the conductor $\mathfrak{c}_{L/K}$.

Proposition 3.13 (Class field theory)**.** [7, II.3.2, p. 118]. *Let L/K be a finite abelian extension of number fields, and let $\mathfrak{c}$ be an integral ideal of K.*

(a) *The Artin map $\left(\frac{L/K}{\cdot}\right)\colon I(\mathfrak{c}_{L/K}) \longrightarrow \mathrm{Gal}(L/K)$ is a surjective homomorphism.*

(b) *The kernel of the Artin map is $N_K^L(I_L)\, P(\mathfrak{c}_{L/K})$, where I_L is the group of non-zero fractional ideals of L coprime to $\mathfrak{c}_{L/K}$.*

(c) *There exists a unique ray class field $K_\mathfrak{c}$ of K (modulo $\mathfrak{c}$). The conductor of the extension $K_\mathfrak{c}/K$ is not necessarily $\mathfrak{c}$, but divides $\mathfrak{c}$.*

(d) *The ray class field $K_\mathfrak{c}$ is characterized by the property that it is an abelian extension of K and satisfies the following condition:*

$$\left\{ \begin{array}{c} \textit{primes of } K \textit{ that} \\ \textit{split completely in } K_\mathfrak{c} \end{array} \right\} = \{ \textit{ prime ideals in } P(\mathfrak{c}) \}\,.$$

Proof. (a) We already proved this fact in theorem (3.8).

(b) As we observed, by the Artin reciprocity (3.9) it follows that the kernel of the Artin map contains $P(\mathfrak{c}_{L/K})$.

Then we need to show that also the norm ideal $N_K^L(I_L)$ is contained into the kernel of the Artin map. Let $\mathfrak{q}$ be a prime ideal in I_L: it is a non-zero fractional ideal of L coprime to $\mathfrak{c}_{L/K}$ and so, by the definition of $\mathfrak{c}_{L/K}$, it is coprime to every prime ideal of K that ramifies in L. It means that the prime ideal $\mathfrak{p} = \mathfrak{q} \cap R_K$ of K that lies below $\mathfrak{q}$ is unramified in L. Then we can compute the norm of the prime ideal $\mathfrak{q}$, that is

$$N_K^L(\mathfrak{q}) = \mathfrak{p}^f$$

where $f = f(\mathfrak{q}/\mathfrak{p})$ is the inertia index of $\mathfrak{q}$ above $\mathfrak{p}$. Next, we apply the Artin map:

$$\left(\frac{L/K}{N_K^L(\mathfrak{q})}\right) = \sigma_\mathfrak{p}^f = 1$$

since the order of the Frobenius element $\sigma_\mathfrak{p} \in \mathrm{Gal}(L/K)$ equals $f(\mathfrak{q}/\mathfrak{p})$ for every prime above $\mathfrak{p}$ (since we work with abelian extensions, the Frobenius element depends only on $\mathfrak{p}$ and not on its prime factors, and since we consider unramified primes the inertia index of the factors over $\mathfrak{p}$ has the same value). Thus for every $\mathfrak{a} \in I_L$, it can be factored as product of powers of prime ideals $\mathfrak{q}_i$ of L, and, by applying the Artin map on the norm of each prime factor we obtain 1, so by the definition of the Artin map it follows that

$$\left(\frac{L/K}{N_K^L(\mathfrak{a})}\right) = 1.$$

so $N_K^L(I_L)$ is contained into the kernel of the Artin map.

Hence the ideal $N_K^L(I_L)\,P(\mathfrak{c}_{L/K})$ is contained into the kernel. Then using the *universal norm index inequality* (see [2, VIII.3, p. 164]) we obtain that it is actually an equality,

$$\ker\left(\left(\frac{L/K}{\cdot}\right)\right) = N_K^L(I_L)\,P(\mathfrak{c}_{L/K})$$

and this concludes the proof of (b).

(c) The *existence theorem* (see [1, 2.8.A, Theorem 8.6, p. 162]) asserts that every generalized ideal class group is the Galois group of some abelian extension L of K. So, given any ideal $\mathfrak{c}$ in K, the theorem ensures that there is a unique abelian extension $K_\mathfrak{c}$ of K such that

$$P(\mathfrak{c}) = \ker\left(\left(\frac{L/K}{\cdot}\right)\right)$$

where $P(\mathfrak{c})$ is the subgroup of $P_\mathbb{Z}(\mathfrak{c})$ of the principal ideals coprime to $\mathfrak{c}$ with a generator congruent to 1 modulo $\mathfrak{c}$. The field $K_\mathfrak{c}$ is exactly the ray class field of K modulo $\mathfrak{c}$ and then it is unique.

The statement about the conductor of the ray class field follows from the definition.

(d) From [4, Theorem 0.7, p. 9], let L be an abelian extension of K of conductor $\mathfrak{c}_{L/K}$, then the Artin map $\left(\frac{L/K}{\cdot}\right)\colon I(\mathfrak{c}_{L/K}) \longrightarrow \mathrm{Gal}(L/K)$ factors through $G_{\mathfrak{c}_{L/K}}$ and defines an isomorphism

$$I(\mathfrak{c}_{L/K})/N_K^L(I_L)\,P(\mathfrak{c}_{L/K}) \longrightarrow G_{\mathfrak{c}_{L/K}}.$$

In particular, the prime ideals of K splitting in L are exactly those in the subgroup of $I(\mathfrak{c}_{L/K})$

$$\tilde{H} = N_K^L(I_L)\,P(\mathfrak{c}_{L/K}).$$

Then, if we apply this theorem with $L = K_\mathfrak{c}$ and recall that if we apply the Artin map to the extension $K_\mathfrak{c}/K$, it induces an isomorphism

$$G_\mathfrak{c} = I(\mathfrak{c})/P(\mathfrak{c}) \longrightarrow \mathrm{Gal}(K_\mathfrak{c}/K),$$

it follows that $\tilde{H} = P(\mathfrak{c})$. This concludes the proof of (d).

□

In particular, from (3.13.a) and (3.13.b), by applying the I^{st} *homomorphism theorem*, we see that the Artin map induces the follows isomorphism

$$I(\mathfrak{c}_{L/K})/(N_K^L I_L)P(\mathfrak{c}_{L/K}) \cong \mathrm{Gal}(L/K).$$

3.2 Hilbert class field

Definition 3.14 (Hilbert class field)**.** Consider the ray class field of K modulo the unit ideal $\mathfrak{c} = (1)$. It is the maximal abelian extension of K which is unramified at all primes. We call the field $K_{(1)}$ the *Hilbert class field of* K and denote it by H or H_K.

We notice that, by (3.13.c), the conductor of the extension divides the modulus $\mathfrak{c} = (1)$, so $\mathfrak{c}_{H/K} \mid (1)$, that implies necessarily that $\mathfrak{c}_{H/K} = (1)$. Then

$$I(\mathfrak{c}_{H/K}) = I((1)) = \{ \text{ all non-zero fractional ideals of } K \}$$
$$P(\mathfrak{c}_{H/K}) = P((1)) = \{ \text{ all non-zero principal ideals of } K \}$$

so the Artin map induces an isomorphism between the ideal class group of K and the Galois group of the Hilbert class field of K:

$$\left(\frac{H/K}{\cdot}\right) \colon C\mathcal{L}(R_K) \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

We can see some easy examples of the things we defined above, in particular [4, V.3, Examples 3.9, 3.10, p. 155], [7, II.6, Example 6.2.1, 6.2.2, p. 141-142] and [7, II, Exercise 2.13, p. 180].

Example 3.15. The Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself, since its class number is $h_{\mathbb{Q}} = 1$.

As it is well known, there are only nine quadratic imaginary fields of class number equal to 1, namely

$$K_m = \mathbb{Q}(\sqrt{-m}) \qquad \text{with } m \in \{ 1, 2, 3, 7, 11, 19, 43, 67, 163 \}.$$

For each of these fields then

$$h_{K_m} = [H_m : K_m] = 1 \qquad \Longrightarrow \qquad H_m = K_m$$

namely, each of these fields is equal to its Hilbert class field.

Now let's look at an example with class number larger than 1. Consider the field $K = \mathbb{Q}(\sqrt{-15})$. Since $m = -15 \equiv 1 \pmod 4$, then its ring of integers is

$$R_K = \mathbb{Z}[\alpha] \qquad \text{where } \alpha = \frac{1 + \sqrt{-15}}{2}.$$

The class number of the field is $h_K = 2$ and a non-trivial ideal class is given by the ideal $\mathfrak{a} = 2\mathbb{Z} + \alpha\mathbb{Z}$. Further, in order to find the Hilbert class field of K we look for the primes that ramify in K. Let p be a prime divisor of m, namely $p = 3$ or $p = 5$. Since in both the cases p is an odd prime, then both the ideals (3) and (5) ramify in R_K as

$$3R_K = (3, \sqrt{-15})^2 \qquad\qquad 5R_K = (5, \sqrt{-15})^2.$$

If we consider the prime $p = 2$, since $-15 \equiv 1 \pmod 8$ then the ideal $2R_K$ splits completey, while if we take p as any other prime it totally decomposes or is inert.

Then we consider the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$: the only ramified prime in the former is $p = 5$, in the latter is $p = 3$. This means that the field $H = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ is everywhere unramified over $K = \mathbb{Q}(\sqrt{-15})$, so H is the Hilbert class field of K.

The Hilbert class field of the field $L = \mathbb{Q}(\sqrt{-5})$ is $H = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$. In fact, let $m = -5 \equiv 3 \pmod 4$, then the ring of integers of L is

$$R_L = \mathbb{Z}[\sqrt{-5}].$$

If $p \in \mathbb{Z}$ is a prime that divides -5, namely $p = 5$, then the ideal $(p) = (5)$ ramifies in L as

$$5\, R_L = (5, \sqrt{-5})^2.$$

If $p = 2$ then also the ideal $(p) = (2)$ ramifies in L as

$$2\, R_L = (2, \sqrt{-5} + 1)^2.$$

Any other prime is inert or unramified. Then we observe that

- in the field $\mathbb{Q}(\sqrt{5})$ the only prime that ramifies is exactly $p = 5$;
- in the field $\mathbb{Q}(\sqrt{-1})$ the only prime that ramifies is exactly $p = 2$.

so the primes of $\mathbb{Q}(\sqrt{-5})$ that divide 5 and 2, precisely the ideals $(5, \sqrt{-5})$ and $(2, \sqrt{-5} + 1)$ respectively, do not ramify in the field $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$. So we can conclude that this field is the Hilbert class field of $L = \mathbb{Q}(\sqrt{-5})$.

Example 3.16. Let m be a positive integer which is odd or divisible by 4. The ray class field for the ideal $= (m)$ is $K_{(m)} = \mathbb{Q}(\zeta_m + \bar{\zeta_m})$ where ζ_m is a m^{th}-primitive root of the unit.

Thus, the reciprocity law implies the *Kronecker-Weber theorem*: every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Example 3.17. Let $K = \mathbb{Q}(\imath)$. We denote, as usual, by $K_{(c)}$ the ray class field of K modulo the principal ideal (c) for $c \in \mathbb{Z}$. Then we will compute in the next chapter, precisely in the example (4.24), the ray class fields of K with respect to the ideals (2), (3), (4):

$$K_{(2)} = K, \qquad K_{(3)} = K(\sqrt{3}), \qquad K_{(4)} = K(\sqrt{2}).$$

Chapter 4

Applications of the theory of complex multiplication to class field theory

4.1 Rationality of j

In this section we will study the field of definition for elliptic curves with complex multiplication and their endomorphisms. First of all we can show that any CM elliptic curve is defined over an algebraic extension of $\mathbb{Q}$.

It is useful to recall the definition of the field of algebraic numbers

$$\bar{\mathbb{Q}} = \{\, z \in \mathbb{C} \colon \text{ there exists a non-zero } f(x) \in \mathbb{Q}[x] \text{ such that } f(z) = 0 \,\}$$

and the fact that $\mathbb{Q} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$.

Given an elliptic curve $E/\mathbb{C}$, we can associate to it a Weierstrass equation with coefficients in $\mathbb{C}$ of the form

$$E \colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let $\sigma \colon \mathbb{C} \to \mathbb{C}$ be any field automorphism of $\mathbb{C}$. Then we can construct a new elliptic curve E^σ from E simply by letting σ act on the coefficients of the Weierstrass equation of E

$$E^\sigma \colon y^2 + a_1^\sigma xy + a_3^\sigma y = x^3 + a_2^\sigma x^2 + a_4^\sigma x + a_6^\sigma.$$

Proposition 4.1. [7, II.2.1, p. 104].

(a) *Let $E/\mathbb{C}$ be an elliptic curve, let $\sigma\colon \mathbb{C} \to \mathbb{C}$ be any field automorphism of $\mathbb{C}$. Then* $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

(b) *Let K be a quadratic imaginary field, let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by R_K. Then the j-invariant of E is algebraic, namely, $j(E) \in \bar{\mathbb{Q}}$.*

(c) *It holds*

$$\mathcal{ELL}(R_K) = \frac{\left\{ \textit{elliptic curves } E/\bar{\mathbb{Q}} \textit{ with } \mathrm{End}(E) \cong R_K \right\}}{\textit{isomorphism over } \bar{\mathbb{Q}}}$$

(the point is that the definition of $\mathcal{ELL}(R_K)$ is in terms of isomorphism classes of elliptic curves over $\mathbb{Q}$, not over $\bar{\mathbb{Q}}$).

Proof. (a) If $\phi\colon E \to E$ is an endomorphism of E, clearly $\phi^\sigma\colon E^\sigma \to E^\sigma$ is an endomorphism of E^σ. This gives the isomorphism between the two spaces of endomorphism.

(b) Let $\sigma \in \mathrm{Aut}(\mathbb{C})$, given E we obtain E^σ as previously showed. Since $j(E)$ is a rational combination of the coefficients of the Weierstrass equation, it is clear that $j(E^\sigma) = (j(E))^\sigma$. On the other hand, by (a)

$$\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong R_K$$

(the latter relation is by assumption). So, by the proposition (2.26.b), E^σ is contained in one of the $\mathbb{C}$-isomorphism classes of elliptic curves, which are finitely many. By the proposition (1.5.b), the isomorphism class of an elliptic curves is determined by its j-invariant, so it follows that $j(E)^\sigma$ takes on only finitely many values as σ runs over $\mathrm{Aut}(\mathbb{C})$, namely the set of conjugates of $j(E)$ is finite. It means that the degree of the extension of fields $[\mathbb{Q}(j(E))\colon \mathbb{Q}]$ is finite, i.e. $j(E)$ is an algebraic number.

(c) For any subfield $F \subset \mathbb{C}$, we denote

$$\mathcal{ELL}_F(R_K) = \frac{\{\text{ elliptic curves } E/F \text{ with } \mathrm{End}(E) \cong R_K \}}{\text{isomorphism over } F}.$$

Fix an embedding $\bar{\mathbb{Q}} \subset \mathbb{C}$: then it induces a natural map

$$\varepsilon\colon \mathcal{ELL}_{\bar{\mathbb{Q}}}(R_K) \longrightarrow \mathcal{ELL}_{\mathbb{C}}(R_K)$$

We *claim* that ε is a bijection:

- to prove the *surjectivity*: let $E/\mathbb{C}$ be a representative of its isomorphism class in $\mathcal{ELL}_{\mathbb{C}}(R_K)$, then
  - $j(E) \in \bar{\mathbb{Q}}$, by (b);
  - there exists an elliptic curve $E'/\mathbb{Q}(j(E))$ with $j(E') = j(E)$, by (1.5.c);
  - E' is isomorphic to E over $\mathbb{C}$.

  These three facts tell us that $\varepsilon(E') = E$, so that ε is surjective.
- to prove the *injectivity*: let $E_1/\bar{\mathbb{Q}}$ and $E_2/\bar{\mathbb{Q}}$ be representatives of their isomorphism classes in $\mathcal{ELL}_{\bar{\mathbb{Q}}}(R_K)$ and suppose that $\varepsilon(E_1) = \varepsilon(E_2)$, i.e., they generate the same class in $\mathcal{ELL}_{\mathbb{C}}(R_K)$. Then, by the proposition (1.5.b), we can deduce that $j(E_1) = j(E_2)$. Again from (1.5.b), it follows that E_1 and E_2 are isomorphic over $\bar{\mathbb{Q}}$, so they actually represent the same element in $\mathcal{ELL}_{\bar{\mathbb{Q}}}(R_K)$ and it implies that ε is injective.

□

Then we can study the effect of the field automorphisms over the maps $[\alpha]\colon E \to E$ described in the proposition (2.4) and find a field of definition for them. Note that if ϕ is an endomorphism of E and σ is any automorphism of $\mathbb{C}$, then ϕ^σ is an endomorphism of E^σ.

Theorem 4.2. [7, II.2.2, p. 105].

(a) *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring $R \subset \mathbb{C}$, then*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}, \qquad \text{for all } \alpha \in R \text{ and for all } \sigma \in \mathrm{Aut}(\mathbb{C})$$

where the isomorphism $[\,\cdot\,]_E\colon R \xrightarrow{\sim} \mathrm{End}(E)$ and $[\,\cdot\,]_{E^\sigma}\colon R \xrightarrow{\sim} \mathrm{End}(E^\sigma)$ are normalized as in (2.4).

(b) *Let E be an elliptic curve defined over a field $L \subset \mathbb{C}$, with complex multiplication by the quadratic imaginary field $K \subset \mathbb{C}$. Then every endomorphism of E is defined over the compositum LK.*

(c) *Let E_1/L and E_2/L be two elliptic curves defined over a field $L \subset \mathbb{C}$. Then there is a finite extension L'/L such that every isogeny from E_1 to E_2 is defined over L'.*

Proof. (a) Let $\omega \in \Omega_E$ be a non-zero invariant differential on E, then the normalization of $[\,\cdot\,]$ says that

$$[\alpha]_E^* \omega = \alpha\omega.$$

Further, for all $\sigma \in \mathrm{Aut}(\mathbb{C})$, ω^σ is an invariant differential on E^σ, so again by the normalization of $[\,\cdot\,]$ it follows that

$$([\beta]_{E^\sigma})^* \omega^\sigma = \beta\omega^\sigma \qquad \text{for all } \beta \in R.$$

Now, for any $\alpha \in R$ and for any $\sigma \in \mathrm{Aut}(\mathbb{C})$ we get

$$([\alpha]_E^\sigma)^*(\omega^\sigma) = ([\alpha]_E^* \omega)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma \omega^\sigma = ([\alpha^\sigma]_{E^\sigma})^*(\omega^\sigma).$$

Thus $[\alpha]_E^\sigma$ and $[\alpha^\sigma]_{E^\sigma}$ have the same effect on the invariant differential ω^σ. It follows that the natural map $\mathrm{End}(E^\sigma) \longrightarrow \mathrm{End}(\Omega_{E^\sigma})$, $\psi \mapsto \psi^*$ is injective: for all $\phi, \psi \in \mathrm{End}(E^\sigma)$ suppose that $\phi^* = \psi^*$. Since we work with fields of $\mathrm{char}(K) = 0$, any finite function is separable, in particular ϕ, ψ are separable: by [6, II.4.2, p. 30], already cited at the beginning of the subsection (1.1.6), both ϕ^*, ψ^* are injective. If we take dx as a basis for $\mathrm{End}(\Omega_{E^\sigma})$, then

$$\phi^*(dx) = \psi^*(dx) \Leftrightarrow d(\phi^* x) = d(\psi^* x) \Leftrightarrow d(x \circ \phi) = d(x \circ \psi)$$

and then we can conclude that $\phi = \psi$. This implies, then, that $[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}$.

(b) Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be an automorphism that fixes L: since, by definition, E is defined over L, then we can take a Weierstrass equation with coefficients in L, so $E^\sigma = E$. By (a), for all $\alpha \in R$

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} = [\alpha^\sigma]_E.$$

Then we suppose that σ fixes also K, so $\alpha^\sigma = \alpha$. This proves that

$$[\alpha]_E^\sigma = [\alpha]_E \qquad \text{for all } \sigma \in \mathrm{Aut}(\mathbb{C}) \text{ such that } \sigma \text{ fixes } LK.$$

Hence the endomorphism $[\alpha]$ is defined over LK.

(c) As in (b), we can take Weierstrass equations for E_1 and E_2 with coefficients in L. Let $\phi \in \mathrm{Hom}(E_1, E_2)$ be an isogeny, then for any $\sigma \in \mathrm{Aut}(\mathbb{C})$ that fixes L we have that also $\phi^\sigma \in \mathrm{Hom}(E_1, E_2)$, and that $\deg(\phi^\sigma) = \deg(\phi)$. From [6, III.4.11, p. 73] it follows that an isogeny as ϕ is determined by

its kernel, up to isomorphism of E_1 and E_2. Since E_1 has only finitely many subgroups of any finite order and both $\mathrm{Aut}(E_1)$ and $\mathrm{Aut}(E_1)$ are finite, then $\mathrm{Hom}(E_1, E_2)$ contains only finitely many isogenies of a given degree. Therefore $\{\, \phi^\sigma : \phi \in \mathrm{Aut}(\mathbb{C}), \sigma \text{ fixes } L \,\}$ is a finite set, which implies that ϕ is defined over a finite extension of L. Finally, by [6, III.7.5, p. 91], $\mathrm{Hom}(E_1, E_2)$ is a finitely generated group, so it suffices to take a field of definition for some finite set of generators.

□

Remark 4.3. [7, II.2.2.1, p. 107]. Using (2.26.b) and (4.1.b) we can deduce that, if $\mathrm{End}(E) \cong R_K$, then

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$$

where $h_K = |C\mathcal{L}(R_K)|$ is the class number of K.

Actually we will prove in the theorem (4.15.a) that also the other inequality holds, so it is an equality.

In particular $j(E) \in \mathbb{Q}$ if and only if $h_K = 1$.

Example 4.4. [7, II.2.2.2, p. 107]. In view of this observation we see that, if R_K has class number 1, then E has a model over $\mathbb{Q}$. We have already seen an example of this, precisely in the example (2.27), where we looked at curves with complex multiplication by the ring $\mathbb{Z}[\imath]$. From what we computed into the example, the curve of Weierstrass equation

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

has this property. By the proposition (2.4) there is a unique isomorphism $[\,\cdot\,] : \mathbb{Z}[\imath] \xrightarrow{\sim} \mathrm{End}(E)$ that normalizes the curve E, namely, such that for every invariant differential $\omega \in \Omega_E$ on E

$$[\alpha]^*\omega = \alpha\omega, \quad \text{for all } \alpha \in \mathbb{Z}[\imath].$$

We can easily show that the isomorphism

$$[\imath] : \mathbb{Z}[\imath] \xrightarrow{\sim} \mathrm{End}(E), \qquad (x, y) \mapsto [\imath](x, y) = (-x, \imath y)$$

is the correct one: it suffices to show that it satisfies the characterizing property and then we can conclude by unicity. Let $\omega = \dfrac{dx}{y}$ be an invariant differential on E, then

$$[\imath]\frac{dx}{y} = \frac{d(-x)}{\imath y} = \imath\frac{dx}{y}.$$

We can show that E satisfies the theorem (4.2.a) with the isomorphism $[\imath]$. If $\sigma \in \mathrm{Aut}(\mathbb{C})$ is the complex conjugation automorphism, then

$$\begin{aligned}([\imath](x,y))^\sigma &= ((-x,\imath y))^\sigma = (-x^\sigma, (\imath y)^\sigma) = (-x^\sigma, \imath^\sigma y^\sigma) \\ &= (-x^\sigma, -\imath y^\sigma) = [-\imath](x^\sigma, y^\sigma) = [\imath^\sigma](x^\sigma, y^\sigma)\end{aligned}$$

and we conclude that $[\imath]^\sigma = [\imath^\sigma]$, as it should be by (4.2.a).

An immediate consequence of (2.31.b) and (4.2.b) is that the torsion points of E generate abelian extensions of $K(j(E))$.

Theorem 4.5. [7, II.2.3, p. 108]. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring of integers R_K of the quadratic imaginary field K. Let*

$$L = K(j(E), E_{tors})$$

be the field generated by the j-invariant of E and the coordinates of the torsion points of E. Then L is an abelian extension of the field $K(j(E))$.

Proof. We denote by $H = K(j(E))$ the extension field and, for all $m \in \mathbb{Z}$, define the family of fields

$$L_m = K(j(E), E[m]) = H(E[m]),$$

namely, the extensions of H generated by the m-torsion points of E for each m. Since L is the compositum of all the L_m's, it suffices to show that each L_m is an abelian extension of H. So we fix $m \in \mathbb{Z}$ and define an action of $\mathrm{Gal}(\bar{K}/H)$ over $E[m]$ as follows:

$$\mathrm{Gal}(\bar{K}/H) \times E[m] \longrightarrow E[m], \qquad (\sigma, P) \mapsto \sigma \circ P := P^\sigma.$$

It is easy to see that the action is well defined (for all $P \in E[m]$ by definition $[m]P = 0$, so $[m](P^\sigma) = ([m]P)^\sigma = 0^\sigma = 0$, so actually $P^\sigma \in E[m]$). It follows that there is a representation

$$\rho\colon \mathrm{Gal}(\bar{K}/H) \longrightarrow \mathrm{Aut}(E[m]), \qquad \sigma \mapsto \rho(\sigma)\colon E[m] \longrightarrow E[m]$$

such that $\rho(\sigma)(P) = P^\sigma$ for all $\sigma \in \mathrm{Gal}(\bar{K}/H), P \in E[m]$. For an arbitrary elliptic curve, this tells us that $\mathrm{Gal}(L_m/H)$ injects into the automorphism group of the abelian group $E[m]$:

$$\mathrm{Gal}(\bar{K}/H) \lesssim \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

namely, $\mathrm{Gal}(L_m/H)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. But E has complex multiplication, so we can take a model for E defined over H and, by (4.2.b), every endomorphism of E is also defined over H. So every element $\sigma \in \mathrm{Gal}(L_m/H)$ will commute with every element $\alpha \in R_K$ in their action on $E[m]$:

$$([\alpha]P)^\sigma = [\alpha](P^\sigma).$$

It means that ρ is an homomorphism from the group $\mathrm{Gal}(\bar{K}/H)$ to the group of R_K/mR_K-module automorphism of $E[m]$, hence it induces an injection

$$\phi\colon \mathrm{Gal}(L_m/H) \hookrightarrow \mathrm{Aut}_{R_K/mR_K}(E[m]).$$

Then, by using (2.31.b) that says that $E[m]$ is a free R_K/mR_K-module of rank 1, we get that

$$\mathrm{Aut}_{R_K/mR_K}(E[m]) \cong (R_K/mR_K)^\times$$

so we can conclude that $\mathrm{Gal}(L_m/H)$ is abelian. □

Remark 4.6. In general L is not an abelian extension of K.

From now on, we will use (4.1) to identify $\mathcal{ELL}(R_K)$ with the $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves with complex multiplication by R_K. Then there is a natural action of $\mathrm{Gal}(\bar{K}/K)$ on $\mathcal{ELL}(R_K)$ defined as follows:

$$\mathrm{Gal}(\bar{K}/K) \times \mathcal{ELL}(R_K) \longrightarrow \mathcal{ELL}(R_K), \quad (\sigma, [E]) \mapsto [E^\sigma]$$

where $[E]$ denotes the isomorphism classe of the curve E. On the other hand, we showed in (2.26.b) that the class group $C\ell(R_K)$ acts on $\mathcal{ELL}(R_K)$ with a simply transitive action, so there is a unique $\bar{\mathfrak{a}} \in C\ell(R_K)$, depending on σ, such that

$$\bar{\mathfrak{a}} * E = E^\sigma.$$

In other words, there is a well defined map

$$F\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow C\ell(R_K), \qquad \sigma \longmapsto F(\sigma) = \mathfrak{a}$$

such that $E^\sigma = F(\sigma) * E$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Our goal is to study this map F in order to describe completely the field $K(j(E))$. It is easy to show that F has the following properties:

- F is a homomorphism;
- F is independent of the choice of the curve $E \in \mathcal{ELL}(R_K)$;

- F is actually well defined on the larger group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, but only on $\mathrm{Gal}(\bar{K}/K)$ the independence on the curve holds.

Before proving those properties, we note that the definition of F has an essential analytic component, since $F(\sigma)$ depends on the way the in which the lattice associated to the elliptic curve changes when the lattice is multiplied by an ideal. Thus, if we denote by $j(\Lambda)$ the j-invariant of the curve E_Λ, we know it is an analytic function of Λ, and the map F is characterized by the formula

$$j(\Lambda)^\sigma = j(F(\sigma)^{-1}\Lambda)$$

so F converts the algebraic action of σ into the analytic action of multiplication by $F(\sigma)^{-1}$.

Proposition 4.7. [7, II.2.4, p. 112]. *Let $K/\mathbb{Q}$ be a quadratic imaginary field. There exists a homomorphism*

$$F\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathcal{CL}(R_K), \qquad \sigma \longmapsto F(\sigma)$$

uniquely characterized by the following condition:

$$E^\sigma = F(\sigma) * E \qquad \text{for all } \sigma \in \mathrm{Gal}(\bar{K}/K) \text{ and for all } E \in \mathcal{ELL}(R_K).$$

This tells us exactly that F is independent on the choice of the curve E.

Proof. By (2.26.b) and (4.1) it follows that, for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and for all $E \in \mathcal{ELL}(R_K)$ there exists a unique $\bar{\mathfrak{a}} \in \mathcal{CL}(R_K)$ such that $E^\sigma = \bar{\mathfrak{a}} * E$. So, for a fixed elliptic curve E, we get a well-defined map F as in the proposition.

We first show that F is a *homomorphism*: for all $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$

$$\begin{aligned} F(\sigma\tau) = E^{\sigma\tau} &= (E^\sigma)^\tau = (F(\sigma) * E)^\tau \\ &= F(\tau) * (F(\sigma) * E) = (F(\tau)F(\sigma)) * E \\ &= (F(\sigma)F(\tau)) * E \end{aligned}$$

(where, in the last equality, we use the fact that the group $\mathcal{CL}(R_K)$ is abelian).

Then we show that F is *independent of the choice of E*: let $E_1, E_2 \in \mathcal{ELL}(R_K)$, let $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we can write $E_1^\sigma = \bar{\mathfrak{a}}_1 * E_1$, $E_2^\sigma = \bar{\mathfrak{a}}_2 * E_2$ and we need to show that $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$. Since $\mathcal{CL}(R_K)$ acts transitively on $\mathcal{ELL}(R_K)$, then there exists $\bar{\mathfrak{b}}$ such that $E_2 = \bar{\mathfrak{b}} * E_1$. Then

$$(\bar{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \bar{\mathfrak{a}}_2 * E_2 = \bar{\mathfrak{a}}_2 * (\bar{\mathfrak{b}} * E_1) = (\bar{\mathfrak{a}}_2\bar{\mathfrak{b}}\bar{\mathfrak{a}}_1^{-1}) * E_1^\sigma.$$

In order to go on with the proof, we need the following

Proposition 4.8. [7, II.2.5, p. 112]. *Let $E/\bar{\mathbb{Q}}$ be an elliptic curve representing an element of $\mathcal{ELL}(R_K)$, let $\bar{\mathfrak{a}} \in \mathcal{ELL}(R_K)$ and let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then*

$$(\bar{\mathfrak{a}} * E)^\sigma = \bar{\mathfrak{a}}^\sigma * E^\sigma.$$

This statement gives us the relationship between the algebraic action of σ and the analytic action of multiplication by $\bar{\mathfrak{a}}$. The idea behind the proof is that $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \bar{\mathfrak{a}} * E \cong \mathrm{Hom}(\mathfrak{a}, E)$ and we want to describe $\mathrm{Hom}(\mathfrak{a}, E)$ as an algebraic variety and not just as an R_K-module.

Proof. We choose a lattice Λ such that $E_\Lambda \cong E$ and fix an exact sequence

$$R_K^m \xrightarrow{A} R_K^n \longrightarrow \mathfrak{a} \longrightarrow 0$$

where A denotes a $n \times m$ matrix with coefficients in R_K. Let $\mathrm{Hom}(-,-)$ denote the homomorphism of R_K-modules: we apply it to the product of the previous exact sequence with the following one:

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{C} \longrightarrow E \longrightarrow 0$$

and, recalling that $\mathrm{Hom}(-,-)$ is covariant on the first entry, contravariant on the second, we obtain the following commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathfrak{a}, \Lambda) & \longrightarrow & \mathrm{Hom}(\mathfrak{a}, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathfrak{a}, E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(R_K^n, \Lambda) & \longrightarrow & \mathrm{Hom}(R_K^m, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(R_K^n, E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(R_K^m, \Lambda) & \longrightarrow & \mathrm{Hom}(R_K^m, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(R_K^n, E)
\end{array}$$

For any R_K-module M we have that $\mathrm{Hom}(R_K^n, M) \cong M^n$; moreover, we have also the following tool:

Lemma 4.9. [7, II.2.5.1, p. 113]. *Let R be a Dedekind domain, let $\mathfrak{a}$ be a fractional ideal of R and let M be a torsion-free R-module. Then the natural map*

$$\phi\colon \mathfrak{a}^{-1}M \longrightarrow \mathrm{Hom}_R(\mathfrak{a}, M) \qquad x \mapsto (\phi_x\colon \alpha \mapsto \alpha x)$$

is an isomorphism.

So, using this lemma first with $M = \Lambda$, then with $M = \mathbb{C}$, the previous commutative diagram can be rewritten as

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathfrak{a}^{-1}\Lambda & \longrightarrow & \mathbb{C} & \longrightarrow & \mathrm{Hom}(\mathfrak{a}, E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \Lambda^n & \longrightarrow & \mathbb{C}^n & \longrightarrow & E^n \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \Lambda^m & \longrightarrow & \mathbb{C}^m & \longrightarrow & E^m
\end{array}$$

where A^t denotes the transpose of the matrix A. The bottom two rows are exact on the right, since they are just a number of copies of the exact sequence $0 \to \Lambda \to \mathbb{C} \to E \to 0$. So we can apply the *Snake lemma* to the bottom two rows and get a new exact sequence:

$$0 \longrightarrow \mathfrak{a}^{-1}\Lambda \longrightarrow \mathbb{C} \longrightarrow \ker(E^n \xrightarrow{A^t} E^m) \longrightarrow \Lambda^m/A^t\Lambda^n.$$

Note that, since A^t is a matrix with coefficients in $\mathrm{End}(R_K) = R_K$, the map $E^m \xrightarrow{A^t} E^n$ is an algebraic map of algebraic varieties. Hence its kernel, namely, the inverse image of the point $(0, 0, \ldots, 0) \in E^m$ is an algebraic subvariety of E^n. Both E^n and E^m are group varieties, so this kernel is an algebraic group variety. Further, by (4.2.a), it follows that, for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, the corresponding map

$$(E^\sigma)^n \xrightarrow{(A^\sigma)^t} (E^\sigma)^m$$

is obtained by considering the entries of A^t as elements of $R_K \subset \mathbb{C}$ and by applying σ to each of them. On the other hand, looking at the complex topology we note that $\Lambda^n/A^t\Lambda^m$ is discrete and $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ is connected. So the last exact sequence gives

$$(\mathfrak{a} * E) = \mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong (\text{identity component of } \ker(E^n \xrightarrow{A^t} E^m)).$$

This describes algebraically $\mathfrak{a} * E$ in terms of the algebraic map $E^n \xrightarrow{A^t} E^m$. Then for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ we apply the characterization first on E, then on E^σ: we

obtain

$$\begin{aligned}(\mathfrak{a} * E)^\sigma &= (\text{identity component of } \ker(E^n \xrightarrow{A^t} E^m)) \\ &= (\text{identity component of } \ker((E^\sigma)^n \xrightarrow{(A^\sigma)^t} (E^\sigma)^m)) \\ &= \mathfrak{a}^\sigma * E^\sigma.\end{aligned}$$

This completes the proof of (4.8). □

Then, the last result in the proof of (4.7) was that $(\bar{\mathfrak{b}} * E_1)^\sigma = (\bar{\mathfrak{a}}_2 \bar{\mathfrak{b}} \bar{\mathfrak{a}}_1^{-1}) * E_1^\sigma$. We note that, since $\mathfrak{b} \subset K$ and $\sigma \in \mathrm{Gal}(\bar{K}/K)$, surely $\bar{\mathfrak{b}}^\sigma = \bar{\mathfrak{b}}$. Using this observation and the proposition (4.8), we obtain that

$$(\bar{\mathfrak{a}}_2 \bar{\mathfrak{b}} \bar{\mathfrak{a}}_1^{-1}) * E_1^\sigma = (\bar{\mathfrak{b}} * E_1)^\sigma = \bar{\mathfrak{b}} * E_1^\sigma$$

and we can cancel $\bar{\mathfrak{b}}$ from both sides, so

$$E_1^\sigma = (\bar{\mathfrak{a}}_2 \bar{\mathfrak{a}}_1^{-1}) * E_1^\sigma$$

and we can conclude, by (2.26.a.iii) that $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$. □

4.2 Hilbert class field of K

Our goal in this section is to prove the following theorem:

Theorem 4.10. [7, II.4.1, p. 121]. *Let $K/\mathbb{Q}$ be a quadratic imaginary field with ring of integers R_K and let $E/\mathbb{C}$ be an elliptic curve with* $\mathrm{End}(E) \cong R_K$. *Then $K(j(E))$ is the Hilbert class field H of K.*

In other words, this theorem says that the Hilbert class field of a quadratic imaginary field K is generated by the value of a certain holomorphic function $j(\tau)$ evaluated at a generator of the ring of integers of K. In fact, once we fix the field K we have fixed the ring R_K and then we can produce an elliptic curve E with endomorphism ring $\mathrm{End}(E) = R_K$ in several ways. At the beginning of the section (2.3) we have seen that, if if $\mathfrak{a}$ is a non-zero fractional ideal of K the elliptic curve $E_\mathfrak{a}$ satisfies this request. Another method is to take directly the curve corresponding to the lattice $\Lambda = R_K$. So we consider the second construction. We can associate to the curve a Weierstrass equation of the form

$$Y^2 = X^3 - g_2(R_K)X - g_3(R_K)$$

and finally compute the j-invariant associate to the curve:

$$j(E) = j(R_K) = 1728\frac{g_2(R_K)^3}{g_2(R_K)^3 - 27g_3(R_K)^2},$$

given in terms of series $g_2(R_K)$ and $g_3(R_K)$ involving the elements of R_K.

Alternatively, if we write $R_K = \mathbb{Z} + \tau\mathbb{Z}$ then

$$j(E) = j(R_K) = \frac{1}{e^{2\pi\imath\tau}} + \sum_{n=0}^{\infty} c(n)e^{2\pi\imath n\tau}$$

where $c(n) \in \mathbb{Z}$ are the coefficients in the q-series expansion of j.

We will actually prove much more than the statement of the theorem (4.10), in fact we will give an explicit description of how the Galois group of H/K acts on $j(E)$.

To do this we will use some tools defined into the previous chapters, that we recall here.

We defined, at the beginning of the section (2.3)

$$\begin{aligned}\mathcal{ELL}(R_K) &= \frac{\{\text{ elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong R_K \}}{\text{isomorphism over } \mathbb{C}} \\ &= \frac{\{\text{ lattices } \Lambda \text{ with } \mathrm{End}(E_\Lambda) \cong R_K \}}{\text{homothety}}\end{aligned}$$

and in the definition (2.25) we denoted by

$$C\mathcal{L}(R_K) = \frac{\{\text{ non-zero fractional ideals of } K \}}{\{\text{ non-zero principal ideals of } K \}}$$

the ideal class group of R_K. If $\mathfrak{a}$ is a fractional ideal of K, we denote by $\bar{\mathfrak{a}}$ its class in the quotient.

In proposition (2.26) we showed that there is a well-defined action of $C\mathcal{L}(R_K)$ on $\mathcal{ELL}(R_K)$ given by $\bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$ for all $\bar{\mathfrak{a}} \in C\mathcal{L}(R_K)$, for all $E_\Lambda \in \mathcal{ELL}(R_K)$, and that the action is simply transitive.

Then, in section (4.1), we deduced the existence of the map

$$F\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow C\mathcal{L}(R_K), \qquad \sigma \longmapsto F(\sigma)$$

characterized by the following property: $E^{\sigma} = F(\sigma) * E$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, and proved in proposition (4.7) that there is a well defined map, independent from choice of the curve E.

Since $C\mathcal{L}(R_K)$ is an abelian group, F factors through $F\colon \mathrm{Gal}(K^{ab}/K) \longrightarrow C\mathcal{L}(R_K)$ where K^{ab} is the maximal abelian extension of K. Finally, we recall the Frobenius element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K^{ab}/K)$ corresponding to a prime $\mathfrak{p}$ in K, defined in (3.5).

The following proposition will help us to completely determine F in order to use it in our proof of theorem (4.10).

Proposition 4.11. [7, II.4.2, p. 122]. *There is a finite set of rational primes $S \subset \mathbb{Z}$ such that, if $p \notin S$ is a prime which splits in K, say as $pR_K = \mathfrak{p}\mathfrak{p}'$, then the Frobenius element associated to $\mathfrak{p}$ is sent by F to the class of $\mathfrak{p}$ in the ideal class group, namely*

$$F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}} \in C\mathcal{L}(R_K).$$

Proof. In order to prove this proposition we need the following lemma:

Lemma 4.12. [7, II.4.4, p. 124]. *Let L be a number field, let $\mathfrak{P}$ be a maximal ideal of L, let E_1/L and E_2/L be elliptic curves with good reduction at $\mathfrak{P}$, with $\tilde{E}_1$ and $\tilde{E}_2$ their reductions modulo $\mathfrak{P}$. Then the natural reduction map*

$$Hom(E_1, E_2) \longrightarrow Hom(\tilde{E}_1, \tilde{E}_2), \qquad \phi \mapsto \tilde{\phi}$$

is injective. Further, it preserves degree, so $deg(\phi) = deg(\tilde{\phi})$.

Proof. See [7, II.4.4, p. 124]. □

From (2.26.b) we know that $\mathcal{ELL}(R_K)$ is finite, and in (4.1.c) we have seen that every curve in $\mathcal{ELL}(R_K)$ can be defined over $\bar{\mathbb{Q}}$, so we can choose a finite extension field L/K and representatives $E_1, \ldots, E_n$ defined over L for the distinct $\bar{K}$-isomorphism classes in $\mathcal{ELL}(R_K)$.

Further, by the theorem (4.2.c), we may replace L by a finite extension so that every isogeny connecting every pair of E_i's is defined over L.

Let S be the finite set of rational primes p satisfying one of the following conditions:

(i) p ramifies in L;

(ii) some E_i has bad reduction at some prime of L over p;

(iii) p divides either the numerator or the denominator of one of the numbers $N_{\mathbb{Q}}^{L}(j(E_i) - j(E_k))$ for some $i \neq k$ (it means that, if $p \notin S$ and $\mathfrak{P}$ is a prime of L dividing p, then $\tilde{E}_i \ncong \tilde{E}_k \pmod{\mathfrak{P}}$, since their invariants are not the same modulo $\mathfrak{P}$).

Now let $p \notin S$ be a prime which splits as $pR_K = \mathfrak{p}\mathfrak{p}'$ in K, and let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Let Λ be a lattice for E, so $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Choose some integral ideal $\mathfrak{a} \subset R_K$, relatively prime to p, such that $\mathfrak{a}\mathfrak{p} = (\alpha)$ is principal.

From (1.55.b) there are isogenies ϕ, ψ connecting E, $\bar{\mathfrak{p}} * E$, $\bar{\mathfrak{a}} * \bar{\mathfrak{p}} * E$ respectively, corresponding to the analytic maps f, g, induced by the inclusions $\Lambda \subset \mathfrak{p}^{-1}\Lambda$ and $\mathfrak{p}^{-1}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{p}^{-1}\Lambda = (\alpha)^{-1}\Lambda$ respectively, such that the following diagram commutes:

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda & \xrightarrow[z\mapsto z]{f} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow[z\mapsto z]{g} & \mathbb{C}/(\alpha)^{-1}\Lambda & \xrightarrow[z\mapsto \alpha z]{\sim} & \mathbb{C}/\Lambda \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr \\
E & \xrightarrow{\phi} & \bar{\mathfrak{p}} * E & \xrightarrow{\psi} & (\alpha) * E & \xrightarrow[\sim]{\lambda} & E
\end{array}$$

The composition is, then

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda, \qquad z \mapsto \alpha z$$

i.e., the multiplication by α, that we denote by $[\alpha]$.

Next we choose a Weierstrass equation for E/L, minimal at $\mathfrak{P}$, and let

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

be the associated invariant differential on E. The pull-back of ω to $\mathbb{C}/\Lambda$ will be some multiple of dz. Since the map along the top row of the diagram is simply $[\alpha]$, then dz pulls back to $d(\alpha z) = \alpha dz$. So we can conclude that

$$(\lambda \circ \psi \circ \phi)^* \omega = \alpha\omega.$$

Since the equation for E/L is minimal at $\mathfrak{P}$, by reducing modulo $\mathfrak{P}$ its coefficients we obtain an equation for $\tilde{E}$, so the reduced differential

$$\tilde{\omega} = \frac{dx}{\tilde{2}y + \tilde{a}_1 x + \tilde{a}_3}$$

is a non-zero invariant differential on $\tilde{E}$.

Further, since $(\alpha) = \mathfrak{a}\mathfrak{p}$ and $\mathfrak{P}$ divides $\mathfrak{p}$, we find that

$$(\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi})^* \omega = (\widetilde{\lambda \circ \psi \circ \phi})^* \omega = \tilde{\alpha}\tilde{\omega} = \tilde{0}.$$

From proposition [6, II.4.2, p. 30], already cited at the beginning of the section (1.1.6), it follows that $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable. On the other hand, using (4.12) and (2.32.b) we can compute the degrees of these functions:

$$\begin{aligned} \deg(\tilde{\phi}) &= \deg(\phi) = N_{\mathbb{Q}}^{K}(\mathfrak{p}) = p \\ \deg(\tilde{\psi}) &= \deg(\psi) = N_{\mathbb{Q}}^{K}(\mathfrak{a}) \\ \deg(\tilde{\lambda}) &= \deg(\lambda) = 1. \end{aligned}$$

Since $N_{\mathbb{Q}}^{K}(\mathfrak{a})$ is coprime to p, by assumption, then both $\tilde{\psi}$ and $\tilde{\lambda}$ are separable, so we conclude that $\tilde{\phi}\colon \tilde{E} \longrightarrow \widetilde{\bar{\mathfrak{p}} * E}$ must be inseparable. Recall that, from corollary (1.36), any map of this type factors as a q^{th}-power Frobenius map followed by a separable map. So the fact that $\tilde{\phi}$ has degree p and is inseparable implies that $\tilde{\phi}$ must be the p^{th}-power Frobenius map. More precisely, there is an isomorphism from the curve $\tilde{E}^{(p)}$ (obtained from $\tilde{E}$ by raising to the p^{th}-power the coefficients of the Weierstrass equation of $\tilde{E}$) to $\widetilde{\bar{\mathfrak{p}} * E}$ so that the composition

$$\tilde{E} \xrightarrow[\text{Frobenius}]{p^{th}\text{-power}} \tilde{E}^{(p)} \xrightarrow{\sim} \widetilde{\bar{\mathfrak{p}} * E}$$

equals $\tilde{E}$. In particular, we deduce that

$$j(\widetilde{\bar{\mathfrak{p}} * E}) = j(\tilde{E}^{(p)}) = j(\tilde{E})^{p},$$

from which we obtain the so called *Kronecker congruence*

$$j(\bar{\mathfrak{p}} * E) \equiv j(E)^{p} \pmod{\mathfrak{P}}.$$

Moreover it holds, by using the definition of F and the other results, that

$$j(E)^{p} = j(E)^{N_{\mathbb{Q}}^{K}(\mathfrak{p})} \equiv j(E)^{\sigma_{\mathfrak{p}}} = j(E^{\sigma_{\mathfrak{p}}}) = j(F(\sigma_{\mathfrak{p}}) * E) \pmod{\mathfrak{P}}$$

so we can conclude that

$$j(\bar{\mathfrak{p}} * E) \equiv j(F(\sigma_{\mathfrak{p}}) * E) \pmod{\mathfrak{P}}.$$

But from the original choice of excluded primes S, we have that

$$j(E_i) \equiv j(E_k) \pmod{\mathfrak{P}} \quad \Longleftrightarrow \quad E_i \cong E_k$$

Hence it is $\bar{\mathfrak{p}} * E \cong F(\sigma_{\mathfrak{p}}) * E$. The simplicity of the action of $C\mathcal{L}(R_K)$ on $\mathcal{ELL}(R_K)$ gives the desired conclusion: $F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}}$. □

Then we are able to prove the theorem (4.10).

Theorem 4.13. [7, II.4.3, p. 122]. *Let $K/\mathbb{Q}$ be a quadratic imaginary field with ring of integers R_K and let $E/\mathbb{C}$ be an elliptic curve with* $\mathrm{End}(E) \cong R_K$. *Then $K(j(E))$ is the Hilbert class field H of K.*

Proof. Let L/K be a finite extension corresponding to the homomorphism

$$F\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow C\mathcal{L}(R_K),$$

namely, L is the fixed field of the kernel of F. Then

$$\begin{aligned}
\mathrm{Gal}(\bar{K}/L) &= \ker(F) \\
&= \left\{ \sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ F(\sigma) = 1 \right\} \\
&= \left\{ \sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ F(\sigma) * E = E \right\} \\
&= \left\{ \sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ E^{\sigma} = E \right\} \\
&= \left\{ \sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ j(E^{\sigma}) = j(E) \right\} \\
&= \left\{ \sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ j(E)^{\sigma} = j(E) \right\} \\
&= \mathrm{Gal}(\bar{K}/K(j(E)))
\end{aligned}$$

where the equality $\{\sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ F(\sigma) = 1\} = \{\sigma \in \mathrm{Gal}(\bar{K}/K)\colon\ F(\sigma) * E = E\}$ follows from the simple transitivity of the action, while the last one is obvious since $\sigma \in \mathrm{Gal}(\bar{K}/K)$ fixes K by definition, and also $j(E)$, so it fixes the field $K(j(E))$.

Hence $L = K(j(E))$, i.e., $K(j(E))$ is the fixed field of the kernel of F. Further, since F maps $\mathrm{Gal}(\bar{K}/L)$ injectively into $C\mathcal{L}(R_K)$, $L/K = K(j(E))/K$ is an abelian extension.

Let $\mathfrak{c}_{L/K}$ be the conductor of L/K, consider the composition of the Artin map with F:

$$I(\mathfrak{c}_{L/K}) \xrightarrow{\left(\frac{L/K}{\cdot}\right)} \mathrm{Gal}(L/K) \xrightarrow{F} C\mathcal{L}(R_K)$$

We *claim* that this composition is the natural projection of $I(\mathfrak{c}_{L/K})$ onto $C\mathcal{L}(R_K)$, namely, we need to show that

$$F\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) = \bar{\mathfrak{a}} \qquad \text{for all } \mathfrak{a} \in I(\mathfrak{c}_{L/K}).$$

To prove the claim we will use the following version of *Dirichlet theorem* on primes in arithmetic progressions:

Theorem 4.14. [7, II.3.4, p. 118]. *Let K be a number field and $\mathfrak{c}$ an integral ideal of K. Then every ideal class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many degree 1 primes of K.*

Let $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$ and let S be the fixed set of primes described in proposition (4.11). By the Dirichlet theorem there exists a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ in the same $P(\mathfrak{c}_{L/K})$-ideal class as $\mathfrak{a}$ and not lying over a prime in S. In other words, there is an $\alpha \in K^\times$ satisfying the two conditions

$$\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}}, \qquad \mathfrak{a} = (\alpha)\mathfrak{p}.$$

Then we compute

$$\begin{aligned} F\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) &= F\left(\left(\frac{L/K}{(\alpha)\mathfrak{p}}\right)\right) \\ &= F\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right) && \text{since } \alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}} \\ &= \bar{\mathfrak{p}} && \text{from (4.11), since } N_{\mathbb{Q}}^{K}(\mathfrak{p}) \notin S \\ &= \bar{\mathfrak{a}} && \text{since } \mathfrak{a} = (\alpha)\mathfrak{p} \end{aligned}$$

and this proves the claim.

An immediate consequence is that $F\left(\left(\frac{L/K}{(\alpha)}\right)\right) = 1$ for all principal ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$, not just for those that are congruent to 1 modulo $\mathfrak{c}_{L/K}$. We also know that $F : \mathrm{Gal}(L/K) \longrightarrow C\mathcal{L}(R_K)$ is injective, so it implies that $\left(\frac{L/K}{(\alpha)}\right) = 1$ for all $(\alpha) \in I(\mathfrak{c}_{L/K})$. But the conductor of L/K is the smallest integral ideal $\mathfrak{c}$ such that

$$\alpha \equiv 1 \pmod{\mathfrak{c}} \quad \Rightarrow \quad \left(\frac{L/K}{(\alpha)}\right) = 1$$

so it follows that $\mathfrak{c}_{L/K} = (1)$. Since by Artin reciprocity, proposition (3.9), the conductor is divisible by every prime that ramifies, L/K must be everywhere unramified. So we conclude that L is contained in the Hilbert class field H of K.

On the other hand, the natural map $I(\mathfrak{c}_{L/K}) = I((1)) \longrightarrow C\mathcal{L}(R_K)$ is clearly surjective, so by the *claim* it follows that $F\colon \mathrm{Gal}(L/K) \longrightarrow C\mathcal{L}(R_K)$ is also surjective, hence an isomorphism. Therefore

$$[L\colon K] = |\mathrm{Gal}(L/K)| = |C\mathcal{L}(R_K)| = |\mathrm{Gal}(H/K)| = [H\colon K].$$

So L is contained in H and the extensions L/K and H/K have the same degree: it follows that $L = H$, i.e., $K(j(E)) = H$ is the Hilbert class field of K. □

Finally, we deduce some consequences of proposition (4.11), some of which have been already proved into the previous proof.

Theorem 4.15. [7, II.4.3, p. 122]. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{ELL}(R_K)$.*

(a) $[\mathbb{Q}(j(E))\colon \mathbb{Q}] = [K(j(E))\colon K] = h_K$, *where* $h_K = |C\mathcal{L}(R_K)| = |\mathrm{Gal}(H/K)|$ *is the class number of* K.

(b) *Let* $E_1, \dots, E_h$ *be a complete set of representatives for* $\mathcal{ELL}(R_K)$. *Then* $j(E_1), \dots, j(E_h)$ *is a complete set of* $\mathrm{Gal}(\bar{K}/K)$*-conjugates for* $j(E)$.

(c) *For every prime ideal* $\mathfrak{p}$ *of* K

$$j(E)^{\sigma_{\mathfrak{p}}} = j(\bar{\mathfrak{p}} * E).$$

More generally, for every non-zero fractional ideal $\mathfrak{a}$ *of* K

$$j(E)^{\left(\frac{H/K}{\mathfrak{a}}\right)} = j(\bar{\mathfrak{a}} * E).$$

Proof. (a) The second inequality, $[K(j(E))\colon K] = h_K$, has been proved during the proof of the main theorem (4.13). To show the first equality, we use the easy observation (4.3) after the theorem (4.2), that ensures the first inequality we need: if $\mathrm{End}(E) \cong R_K$, then the degree of the extension $\mathbb{Q}(j(E))/\mathbb{Q}$ satisfies

$$[\mathbb{Q}(j(E))\colon \mathbb{Q}] \leq h_K.$$

This inequality, combined with the second equality and the assumption that $[K\colon \mathbb{Q}] = 2$, implies that

$$[\mathbb{Q}(j(E))\colon \mathbb{Q}] = h_K$$

and this completes the proof.

(b) From (2.26.b) we know that $C\mathcal{L}(R_K)$ acts transitively on the set of j-invariants $\mathcal{J} = \{\, j(E_1), \dots, j(E_h) \,\}$ and by (1.5.b) two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j- invariant, so the set $\mathcal{ELL}(R_K)$ may be identified with the set $\mathcal{J}$ simply by the correspondence

$$\mathcal{ELL}(R_K) \xrightarrow{1:1} \mathcal{J}, \qquad [E] \mapsto j(E).$$

The map $F\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathcal{CL}(R_K)$ is defined by identifying the action of $\mathrm{Gal}(\bar{K}/K)$ on $\mathcal{J}$ with the action of $\mathcal{CL}(R_K)$ on $\mathcal{J}$, so $\mathrm{Gal}(\bar{K}/K)$ acts transitively on $\mathcal{J}$. Therefore $\mathcal{J}$ is a complete set of $\mathrm{Gal}(\bar{K}/K)$-conjugates of $j(E)$, and this proves the statement.

(c) The *claim* proved into the proof of (4.13) gives the assertion for all ideals in $I(\mathfrak{c}_{L/K})$. But $\mathfrak{c}_{L/K} = (1)$ so $I(\mathfrak{c}_{L/K})$ is exactly the set of all non-zero fractional ideals of K, so also the second relation is proved.

□

4.3 Maximal abelian extension of K

Let K be a quadratic imaginary field, let R_K be the ring of integers of K and let E be an elliptic curve with complex multiplication by R_K. We assume that the isomorphism $[\,\cdot\,] : R_K \to \mathrm{End}(E)$ is normalized as in (2.4).

In this section, we want to show how to generate the ray class field for a given modulo $\mathfrak{c}$ and the maximal abelian extension K^{ab} of K.

Let L/K be an abelian extension. The following lemma tells us when an endomorphism of the reduced curve $\tilde{E} \pmod{\mathfrak{P}}$ actually comes from an endomorphism of E.

Lemma 4.16. [7, II.5.2, p. 129]. *Suppose that E is defined over the number field L, let $\mathfrak{P}$ be a prime of L at which E has good reduction and let $\tilde{E}$ be the reduction of E modulo $\mathfrak{P}$. Let $\theta\colon \mathrm{End}(E) \longrightarrow \mathrm{End}(\tilde{E})$ be the natural map that sends any endomorphism of E to its reduction modulo $\mathfrak{P}$. Then $\gamma \in \mathrm{Image}(\theta)$ if and only if γ commutes with every element in* $\mathrm{Image}(\theta)$.

In other words, $\mathrm{Image}(\theta)$ is its own commutator inside $\mathrm{End}(\tilde{E})$.

Proof. We prove the two implications separately:

($\Rightarrow$) Let $\gamma \in \mathrm{Image}(\theta)$. Since $\mathrm{End}(E) \cong R_K$ then $\mathrm{Image}(\theta)$ is a commutative ring: so certainly γ commutes with the other elements of $\mathrm{Image}(\theta)$.

($\Leftarrow$) We note that, from (4.12) it follows that θ is injective. Moreover, from (1.42) there are exactly two cases:

- if $\mathrm{End}(\tilde{E})$ is an order in a quadratic imaginary field, then by assumption $\mathrm{End}(E) \cong R_K$ is the maximal order in K, so θ is an isomorphism: this case is done;

– if $\mathrm{End}(\tilde{E})$ is an order in a quaternion algebra $\mathcal{H}$, then $\mathcal{K} = \mathrm{Image}(\theta) \otimes \mathbb{Q}$ is a quadratic subfield of $\mathcal{H}$. Note that $\mathcal{K} \cong K$, but $\mathcal{H}$ may contain several distinct subfields each isomorphic to K. We choose a $\mathbb{Q}$-basis $\{ 1, \alpha \}$ for $\mathcal{K}$, namely, $\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha$, such that $\alpha^2 \in \mathbb{Q}$, then using again (1.42) we extend it to a $\mathbb{Q}$-basis for $\mathcal{H}$ of the form $\{ 1, \alpha, \beta, \alpha\beta \}$ satisfying the following conditions:

$$\alpha^2, \beta^2, (\alpha\beta)^2 \in \mathbb{Q}, \qquad\qquad \alpha\beta = -\beta\alpha$$

so $\mathcal{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$.

Now we need to find the commutator of $\mathcal{K}$ in $\mathcal{H}$: for any $\gamma \in \mathcal{H}$ we write $\gamma = d + a\alpha + b\beta + c\alpha\beta$ where $a, b, c, d \in \mathbb{Q}$, so γ commutes with $\mathcal{K}$ if and only if

$$\begin{aligned}
\gamma\alpha = \alpha\gamma &\Leftrightarrow (d + a\alpha + b\beta + c\alpha\beta)\alpha = \alpha(d + a\alpha + b\beta + c\alpha\beta) \\
&\Leftrightarrow d\alpha + a\alpha^2 + b\beta\alpha + c\alpha\beta\alpha = d\alpha + a\alpha^2 + b\alpha\beta + c\alpha^2\beta \\
&\Leftrightarrow -b\alpha\beta - c\alpha^2\beta = b\alpha\beta + c\alpha^2\beta \qquad \text{since } \alpha\beta = -\beta\alpha \\
&\Leftrightarrow \begin{cases} -b = b \\ -c\alpha^2 = c\alpha^2 \end{cases} \\
&\qquad \text{since } \{ 1, \alpha, \beta, \alpha\beta \} \text{ is a } \mathbb{Q}\text{-basis for } \mathcal{K} \text{ and } \alpha^2 \in \mathbb{Q} \\
&\Leftrightarrow b = c = 0 \\
&\Leftrightarrow \gamma = d + a\alpha \in \mathbb{Q} + \mathbb{Q}\alpha = \mathcal{K}
\end{aligned}$$

So we have found that γ commutes with $\mathcal{K}$ if and only if $\gamma \in \mathcal{K}$.

Finally let $\delta \in \mathrm{End}(\tilde{E})$ commute with $\mathrm{Image}(\theta)$: then δ commutes with $\mathcal{K}$, so δ is in $\mathcal{K}$, by what we have already proved. But we also know that δ is integral over $\mathbb{Z}$ and that $\mathrm{Image}(\theta) \cong R_K$ is the maximal order in $\mathcal{K} \cong K$, so $\delta \in \mathrm{Image}(\theta)$. □

In the theorem (4.10) we showed that, given an elliptic curve E with complex multiplication by R_K, $H = K(j(E))$ is the Hilbert class field of K. Since, by construction, $j(E) \in H$, we can find an equation for E with coefficients in H, so we may assume that E is defined over H. The following proposition shows that we can lift the p^{th}-power Frobenius map $\tilde{E} \longrightarrow \tilde{E}$ to a map in characteristic 0.

Proposition 4.17. [7, II.5.3, p. 131]. *Let K be a quadratic imaginary field, let H be its Hilbert class field, let E/H be an elliptic curve with CM by R_K. Let*

$\sigma_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ be the Frobenius element associated to a prime $\mathfrak{p}$ of R_K, and let $\mathfrak{P}$ be a prime of H lying over $\mathfrak{p}$. Assume that $\mathfrak{p}$ has degree 1 and is not in the finite set S of primes specified in the theorem (4.11), so in particular E has good reduction at $\mathfrak{P}$. Then there exists an isogeny

$$\lambda\colon E \longrightarrow E^{\sigma_{\mathfrak{p}}}$$

whose reduction modulo $\mathfrak{P}$

$$\tilde{\lambda}\colon \tilde{E} \longrightarrow \tilde{E}^{\sigma_{\mathfrak{p}}}$$

is the p^{th}-power Frobenius map.

Proof. To ease notation we will write σ instead of $\sigma_{\mathfrak{P}}$. From what we have shown into the proof of the proposition (4.11), there is an isogeny $E \longrightarrow \bar{\mathfrak{p}} * E$ whose reduction modulo $\mathfrak{P}$, $\tilde{E} \longrightarrow \widetilde{\bar{\mathfrak{p}} * E}$, is purely inseparable of degree p. Composing this isogeny with the isomorphism

$$\bar{\mathfrak{p}} * E \cong E^{\sigma},$$

by (4.13), we get a third isogeny

$$\tilde{\lambda}\colon \tilde{E} \longrightarrow \widetilde{E^{\sigma}}$$

that is purely inseparable of degree p. From (1.36) it follows that $\tilde{\lambda}$ factors as

$$\tilde{E} \xrightarrow{\ \phi\ } \tilde{E}^{(p)} \xrightarrow{\ \varepsilon\ } \widetilde{E^{\sigma}}$$

where $\tilde{E}^{(p)}$ is the elliptic curve obtained from E by raising to the p^{th}-power the coefficients of the Weierstrass equation, while ϕ is the p^{th}-power Frobenius map and ε is a map of degree 1. But, by definition, the reduction of E^{σ} is precisely $\tilde{E}^{(p)}$, so ε is an automorphism of $\widetilde{E^{\sigma}}$.

Now we *claim* that ε lies in the image of $\mathrm{Aut}(E^{\sigma})$ inside $\mathrm{Aut}(\widetilde{E^{\sigma}})$: from (4.16) it suffices to show that ε commutes with the image of $\mathrm{End}(E^{\sigma})$ inside $\mathrm{End}(\widetilde{E^{\sigma}})$. Recall that we have two normalized isomorphisms

$$[\,\cdot\,]_E\colon R_K \xrightarrow{\sim} \mathrm{End}(E) \qquad \text{and} \qquad [\,\cdot\,]_{E^{\sigma}}\colon R_K \xrightarrow{\sim} \mathrm{End}(E^{\sigma})$$

and, by the corollary (2.5), these isomorphisms satisfy

$$\lambda \circ [\alpha]_E = [\alpha]_{E^{\sigma}} \circ \lambda \qquad \text{for all } \alpha \in R_K.$$

Now we look at the reduction of $[\alpha]$ modulo $\mathfrak{P}$.

Remark 4.18. In general, suppose that $f\colon V \longrightarrow W$ is a rational map of algebraic varieties over a field k of characteristic p, let

$$\phi_V\colon V \longrightarrow V^{(p)}, \qquad\qquad \phi_W\colon W \longrightarrow W^{(p)}$$

be the p^{th}-power Frobenius maps, let $\sigma \in \mathrm{Aut}(k)$ be the p^{th}-power Frobenius automorphism of k. Then $f^\sigma\colon V^{(p)} \longrightarrow W^{(p)}$ is a rational map and the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{\phi_V} & V^{(p)} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^\sigma} \\ W & \xrightarrow{\phi_W} & W^{(p)} \end{array}$$

namely, $\phi_W \circ f = f^\sigma \circ \phi_V$.

Indeed, we can write $f = [f_0, \ldots, f_n]$ (locally) as a map given by homogeneous polynomials. For a polynomial $f(x) = f(x_1, \ldots, x_m) = \sum_i a_i x^i$ it holds

$$f^\sigma(\phi(x)) = \sum_i a_i^p x^{ip} = \left(\sum_i a_i x^i\right)^p = \phi(f(x))$$

and this ends the proof of observation (4.18).

From the theorem (4.2.a), since $\sigma \in \mathrm{Gal}(H/K)$ fixes $\alpha \in K$, then

$$[\alpha]_E^\sigma = [\alpha]_{E^\sigma}.$$

Using this fact and the observation on $[\alpha]_E\colon \tilde{E} \longrightarrow \tilde{E}$ we obtain

$$\phi \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^\sigma} \circ \phi = \widetilde{[\alpha]_{E^\sigma}} \circ \phi.$$

Moreover, since $\varepsilon \circ \phi = \tilde{\lambda}$ then

$$\begin{aligned} \widetilde{[\alpha]_{E^\sigma}} \circ \varepsilon \circ \phi &= \widetilde{[\alpha]_{E^\sigma}} \circ \tilde{\lambda} = \tilde{\lambda} \circ \widetilde{[\alpha]_E} \\ &= \varepsilon \circ \phi \circ \widetilde{[\alpha]_E} = \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}} \circ \phi. \end{aligned}$$

Therefore,

$$\widetilde{[\alpha]_{E^\sigma}} \circ \varepsilon = \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}}$$

and this completes the proof of the *claim*.

So, from the *claim* it follows that we can lift ε to $\varepsilon_0 \in \mathrm{End}(E^\sigma)$ and, by (4.12), ε_0 has degree 1. then it is in $\mathrm{Aut}(E^\sigma)$. We obtain that ε is the reduction modulo $\mathfrak{P}$ of $\varepsilon_0 \in \mathrm{Aut}(E^\sigma)$: so we can replace λ by $\varepsilon_0^{-1} \circ \lambda$ and conclude. □

Remark 4.19. [7, II.5.3.1, p. 131]. In general, there is no reason to expect an elliptic curve to be isogenous to one of its Galois conjugate. Of course there are always maps

$$\begin{array}{ccc} E & \overset{\exists\lambda}{\dashrightarrow} & E^{\sigma_{\mathfrak{p}}} \\ {\scriptstyle mod\,\mathfrak{P}}\downarrow & & \downarrow{\scriptstyle mod\,\mathfrak{P}} \\ \tilde{E} & \xrightarrow{\tilde{\lambda}} & \tilde{E}^{(p)} \end{array}$$

But (4.17) says exactly that there exist an isogeny $\lambda\colon E \longrightarrow E^{\sigma_{\mathfrak{p}}}$ that makes the diagram commutative. Thus, λ lifts the Frobenius map from characteristic p to characteristic 0.

An important special case of (4.17) occurs when $\mathfrak{p}$ is a principal ideal: in this case $\sigma_{\mathfrak{p}} = \left(\frac{H/K}{\mathfrak{p}}\right) = 1$, then λ is an endomorphism of E. The following proposition enable us to identify that endomorphism.

Corollary 4.20. [7, II.5.4, p. 133]. *Let K be a quadratic imaginary field, H be the Hilbert class field of K and E/H an elliptic curve with complex multiplication by R_K. For all but finitely many degree 1 prime ideals $\mathfrak{p}$ of K that satisfy $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$ there is a unique $\pi = \pi_{\mathfrak{p}} \in R_K$ such that $\mathfrak{p} = \pi R_K$ and the diagram*

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array}$$

is commutative, where ϕ is the p^{th}-power Frobenius map.

Note that $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$ is equivalent to say that that $\mathfrak{p}$ is a principal ideal.

Proof. Let $\mathfrak{P}$ be a prime of H lying over $\mathfrak{p}$. By hypothesis we have escluded finitely many $\mathfrak{p}$'s, including those for which $\tilde{E}\ (\mathrm{mod}\mathfrak{P})$ is singular, so we may use (4.17) to obtain a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{\sigma_{\mathfrak{p}}} \\ {\scriptstyle mod\,\mathfrak{P}}\downarrow & & \downarrow{\scriptstyle mod\,\mathfrak{P}} \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E}^{(p)} \end{array}$$

where $\sigma_{\mathfrak{p}} = \left(\frac{H/K}{\mathfrak{p}}\right)$, λ is an isogeny and ϕ is the p^{th}-power Frobenius map. The assumption $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$ means that $E^{\sigma_{\mathfrak{p}}} = E$, so λ is an endomorphism of E, say $\lambda = [\pi]$. It also implies that $\tilde{E}^{(p)} = \tilde{E}$, so the diagram becomes

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E \\ {\scriptstyle mod\,\mathfrak{P}}\downarrow & & \downarrow{\scriptstyle mod\,\mathfrak{P}} \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E}. \end{array}$$

Now we can compute the norm of $\mathfrak{p}$:

$$\begin{aligned} N_{\mathbb{Q}}^{K}\mathfrak{p} &= p && \text{since } \mathfrak{p} \text{ has degree 1} \\ &= \deg\phi && \text{since } \phi \text{ is the } p^{th}\text{-power Frobenius} \\ &= \deg[\pi] && \text{from (4.12), since } \widetilde{[\pi]} = \phi \\ &= \left|N_{\mathbb{Q}}^{K}\pi\right| && \text{from (2.31.b).} \end{aligned}$$

Since $\mathfrak{p}$ is a prime ideal in the quadratic field K, either $\mathfrak{p} = \pi R_K$ or $\mathfrak{p} = \pi' R_K$, where π' is the $\mathrm{Gal}(K/\mathbb{Q})$-conjugate of π. To decide which one is the correct form of $\mathfrak{p}$ we use the fact that $(E, [\cdot])$ is normalized: we take an equation for E/H with good reduction at $\mathfrak{P}$, let $\omega \in \Omega_E$ be a non-zero invariant differential whose reduction $\tilde{\omega}$ is a non-zero invariant differential on $\tilde{E}$. The normalization (2.4) says that $[\pi]^*\omega = \pi\omega$, so

$$\tilde{\pi}\tilde{\omega} = \widetilde{\pi\omega} = \widetilde{[\pi]^*\omega} = \widetilde{[\pi]}^*\,\tilde{\omega} = \phi^*\tilde{\omega} = 0$$

where the last equality follows from [6, II.4.2, p. 30], cited at the beginning of the subsection (1.1.6), since the Frobenius map ϕ is separable. Now ω_E is a one-dimensional vector space generated by $\tilde{\omega}$, so $\tilde{\pi} = 0$. In other words $\pi \equiv 0 \pmod{\mathfrak{P}}$, so $\pi \in \mathfrak{P} \cap K = \mathfrak{p}$. We can conclude that $\mathfrak{p} = \pi R_K$. This proves the first half of the proposition, the *existence* of π.

To show the second half, the *uniqueness* of π, we need to observe that the composition

$$R_K \xrightarrow{[\cdot]} \mathrm{End}(E) \longrightarrow \mathrm{End}(\tilde{E})$$

is injective. Since π has to satisfy $\widetilde{[\pi]} = \phi \in \mathrm{End}\tilde{E}$ there is at most one such π. □

Our goal is to show that the torsion points of an elliptic curve E with complex multiplication by R_K can be used to generate abelian extensions of K. We need to

remark that the points themselves do not generate abelian extensions of K: they only generate such extensions of the Hilbert class field $H = K(j(E))$.

In order to pick out the correct subfield, we take a model for $E \cong \mathbb{C}/\Lambda$ defined over H, namely we fix Λ, the function

$$f\colon \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \qquad z \mapsto (\wp(z,\Lambda), \wp'(z,\Lambda))$$

and a Weierstrass equation

$$Y^2 = X^2 - g_2(\Lambda)X - g_3(\Lambda).$$

Definition 4.21 (Weber function)**.** We define the *Weber function of* E/H as

$$h_E\colon E \longrightarrow E/\mathrm{End}(E) \cong \mathbb{P}^1,$$

$$h_E(f(z)) = \begin{cases} \dfrac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda) & \text{if } j(E) \neq 0, 1728 \\ \dfrac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z,\Lambda)^2 & \text{if } g_3(\Lambda) = 0 \\ \dfrac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda)^3 & \text{if } g_2(\Lambda) = 0. \end{cases}$$

Into this definition $\Delta(\Lambda) = g_2(\Lambda)^2 - 27g_3(\Lambda^3)$ is the usual modular discriminant.

An important property of the Weber function is that it is model independent, namely, it does not change if we take another lattice for E, or equivalently a new Weierstrass equation for E. So we can consider g_2 and g_3 as constants. This means that, if $g_2g_3 \neq 0$, h_E is just a constant multiple of the $\wp$ function, once we fixed the lattice Λ. Since h_E vanishes identically when $g_2g_3 = 0$, we need to exclude this case, which corresponds to $j(E) = 0, 1728$, and define separately these two cases. In any case, h_E is a rational function on E. Moreover, since we already noticed that it is possible to define a Weierstrass equation for E over H, from the model independence we can deduce that $h_E\colon E \longrightarrow \mathbb{P}^1$ is defined over H.

Example 4.22. [7, II.5.5.1, p. 134]. Consider a Weierstrass equation for E of the form

$$y^2 = x^3 + Ax + B \qquad \text{for some } A, B \in H$$

then the following function is a Weber function for E/H:

$$h_E(P) = h_E(x,y) = \begin{cases} x & \text{if } AB \neq 0 \\ x^2 & \text{if } B = 0 \\ x^3 & \text{if } A = 0. \end{cases}$$

So, except for the two particular cases $j = 0$ and $j = 1728$, a Weber function is just a x-coordinate for the curve.

To generate abelian extensions of K we will use the values of a Weber function on torsion points, so essentially we will take their x-coordinate.

Theorem 4.23. [7, II.5.6, p. 135]. *Let K be a quadratic imaginary field, let E be an elliptic curve with complex multiplication by R_K and let $h\colon E \longrightarrow \mathbb{P}^1$ be a Weber function for E/H. Let $\mathfrak{c}$ be an integral ideal of R_K. Then the field*

$$L = K(j(E), h(E[\mathfrak{c}]))$$

is the ray class field of K modulo $\mathfrak{c}$.

Proof. We gave the definition of *ray class field* in (3.11).

We know, from the theorem (4.13) that $H = K(j(E))$ is the Hilbert class field of K and, by definition, $H \subset L$. In order to prove that L is the ray class field of H we need to prove that

$$\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \quad \Leftrightarrow \quad \mathfrak{p} \in P(\mathfrak{c})$$

and it suffices to prove it for all but finitely many primes of degree 1 in K.

($\Rightarrow$) We take a prime $\mathfrak{p}$ of degree 1 satisfying $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. Then

$$\left(\frac{H/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)\Big|_H = 1$$

so, excluding finitely many primes, we can apply the corollary (4.20) to get a $\pi \in R_K$ such that

- $\mathfrak{p} = \pi R_K$,
- $\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array}$ is a commutative diagram,

where we denote ϕ the p^{th}-power Frobenius map.

We also choose $\sigma \in \mathrm{Gal}(\bar{K}/K)$ whose restriction to K^{ab}, the largest abelian extension of K, is $\sigma|_{K^{ab}} = \left(\frac{K^{ab}/K}{\mathfrak{p}}\right)$. Then in particular $\sigma|_L = \left(\frac{L/K}{\mathfrak{p}}\right) = 1$, and

also $\sigma|_H = 1$, since $H \subset L$. Now let $P \in E[\mathfrak{c}]$ be any $\mathfrak{c}$-torsion point: we compute

$$\begin{aligned}
\tilde{h}(\widetilde{[\pi]}\tilde{P}) &= \tilde{h}(\widetilde{[\pi]P}) \\
&= \tilde{h}(\phi(\tilde{P})) \quad \text{from the commutativity of the diagram} \\
&= \tilde{h}(\widetilde{P^{\sigma}}) \quad \text{since } \omega \text{ reduces to } p^{th}\text{-power Frobenius} \\
&= \widetilde{h(P^{\sigma})} \\
&= \widetilde{h(P)}^{\sigma} \quad \text{since } \omega|_H = 1 \text{ and } h \text{ is defined over } H \\
&= \widetilde{h(P)} \quad \text{since } h(P) \in L \text{ and } \omega|_L = 1 \\
&= \tilde{h}(\tilde{P}).
\end{aligned}$$

Next we observe that the reduction of h modulo $\mathfrak{P}$ is the map

$$\tilde{h}\colon \tilde{E} \longrightarrow E/\widetilde{\mathrm{Aut}(E)} \cong \tilde{E}/\widetilde{\mathrm{Aut}(E)}$$

(since $\mathrm{Aut}(\tilde{E})$ may be larger than $\widetilde{\mathrm{Aut}(E)}$, the image is not $\tilde{E}/\mathrm{Aut}(\widetilde{E})$). Using this fact and the last computation, we deduce that there is an automorphism $[\xi] \in \mathrm{Aut}(E)$ such that

$$\widetilde{[\pi]}\tilde{P} = \widetilde{[\xi]}\tilde{P}.$$

By the injectivity of the torsion, [6, VII.3.1.b, p. 192], $E[\mathfrak{c}] \hookrightarrow \tilde{E}[\mathfrak{c}]$ so we get $[\pi - \xi]P = 0$. A priori the particular ξ that satisfies this relation may depend on the choice of the $\mathfrak{c}$-torsion point P, but from (2.31.b) we know that $E[\mathfrak{c}]$ is a free $R_K/\mathfrak{c}$-module of rank 1, hence there is a single $\xi \in R_K^{\times}$ such that $[\pi - \xi]$ annihilates all of $E[\mathfrak{c}]$. This implies that $\pi \equiv \xi \pmod{\mathfrak{c}}$, therefore $\xi^{-1}\pi \equiv 1 \pmod{\mathfrak{c}}$ and we have that $\mathfrak{p} = \pi R_K = (\xi^{-1}\pi)R_K$ since ξ is a unit. This proves that $\mathfrak{p} \in P(\mathfrak{c})$.

($\Leftarrow$) Suppose that $\mathfrak{p} \in P(\mathfrak{c})$ is a prime of K of degree 1. This means, by definition of $P(\mathfrak{c})$, that

$$\mathfrak{p} = \mu R_K \quad \text{for some } \mu \in R_K \text{ with } \mu \equiv 1 \pmod{\mathfrak{c}}.$$

In particular $\mathfrak{p}$ is principal, so $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$. Hence, after excluding finitely many primes, we can apply the corollary (4.20) to get some $\pi \in R_K$ such that

- $\mathfrak{p} = \pi R_K$,

– $\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array}$ is a commutative diagram,

where, as usual, ϕ is the p^{th}-power Frobenius map.

So now we have that $\mathfrak{p} = \pi R_K = \mu R_K$: there must be a unit $\xi \in R_K^\times$ such that $\pi = \xi\mu$. Note that $[\xi] \in \mathrm{Aut}(E)$, so $[\pi]$ and $[\mu]$ differ by an automorphism of E.

We already know that $\left(\frac{L/K}{\mathfrak{p}}\right)$ fixes H; we need to show that it fixes all of L: in order to do it we need to show that it fixes $h(E[\mathfrak{c}])$. Let $P \in E[\mathfrak{c}]$ be any $\mathfrak{c}$-torsion point, then the commutativity of the diagram gives

$$\widetilde{\left(\frac{L/K}{\mathfrak{p}}\right)}(P) = \phi(\tilde{P}) = \widetilde{[\pi]P}.$$

On the other hand, the proposition [6, VII.3.1.b, p. 192] tells us that the reduction map $E \longrightarrow \tilde{E}$ is injective on torsion points whose order is prime to $\mathfrak{p}$: if we exclude the finitely many $\mathfrak{p}$'s which divide the order $|E[\mathfrak{c}]|$, then the reduction map $E[\mathfrak{c}] \longrightarrow \tilde{E}[\mathfrak{c}]$ is injective. Therefore $\left(\frac{L/K}{\mathfrak{p}}\right)(P) = [\pi]P$. Now we compute

$$\begin{aligned}
\left(\frac{L/K}{\mathfrak{p}}\right)(h(P)) &= h\left(\left(\frac{L/K}{\mathfrak{p}}\right)(P)\right) && \text{since } \left(\frac{H/K}{\mathfrak{p}}\right) = 1 \text{ and } h \text{ is defined over } H \\
&= h([\pi]P) \\
&= h([\xi] \circ [\mu]P) && \text{since } \pi = \xi\mu \\
&= h([\mu]P) && \text{since } h \text{ is } \mathrm{Aut}(E)\text{-invariant and } [\xi] \in \mathrm{Aut}(E) \\
&= h(P) && \text{since } P \in E[\mathfrak{c}] \text{ and } \mu \equiv 1 \pmod{\mathfrak{c}}
\end{aligned}$$

so $\left(\frac{L/K}{\mathfrak{p}}\right)$ fixes any element of $h(E[\mathfrak{c}])$ and this completes the proof.

□

Example 4.24. [7, II.5, Example 5.8.1, p. 138]. We can illustrate the theorem (4.23) with the curve of Weierstrass equation

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

which has complex multiplication by the ring of Gaussian integers $\mathbb{Z}[\imath]$ in the field $K = \mathbb{Q}(\imath)$. In particular, we will compute the ray class field of K modulo the ideals

(2), (3), (4) and prove what we claimed in the example (3.17). From the example (3.15) we know that the class number of the field K is $h_K = 1$, so the Hilbert class field coincides with the field K itself.

Let $\mathfrak{c} = (2)$, then the set of (2)-torsion points of E is

$$E[(2)] = E[2] = \{ O, (0,0), (\imath, 0), (-\imath, 0) \}$$

and then if we apply the Weber function to the points in $E[(2)]$ we obtain the set of values $\{ 0, \pm\imath \}$. So the ray class field of K modulo (2) is

$$K_{(2)} = K(j(E), h(E[(2)]) = K$$

as we claimed in the example (3.17).

Let $\mathfrak{c} = (3)$, if $P = (x, y)$ is a point of the curve, then the *duplication formula* cited in (1.27) reads

$$2P = \left(\frac{x^4 - 2x^2 + 1}{4x^3 + 4x}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} \right)$$

and, from the explicit formulas derived in the first chapter, we know that $3P = P + 2P = O$ if and only if $x(P) = x(2P)$, namely

$$x = \frac{x^4 - 2x^2 + 1}{4x^3 + 4x} \qquad\qquad 3x^4 + 6x^2 - 1 = 0.$$

The roots of this polynomial are $\alpha, -\alpha, \frac{1}{\sqrt{3}\alpha}, -\frac{1}{\sqrt{3}\alpha}$ where $\alpha = \sqrt{\frac{2\sqrt{3}-3}{3}}$, and from them we can compute the coordinates of the 3-torsion points. Then, the Weber function on E is $h(x, y) = x^2$, so the ray class field of K modulo (3) is

$$K_{(3)} = K(j(E), h(E[(3)]) = K(\sqrt{3})$$

and this coincides with the field in the example (3.17).

Let $\mathfrak{c} = (4)$, the point $P = (x, y)$ is a point of the curve of order 4 if and only if $y(2P) = 0$. Using again the duplication formula, this condition is equivalent to $x^6 + 5x^4 - 5x^2 - 1 = 0$. The roots of this polynomial are $1, -1, \gamma, -\gamma, \gamma^{-1}, -\gamma^{-1}$ where $\gamma = (\sqrt{2} - 1)\imath$. Hence, the ray class field of K modulo (4) is

$$K_{(4)} = K(j(E), h(E[(4)]) = K(\sqrt{2})$$

and again, this coincides with the field in the example (3.17).

Finally, we can characterize the maximal abelian extension of the field K.

Corollary 4.25. [7, II.5.7, p. 135]. *With notation as above, the maximal abelian extension of K is*

$$K^{ab} = K(j(E), h(E_{tors})).$$

In particular, if $j(E) \neq 0, 1728$ and if we take an equation for E with coefficients in $H = K(j(E))$, then the maximal extension of K is generated by $j(E)$ and the x-coordinates of the torsion points of E.

Proof. To show the first part of the corollary, let L/K be a finite abelian extension and let $\mathfrak{c}_{L/K}$ be the conductor of L/K. By class field theory (3.13.c), L is contained in the ray class field of K modulo $\mathfrak{c}$. Using theorem (4.23), this means that

$$L \subset K(j(E), h(E[\mathfrak{c}_{L/K}])).$$

Taking the compositum over all conductors gives

$$L \subset K(j(E), h(E_{tors}))$$

then taking the union over all the abelian extensions L's gives

$$K^{ab} \subset K(j(E), h(E_{tors})).$$

But theorem (4.23) says that $K(j(E), h(E_{tors}))$ is a compositum of abelian extensions, so it is necessarily abelian: then by maximality of K^{ab}, it must be

$$K^{ab} = K(j(E), h(E_{tors})).$$

To show the second part, it suffices to observe that, by the example (4.22), if $j(E) \neq 0, 1728$ then the x-coordinate on a Weierstrass equation for $E/\mathbb{Q}(j(E))$ is a Weber function for E. □

Remark 4.26. Using all the results we derived, we can characterize any abelian extension of the quadratic imaginary field K. We have that any abelian extension L/K is contained in a ray class field $K_{\mathfrak{c}}/K$ for some integral ideal $\mathfrak{c}$ of K. On the other hand, the union of the ray class fields of K gives the maximal abelian extension of K, so we can conclude that the abelian extensions L of K are exactly the subfields of the ray class fields $K_{\mathfrak{c}}$ of K, for integral ideal $\mathfrak{c}$ of K.

Remark 4.27. [7, II.5.8, p. 138]. In light of corollary (4.25), we naturally wonder what happens if we adjoin all of E_{tors} to K, rather than just the values of a Weber function. In general, it does not generate an abelian extension of K, although E_{tors} generates an abelian extension of the Hilbert class field H of K, as we have already seen in (4.5).

Suppose now we look at the special case of K of class number 1, so that $H = K$. Then we have the inclusions

$$K^{ab} = H(h(E_{tors})) \subset H(E_{tors}) \subset H^{ab} = K^{ab}$$

so the inclusions are actually equalities. Thus if K has class number 1 then

$$K^{ab} = K(h(E_{tors})) = K(E_{tors})$$

and the j-invariants of these curves will be in $\mathbb{Q}$.

4.4 Integrality of j

We have seen in the proposition (4.1.b) that the j-invariant of an elliptic curve E with complex multiplication is an algebraic number. In this section we are going to prove that it is in fact an algebraic integer, or equivalently that E has everywhere potential good reduction. In other words, our goal is to show the following theorem.

Theorem 4.28. [7, II.6.1, p. 140]. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

It is not hard to see that an elliptic curve E has complex multiplication if and only if there is an endomorphism $E \to E$ whose degree is not a square. In fact, we proved in the proposition (1.61.b) that, for any $m \in \mathbb{Z}$, the multiplication-by-m endomorphism has degree m^2, so if there is an endomorphism of degree not a square it cannot be a multiplication-by-m endomorphism. Thus $\mathrm{End}(E)$ contains some extra endomorphisms: E has complex multiplication.

This suggest us how to prove our sentence: we take an arbitrary elliptic curve E and a positive integer n and study the set of all the elliptic curves E' such that there is an isogeny $E \to E'$ of degree n. Then we are going to show that, in this situation, $j(E')$ is integral over $\mathbb{Z}[j(E)]$, by explicitly constructing a monic polynomial $F_n(j(E), X) \in \mathbb{Z}[j(E)][X]$ having $j(E')$ as a root. Finally, if E has complex multiplication, for an appropriate choice of n we can take $E' = E$: then $F_n(j(E), j(E)) = 0$, which means that $j(E')$ is integral over $\mathbb{Z}$.

Definition 4.29 $(\mathcal{D}_n, \mathcal{S}_n)$**.** Fix an integer n, we define the sets

$$\mathcal{D}_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \colon ad - bc = n \right\}$$
$$\mathcal{S}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \colon ad = n,\ d > 0,\ 0 \le b < d \right\}.$$

We first observe that $\mathcal{S}_n$ is a finite subset of $\mathcal{D}_n$ and that $SL_2(\mathbb{Z}) = \Gamma$ acts on $\mathcal{D}_n$ via multiplication:

$$\Gamma \times \mathcal{D}_n \longrightarrow \mathcal{D}_n, \qquad (\gamma, \alpha) \mapsto \gamma\alpha$$

(clearly $\det(\alpha) = n$ and $\det(\gamma) = 1$ so $\det(\gamma\alpha) = n$, i.e., $\gamma\alpha \in \mathcal{D}_n$, so the map is well defined; moreover it is easy to see that this is actually an action). Thus, we can show that the natural inclusion $\mathcal{S}_n \subset \mathcal{D}_n$ induces a one-to-one correspondence $\mathcal{S}_n \cong \Gamma\backslash\mathcal{D}_n$.

Then for any matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{R})$ with $\det(\alpha) > 0$ we define the function $j \circ \alpha$ as the composition of the function j with the fractional linear transformation defined by α :

$$(j \circ \alpha)(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right)$$

and observe that, if $\alpha \in SL_2(\mathbb{Z})$ then $j \circ \alpha = j$.

Remark 4.30. [5, 5, p. 300]. We recall that the j-invariant is an invariant function for the group $\Gamma = SL_2(\mathbb{Z})$ which s holomorphic on the upper half plane and has Fourier expansion $q^{-1} + \dots$ at infinity. Instead of define $\mathcal{D}_n$ and $\mathcal{S}_n$ we could consider a positive integer n and the *set of integral primitive matrices*

$$\Delta_n^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \colon ad - bc = n, (a, b, c, d) = 1 \right\}.$$

The matrices in Δ_n^* are said to be *primitive*, since their determinant is positive and have coprime coefficients. Then we can prove that it is actually equivalent to choose either the former or the latter definition, due to the following fact:

Proposition 4.31. [5, 5.1, p. 301]. *We can decompose Δ_n^* using $\Gamma = SL_2(\mathbb{Z})$ as follows:*

$$\Delta_n^* = \Gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \Gamma.$$

Moreover $\Delta_n^* = \bigcup_{\alpha_i} \Gamma\alpha_i$ where α_i runs over the matrices of the form

$$\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \textit{with } 0 < a,\ 0 \le b < d,\ (a, b, d) = 1 \textit{ and } ad = n.$$

Proof. [3, 5.1, pp. 51-52]. Multiplication on the right (and on the left) by elements of Γ maps Δ_n^* into itself. We can show that Γ operates left transitively on the right Γ-cosets (and right transitively on the left Γ-cosets). In fact, the map

$$\begin{aligned} \Gamma \times \{\, \Gamma\alpha \colon \alpha \in \Delta_n^* \,\} &\longrightarrow \{\, \Gamma\alpha \colon \alpha \in \Delta_n^* \,\} \\ (\gamma, \Gamma\alpha) &\mapsto \gamma \circ \Gamma\alpha = \Gamma(\gamma\alpha) \end{aligned}$$

is an action of Γ over the set of right cosets of Γ in Δ_n^*:

- if $\gamma = \mathbb{1}_2$ clearly $\mathbb{1}_2 \circ \Gamma\alpha = \Gamma(\mathbb{1}_2\alpha) = \Gamma\alpha$;
- $\gamma \circ \gamma' \circ (\Gamma\alpha) = \gamma \circ (\Gamma(\gamma'\alpha)) = \Gamma(\gamma(\gamma'\alpha)) = \Gamma((\gamma\gamma')\alpha) = (\gamma\gamma') \circ \Gamma\alpha$.

Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ an integral primitive matrix, i.e., an element of Δ_n^* and let

$$L = [1, \tau] = \mathbb{Z} + \tau\mathbb{Z} = \{\, x + \tau y \colon x, y \in \mathbb{Z} \,\} \leftrightarrow \{\, \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) \colon x, y \in \mathbb{Z} \,\}$$

be a lattice, then $M = [a\tau + b, c\tau + d]$ is a sub-lattice. By the *elementary divisor theorem* there exists a basis $\{\omega_1, \omega_2\}$ of L and a basis $\{\omega_1', \omega_2'\}$ of M such that

$$\begin{cases} \omega_1' = e_1\omega_1 \\ \omega_2' = e_2\omega_2 \end{cases} \qquad \text{where } e_1, e_2 \in \mathbb{Z} \text{ and } e_1 \mid e_2.$$

Since, by hypothesis, $(a, b, c, d) = 1$, necessarily $e_1 = 1$, so there exist $\gamma, \gamma' \in L$ such that

$$\gamma\alpha\gamma' = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \alpha = \gamma^{-1} \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \gamma'^{-1}$$

so we see that the decomposition $\Delta_n^* = \Gamma\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma$ holds. This proves that Γ operates transitively on the cosets.

To show the second part of the sentence, we need to find a simple set of representatives for the left cosets of Γ in Δ_n^*. Given α as above, we can always find $\gamma \in \Gamma$ such that

$$\gamma\alpha = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$$

(namely, we can select relatively prime integers z, w such that $za + wc = 0$, and integers x, y such that $xw - zy = 1$: then $\gamma = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ satisfies this property). So we can always assume that α is upper triangular: $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$.

Then, since

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b + kd \\ 0 & d \end{pmatrix}$$

a left coset always contains a representative with $0 \leq b < d$. Finally, matrices $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $0 < a$, $0 \leq b < d$ and $ad = n$ generate different left cosets, i.e. no two of them lie in the same coset. □

This tells us exactly that from each element in Δ_n^* we can find an element of $\mathcal{S}_n$, by taking a representative of the coset of Γ in Δ_n^*, and viceversa, by taking, for any element of $\mathcal{S}_n$, a scalar multiple with coprime integers.

Then we consider the following useful lemma:

Lemma 4.32. [5, 5.2, p. 301]. *Suppose that f is a holomorphic function on the upper half plane which is invariant under the action of Γ by fractional linear transformation and which is meromorphic at infinity. Then f is a polynomial in the function $j(z)$, with coefficients in the $\mathbb{Z}$-module generated by the Fourier coefficients of f.*

Proof. Consider the q-expansion of the function f,

$$f = \sum c_n q^n,$$

so from the assumption we can assume that

$$f = c_{-m} q^{-m} + \text{terms of higher degree.}$$

Then $f - c_{-m} j^m$ has the properties of the statement and a pole of order at most $m-1$ at infinity. Repeating this process we find a polynomial P in j with coefficients in the module generated by all the c_n's over $\mathbb{Z}$, namely, linear combinations of the coefficients of f such that $f - P(j)$ vanishes at infinity and is holomorphic on the upper half plane. It follows that $f - P(j)$ is identically zero, so f satisfies the statement. □

Now, we are going to study the polynomial

$$F_n(X) = \prod (X - j \circ \alpha) = \sum_m s_m X^m$$

where α runs over $\mathcal{S}_n$ (if we consider the definitions in (4.29)) or equivalently over the representatives for the right cosets of Δ_n^* (if we consider the situation described in the observation (4.30)) and the function $j \circ \alpha$ denotes the composition of the function j with the fractional linear transformation defined by α, as defined above.

The coefficients $s_m = s_m(\tau)$ are holomorphic functions on the upper half-plane $\mathbb{H}$. More precisely, s_m is the m-th elementary symmetric function in the $j \circ \alpha$'s. So, $F_n(X)$ is a polynomial in the variable X whose coefficients are holomorphic fuctions of the upper half plane, but there are several other properties, that we are going to show.

Claim 1. [7, II.6, p. 144], [5, 5.3, p. 301]: The coefficients of $F_n(X)$ are invariant under the action of $SL_2(\mathbb{Z})$, namely,

$$s_m(\gamma\tau) = s_m(\tau) \quad \text{for all } \gamma \in SL_2(\mathbb{Z}) \text{ and all } \tau \in \mathbb{H}.$$

Moreover, they are meromorphic at infinity and holomorphic on the upper half-plane.

Proof. By definition, the coefficients of $F_n(X)$ are elementary symmetric functions of the $j \circ \alpha$. Let $\gamma \in \Gamma$, for every $\alpha \in \mathcal{S}_n$ we have $\alpha\gamma \in \mathcal{D}_n$. Then, since $\mathcal{S}_n \cong \Gamma\backslash\mathcal{D}_n$, there exist a unique $\delta_\alpha \in \Gamma$ such that $\delta_\alpha\alpha\gamma \in \mathcal{S}_n$. Moreover, if $\delta_\alpha\alpha\gamma = \delta_\beta\beta\gamma$ for some $\delta_\alpha, \delta_\beta \in \mathcal{S}_n$ then

$$\beta = \delta_\beta^{-1}\delta_\alpha\alpha\gamma\gamma^{-1} = \delta_\beta^{-1}\delta_\alpha\alpha$$

but then, by [7, I.9, p. 72], we can deduce that $\alpha = \beta$. In other words, we have proved that the function

$$\mathcal{S}_n \longrightarrow \mathcal{S}_n, \qquad \alpha \mapsto \delta_\alpha\alpha\gamma$$

is an injective map between two finite sets of the same cardinality, thus it is a bijective function. Now we observe that

$$\begin{aligned}
\{\, j \circ (\alpha\gamma) \colon \alpha \in \mathcal{S}_n \,\} &= \left\{\, j \circ (\delta_\alpha^{-1}\delta_\alpha\alpha\gamma) \colon \alpha \in \mathcal{S}_n \right\} \\
&= \left\{\, j \circ \delta_\alpha^{-1} \circ (\delta_\alpha\alpha\gamma) \colon \alpha \in \mathcal{S}_n \right\} \\
&= \{\, j \circ (\delta_\alpha\alpha\gamma) \colon \alpha \in \mathcal{S}_n \,\} \quad \text{since } j \text{ is } \Gamma\text{-invariant} \\
&= \{\, j \circ \gamma \colon \alpha \in \mathcal{S}_n \,\} \quad \text{using the bijection } \mathcal{S}_n \to \mathcal{S}_n.
\end{aligned}$$

Using the equivalent notation, we are just saying that the right action of Γ permutes the cosets $\Gamma\alpha$ in Δ_n^*. Hence, any symmetric function on the set $\{j \circ \gamma \colon \alpha \in \mathcal{S}_n\}$ will be invariant under the action $\tau \mapsto \gamma\tau$ for $\gamma \in \Gamma$.

By applying this result to the functions $s_m(\tau)$'s we can conclude the first part of the proof.

To show the second part we observe that, since j is a holomorphic function on the upper half plane, necessarily each $j\circ\alpha$ is holomorphic too; the meromorphicity comes from the explicit formula for $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$: j has Fourier expansion

$$j = q^{-1} + \sum_{k=0}^{\infty} c_k q^k$$

so it has a pole in $q = 0$ of order 1. Then

$$j \circ \alpha = e^{-2\pi\imath \frac{a\tau+b}{d}} + \sum_{k=0}^{\infty} c_k e^{2\pi\imath k \frac{a\tau+b}{d}}$$

so in particular $q^{n+1}(j \circ \alpha)(\tau) \to 0$ as $q \to 0$. From the definition of the s_m's, it follows that there exists $N \in \mathbb{Z}$ such that $q^N s_m(\tau) \to 0$ as $q \to 0$: this means exactly that each $s_m(\tau)$ is meromorphic at infinity. □

Claim 2. [7, II.6, p. 144]. There is a polynomial $f_m(X) \in \mathbb{C}[X]$ such that $s_m(\tau) = f_m(j(\tau))$ for all $\tau \in \mathbb{H}$, namely,

$$s_m \in \mathbb{C}[j].$$

Proof. From *claim* 1, s_m is holomorphic on $\mathbb{H}$, so meromorphic on $\mathbb{H}$, and Γ-invariant. In particular it is invariant with respect to the fractional linear transformation defined by the matrices $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i.e.

$$s_m(\tau + 1) = s_m(\tau), \qquad s_m\left(-\frac{1}{\tau}\right) = s_m(\tau)$$

so s_m is a weakly modular function of weight 0. Further, we have seen in *claim* 1 that each s_m is also meromorphic at ∞, so actually each s_m is a modular function of weight 0. Finally, the lemma [7, I.4.2, p. 35] says that, given f a modular function of weight 0 then it is a rational function of j, that is, $f \in \mathbb{C}(j)$ and if, in addition, f is also holomorphic on $\mathbb{H}$, then f is a polynomial function of j, that is, $f \in \mathbb{C}[j]$. Using the lemma, it follows immediately that, since each s_m is holomorphic on $\mathbb{H}$, it is a polynomial function of j, i.e. $s_m \in \mathbb{C}[j]$ for each m. □

Claim 3. [7, II.6, p. 145]. The Fourier expansion of s_m has coefficients in $\mathbb{Z}$.

Proof. To ease notation, we set $\zeta = e^{\frac{2\pi\imath}{n}}$ and $Q = q^{\frac{1}{n}}$. For any $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{S}_n$ we have that $ad = n$ and so

$$\begin{aligned} q \circ \alpha(\tau) = e^{2\pi\imath\alpha(\tau)} = e^{2\pi\imath \frac{a\tau+b}{d}\frac{a}{a}} = e^{2\pi\imath \frac{(a\tau+b)a}{n}} \\ = e^{2\pi\imath \frac{\tau}{n}a^2} e^{2\pi\imath \frac{ab}{n}} = Q^{a^2}\zeta^{ab}. \end{aligned}$$

Similarly, using the q-expansion of $j(\tau)$ we find that $j \circ \alpha$ has a Q-expansion

$$j \circ \alpha(\tau) = e^{-2\pi\imath\frac{a\tau+b}{d}} + \sum_{k=0}^{\infty} c_k e^{2\pi\imath k\frac{a\tau+b}{d}} = Q^{-a^2}\zeta^{-ab} + \sum_{k=0}^{\infty} c_k Q^{a^2 k}\zeta^{abk}$$

where $c_k \in \mathbb{Z}[\zeta]$ for all k. In particular the Fourier coefficients of $j\circ\alpha$ lie in $\mathbb{Z}[\zeta]$ so the same holds for the Fourier coefficients of s_m, for all m. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, we write $\zeta^\sigma = \zeta^{r(\sigma)}$ for some integer $r(\sigma)$ relatively prime to n. If we apply σ to the Q-Fourier coefficients of $j \circ \alpha$ we get

$$(j \circ \alpha)^\sigma = Q^{-a^2}\zeta^{-r(\sigma)ab} + \sum_{k=0}^{\infty} c_k Q^{a^2 k}\zeta^{r(\sigma)abk}$$

then, comparing the series for $j \circ \alpha$ and $(j \circ \alpha)^\sigma$ we see that

$$\left(j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right)^\sigma = j \circ \begin{pmatrix} a & r(\sigma)b \\ 0 & d \end{pmatrix}.$$

In general, the value of $j \circ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ only depends on $b \pmod d$, since

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b+kd \\ 0 & d \end{pmatrix}$$

and j is Γ-invariant. Further, if r is any integer coprime with $n = ad$, then the set $\{rb\colon 0 \le b < d\}$ is a complete set of residue classes modulo d. So, for any integer r relatively prime to n

$$\left\{ j \circ \begin{pmatrix} a & rb \\ 0 & d \end{pmatrix}\colon \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{S}_n \right\} = \{\, j \circ \alpha\colon \alpha \in \mathcal{S}_n \,\}.$$

Applying this result with $r = r(\sigma)$ it follows that

$$\{\, (j \circ \alpha)^\sigma\colon \alpha \in \mathcal{S}_n \,\} = \{\, j \circ \alpha\colon \alpha \in \mathcal{S}_n \,\}.$$

Now consider the Q-Fourier coefficients of the $s_m(\tau)$'s: we know they lie in $\mathbb{Z}[\zeta]$; further, since $s_m(\tau)$ is a symmetric polynomial in the functions $\{j \circ \alpha\colon \alpha \in \mathcal{S}_n\}$, its Q-Fourier coefficients are fixed by any element in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so they lie in $\mathbb{Q}$. But then they lie in $\mathbb{Q} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$.

Finally, we note that, from *claim* 1, $s_m(\tau + 1) = s_m(\tau)$, so s_m is in fact represented by a Fourier series in $q = Q^n$. This completes the proof of *claim* 3. □

Claim 4. [7, II.6, p. 146]. It holds

$$s_m(\tau) \in \mathbb{Z}[j].$$

Proof. From *claim* 2 we know that $s_m \in \mathbb{C}[j]$, while from *claim* 3 we can deduce that $s_m \in \mathbb{Z}[[q, q^{-1}]]$. So we need to show that

$$\mathbb{C}[j] \cap \mathbb{Z}[[q, q^{-1}]] = \mathbb{Z}[j].$$

Let $f(j) \in \mathbb{C}[j] \cap \mathbb{Z}[[q, q^{-1}]]$ be a polynomial of degree d, $f(j) = a_0 j^d + a_1 j^{d-1} + \cdots + a_d$ with $a_i \in \mathbb{C}$. Substituting in the q-expansion of j gives

$$f = \frac{a_0}{q^d} + \frac{a_1 + 744 d a_0}{q^{d-1}} + \dots$$

and since $f \in \mathbb{Z}[[q, q^{-1}]]$ necessarily $a_0 \in \mathbb{Z}$. Then

$$f - a_0 j^d = a_1 j^{d-1} + \cdots + a_d \in \mathbb{C}[j] \cap \mathbb{Z}[[q, q^{-1}]]$$

and we can repeat the same argument, that gives $a_1 \in \mathbb{Z}$. After a finite number of steps we find that every coefficient of f is in $\mathbb{Z}$. The converse is obvious. □

Then combining these four observations we have shown the following

Theorem 4.33. [7, II.6.3.a, p. 146]. *There exists a polynomial $F_n(Y, X) \in \mathbb{Z}[Y, X]$ so that*

$$\prod_{\alpha \in S_n} (X - j \circ \alpha) = F_n(j, X)$$

Moreover, some other properties hold.

Theorem 4.34. [5, 5.5, p. 302],[7, II.6.3, p. 146].

(a) *$F_n(j, X)$ is irreducible over $\mathbb{C}(j)$ and symmetric in X and j.*

(b) *Let $\beta \in M_2(\mathbb{Z})$ such that $\det(\beta) > 0$. Then the function $j \circ \beta$ is integral over the ring $\mathbb{Z}[j]$.*

(c) *If n is not a perfect square, then the polynomial $H_n(X) = F_n(X, X)$ is non-constant and has leading coefficient ± 1.*

Proof. (a) (See [3, 5.2, Theorem 3, p. 55]). The assertion about the irreducibility follows from the fact that Γ permutes the functions $j \circ \alpha$ transitively and acts as a group of automorphisms on the field $\mathbb{C}(\{j \circ \alpha \colon \alpha \in \mathcal{S}_n\})$.

To show the symmetry we first observe that $j(\tau/n)$ is a root of $F_n(j, X)$, since the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$ is an element of $\mathcal{S}_n$, so by the definition of $F_n(j, X)$ clearly

$$F_n(j(\tau), j(\tau/n)) = 0$$

identically. It follows that

$$F_n(j(n\tau), j(\tau)) = 0$$

identically as well, thus $j(n\tau)$ is a root of the polynomial $F_n(X, j)$. On the other hand also the matrix $\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is in $\mathcal{S}_n$, so similarly we see that $j(n\tau)$ is a root of $F_n(j, X)$. Since $F_n(j, X)$ is irreducible and has a common root with $F_n(X, j)$, necessarily $F_n(j, X)$ divides $F_n(X, j)$. By *Gauss' Lemma* we must have

$$F_n(X, j) = g(X, j)F_n(j, X) \in \mathbb{Z}[j, X],$$

and hence

$$F_n(X, j) = g(X, j)g(j, X)F_n(X, j).$$

It follows that $g(X, j) = \pm 1$.

If we suppose that $g(X, j) = -1$ then $F_n(X, j) = -F_n(j, X)$ that implies that $F_n(j, j) = -F_n(j, j)$ and so $F_n(j, j) = 0$, but this contradicts the fact that $F_n(j, X)$ is irreducible over $Z[j]$. Thus $g(X, j) = 1$, so $F_n(j, X) = F_n(X, j)$.

(b) (See [7, II.6.3.b, p. 146]). Let $n = \det(\beta)$, so clearly $\beta \in \mathcal{D}_n$. As above, we can find a matrix $\gamma \in \Gamma$ such that $\gamma\beta \in \mathcal{S}_n$ The Γ-invariance of j says that $j \circ \beta = j \circ (\gamma\beta)$, while the definition of F_n shows that $X = j \circ (\gamma\beta)$ is a root of $F_n(j, X)$. Since F_n is monic by definition and has coefficients in $\mathbb{Z}[j]$ from the theorem (4.33), then $j \circ \beta$ is integral over $\mathbb{Z}[j]$.

(c) (See [7, II.6.3.c, p. 146]). Let $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{S}_n$. Using the Q-expansion of $j \circ \alpha$ described into the proof of *claim* 3, we see that the Q-expansion of $j - j \circ \alpha$, using the same notations, is

$$j - j \circ \alpha = \left(\frac{1}{Q^n} + \sum_{k=0}^{\infty} c_k Q^{nk}\right) - \left(\frac{1}{\zeta^{ab} Q^{a^2}} + \sum_{k=0}^{\infty} c_k \zeta^{abk} Q^{a^2 k}\right)$$

By assumption $n = ad$ is not a square, so $a \neq d$. The leading terms cannot cancel: this means that $j - j \circ \alpha$ has a pole as $Q \to 0$ and the coefficient of the leading term is

$$\begin{cases} 1 & \text{if } n > a^2 \\ -\zeta^{-ab} & \text{if } n < a^2 \end{cases}$$

in both the cases a root of unity. It follows that $F_n(j, j)$ has a pole as $Q \to 0$ and that the leading Q-coefficient is a root of unity; but its Q-expansion has integer coefficients, so the leading coefficient is a root of unity in $\mathbb{Z}$, hence ± 1. Further, $F_n(j, j)$ is actually a series in $q = Q^n$: so we have proven that

$$F_n(j, j) = \pm \frac{1}{q^m} + \cdots \in q^{-m}\mathbb{Z}[[q]] \qquad \text{for some } m \geq 1.$$

But we also know that $F_n(j, j) \in \mathbb{Z}[j]$ and that j has a pole at $q = 0$, hence

$$F_n(j, j) = \pm j^m + \cdots \in \mathbb{Z}[j].$$

This proves that $F_n(X, X)$ is a non-constant polynomial with leading coefficient ± 1.

□

The following lemma gives a basic fact about the polynomial $F_n(j, X)$.

Lemma 4.35. [5, 5.6, p. 302]. *If τ is an element of the upper half plane and E is an elliptic curve corresponding to the lattice $\mathbb{Z} + \tau\mathbb{Z}$, then the roots of $F_n(j(\tau), X)$ are precisely the j-invariants of elliptic curves E' such that there exist a cyclic isogeny $E' \to E$ of degree n.*

Proof. [3, 5.3, Theorem 5, p. 59]. Let $E \cong \mathbb{C}/L$ be an elliptic curve, where $L = [1, \tau] = \mathbb{Z} + \tau\mathbb{Z}$ is the corresponding lattice. We say that $M \subset L$ is a *primitive sublattice* if, when we express a $\mathbb{Z}$-basis for M in terms of $\mathbb{Z}$-basis of L, namely $M = [a\tau + b, c\tau + d]$, then $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_n^*$ is a primitive matrix. Moreover, from the *elementary divisor theorem*, M is a primitive sublattice in L if and only if the factor group L/M is cyclic.

Then let $E' \cong \mathbb{C}/M$ be the elliptic curve associated to the sublattice M of L: there exists an isogeny λ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{C}/M & \xrightarrow{\phi} & \mathbb{C}/L \\ \downarrow \wr & & \downarrow \wr \\ E' & \xrightarrow{\lambda} & E \end{array}$$

where the vertical maps are the isomorphisms between the curves and the complex tori, while ϕ is the canonical homomorphism induced by the inclusion $M \subset L$. We observe that the kernel of ϕ is exactly the factor group L/M, so we can deduce that primitive sublattices M of L correspond to the isogenies with cyclic kernel, whose order is precisely $\det(\alpha)$ or, equivalently, the index $(L\colon M)$.

Then let $M \subset L$ be a primitive sublattice: there exists $M = [a\tau + b, c\tau + d]$ where $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_n^*$ is a primitive matrix. Consider the j-invariants of the curves:

$$j_E = j(\tau) = j(L), \qquad\qquad j_{E'} = j(\alpha\tau) = j(M).$$

From the definition of the polynomial $F_n(j, X) = \prod_{\alpha\in\Delta_n^*}(X - j \circ \alpha)$, by evaluating it on τ, we see directly that $j(\alpha\tau)$ is one of its roots.

Viceversa, let $j = j(E) = j(L)$, a root of the polynomial is of the form $j \circ \alpha$ with $\alpha \in \Delta_n^*$. But to any primitive matrix corresponds a primitive sublattice M of L, to which corresponds a cyclic isogeny of degree n, so there exists a cyclic isogeny $E' \to E$ of degree n, with $E' = \mathbb{C}/M$. □

Finally, using these results, we are able to prove Theorem (4.28) at the beginning of this section.

Theorem 4.36. [7, II.6.3.1, p. 147]. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

Proof. Let $R \cong \mathrm{End}(E)$ be an order in the quadratic imaginary field K.

- We first consider the case $R = R_K$, the ring of integers of K. Choose an element $\rho \in R$ such that $n = |N_{\mathbb{Q}}^K \rho|$ is not a perfect square. For example,

$$\rho = \begin{cases} 1 + \imath & \text{if } K = \mathbb{Q}(\imath) \\ \sqrt{-D} & \text{if } K = \mathbb{Q}(\sqrt{-D}) \text{ with squarefree } D \geq 2. \end{cases}$$

  Then we know, from (2.32.b), that the isogeny $[\rho]\colon E \longrightarrow E$ has degree n. Fix $\tau \in \mathbb{H}$ with $j(\tau) = j(E)$, then the multiplication by ρ sends the lattice $\Lambda_1 = [1, \tau]$ to a sublattice $\Lambda_2 = [\rho\tau, \rho] = [a\tau + b, c\tau + d]$ for some $a, b, c, d \in \mathbb{Z}$ and with $ad - bc = n$. In other words, the matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an element of $\mathcal{D}_n$. Then,

$$j(\alpha\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) = j(E)$$

and by definition $j \circ \alpha$ is a root of the polynomial $F_n(j, X)$: if we substitute $X = j \circ \alpha$ and evaluate in τ we get

$$0 = F_n(j(\tau), j \circ \alpha(\tau)) = F_n(j(E), j(E)) = H_n(j(E))$$

From the theorem (4.34.b), the polynomial $H_n(X)$ has integer coefficients and leading coefficient equal to ± 1. This proves exactly that, in this first case, $j(E)$ is integral over $\mathbb{Z}$.

- If R is an arbitrary order in K, let $\Gamma = [\omega_1, \omega_2]$ be a lattice for E. We know, from the theorem (1.64), that $K = \mathbb{Q}(\omega_1/\omega_2)$. So, replacing Γ with $\lambda\Gamma$ for a suitable $\lambda \in \mathbb{C}^\times$ we may assume that $\Gamma \subset R_K$. We also choose $\tau \in \mathbb{H}$ such that $R_K = [1, \tau]$, then we can consider Γ as a sub-lattice of R_K, so we can write

$$\begin{cases} \omega_1 = a\tau + b \\ \omega_2 = c\tau + d \end{cases} \qquad \text{for some } a, b, c, d \in \mathbb{Z}.$$

Switching ω_1 and ω_2 if necessary, we may assume that $n = ad - bc \geq 1$. Since the matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an element of $\mathcal{D}_n$, by the theorem (4.34.b), it follows that $j \circ \alpha$ is integral over the ring $\mathbb{Z}[j]$ and the integrality is given by the equation $F_n(j, X) = 0$. Evaluating it at τ gives that also $j(\alpha\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. But we computed that $j(\alpha\tau) = j(E)$ and we already know that $j(\tau)$ is integral over $\mathbb{Z}$, since it is the j-invariant of an elliptic curve with complex multiplication by R_K. Therefore $j(E)$ is integral over $\mathbb{Z}$.

□

Bibliography

[1] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, 1st edition (1989), Wiley.

[2] Serge Lang, *Algebraic number theory*, volume 110 of Graduate text in Mathematics, 2nd edition (1994), Springer-Verlag, New York.

[3] Serge Lang, *Elliptic functions*, volume 112 of Graduate text in Mathematics, 2nd edition (1987), Springer-Verlag, New York.

[4] James S. Milne, *Class field theory*, notes available at jmilne.org, version 4.02, March 23, 2013.

[5] Vinayak Vatsal, *Arithmetic of L-functions, "Complex multiplication: a Concise Introduction"*, volume 18 of IAS/Park City Mathematics Series, (2011), American Mathematical Society.

[6] Joseph H. Silverman, *Arithmetic of elliptic curves*, volume 106 of Graduate text in Mathematics, 2nd edition (2009), Springer-Verlag, New York.

[7] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, volume 151 of Graduate text in Mathematics, (1991), Springer-Verlag, New York.