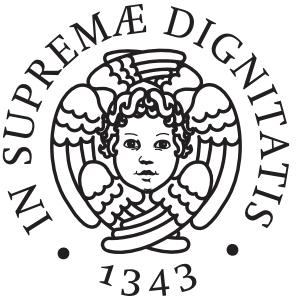
Università di Pisa



Facoltà di Matematica

Elliptic curves with complex multiplication and their application to class field theory

Tesi di Laurea Triennale
in Matematica

Anno Accademico 2020/2021

Candidato
Tommaso Faustini

Relatore
Davide Lombardo
Università di Pisa

Anno Accademico 2020 - 2021

Al nonno Silvano e alla nonna Faustina,
per tutto l'a etto che n da piccolo mi avete saputo dare

Contents

Acknowledgement

This thesis comes at the end of a very rewarding course of studies in which I have discovered branches of mathematics that I did not know before, met new fantastic friends and profited of the preparation and professionality of my teachers. It has been a very stimulating journey which I have enjoyed also thanks to the generous support that I received from many. In the first place, I wish to thank my supervisor, Professor Davide Lombardo, for his generous guidance throughout the preparation of this thesis. His corrections, comments, suggestions and explanations have been fundamental to achieve the final result and to guide me through the difficulties I encountered. I also wish to thank my university friends for the constant closeness and for the tough discussions they had with me on mathematics and life! Equally, I want to acknowledge the support of my "Big family" and my girlfriend, Eleonora, for being there, always, also when I get unbearable!

Thank you all!

Abstract

In algebraic number theory, the Hilbert class field H of a number field K is the maximal abelian unramified extension of K. The existence of this particular extension is an important tool in studying the structure of the ideal class group of a number field, and for this reason the explicit construction of the Hilbert class field of a given number field is an important problem. Although the problem is still open, the particular case of quadratic imaginary fields is completely understood, thanks to the theory of elliptic curves with complex multiplication. The purpose of this dissertation is to show how tools from the theory of elliptic curves with complex multiplication and of modular forms can be brought to bear on studying the Hilbert class field of an imaginary quadratic field.

The first step in the study of elliptic curves over C is to prove the Uniformization Theorem: for every elliptic curve E/C there exists a lattice Λ, unique up to homothety, such that $E \simeq E_\Lambda$. This theorem is very important because it connects algebraic notions with analytic notions. In order to prove this theorem, in the first chapter we introduce some definitions and proprieties of modular forms. In the second chapter we discuss elliptic curve with complex multiplication and their endomorphism rings.

Then, in the third chapter, we present some results about the so-called congruence subgroups of $\mathbf{SL}_2(\mathsf{Z})$ and their corresponding modular forms, in particular we investigate the congruence subgroup $\Gamma_0(N)$. At the end of the chapter, using these tools and some proprieties of the modular polynomial and its coefficients we prove the following theorem: Let R be an order in an imaginary quadratic field and let Λ be a lattice with $R\Lambda \subset \Lambda$, then $j(\Lambda)$ is an algebraic integer. In the last chapter we give a brief review of class field theory and finally we prove the following theorem: Let K/Q be a quadratic imaginary field with ring of integers $\mathcal{O}_K$, and let E be an elliptic curve with $End(E) \simeq \mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.

CHAPTER 0

Preliminaries

In this chapter we review, mostly without proof, some fundamental facts on elliptic curves. All the definitions, propositions and theorems in this chapter can be found in [4, Chaper II and III] and [6, Chapter 2].
An elliptic curve over a field K is an smooth projective algebraic curve of genus one defined over K having a specified base point with coordinates in K. Every such curve can be written as the locus in P^2 of a cubic equation with only one point on the line at ∞, corresponding to the marked point of E. Up to isomorphism, every elliptic curve can be defined by a *long Weiestrass equation*:

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

If we suppose that $\mathrm{char}(\overline{K}) \neq 2, 3$ we can consider the short Weierstrass equation:

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

Definition 0.1. A Weierstrass equation is in Legendre form if it can be written as

$$y^2 = x(x-1)(x-\lambda)$$

We can define some useful quantities associated with a short Weierstrass equation:

- discriminant: $\triangle = -16(4a^3 + 27b^2)$
- j-invariant: $j = 1728\frac{4a^3}{4a^3+27b^2}$

As E is smooth by definition, it is easy to see that $\triangle \neq 0$.

Proposition 0.2. *Assume that char$(K) \neq 2, 3$. Then every elliptic curve is isomorphic over $\overline{K}$ to an elliptic curve in Legendre form*

$$E : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \overline{K}$ with $\lambda \neq 0, 1$.

Proof. Since $\text{char}(K) \neq 2, 3$ we can consider a Weierstrass equation for E of the form $E : y^2 = x^3+ax+b = (x-x_1)(x-x_2)(x-x_3)$ for some $x_1, x_2, x_3 \in \overline{K}$. Further, since $\triangle = 16(x_1 - x_3)^2(x_1 - x_2)^2(x_2 - x_3)^2 \neq 0$ we see that the x_i's are distinct. Now using the substitution

$$x = (x_2 - x_1)x^{\prime} + x_1, \quad y = (x_2 - x_1)^{3/2}y^{\prime}$$

we find a Weierstrass equation in Legendre form. □

We now state two important results about the j-invariant. The first one justifies the name "invariant".

Theorem 0.3. *Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.*

Proposition 0.4. *Let $j_0 \in \overline{K}$. There exists an elliptic curve de ned over $K(j_0)$ whose j-invariant is equal to j_0.*

0.1 Divisors

Definition 0.5. A *divisor* is a formal sum $D = \sum_{P2E} n_P(P)$, where $n_P \in \mathsf{Z}$ and $n_P = 0$ for all but finitely many $P \in E$.

Now we define a particular set of divisors and we state a characterization of them, that will be useful in the proof of Theorem 1.23.

Definition 0.6. A divisor $D \in Div(E)$ is *principal* if it is of the form $D = div(f)$ for some $f \in \overline{K}(C)$

Proposition 0.7. *Let E/K be an elliptic curve and let $D = \sum n_P(P) \in Div(E)$. Then D is a principal divisor if and only if*

$$\sum_{P2E} n_P = 0 \quad \textit{and} \quad \sum_{P2E} [n_P]P = 0.$$

For a proof of the case $K = \mathsf{C}$, see Corollary 1.19.

Now we also introduce the notion of divisor of a quotient of C by a lattice.

Definition 0.8. The *divisor group* of $\mathbb{C}/\Lambda$ is:

$$Div(\mathbb{C}/\Lambda) = \{ \sum_{\omega \in \mathbb{C}/\Lambda} n_\omega(\omega) | n_\omega \in \mathbb{Z}, n_\omega \neq 0 \text{ for finitely many } \omega\}.$$

Definition 0.9. For $D = \sum n_\omega(\omega) \in Div(\mathbb{C}/\Lambda)$ we define the *degree of* D as $deg(D) = \sum n_\omega$ and the subgroup of $Div(\mathbb{C}/\Lambda)$ of degree 0 divisors $Div_0(\mathbb{C}/\Lambda) = \{D \in Div(\mathbb{C}/\Lambda) : deg(D) = 0\}$.

0.2 Differentials

Definition 0.10. Let E be a curve. The *space of differential forms* on E, denoted by Ω_E, is the $\overline{K}$-vector space generated by symbols of the form dx for $x \in \overline{K}(E)$, subject to the usual relations:

1. $d(x + y) = dx + dy$ for all $x, y \in \overline{K}(E)$.
2. $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(E)$.
3. $da = 0$ for all $a \in \overline{K}$.

Proposition 0.11. *Let E be an elliptic curve over an algebraically closed field $\overline{K}$.*

1. *Ω_E is a 1-dimensional $\overline{K}(E)$-vector space.*
2. *Let $x \in \overline{K}(E)$. Then dx is a $\overline{K}(E)$-basis for Ω_E if and only if $\overline{K}(E)/\overline{K}(x)$ is a finite separable extension.*
3. *Let $\Phi : E_1 \to E_2$ be a noncostant map of elliptic curves. Then Φ is separable if and only if the map*

$$\Phi^* : \Omega_{E_2} \to \Omega_{E_1}$$

is injective.

In the case of elliptic curve we have an important differential.

Definition 0.12. The invariant differential of an elliptic curve is $\omega = \frac{dx}{2y}$.

Next we state two important proprieties of the invariant differential. The second one justifies the adjective "invariant".

Proposition 0.13. *Let E be an elliptic curve. The invariant differential ω associated with a Weierstrass equation for E is holomorphic and nonvanishing.*

Proposition 0.14. *Let E be an elliptic curve, let ω be the invariant di erential, let $Q \in E(\overline{K})$ and let $\tau_Q : E \to E$ be the translation-by-Q map. Then*

$$\tau_Q \omega = \omega.$$

Proof. The statement is invariant under extension of the base field, so we may assume $K = \overline{K}$. We restrict to the case $\mathrm{char}(K) \neq 2, 3$. Let us consider a Weierstrass equation in Legendre form for E:

$$E : y^2 = x(x-1)(x-\lambda).$$

From Proposition 0.11 we know that Ω_E is a one-dimensional $\overline{K}(E)$-vector space, so there is a function $a_Q \in \overline{K}(E)$ such that

$$\tau_Q \omega = a_Q \omega.$$

We note that $a_Q \neq 0$ because τ_Q is an isomorphism. We compute

$$div(a_Q) = div(\tau_Q \omega) - div(\omega) = \tau_Q div(\omega) - div(\omega) = 0,$$

where in the last equality we use Proposition 0.13 which says that $div(\omega) = 0$. Thus a_Q has no zeros and no poles, so it is constant. Next we consider the map

$$f : E \to \mathsf{P}^1, \quad Q \mapsto [a_Q : 1].$$

This map is rational because a_Q algebraically (rationally) depends on Q. Moreover f is not surjective, because $[0 : 1]$ is not hit, so it must be constant. We can compute, for instance, the value a_0, that is 1. This proves that $a_Q = 1$ for all $Q \in E$. □

0.3 Isogenies

Definition 0.15. Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism

$$\Phi : E_1 \longrightarrow E_2 \text{ satisfying } \Phi(O) = O.$$

The following result is a useful tool to construct isogenies:

Theorem 0.16. *Let*

$$\Phi : E_1 \to E_2 \quad \textit{and} \quad \Psi : E_1 \to E_3$$

be noncostant isogenies, and assume that Φ is separable. If $\ker \Phi \subset \ker \Psi$ then there is a unique isogeny

$$\lambda : E_2 \to E_3$$

satisfying $\Psi = \lambda \circ \Phi$.

We can also describe isogenies in terms of explicit equations:

Lemma 0.17. *Let E_1 and E_2 be elliptic curves over K given by Weierstrass equations in short form. Let $\varphi : E_1 \to E_2$ be an isogeny de ned over K. Then φ can be uniquely represented by an a ne rational map of the form*

$$\varphi(x, y) = \left(\frac{f_{1,1}(x)}{f_{1,2}(x)}, \frac{f_{2,1}(x)}{f_{2,2}(x)} y \right),$$

where $f_{1,1}, f_{1,2}, f_{2,1}, f_{2,2} \in K[x]$ and the polynomials $f_{1,1}, f_{1,2}$ and $f_{2,1}, f_{2,2}$ are relatively prime.

Proof. Suppose that φ is defined by the rational map $[\varphi_x : \varphi_y : \varphi_z]$. Then we can write

$$\varphi(x, y) = (\varphi_1(x, y), \varphi_2(x, y))$$

where $\varphi_1(x, y) = \frac{\varphi_x[x,y,1]}{\varphi_z[x,y,1]}$ and $\varphi_2(x, y) = \frac{\varphi_y[x,y,1]}{\varphi_z[x,y,1]}$. Using the equation $y^2 = x^3 + a_1 x + b_1$ for E_1 and the equation $y^2 = x^3 + a_2 x + b_2$ for E_2 we can cancel the factors of the form y^k with $k > 1$. So, we reduce to the form

$$\varphi(x, y) = \left(\frac{g_{1,1}(x) + g_{1,2}(x)y}{g_{1,3}(x) + g_{1,4}(x)y}, \frac{g_{2,1}(x) + g_{2,2}(x)y}{g_{2,3}(x) + g_{2,4}(x)y} \right)$$

where $g_{i,j} \in K[x]$. Next we can multiply term by term by

$$\left(\frac{g_{1,3}(x) - g_{1,4}(x)y}{g_{1,3}(x) - g_{1,4}(x)y}, \frac{g_{2,3}(x) - g_{2,4}(x)y}{g_{2,3}(x) - g_{2,4}(x)y} \right),$$

and using again the equation for E_1 and E_2 we write $\varphi(x, y)$ in the form

$$\varphi(x, y) = \left(\frac{h_{1,1}(x) + h_{1,2}(x)y}{h_{1,3}(x)}, \frac{h_{2,1}(x) + h_{2,2}(x)y}{h_{2,3}(x)} \right).$$

Finally, since φ is a homomorphism $\varphi((x, y)\ ^1) = \varphi(x, -y) = -\varphi(x, y)$, then

$$\left(\frac{h_{1,1}(x) - h_{1,2}(x)y}{h_{1,3}(x)} \right) = \left(\frac{h_{1,1}(x) + h_{1,2}(x)y}{h_{1,3}(x)} \right)$$

which implies that $h_{1,2}(x)$ is the zero polynomial. We proceed similarly for the other coordinate. After eliminating any common factors we obtain the claim. □

The set $Hom(E_1, E_2)$ has a natural structure of abelian group, when $E_1 = E_2$ it is also a ring. Now we state an important result on the structure of $Hom(E_1, E_2)$.

Theorem 0.18. *Let E_1 and E_2 be elliptic curves. Then*

$$Hom(E_1, E_2)$$

is a free $\mathbb{Z}$-module of rank at most 4.

0.4 Elliptic Curves over Local Fields

Now we introduce some facts about elliptic curves defined over a field that is complete with respect to a discrete valuation. In this discussion we assume that v is normalized and that K and k, the residue field of $\mathcal{O}_K$, are perfect fields.

Definition 0.19. Let E/K be an elliptic curve. A Weierstrass equation for E is called a minimal (Weierstrass) equation for E at v if $v(\triangle)$ is minimized subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in R$. This minimal value of $v(\triangle)$ is called the valuation of the minimal discriminant of E at v.

The following proposition is a basic result that will be very useful in the last chapter.

Proposition 0.20.

1. *Every elliptic curve E/K has a minimal Weierstrass equation.*
2. *The invariant differential*

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

associated to a minimal Weierstrass equation is unique up to multiplication by an element of R .

We next look at the operation, $\sim$, of "reduction modulo π".

Definition 0.21. Having chosen a minimal Weierstrass equation for E/K, we can reduce its coefficients modulo π to obtain a (possibly singular) curve over k, namely

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

This curve is called the reduction of E modulo π.

We classify E according to the singularity types of $\tilde{E}$.

Definition 0.22. Let E/K be an elliptic curve, and let $\tilde{E}$ be the reduction modulo π of a minimal Weierstrass equation for E.

1. E has good (or stable) reduction if $\tilde{E}$ is nonsingular.
2. E has multiplicative (or semistable) reduction if $\tilde{E}$ has a node.
3. E has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

In the last two cases we say that E has bad reduction.

0.5 Tate module and Weil pairing

Definition 0.23. Let E be an elliptic curve and let $l \in \mathsf{Z}$ be a prime. The (l-adic) *Tate module* of E is the group

$$T_l(E) = \varprojlim_n E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

An introduction to the Weil pairing can be found in [1, Chapter III.8].

Proposition 0.24. *There exists a bilinear, alternating, nondegenerate, Galois equivariant pairing*

$$e : T_l(E) \times T_l(E) \to T_l(\mu).$$

Further, if $\Phi : E_1 \to E_2$ is an isogeny, then Φ and its dual $\tilde{\Phi}$ are adjoints for the pairing, i.e., $e(\Phi S, T) = e(S, \tilde{\Phi} T)$ for all $S, T \in T_l(E)$.

Now we state a proposition that will be useful in the last chapter.

Proposition 0.25. *Let E/K be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to char(k). Assume further that the reduced curve $\tilde{E}/k$ is nonsingular. Then the reduction map*

$$E(K)[m] \to E(k)$$

is injective, where $E(K)[m]$ denotes the set of points of order m in $E(K)$.

CHAPTER 1

Elliptic curves over C

In this chapter we will consider elliptic curves over the complex numbers. We want to prove the correspondence between elliptic curves over C and tori $\mathbb{C}/\Lambda$ defined by a lattice Λ. The following will be one of our main tools in the following chapter.

Teorema (Riemann-Hurwitz)**.** *Let S, S^0 be two compact, connected Riemann surfaces of genera $g(S)$, $g(S^0)$ and π a complex analytic map between them. Then we have the formula*

$$2 - 2g(S) = (deg\pi)(2 - 2g(S^0)) + \sum_{P2S}(1 - e_P),$$

where e_P is the rami cation index of the point P.

Proof. Let us take a triangulation T of S^0 such that the branching points are vertices of it; we consider on S the triangulation given by $\pi^{-1}(T)$. If we let V, E, F be the number of vertices, edges and faces of the triangulation on S^0 then the faces on S are $deg(\pi) \cdot F$ and the edges $deg(\pi) \cdot E$. It is different for the vertices because here we have the ramification points:

$$\sum_{v2V} \#\pi^{-1}(v) = \sum_{v2V} \sum_{\substack{q2S \\ \pi(q)=v}} 1 = \sum_{v2V} \sum_{\substack{q2S \\ \pi(q)=v}} (1 - e_q) + e_q =$$

$$= \sum_{v2V} \sum_{\substack{q2S \\ \pi(q)=v}} (1 - e_q) + \sum_{v2V} \sum_{\substack{q2S \\ \pi(q)=v}} e_q = \sum_{v2V} \sum_{\substack{q2S \\ \pi(q)=v}} (1 - e_q) + deg(\pi) \cdot V.$$

So, if we use the fact that $\chi(S) = 2 - 2g(S)$, we have:

$$\begin{aligned} 2 - 2g(S) &= \sum_{q \in S}(1 - e_q) + deg(f) \cdot V - deg(f) \cdot E + deg(f) \cdot F \\ &= \sum_{q \in S}(1 - e_q) + deg(f) \cdot \big(2 - 2g(S')\big). \end{aligned}$$

□

We apply the theorem above to the case of elliptic curves over $\mathbb{C}$.
Let $E/\mathbb{C}$ be the elliptic curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$ and let us consider the map $\phi : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ given by $[x : y : z] \mapsto [x : z]$ that is continuous and has degree 2. It is ramified, with $e_P = 2$, in $[x_1 : 0 : 1], [x_2 : 0 : 1], [x_3 : 0 : 1], \infty$ where x_1, x_2, x_3 are the zeros of the polynomial $x^3 + Ax + B$. We find

$$\chi(E(\mathbb{C})) = 2 \cdot 2 - 4 = 0,$$

so $E(\mathbb{C})$ has the same genus as a torus. We recall that for any lattice $\Lambda \subset \mathbb{C}$ we have $\frac{\mathbb{C}}{\Lambda} \simeq \frac{\mathbb{R}^2}{\mathbb{Z}^2} \simeq \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^2 \simeq (\mathbb{S}^1)^2$. This leads us to think that there is a relation between elliptic curves over $\mathbb{C}$ and the quotient spaces $\mathbb{C}/\Lambda$, were Λ is a lattice.

1.1 Elliptic Integrals

The results of this section could be found in [4, Chapter VI]. Elliptic curves were originally introduced for the computation of the integral giving the arc length of an ellipse. Let us start with the case of a circle, for which the integral is $\int \omega = \int \frac{dt}{\sqrt{1 - t^2}}$. There is a problem with the definition of this integral, because there is no canonical definition of a square root in $\mathbb{C}$. However for the circle the integral could be computed using the following parameterization of $\mathbb{S}^1$

$$t \mapsto \left(\frac{1 - t^2}{\sqrt{1 + t^2}}, \frac{2t}{1 + t^2}\right).$$

In the general case, let us consider

$$y^2 = f(t),$$

with f a polynomial of degree 3 or 4. Up to a Möbius trasformation $t \mapsto \frac{at+b}{ct+d}$, every arc of ellipse can be parametrized with a polynomial f that has one the following shapes

$$f(t) = t^3 + at + b, \quad f(t) = t(t - 1)(t - \lambda).$$

The arc length is then given by

$$\int \sqrt{1+(f(t)^{\emptyset})^2}dt.$$

There are two problems with this integral. The first one is the same that we have in the case of a circle, namely the square root is a multivalued function. In order to avoid this problem, the integral is more naturally studied on an appropriate Riemann surface, which turns out to be $E(\mathsf{C})$.

$$E(\mathsf{C}) = \{y^2 = x^3+ax+b : (x,y) \in \mathsf{C}^2\} \cup \{\infty\} \simeq \{y^2 = x(x+1)(x+\lambda) : (x,y) \in \mathsf{C}^2\} \cup \{\infty\}$$

In the equivalence above, in order to pass to the Legendre form, we used the Proposition 0.2.
Let us consider the map:

$$F : E(\mathsf{C}) \to \mathsf{C} \quad , \quad P \mapsto \int_O^P \omega \tag{1.1}$$

where $\omega = dx/y$ is a holomorphic differential form on E.
Now a new problem arises: the integral is not well defined, because it depends on the choice of the connecting path between O and P. Next we recall that any elliptic curve has only one point at infinity, so there is a bijection between $\infty \neq [x,y,z] \in E(\mathsf{C})$ and $\{(x,y) \in \mathsf{C}^2 \mid y^2 = x(x-1)(x-\lambda)\}$. So, if we consider $\infty \neq P = [x,y,z]$, $\omega = dt/y$ and $y = \sqrt{t(t-1)(t-\lambda)}$ we find that our integral is $\int_1^x \frac{dt}{\sqrt{t(t\ \ 1)(t\ \ \lambda)}}$.
In order to make the integral well-defined, it is necessary to make branch cuts.

Definition 1.1. A branch cut is a curve in the complex plane such that it is possible to define a single analytic branch of a multivalued function on the plane minus that curve.

In our case we consider

$$\begin{cases} \gamma_1(t) = (1-t) + t\lambda \\ \gamma_2(t) = t\ \ ^1 \end{cases} \quad t \in [0,1] \tag{1.2}$$

On the set $\mathsf{C} \backslash Im(\gamma_1) \cup Im(\gamma_2)$ both the functions $\pm\sqrt{t(t-1)(t-\lambda)}$ are well defined and analytic. Let us consider two copies of $\mathsf{P}^1(\mathsf{C})$, that topologically is a 2-sphere, and glue them together along the branch cuts in order to form a Riemann surface that is homeomorphic to a torus.

We see that the indeterminacy comes from the integration across branch cuts in $\mathsf{P}^1(\mathsf{C})$, or equivalently around noncontractible loops on the torus. Let

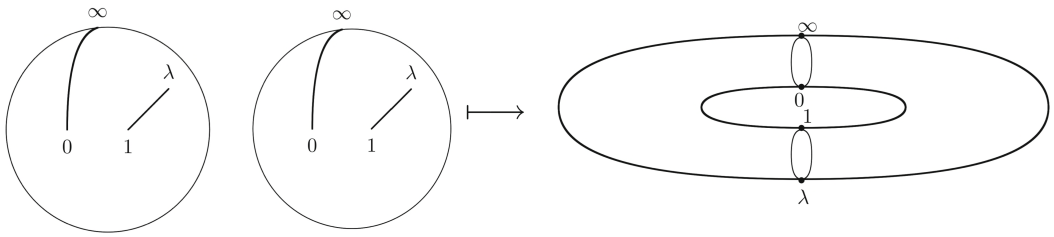


Figure 1.1:

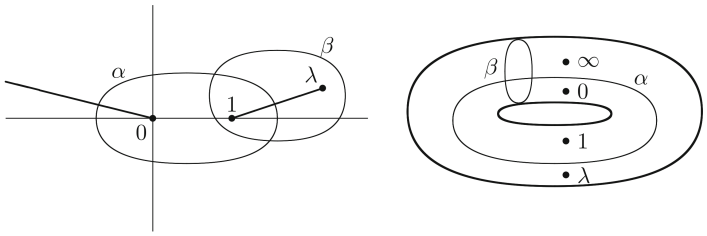


Figure 1.2:

us take α and β the two paths illustrated in Figure 1.2. They generate the fundamental group of the torus, $\mathbb{Z}^2$. Thus, any two paths from O to P differ by a path that is homotopic to $n\alpha + m\beta$ for some $n, m \in \mathbb{Z}$. We define two numbers, associated with the curve $E(\mathbb{C})$, called periods of E:

$$\omega_1 = \int_\alpha \omega, \qquad \omega_2 = \int_\beta \omega$$

From the consideration on the paths from O to P, the map (1.1) is well defined up to addition of $n\omega_1 + m\omega_2$ for some $n, m \in \mathbb{Z}$. This suggests to define the set $\Lambda = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}$.
The set Λ is clearly a subgroup of $\mathbb{C}$, so the quotient $\mathbb{C}/\Lambda$ is a group. We obtain that F is a homomorphism with values in $\mathbb{C}/\Lambda$ by using the translation invariance of ω:

$$F(P+Q) = \int_O^{P+Q} \omega \equiv \int_O^P \omega + \int_P^{P+Q} \omega \equiv \int_O^P \omega + \int_O^P \tau_P\omega \equiv F(P)+F(Q) \pmod{\Lambda}.$$

Later in this chapter we will prove that F is a isomorphism and Λ is a lattice.

1.2 Elliptic Functions

In this section we will study meromorphic functions on the quotient space $\mathbb{C}/\Lambda$, where Λ is a lattice. The results of this Chapter can be found in [4,

Chapter VI] and [5, Lecture 15,16]

Definition 1.2. An *elliptic function*, or *doubly periodic function*, for a lattice Λ is a complex function $f(z)$ such that:

1. f is meromorphic;
2. $f(z+\omega) = f(z) \quad \forall z \in \mathbb{C}\ \forall \omega \in \Lambda$.

It follows from the definition that an elliptic function can be also be viewed as a function on $\mathbb{C}/\Lambda$. It is also an immediate consequence of the definition that the set of elliptic functions $\mathbb{C}(\Lambda)$ is a field that contains every constant function.

Definition 1.3. Let $\{\omega_1, \omega_2\}$ be a basis for Λ. A *fundamental parallelogram* for Λ is a set of the form:

$$D = \{a + t\omega_1 + s\omega_2 : 0 \leq t, s < 1\} \quad \text{for some } a \in \mathbb{C}.$$

Theorem 1.4. *A holomorphic elliptic function is constant. Similarly, an elliptic function with no zeros is constant.*

Proof. Let D be a fundamental parallelogram for Λ and suppose that $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. It follows from the definition of elliptic function that $\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in D} |f(z)|$. f is continuous on the compact set $\overline{D}$ so $|f(z)|$ is bounded on $\overline{D}$. Hence, it is bounded on $\mathbb{C}$, so the first claim follows by using Liouville's theorem. The second statement follows from the first one by using that: if f has no zeros, then $1/f$ is an holomorphic elliptic function. □

Remark 1.5. Let f be a meromorphic function and $\omega \in \mathbb{C}$. Then we can consider:

$$\begin{cases} \mathrm{ord}_\omega(f) = \text{order of vanishing of } f \text{ at } \omega \\ \mathrm{res}_\omega(f) = \text{residue of } f \text{ at } \omega \end{cases} \tag{1.3}$$

In the rest of the section the notation $\sum_{w \in \mathbb{C}/\Lambda}$ will denote a sum over a fundamental parallelogram D.

Theorem 1.6. *Let $f \in \mathbb{C}(\Lambda)$ be an elliptic function relative to Λ.*

1. $\sum_{\omega \in \mathbb{C}/\Lambda} res_\omega(f) = 0$;
2. $\sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f) = 0$;
3. $\sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f)\omega \in \Lambda$.

Proof. We note that the sum is independent of the choice of the fundamental parallelogram because $res_{\omega_0}(f) = res_{\omega_0+\omega}(f) \quad \forall \omega \in \Lambda$.
Let D be a fundamental parallelogram such that $f(x) \neq 0 \wedge f(x) \neq \infty \ \ \forall x \in \partial D$.

1. If we use the residue theorem on f, we obtain:

$$\sum_{w \in \mathbb{C}/\Lambda} res_\omega(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)dz.$$

   The periodicity of f implies that the integrals along the opposite sides of the parallelogram cancel, so the integral is zero;

2. We apply the residue theorem to f'/f noting that this is again an elliptic function and that $res_\omega(f'/f) = ord_\omega(f)$.

3. We apply the residue theorem to zf'/f. This is no longer an elliptic function, but the integral of it around ∂D lies in Λ.

□

Definition 1.7. The order of an elliptic function is the number of its poles (or equivalently of zeros), counted with multiplicity, in a fundamental parallelogram.

Corollary 1.8. *A nonconstant elliptic function has order at least 2.*

Proof. Let us suppose that $f(z)$ has a single simple pole, then the Theorem 1.6(1) tells us that residue is 0, so $f(z)$ is holomorphic. The claim follows using Theorem 1.1. □

Definition 1.9. $\forall f \in \mathbb{C}(\Lambda)$, i.e. a nonzero elliptic function, we define the *divisor of f* as $\mathrm{div}(f) = \sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f)(w)$.

By Theorem 1.6 $div(f) \in Div_0(\mathbb{C}/\Lambda)$. Hence, we can consider the well-defined map:

$$div : (\mathbb{C}(\Lambda) \ , \cdot) \to (Div_0(\mathbb{C}/\Lambda), +),$$

which is a homomorphism because $ord_\omega(f)$ is a valuation (i.e. $ord_\omega(f \cdot g) = ord_\omega(f) + ord_\omega(g)$).

Definition 1.10. We define a *sum(mation) map*:

$$sum : Div_0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda, \qquad sum(\sum n_\omega(\omega)) = \sum n_\omega(\omega) \pmod{\Lambda}$$

Theorem 1.11. *The sequence*

$$1 \to \mathbb{C} \xrightarrow{i} \mathbb{C}(\Lambda) \xrightarrow{div} Div_0(\mathbb{C}/\Lambda) \xrightarrow{sum} \mathbb{C}/\Lambda \to 0,$$

is exact.

Proof. The map i is clearly injective. The map sum is surjective because $((\omega) - (0)) \in Div_0(\mathbb{C}/\Lambda) \quad \forall \omega \in \mathbb{C}/\Lambda$ so $sum((\omega) - (0)) = \omega$. Exactness at $\mathbb{C}(\Lambda)$ follows from Theorem 1.4. The fact that $\mathrm{im}(div) \subseteq \ker(sum)$ follows from Theorem 1.6. The other inclusion will be proved in the next section (Proposition 1.18). □

1.3 From lattice to elliptic curve

The results of this Chapter can be found in [4, Chapter VI] and [2, Chapter 9]. We now want to define some examples of non-constant elliptic functions. In order to do this, we first consider a finite group G acting on a set A. It is easy to construct functions invariant under the action of G: take f to be any function $f : S \to \mathbb{C}$, and define $F(a) = \sum_{g \in G} f(g * a)$. Then F is a G-invariant function, and all G-invariant $\mathbb{C}$-valued functions are of this form. When G is not finite, one has to verify that the series converges. Using these ideas we define our first examples of non-constant elliptic functions:

Definition 1.12. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function* (relative to Λ) is defined by the series:

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

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

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

From the definition it is clear that $\wp(z)$ has a pole of order 2 at each point $z \in \Lambda$.
The following theorem shows it has no other poles.

Theorem 1.13. *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

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

2. *The series defining $\wp$ converges absolutely and defines a meromorphic function on* C *having a double pole with residue* 0 *at* $x \in \Lambda$ *and no other poles.*

Proof. 1. Since Λ is discrete in C and $\delta = \min_{\lambda,\omega \in \Lambda} \{|\lambda - \omega|\} > 0$, we have[1]:

$$\exists c \text{ such that } \#\{\omega \in \Lambda \mid N \leq |\omega| < N+1\} < cN \quad \forall N \in \mathbb{N}.$$

Hence, we may use this to estimate the sum of the absolute values of summands in the series defining $G_{2k}(\Lambda)$:

$$\sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} |\omega|^{-2k} \leq \sum_{N=1}^{\infty} \frac{\#\{\omega \in \Lambda \mid N < |\omega| < N+1\}}{N^{2k}} \leq \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty.$$

2. We may assume without loss of generality that $|\omega| \geq 2|z|$, since this holds for all but finitely many terms. We can estimate the terms of the series as follows:

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{|z|(2|\omega| + |z|)}{|\omega|^2 (|z| - |\omega|)^2} \leq \frac{10|z|}{|\omega|^3},$$

where the first estimate comes from the triangular inequality and the second one from the inequalities $|\omega| - |z| \geq \frac{1}{2}|\omega|$ and $|2\omega| + |z| \leq \frac{5}{2}|\omega|$. From the first part it follows that the series for $\wp(z)$ is absolutely convergent for all $z \in \mathbb{C} \backslash \Lambda$, hence it is uniformly convergent on every compact subset of $\mathbb{C} \backslash \Lambda$. Hence, the series is analytic on $\mathbb{C} \backslash \Lambda$, so it defines a holomorphic function. Finally, from the series expansion it is clear that $\wp(z)$ has a double pole with residue 0 for all $x \in \Lambda$.

□

With Theorem 1.13 in hand, we can now summarize the key properties of $\wp(z)$ and $\wp'(z)$.

Theorem 1.14. *The Weierstrass $\wp(z)$-function is a meromorphic even elliptic function. Its derivative, $\wp'(z)$, is a meromorphic odd elliptic function.*

Proof. Using the series expansion we obtain that $\wp(z)$ is an even function:

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

[1] In order to prove this we can consider the annulus $U_N = \{x \in \mathbb{C} \mid N \leq |x| < N+1\}$ and for each point of the lattice the open set $V_\omega = \{x \in \mathbb{C} \mid |x - \omega| < \delta\}$. These open sets are all disjoint, so we can estimate their number.

From the previous theorem we know that the series is uniformly convergent, so we can compute its derivative by differentiating term by term

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

From this expression it is clear that $\wp^{\emptyset}$ is an elliptic function. From the integration of the condition of being an elliptic function with respect to z we obtain that there exist a function $c : \Lambda \to \mathsf{C}$ such that

$$\wp(z+\omega) = \wp(z) + c(\omega) \qquad \forall z \ \in \ \mathsf{C}.$$

If $z = -\frac{1}{2}\omega$, using the evenness of $\wp$, $\wp(\frac{1}{2}\omega) = \wp(-\frac{1}{2}\omega)$. Hence $c(\omega) = 0$, this implies the theorem. □

Theorem 1.15. *Let $\Lambda \subset \mathsf{C}$ be a lattice. Then:*

$$\mathsf{C}(\Lambda) = \mathsf{C}(\wp(z), \wp(z)^{\emptyset}).$$

Proof. Let $f(z) \in \mathsf{C}(\Lambda)$. Using the equality

$$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2},$$

we are reduced to the study of odd and even functions. Moreover, we can study only even functions: if $f(z)$ is odd, then $f(z)\wp(z)^{\emptyset}$ is even.
The evenness of f implies that $ord_\omega f = ord\ _\omega f \quad \forall \omega \in \mathsf{C}$.
We now show that if $2\omega \in \Lambda$ then $ord_\omega f$ is even. First we suppose that $ord_\omega f > 0$, so differentiating the evenness condition and using $\omega = -\omega + 2\omega$ we obtain

$$f^{(i)}(\omega) = 0 \quad \forall i \text{ odd}.$$

So $ord_\omega f$ is even, as it can be seen by using De l'Hopital's rule. On the other hand, if $ord_\omega f < 0$ we may consider $1/f$ that is an elliptic function with all the proprieties of f such that $ord_\omega 1/f = -ord_\omega f > 0$.
Let D be a fundamental parallelogram for Λ, and let H be "half" of it. In other words, H is a fundamental domain for $(\mathsf{C}/\Lambda)/\{\pm 1\}$
The above discussion implies that the divisor of f has the form

$$\sum_{\omega 2 H} n_\omega((\omega) + (-\omega)) \quad n_\omega \in \mathsf{Z}.$$

The evenness of $ord_\omega f$, in the case $2\omega \in \Lambda$, is used for the points on the boundary of D.
Let us consider the function

$$g(z) = \prod_{\omega 2 H n f 0 g} (\wp(z) - \wp(\omega))^{n_\omega}.$$

The divisor of $(\wp(z) - \wp(\omega))$ is $(\omega) + (-\omega) - 2(0)$, so f and g have the same zeros and poles, except possibly in $\omega = 0$. From Theorem 1.6 it follows that they have the same order at 0 too. Thus $f(z)/g(z)$ is a holomorphic elliptic function, and from Theorem 1.4 it is constant. Hence, there exists a constant c such that $f(z) = cg(z) \in \mathbb{C}(\wp(z), \wp(z)^{\prime})$. □

In order to construct functions with prescribed properties, it is convenient to introduce

Definition 1.16. The *Weierstrass σ-function (relative to Λ)* is the function

$$\sigma(z) = \sigma(z; \Lambda) = z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{(\frac{z}{\omega}) + \frac{1}{2}(\frac{z}{\omega})^2}.$$

This is not an elliptic function, but it satisfies a simple transformation law under translation by elements of Λ. The following proposition proves this transformation law and some other basic properties of the function $\sigma(z)$ introduced above.

Lemma 1.17.

1. *$\sigma(z)$ is a holomorphic function on $\mathbb{C}$. It has simple zeros for all $z \in \Lambda$ and no other.*
2. $\dfrac{d^2}{dz^2} log\sigma(z) = -\wp(z) \ \forall \ z \in \mathbb{C} \backslash \Lambda$.
3. *For every $\omega \in \Lambda$ there are constants $a, b \in \mathbb{C}$, depending on ω, such that $\sigma(z + \omega) = e^{az+b}\sigma(z) \ \forall \ z \in \mathbb{C}$*

Proof.

1. It is sufficient to consider the logarithm

$$log\sigma(z) = logz + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left\{ log\left(1 - \frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2 \right\}.$$

   The absolute and uniform convergence follows from Theorem 1.13. It is clear that there is a simple zero for all $\omega \in \Lambda$ and that they are the only ones.

2. From the previous point it follows that we may differentiate term by term to compute the derivative of $log\sigma(z)$. The second derivative is exactly the series defining $-\wp(z)$.

3. $\wp(z)$ is an elliptic function, so $\wp(z+\omega) = \wp(z)$. Integrating twice this equation with respect to z and using the previous point we obtain

$$log\sigma(z+\omega) = log\sigma(z) + az + b,$$

where $a,\ b\ \in\ \mathsf{C}$ are the constants of integration.

□

The next proposition concludes the proof of the exactness of the sequence of Theorem 1.11.

Proposition 1.18. *Let $n_1, ..., n_r$ be integers and $z_1, ..., z_r$ be complex numbers such that $\sum n_i = 0$ and $\sum n_i \cdot z_i \in \Lambda$. Then there exists an elliptic function $f(z) \in \mathsf{C}(\Lambda)$ satisfying $div(f) = \sum n_i(z_i)$.*

Proof. Let $n_{r+1} = 1,\ n_{r+2} = -1$ and $z_{r+1} = 0,\ z_{r+2} = \sum n_i \cdot z_i\ \in \Lambda$. Then $\sum_{i=1}^{n} n_i(z_i) = \sum_{i=1}^{n+2} n_i(z_i)$ in $Div_0(\mathsf{C}/\Lambda)$, because $(0) = (\lambda)$ in C/Λ. Hence we may assume that $\sum n_i \cdot z_i = 0$. Then Lemma 1.17 implies that $f(z) = \prod \sigma(z - z_i)^{n_i}$ is such that $ord_{z_i} f = n_i$.
To conclude let us check that f is elliptic: for every $\omega \in \Lambda$ we have

$$\frac{f(z+\omega)}{f(z)} = \prod e^{(a(z\ \ z_i)+b)n_i} = e^{(az+b)\sum n_i} \cdot e^{\ a\sum n_i z_i} = 1$$

where we have used Lemma 1.17. □

The following corollary is a special case of what is known as the Abel-Jacobi theorem.

Corollary 1.19. *Let $D = \sum n_i[z_i]$ be a divisor. Then D is the divisor of a function if and only if $deg(D) = 0$ and $\sum n_i \cdot z_i \in \Lambda$.*

Proof. It is an immediate consequence of Theorem 1.6 and Proposition 1.18. □

In the next theorem we will derive the Laurent series expansion for $\wp$ around 0, and from it we will deduce an algebraic relation between $\wp$ and $\wp^{\emptyset}$. This relation will have a central role in the construction of an elliptic curve associated with a given lattice.

Theorem 1.20.

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

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

2.

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6 \qquad \forall z \in \mathbb{C}\backslash\Lambda. \tag{1.4}$$

Proof.

1. Let us study a term of the series for $\wp$: for all z with $|z| < |\omega|$ we have

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

Substituting this formula into the series for $\wp$ and taking into account that by Theorem 1.13 we are allowed to change the order of summation

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}} =$$

$$= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\frac{1}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n G_{n+2}(\Lambda) =$$

$$= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n},$$

where the last identity is true because if k is odd then $G_k(\Lambda) = 0$, since the terms $\frac{1}{\omega^k}$ and $\frac{1}{(-\omega)^k}$ in the sum cancel each other.

2. We write out the first few terms of various Laurent expansions:

$$\wp(z) = z^{-2} + 3G_4z^2 + \ldots$$

$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + \ldots$$

$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \ldots$$

Let consider the function $f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$. It is holomorphic in 0 because if we replace the Laurent expansions in it, the terms of the form z^{-n} for $n \in \mathbb{N}\backslash\{0\}$ simplify each other. It is also an elliptic function because $f(z) \in \mathbb{C}(\wp(z), \wp'(z))$, so Theorem 1.4 gives that f is constant. The result follows by observing that $f(0) = 0$.

□

Notation 1.21. *It is standard notation to set*

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \quad \textit{and} \quad g_3 = g_3(\Lambda) = 140G_6(\Lambda).$$

These functions will be considered in the next section when we will de ne modular forms and modular functions.

We will prove that every lattice Λ in C gives rise to an elliptic curve E/C, but before that we need the following lemma:

Lemma 1.22. *The polynomial $f(x) = 4x^3 - g_2x - g_3$ has distinct roots.*

Proof. Let $\{\omega_1, \omega_2\}$ be a basis of Λ and $\omega_3 = \omega_1 + \omega_2$. Therefore, since $\wp'(z)$ is odd and $\frac{\omega_i}{2} \equiv -\frac{\omega_i}{2} \pmod{\Lambda}$:

$$\wp'(\frac{\omega_i}{2}) = -\wp'(-\frac{\omega_i}{2}) = -\wp'(\frac{\omega_i}{2}) \implies \wp'(\frac{\omega_i}{2}) = 0.$$

Hence, $\wp(\frac{\omega_i}{2})$ for $i = 1, 2, 3$ are three roots of $f(z)$. We now prove that they are distinct.
For $i = 1, 2, 3$ consider the even function $h_i(z) = \wp(z) - \wp(\frac{\omega_i}{2})$, whose order at $\frac{\omega_i}{2}$ is at least[2] 2. However $h_i(z)$ is an elliptic function of order 2, so it has only these zeros in an appropriate fundamental parallelogram. Hence the numbers $\wp(\frac{\omega_i}{2})$ are not distinct if and only if $\frac{\omega_i}{2}$ differ by some $\omega \in \Lambda$, but this is not possible because ω_1, ω_2 are a basis of Λ. □

Theorem 1.23. *Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ for a lattice $\Lambda \subset \mathsf{C}$ and E/C be the elliptic curve*

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

Then the map

$$\Phi : \mathsf{C}/\Lambda \to E(\mathsf{C}) \subset \mathsf{P}^2(\mathsf{C}), \qquad z \to \begin{cases} [0, 1, 0], & z = 0, \\ [\wp(z), \wp'(z), 1], & z \neq 0 \end{cases}$$

is a complex analytic isomorphism of complex Lie groups.

Proof. From Theorem 1.20 the map is well-defined. To see that Φ is surjective, let $(x, y) \in E(\mathsf{C})$. Then $\wp(z) - x$ is a non-constant elliptic function, so it has a zero, $z = a$. Hence, by Theorem 1.20 $(\wp(a))^2 = y^2$, and so from the oddness of $\wp'$ it follows that $\wp'(a) = y$ or $\wp'(-a) = y$.
Now suppose that $\Phi(z_1) = \Phi(z_2)$. If $2z_1 \notin \Lambda$, then the elliptic function of

[2] Consider an even elliptic function, f, and ω such that $2\omega \not\in \Lambda$. Then $ord_\omega f$ is even as proven in Theorem 1.15.

order 2 $\wp(z) - \wp(z_1)$ vanishes in $z_1, -z_1, z_2$. So, two of them are congruent modulo Λ, but the hypothesis $2z_1 \notin \Lambda$ tells us that $z_2 \equiv \pm z_1 \pmod{\Lambda}$. Then

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$$

implies that $z_2 \equiv z_1 \pmod{\Lambda}$[3]. Similarly, if $2z_1 \in \Lambda$, then the elliptic function of order 2 $\wp(z) - \wp(z_1)$ has a double zero in z_1 and another zero in z_2. So $z_2 \equiv z_1 \pmod{\Lambda}$. This proves that Φ is injective.
Now we show that Φ is an analytic isomorphism. We know that: let M, N be complex $1-$manifolds and let $f : M \to N$ be a holomorphic map. If M is compact, then f is an analytic isomorphism if and only if it is injective [4]. It is easy to see that Φ is a holomorphism, so the claim follows.
Finally, we check that Φ is a homomorphism.
FIRST METHOD:
In order to do that we prove the following addition formula:

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2).$$

Let $h(z_1)$ be the difference between the left and right hand sides. The only possible poles for h are at 0 and $\pm z_2$. Using the Laurent series, we can easily find that only $-z_2$ is a possible pole, and at worst simple. But since $\wp(z_1+z_2)$ is an elliptic function this means, by Theorem 1.4, that it must be constant, and thus identically zero since $h(0) = 0$.
Now we show that what we have proved agrees with the elliptic curve group law: let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the elliptic curve $Y^2 = 4X^3 - g_2X - g_3$ and let $Y = mX + b$ be the line passing through them. Then, by the definition of the group law, x_1, x_2 and $x(P_1 + P_2)$ are the roots of the cubic equation

$$(mX + b)^2 - 4X^3 + g_2X + g_3 = 0.$$

So we get $x(P_1 + P_2) + x_1 + x_2 = \frac{m^2}{4} = \frac{1}{4}\left(\frac{y_1 \;\; y_2}{x_1 \;\; x_2}\right)^2$.
We now need to compute $\wp'(z_1 + z_2)$. Differentiating with respect to z_1 the formula for $\wp(z_1 + z_2)$ we obtain that $\wp'(z_1 + z_2)$ is equal to

$$\frac{1}{2}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\left[\frac{\wp''(z_1)(\wp(z_1) - \wp(z_2)) - (\wp'(z_1) - \wp'(z_2))\wp'(z_1)}{(\wp(z_1) - \wp(z_2))^2}\right] - \wp'(z_1).$$

In order to express $\wp''$ in term of $\wp$ and $\wp'$, we differentiate (1.4) and we obtain

$$2\wp''(z_1)\wp'(z_1) = (12\wp(z_1)^2 - g_2)\wp'(z_1).$$

[3] From Lemma 1.22 it follows that if $\wp'(z_1) = 0$ then $2z_1 \in \Lambda$.

[4] In order to prove this claim one could use that f is locally injective iff $f' \neq 0$, that a injective holomorphism is bijective, and the Inverse function theorem.

Dividing by $\wp'(z_1)$ yields[5] $2\wp''(z_1) = (12\wp(z_1)^2 - g_2)$. Substituting this into the expression for $\wp'(z_1+z_2)$ and using the two conditions $\wp'(z_i)^2 = 4\wp(z_i)^3 - g_2\wp(z_i) - g_3$ for $i = 1, 2$ we obtain

$$\begin{pmatrix} \wp'(z_1) & \wp'(z_2) \\ \wp(z_1) & \wp(z_2) \end{pmatrix} \left[\frac{(\wp'(z_1) \quad \wp'(z_2))^2 + 8\wp(z_1)^2(\wp(z_1) \quad \wp(z_2)) + \wp(z_2)^3 \quad 4\wp(z_1)^2\wp(z_2)}{4(\wp(z_1) \quad \wp(z_2))^2} \right] \quad \wp'(z_1).$$

In order to find an expression for $y(P_1 + P_2)$ in terms of y_1, y_2, x_1, x_2 we substitute the formula for $x(P_1 + P_2)$ in $y = mx + b$. Using that $m = \frac{\wp'(z_1) \quad \wp'(z_2)}{\wp(z_1) \quad \wp(z_2)}$ and $b = y_1 - mx_1$ we obtain

$$y(P_1 + P_2) = m\left[-\frac{m^2}{4} + 2x_1 + x_2\right] - y_1.$$

Some algebraic manipulations show that $\wp'(z_1+z_2)$ has the same addition law as $y(P_1+P_2)$. This is exactly our statement. Similarly we can prove the cases where the formula for $\wp(z_1 + z_2)$ is not defined.
SECOND METHOD:
Let $z_1, z_2 \in \mathbf{C}$. From Proposition 1.18 it follows that there exists an elliptic function for Λ, f, such that

$$div(f) = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Using Theorem 1.15 we can find $F(X, Y) \in \mathbf{C}(X, Y)$ such that $f(z) = F(\wp(z), \wp'(z))$. Treating $F(X, Y)$ as element of $\mathbf{C}(X, Y) \simeq \mathbf{C}(E)$, we have

$$div(F) = (\Phi(z_1 + z_2)) - (\Phi(z_1)) - (\Phi(z_2)) + (\Phi(0)).$$

From Proposition 0.7 it follows that $\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2)$.

□

1.4 Mappings between elliptic curves

The results of this Chapter can be found in [4, Chapter VI]. In this section we will study complex analytic maps between complex tori, proving in particular that the maps they induce on the corresponding elliptic curves are isogenies. Let Λ_1 and Λ_2 be two lattices in $\mathbf{C}$, and $\alpha \in \mathbf{C}$ be such that $\alpha\Lambda_1 \subset \Lambda_2$. Then we can define the homomorphism

$$\Phi_\alpha : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2, \qquad \Phi_\alpha(z) = \alpha z \ (\text{mod } \Lambda_2).$$

The next theorem proves that Φ_α for $\alpha \in \mathbf{C}$ are the only holomorphic maps between $\mathbf{C}/\Lambda_1, \mathbf{C}/\Lambda_2$.

[5] For $\wp'(z_1) \neq 0$ there are no problems; on the other hand the cases where $\wp'(z_1) = 0$ are filled in by continuity

Theorem 1.24.

1. *Let Λ_1, Λ_2 be lattices. Then:*

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\} \to \{\Phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ holomorphic with } \Phi(0) = 0\}$$

   is a bijection.

2. *Let E_1, E_2 be the elliptic curves corresponding to Λ_1, Λ_2. Then:*

$$\{\text{isogenies } \Phi : E_1 \to E_2\} \to \{\Phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ holomorphic with } \Phi(0) = 0\}$$

   is a bijection.

Proof.

1. In order to prove injectivity, let α, β be such that $\Phi_\alpha = \Phi_\beta$. The previous condition is equivalent to $\alpha z \equiv \beta z \pmod{\Lambda_2}$ $\forall z \in \mathbb{C}$. Hence the map $z \to (\alpha - \beta)z$ sends $\mathbb{C}$ in Λ_2. However Λ_2 is a lattice so it's discrete. This implies that the map must be constant, more precisely that the map must be zero, i.e. $\alpha = \beta$. Next, let $\Phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ be a holomorphic map with $\Phi(0) = 0$. As $\mathbb{C}$ is simply connected, we can lift Φ to a map $f : \mathbb{C} \to \mathbb{C}$ such that $f(0) = 0$ and the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\quad f \quad} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\quad \Phi \quad} & \mathbb{C}/\Lambda_2 \end{array}$$

   We know $f(z+\omega) \equiv f(z) \pmod{\Lambda_2}$ by definition, so as in the proof of injectivity $f(z+\omega) - f(z)$ is constant. Differentiating:

$$f'(z+\omega) = f'(z) \ \forall z \in \mathbb{C} \quad \forall \omega \in \Lambda_1$$

   so $f'(z)$ is a holomorphic elliptic function for Λ. From Theorem 1.4 it follows that $f'(z)$ is constant, so $f(z) = az + b$ for some $a, b \in \mathbb{C}$. The hypothesis $f(0) = 0$ implies that $b = 0$, then $f(\Lambda_1) = a\Lambda \subset \Lambda_2$. From these properties of f we conclude that $\Phi = \Phi_a$.

2. First, note that since an isogeny is a morphism, it is given locally by rational functions defined on C, so the map induced between the corresponding complex tori is holomorphic. The map is clearly well-defined and injective.
   From the previous point it follows that it is sufficient to consider maps of the form Φ_α for some $\alpha \in \mathsf{C}$ that satisfies $\alpha\Lambda_1 \subset \Lambda_2$. This map induces on the Weierstrass equations the following map:

$$E_1 \ \rightarrow \quad E_2$$

$$\left[\wp(z,\Lambda_1), \wp^{\emptyset}(z,\Lambda_1), 1\right] \rightarrow \left[\wp(\alpha z,\Lambda_2), \wp^{\emptyset}(\alpha z,\Lambda_2), 1\right].$$

   In order to show surjectivity, we must prove that $\wp(\alpha z,\Lambda_2), \wp^{\emptyset}(\alpha z,\Lambda_2)$ can be expressed as rational functions in $\wp(z,\Lambda_1), \wp^{\emptyset}(z,\Lambda_1)$. Let us notice that $\forall\omega \in \Lambda_1 \quad \wp(\alpha(z+\omega),\Lambda_2) = \wp(\alpha z + \alpha\omega,\Lambda_2) = \wp(\alpha z,\Lambda_2)$, where the last equality follows from the hypothesis $\alpha\Lambda_1 \subset \Lambda_2$; similarly for $\wp^{\emptyset}(\alpha z,\Lambda_2)$. Thus, both $\wp(\alpha z,\Lambda_2)$ and $\wp^{\emptyset}(\alpha z,\Lambda_2)$ are in $\mathsf{C}(\Lambda_1) = \mathsf{C}(\wp(z,\Lambda_1), \wp^{\emptyset}(z,\Lambda_1))$.

□

An immediate, but really relevant, corollary is:

Corollary 1.25. *Let E_1/C and E_2/C be elliptic curves corresponding to lattices Λ_1 and Λ_2. Then E_1 and E_2 are isomorphic if and only if the corresponding lattices are homothetic.*

This is the first step to prove the Uniformization Theorem.

1.5 Uniformization Theorem

This section is inspired by the lessons of the course "Forme Modulari" taught by professor A. Maffei at the University of Pisa, 2020/2021. These results can be also found in [2]. In this section we introduce some basic definitions and theorems on the theory of modular forms. We consider only the case of modular forms on $\mathbf{SL}_2(\mathsf{Z})$. This theory will be useful to prove the Uniformization Theorem.
We now consider the modular group $\Gamma = \mathbf{SL}_2(\mathsf{Z})$. It is generated by the two matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

It acts on $\mathsf{H} := \{z \in \mathsf{C} : Im(z) > 0\}$ via linear fractional transformations

$$A\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d},$$

where each pair $\pm\gamma \in \Gamma$ of matrices gives the same transformation.

Definition 1.26. Let $\mathsf{H}^* = \mathsf{H} \cup \mathsf{Q} \cup \{\infty\}$. If $z \in \mathsf{H}^*$, we let $\mathbf{SL}_2(\mathsf{Z})(z)$ denote the orbit of z, and we let $\mathsf{H}^*/\mathbf{SL}_2(\mathsf{Z})$ denote the set of orbits of H^* under the action of $\mathbf{SL}_2(\mathsf{Z})$.

This definition is natural because $\mathbf{SL}_2(\mathsf{Z})(\infty) = \mathsf{Q} \cup \{\infty\}$. The quotient space $\mathsf{H}^*/\mathbf{SL}_2(\mathsf{Z})$ has many important properties that we recall without proof in the following proposition.

Proposition 1.27.

1. $\mathsf{H}^*/\mathbf{SL}_2(\mathsf{Z}) = (\mathsf{H}/\mathbf{SL}_2(\mathsf{Z})) \cup \{\infty\}$
2. *The quotient topology on* $\mathsf{H}^*/\mathbf{SL}_2(\mathsf{Z})$ *is* T_2 *and compact.*

We are interested in functions with properties similar to our j-invariant function. Since the points of $\mathsf{H}/\mathbf{SL}_2(\mathsf{Z})$ correspond to equivalence classes of lattices under homothety, it is natural to define a class of meromorphic functions on $\mathsf{H}/\mathbf{SL}_2(\mathsf{Z})$.

Definition 1.28. Let $k \in \mathsf{Z}$. A meromorphic function $f : \mathsf{H} \to \mathsf{C}$ is weakly modular of weight k if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau),$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\tau \in \mathsf{H}$. In particular, a function is weakly modular of weight 0 if and only if it is $\mathbf{SL}_2(\mathsf{Z})$-invariant.

Since T, S generate $\mathbf{SL}_2(\mathsf{Z})$ we have:

Proposition 1.29. *A meromorphic function* $f : \mathsf{H} \to \mathsf{C}$ *is weakly modular of weight* k *if and only if* $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ *for* $\gamma = S, T$.

Example 1.30. The function $G_{2k}(\Lambda)$ defined in Section 1.3 has a lattice as its argument. If we consider lattices $\Lambda = \mathsf{Z} + \tau\mathsf{Z}$ parametrized by $\tau \in \mathsf{H}$, we can view $G_k(\Lambda)$ as a function of τ :

$$G_{2k}(\tau) := G_{2k}(\mathsf{Z} + \tau\mathsf{Z}) = \sum_{\substack{m,n \in \mathsf{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + n\tau)^k}.$$

$G_{2k}(\tau)$ is a weakly modular function of weight $2k$ because it comes from a homogeneous function defined on lattices.

We define $g_2(\tau)$ and $g_3(\tau)$ using the definition of $G_{2k}(\tau)$.

Definition 1.31. If f is a modular function that is holomorphic everywhere (including infinity), we say that f is a *modular form*. If, in addition, it vanishes at infinity, we say that it is a *cusp form*.

Proposition 1.32. *For any integer $k > 1$, the function G_{2k} is a modular form of weight $2k$, and $G_{2k}(\infty) = 2\zeta(2k)$, where ζ is the Riemann zeta function.*

Proof. From Example 1.30 we know that G_{2k} is a weakly modular function of weight $2k$. In order to show that G_{2k} is holomorphic at infinity, we need to show that it has a limit as $Im(\tau) \to \infty$. We can apply Theorem 1.13 and compute the limit termwise. Every term of the form $(m + n\tau)^{-k}$ relative to $n \neq 0$ gives 0, while the terms with $m = 0$ give n^{-2k}. Therefore,

$$\lim_{Im(\tau) \to 1} G_{2k}(\tau) = \sum_{n \in \mathbb{Z} \setminus \{0\}} n^{-2k} = 2\sum_{n=1}^{1} n^{-2k} = 2\zeta(2k).$$

. □

Remark 1.33. From this proposition it follows that $g_2(\tau)$ and $g_3(\tau)$ are both modular functions of weight respectively 4 and 6. We then have $g_2(\infty) = 120\zeta(4) = \frac{4}{3}\pi^4$ and $g_6(\infty) = 280\zeta(6) = \frac{8}{27}\pi^6$. Hence, if we let

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

then $\triangle(\infty) = 0$, so it is a cusp form of weight 12.

Now we introduce the j-invariant of an element of the upper plane $\mathbb{H}$ as follows: for $\tau \in \mathbb{H}$ let Λ_τ be the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. Similarly to what we did for $G_{2k}(\tau)$ we define $j(\tau) = j(\Lambda_\tau) = j(E_{\Lambda_\tau})$ where E_{Λ_τ} is the elliptic curve corrisponding to the lattice Λ.

Proposition 1.34. *The j-invariant is a modular form of weight 0 that is holomorphic on the upper half plane.*

Proof. From the definition we have

$$j(\tau) = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}$$

where, from Remark 1.33, we have that g_2, g_3 are holomorphic modular forms. Since the discriminant of the polynomial defined in Lemma 1.22 is non zero, the function j is holomorphic as well. The lattice $\mathbb{Z} + S(\tau)\mathbb{Z} = \mathbb{Z} + (-1/\tau)\mathbb{Z} = (-1/\tau)[\mathbb{Z} + \tau\mathbb{Z}]$, is homothetic to Λ, similarly for $\mathbb{Z} + T(\tau)\mathbb{Z}$. Hence, from Theorems 1.24 and 0.3 it follows that $j(\tau) = j(S(\tau)) = j(T(\tau))$. Otherwise we could have used that $g_2(\tau)^3$ and $\triangle(\tau)$ are respectively a modular and a cusp form of weight 12. □

From this proposition it follows that the function j induces a well defined holomorphic map from $\mathsf{H}/\mathbf{SL}_2(\mathsf{Z})$ to $\mathsf{P}^1(\mathsf{C})$. We call this map φ. Before proving that φ is a complex analytic map, we state a useful lemma.

Lemma 1.35. *The holomorphic functions $g_2(\tau)^3$ and $g_3(\tau)^2$ are linearly independent.*

Theorem 1.36. *φ is a biolomorphism between $\mathsf{H}/\mathbf{SL}_2(\mathsf{Z})$ and $\mathsf{P}^1(\mathsf{C})$.*

Proof. Because of Proposition 1.34 φ is holomorphic. As we said in Theorem 1.23 we just need to prove that φ is bijective. From Lemma 1.35 it follows that j is not constant because otherwise $g_2(\tau)$ and $g_3(\tau)$ would be linearly dependent. φ is holomorphic, so it is an open map, and it is a closed map because it goes from a compact space to a T_2 space. As $\mathsf{P}^1(\mathsf{C})$ is connected, this implies that φ is surjective. In order to prove injectivity, we will show that $\deg(\varphi) = 1$. We recall that the degree in y is defined by $\sum_{x \in \varphi^{-1}(y)} ord_x\varphi$ and that it is locally constant, so in our case it is constant because the domain is connected. Let us compute the degree in ∞: $\varphi^{-1}(\infty) = \{\infty\}$ and from Remark 1.33 it follows that $g_2(\tau)^3$ is non-zero at infinity whereas $\triangle(\tau)$ has a simple zero at infinity. So, $\deg(\varphi) = 1$. □

Theorem 1.37 (Uniformization Theorem)**.** *For every elliptic curve E/C there exists a lattice Λ, unique up to homothety, such that $E \simeq E_\Lambda$.*

Proof. The uniqueness follows from Corollary 1.25. Let $\tau \in \mathsf{H}$, so that $j(\tau) = j(E)$, and $\Lambda = \mathsf{Z} \oplus \tau\mathsf{Z}$. We have

$$j(E) = j(\tau) = j(\Lambda) = j(E_\Lambda),$$

so, it follows from Theorem 0.3 that E is isomorphic to E_Λ. □

In the first section we have introduced the set $\Lambda = \{n\omega_1 + m\omega_2 : n, m \in \mathsf{Z}\}$, where $\omega_1 = \int_\alpha \frac{dx}{y}$ and $\omega_2 = \int_\beta \frac{dx}{y}$ for α, β a basis for the $\pi_1(E(\mathsf{C}))$. The next theorem proves that they are R-linearly independent, i.e Λ is a lattice in C, and the function F described in the first section is the inverse map of Φ.

Theorem 1.38. *Let E/C be an elliptic curve with Weierstrass equation in x and y.*

1. *In the notation above ω_1 and ω_2 are R-linearly independent;*
2. *Let $\Lambda = \langle \omega_1, \omega_2 \rangle$. Then the function*

$$F : E(\mathsf{C}) \to \mathsf{C}/\Lambda, \qquad F(P) = \int_O^P \frac{dx}{y} \ (mod\ \Lambda)$$

is the inverse of the map Φ described in Theorem 1.23.

Proof.

1. From the uniformization theorem it follows that $\exists\Lambda$ such that $\Phi : \mathbb{C}/\Lambda \to E$ is an isomorphism. Then, the maps $\Phi^{-1} \circ \alpha$ and $\Phi^{-1} \circ \beta$ are a basis for $\pi_1(\mathbb{C}/\Lambda) \simeq \mathbb{Z}^2$.
   The map $\gamma \to \int_\gamma dz$ defines an isomorphism between $\pi_1(\mathbb{C}/\Lambda)$ and Λ. Then, using $\Phi^{-1}\left(\frac{dx}{y}\right) = dz$

$$\omega_1 = \int_\alpha \frac{dx}{y} = \int_{\Phi^{-1}\circ\alpha} dz, \qquad \omega_2 = \int_\beta \frac{dx}{y} = \int_{\Phi^{-1}\circ\beta} dz$$

   generate Λ, so in particular they are $\mathbb{R}$-linearly independent.

2. From the first point it follows that $\Lambda = \langle\omega_1, \omega_2\rangle$ is a lattice.

$$F \circ \Phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \qquad F \circ \Phi(z) = \int_O^{(\wp(z),\wp'(z))} \frac{dx}{y}.$$

   In order to prove that $F \circ \Phi = Id$, let us first study its effect on the cotangent spaces. Using $F^*(dz) = d(\int_O^z \frac{dx}{y}) = \frac{dx}{y}$ and $\Phi^*\left(\frac{dx}{y}\right) = dz$, we see that

$$(F \circ \Phi)^*(dz) = dz \tag{1.5}$$

   We note that $F \circ \Phi$ is a holomorphic map such that $F \circ \Phi(O) = O$, so from Theorem 1.24 it follows that $\exists a \in \mathbb{C}$ such that $F \circ \Phi = \Phi_a$. Since $\Phi_a(dz) = a \cdot dz$ and from (1.5) we see that $a = 1$.

□

1.6 Characterization of *End(E)*

The results of this Chapter can be found in [1, Chapter VI]. Let $E/\mathbb{C}$ be an elliptic curve. If it is associated by F to a lattice Λ, and from Theorem 1.24 it follows that we can identify $End(E)$ with a subring of $\mathbb{C}$. Since the lattice is unique up to homothety, this ring is independent of the choice of the lattice. In the next theorem we will use this description of $End(E)$ to characterize the kind of endomorphism rings that may occur. First let us recall the definition of order

Definition 1.39. Let K be a number field. An order R of K is a subring with unity of K that is finitely generated as a $\mathbb{Z}$-module and satisfies $R \otimes \mathbb{Q} = K$.

Theorem 1.40. *Let be $\Lambda = \langle\omega_1, \omega_2\rangle$, which by Theorem 1.38 is a lattice, and $E = \mathbb{C}/\Lambda$. The following are the only two possibilities:*

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

Proof. Let $\tau = \omega_2/\omega_1$. Multiplying Λ by $1/\omega_1$ we see that Λ is homothetic to $\mathbb{Z} \oplus \tau\mathbb{Z}$. Next we consider

$$\mathcal{O} = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \simeq End(E).$$

Then, for any $\alpha \in \mathcal{O}$, there exist integers a, b, c, d such that $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$.
Thus:

$$\frac{\alpha - a}{b} = \frac{c}{\alpha - d} \Leftrightarrow \alpha^2 - (a+d)\alpha + ad - cb = 0 \tag{1.6}$$

so $\mathcal{O}$ is integral over $\mathbb{Z}$. If $\mathcal{O} \neq \mathbb{Z}$, let us consider $\alpha = a + b\tau \in \mathcal{O}\backslash\mathbb{Z}$ (i.e. $b \neq 0$). By using (1.6) it follows that τ satisfies the following nontrivial quadratic equation

$$b\tau^2 + (a-d)\tau - c = 0. \tag{1.7}$$

Since Λ is a lattice $\tau \notin \mathbb{R}$, then it follows from (1.7) that $\mathbb{Q}(\tau)$ is an imaginary extension of $\mathbb{Q}$. Finally, since $\mathcal{O} \subset \mathbb{Q}(\tau)$ is integral over $\mathbb{Z}$, we have that $\mathcal{O}$ is an order in $\mathbb{Q}(\tau)$. □

Remark 1.41. Theorem 1.40 applies to elliptic curves over $\mathbb{Q}$, number fields, or any field that can be embedded in $\mathbb{C}$.

We know from the introduction that every elliptic curve has at least the multiplication-by-m endomorphisms. From this observation and from the previous theorem it follows that most elliptic curves over $\mathbb{C}$ have only the multiplication-by-m endomorphisms. In the next chapter we will study the elliptic curves that possess extra endomorphisms.

CHAPTER 2

Complex Multiplication

In this chapter we turn our attention to elliptic curves with complex multiplication. These are elliptic curves that have a non-trivial endomorphism ring. The correspondence between elliptic curves and complex tori seen in the first chapter will allow us to consider these endomorphism rings as endomorphism rings of complex tori, which will make matters less complicated. We will show that for any elliptic curve with complex multiplication the j-invariant is algebraic over $\mathbb{Q}$, and in the next chapter we will improve this result proving that j is integral over $\mathbb{Z}$. We will establish a bijection between elliptic curves that have a particular endomorphism ring and the class group of this endomorphism ring. This bijection will be useful when in the last chapter we will talk about the Hilbert Class Field.

2.1 Definition and basic properties

The definitions and properties of this chapter can be found in [3, Chapter II]

Definition 2.1. An elliptic curve $E/\mathbb{C}$ has *complex multiplication* (CM) if $End(E) \supsetneq \mathbb{Z}$.

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

Example 2.2. Let $\Lambda = \mathbb{Z}[i]$ be the Gaussian lattice generated over $\mathbb{Z}$ by 1 and i. Then multiplication by $2i$ takes Λ into Λ, and hence induces an endomorphism of $\mathbb{C}/\Lambda$ denoted by $[2i]$. Such an isomorphism is called a complex multiplication. Another example is the Eisenstein lattice $H = \mathbb{Z}[\zeta_3]$ where $\zeta_3 = e^{2\pi i/3}$. Multiplication by ζ_3 induces an automorphism $\mathbb{C}/H$ (one has $\zeta_3^2 = -\zeta_3 - 1$).

Let E/C be an elliptic curve with complex multiplication. From Theorem 1.40 it follows that $End(E) \otimes \mathsf{Q}$ is isomorphic to a quadratic imaginary field and that $End(E)$ is an order in that field. This leads the following definition

Definition 2.3. If $End(E) \simeq R$, then we will say that that "E has complex multiplication by R".

Remark 2.4. From Theorem 1.24 we know that the endomorphism ring of E_Λ is isomorphic to $\{\alpha \in \mathsf{C} \mid \alpha\Lambda \subset \Lambda\} \neq \mathsf{Z}$. If E_Λ has CM by R, then $R = \{\alpha \in \mathsf{C} \mid \alpha\Lambda \subset \Lambda\}$. So we can define an isomorphism $[\cdot] : R \to End(E_\Lambda)$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathsf{C}/\Lambda & \xrightarrow{\Phi_\alpha} & \mathsf{C}/\Lambda \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda \end{array}$$

The following proposition proves an important property of this isomorphism:

Proposition 2.5. *Let E/C be an elliptic curve with complex multiplication by R. Then for all $\omega \in \Omega_E$ we have:*

$$[\alpha]_\omega = \alpha\omega \quad \forall \alpha \in R$$

Proof. Let Λ be a lattice such that there exists an isomorphism $f : E_\Lambda \to E$. If we take $\omega \in \Omega_E$ and we pull back it via the isomorphism f we obtain:

$$f\ \omega = cdz,$$

because $f\ \omega$ and dz are two invariant differentials for the same elliptic curve[1]. Using the definition of $[\alpha]$ we obtain:

$$[\alpha]\ \omega = (f\ ^{1})\ \circ \Phi_\alpha \circ (f)\ (\omega) = (f\ ^{1})\ \circ \Phi_\alpha(cdz) = (f\ ^{1})\ (c\alpha dz) = \alpha\omega.$$

□

Corollary 2.6. *Let $(E_1, [\cdot]_1)$ and $(E_2, [\cdot]_2)$ be elliptic curves with complex multiplication by R, and let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi \text{ for all } \alpha \in R.$$

Proof. Let $\omega \in \Omega_{E_2}$ be a nonzero invariant differential. Then we have:

$$(\phi \circ [\alpha]_{E_1})\ \omega = [\alpha]_{E_1} \circ (\phi\ \omega) = \alpha\phi\ \omega = \phi\ \alpha\omega = \phi\ \circ ([\alpha]_{E_2}\omega) = (\phi \circ [\alpha]_{E_2})\ \omega.$$

Hence $(\phi \circ [\alpha]_{E_1})\ = (\phi \circ [\alpha]_{E_2})\ \in Hom(\Omega_{E_2}, \Omega_{E_1})$, and from Proposition 0.11 we have the injectivity of -operator, so we obtain the claim. □

[1] 8ω_1, ω_2 2 Ω_{E_Λ} there exists a constant β such that $\omega_1 = \beta\omega_2$. This follows from the fact that ω_1/ω_2 is a translation-invariant function, so it is constant.

2.2 Elliptic curves with a given endomorphism ring

The results of this section can be found in [3, Chapter 2], except for the first part that can be found in [1, Chapter Two]. In order to study elliptic curves with complex multiplication, it turns out to be useful to look at the set of all isomorphism classes of elliptic curves with the same endomorphism ring. This leads us to define [2]:

$$\mathcal{ELL}(R) = \frac{\{\text{elliptic curves E/C with } End(E) \simeq R\}}{\text{isomorphism over C}} = \frac{\{\text{lattices } \Lambda \text{ with } End(E_\Lambda) \simeq R\}}{\text{homothety}}$$

Let We will construct an elliptic curve with complex multiplication by $\mathcal{O}_k$, for a given quadratic imaginary field k. By the Uniformization Theorem, this is equivalent to finding a lattice Λ such that $\mathcal{O}_k = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$.
In this first part we consider the general case of an order R of a quadratic imaginary field. We note that R is a lattice. So, an obvious candidate is $\Lambda = R$. If $\alpha \in End(E_R) = \{\alpha \in \mathbb{C} : \alpha R \subset R\}$, then $\alpha R \subset R$ and therefore $\alpha \in R$. Conversely, if $\alpha \in R$, then $\alpha R \subset R$ and therefore $\alpha \in End(E_R)$. Thus $End(E_R) = R$. The same holds for any lattice homothetic to R.
Are there any lattices Λ not homothetic to R for which we have $End(E_\Lambda) = R$? In order to answer this question we may assume without loss of generality that $\Lambda = \mathbb{Z} \oplus \lambda\mathbb{Z}$ and we can write $R = \mathbb{Z} \oplus \tau\mathbb{Z}$. If $End(E_\Lambda) = R$, then we must have $\tau \cdot 1 = \tau \in \Lambda$, so $\tau = n + m\lambda$ for some integers n, m. Hence

$$m\Lambda = m\mathbb{Z} \oplus m\lambda\mathbb{Z} = m\mathbb{Z} \oplus (\tau - n)\mathbb{Z} \subset R$$

which means that Λ is homothetic to a sublattice of R. Since $\alpha m\Lambda \subset m\Lambda$ for all $\alpha \in R$ we have that the sublattice of R homothetic with $m\Lambda$ must be closed under multiplication by R, so it is an ideal of R. Hence, every lattice Λ such that $End(E_\Lambda) = R$ is homothetic with a fractional ideal of R, but the converse does not hold. This leads us to the following definition

Definition 2.7. Let R be an order in an imaginary quadratic field, and let I be a fractional ideal of R. We say that I is *proper* if $End(E_I) = R$.
Two fractional ideals of R, I and J, are said to be *equivalent* if they are homothetic as lattices; equivalently, $(\alpha)I = (\beta)J$ for some non-zero $\alpha, \beta \in R$.

The second characterisation of equivalent fractional ideals holds because: if $I = \lambda J$, we can always write $\lambda = a/b$ for some $b \in R$. We can then take $\alpha = \lambda b \in R$ and $\beta = b$.

[2] The set $\{\alpha \in \mathbb{C} : \alpha\Lambda \quad \Lambda\}$ does not change if we replace Λ with $\Lambda' = \lambda\Lambda$ for any $\lambda \in \mathbb{C}$, so we are really only interested in lattices up to homethety, or equivalently elliptic curves up to isomorphism over $\mathbb{C}$.

If $\mathcal{O}_k$ is the ring of integers of a quadratic imaginary field, then: I is proper if and only if I is fractional. In the general case of an order of a quadratic imaginary field, proper ideals are only contained in fractional ideals. It can be proved that for the general case I is proper if and only if I is invertible, but we are not interested in proving it.

Next, we recall the definition of ideal class group

Definition 2.8. The ideal class group $CL(\mathcal{O}_k)$ of a number field k is the quotient group between the group of nonzero fractional ideals of the ring of integers of k, and its subgroup of principal ideals.

So, from our discussion follows the following theorem:

Theorem 2.9. *Let $\mathcal{O}_k$ be the ring of integers of an imaginary quadratic field. There is a one-to-one correspondence between elements of the ideal class group $CL(\mathcal{O}_k)$ and homothety classes of lattices $\Lambda \subset \mathbb{C}$ for which $End(E_\Lambda) \simeq \mathcal{O}_k$.*

Let us consider I a non-zero fractional ideal of $\mathcal{O}_k$. We denote by $\overline{I}$ its ideal class in $CL(\mathcal{O}_k)$. So we have seen that there is a map

$$CL(\mathcal{O}_k) \to \mathcal{ELL}(\mathcal{O}_k), \quad \overline{I} \mapsto E_I.$$

In the first part of this chapter, we have seen that in any class of $\mathcal{ELL}(\mathcal{O}_k)$ there is a proper $\mathcal{O}_k$-ideal I, i.e. for any E elliptic curve with $End(E) = \mathcal{O}_k$, there is a proper ideal I such that E_I is isomorphic to E. This induces a simply transitive action of the ideal class group $CL(\mathcal{O}_k)$ on the set of elliptic curves $\mathcal{ELL}(\mathcal{O}_k)$:

$$\overline{I} * E_J = E_{I^{-1}J}$$

(the reason for using $E_{I^{-1}J}$ rather than E_{IJ} will become clear later).

Theorem 2.10. *The action of $CL(\mathcal{O}_k)$ on $\mathcal{ELL}(\mathcal{O}_k)$ described above is simply transitive.*

Proof. Given two proper $\mathcal{O}_k$-ideals I and J, we have

$$j(I * E_J) = j(E_{I^{-1}J}) = j(E_J) \text{ if and only if } J \text{ is homothetic to } I^{-1}J,$$

by Theorems 1.37 and 0.3. In this case we have $IJ = \lambda J$ for some nonzero $\lambda \in \mathcal{O}_k$, and since J is an invertible ideal we have that $I = \lambda\mathcal{O}_k = (\lambda)$ is principal. Thus the only element of $CL(\mathcal{O}_k)$ that fixes any element of $\mathcal{ELL}(\mathcal{O}_k)$ is the identity.
The fact that the sets $CL(\mathcal{O}_k)$ and $\mathcal{ELL}(\mathcal{O}_k)$ have the same cardinality implies that the action must be transitive: if we fix any $E \in \mathcal{ELL}(\mathcal{O}_k)$ the images $\overline{I} * E$ of E under the action of each $\overline{I} \in CL(\mathcal{O}_k)$ must all be distinct. □

In general in the study of elliptic curves it is useful to define the group of $[m]$-torsion points of E. But in the case of elliptic curves with complex multiplication, there are other natural finite subgroups of E to look at.

Definition 2.11. If I is any integral ideal of $\mathcal{O}_k$ and E an elliptic curve with complex multiplication by $\mathcal{O}_k$, we define the *group of I-torsion points of E*:

$$E[I] = \{P \in E \mid [\alpha]P = 0 \ \forall \alpha \in I\}.$$

As in the case of $[m]$-torsion, to every fractional ideal I we can associate an isogeny with kernel $E[I]$:

Definition 2.12. For all integral ideals I we have[3] $\Lambda \subset I\ {}^1\Lambda$, so we may define the following homomorphism

$$\mathbb{C}/\Lambda \to \mathbb{C}/I\ {}^1\Lambda, \quad z \mapsto z.$$

This induces an isogeny

$$E_\Lambda \to \overline{I} * E_\Lambda.$$

The following proposition gives two descriptions of $E[I]$ in terms of the isogeny described above.

Proposition 2.13. *Let $E \in \mathcal{ELL}(\mathcal{O}_k)$, and let I be an integral ideal of $\mathcal{O}_k$.*

1. *$E[I]$ is the kernel of the natural map $E \to \overline{I} * E$,*
2. *$E[I]$ is a free $\mathcal{O}_k/I$-module of rank 1.*

Proof. Let Λ be a lattice such that $E_\Lambda \simeq E$. We may assume Λ to be a fractional ideal.

1. We have:
$$\begin{aligned} E[I] &= \{z \in \mathbb{C}/\Lambda \mid \alpha z = 0 \ \forall \alpha \in I\} = \{z \in \mathbb{C} \mid \alpha z \in \Lambda \ \forall \alpha \in I\}/\Lambda \\ &= \{z \in \mathbb{C} \mid zI \subseteq \Lambda\}/\Lambda = I\ {}^1\Lambda/\Lambda = ker\left(\mathbb{C}/\Lambda \to \mathbb{C}/I\ {}^1\Lambda\right) \\ &= ker\left(E \to \overline{I} * E\right). \end{aligned}$$

2. From the previous point we know that $E[I] = I\ {}^1\Lambda/\Lambda$ as $\mathcal{O}_k/I$-modules. If $J|I$ then
$$(I\ {}^1\Lambda/\Lambda) \otimes_{\mathcal{O}_k} (\mathcal{O}_k/J) \simeq I\ {}^1\Lambda/(\Lambda + JI\ {}^1\Lambda) = I\ {}^1\Lambda/JI\ {}^1\Lambda.$$
From this and the Chinese remainder theorem it follows that we can write

[3] If Λ is any lattice with E_Λ *2* $\mathcal{ELL}(\mathcal{O}_k)$ and I is any non-zero fractional ideal of k, we can form the product
$$I\Lambda = f\alpha_1\lambda_1 + \quad + \alpha_m\lambda_m : \ \alpha_i \ 2 \ I, \ \lambda_i \ 2 \ \Lambda g.$$

$$\mathcal{O}_k/I = \prod_{P2primes} \mathcal{O}_k/P^{e(P)} \Longrightarrow E[I] \simeq \prod_{P2primes} I \ {}^1\Lambda/P^{e(P)} I \ {}^1\Lambda$$

Hence in order to conclude we must prove that: for all J fractional ideal (such as $I \ {}^1\Lambda$) and for all P^e with P a prime ideal, J/P^eJ is a free $\mathcal{O}_k/P^e$-module of rank 1.
We define

$$R^{\emptyset} = \mathcal{O}_k/P^e \qquad P^{\emptyset} = P/P^e \qquad J^{\emptyset} = J/P^eJ$$

We note that $R^{\emptyset}$ is a local ring with $P^{\emptyset}$ as maximal ideal. From the isomorphism theorems, we have

$$J^{\emptyset}/P^{\emptyset}J^{\emptyset} \simeq J/PJ \text{ as vector spaces over } R^{\emptyset}/P^{\emptyset} \simeq \mathcal{O}_k/P$$

We want to show that its dimension is one. Any two elements $x, y \in J$ are $\mathcal{O}_k$-linearly dependent[4] , so the dimension is at most 1. If the dimension is zero, then $J = PJ$ which contradicts the uniqueness of factorization in Dedekind domains. So, from Nakayama's lemma applied to the local ring $R^{\emptyset}$ and the $R^{\emptyset}$-module $J^{\emptyset}$, we obtain that $J^{\emptyset}$ is a free $R^{\emptyset}$-module of rank 1.

□

Using this theorem we can compute the degree of the isogeny $E \to \overline{I} * E$ and the degree of the endomorphism $[\alpha] : E \to E$.

Corollary 2.14. *Let $E \in \mathcal{ELL}(\mathcal{O}_k)$. For all integral ideals $I \subset \mathcal{O}_k$:*

1. *the map $E \to \overline{I} * E$ has degree $N_{k/\mathbb{Q}}I$,*
2. *for all $0 \neq \alpha \in \mathcal{O}_k$, the endomorphism $[\alpha] : E \to E$ has degree $|N_{k/\mathbb{Q}}\alpha|$.*

Proof. Both parts are immediate from Proposition 2.13.

1. $deg(E \to \overline{I} * E) = |ker(E \to \overline{I} * E)| = |E[I]| = |\mathcal{O}_k/I| = N_{k/\mathbb{Q}}I$
2. $deg([\alpha]) = |ker([\alpha])| = |E[(\alpha)]| = |\mathcal{O}_k/(\alpha)| = N_{k/\mathbb{Q}}((\alpha)) = |N_{k/\mathbb{Q}}\alpha|$

□

[4]Since J is fractional, there exists α such that $J \quad \frac{1}{\alpha}\mathcal{O}_k$. So $8x, y \ 2 \ J \quad 9n, m \ 2 \ \mathcal{O}_k$ such that $x = \frac{n}{\alpha}, y = \frac{m}{\alpha} =) \ mx \quad ny = 0$.

2.3 Field of definition

The results of this section can be found in [3, Chapter 2]. 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 Q.
In order to study the rationality of j, it is useful to consider the action of $Aut(\mathsf{C})$ on the coefficients of a Weierstrass equation of an elliptic curve E.
Given an elliptic curve E/C, we can associate to it a Weierstrass equation with coefficients in C

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Let $\sigma \in Aut(\mathsf{C})$. Then we can consider the new elliptic curve

$$E^\sigma : y^2 = x^3 + a^\sigma x^2 + b^\sigma x + c^\sigma.$$

Proposition 2.15. *Let E/C be an elliptic curve and $\sigma \in Aut(\mathsf{C})$.*

1. $End(E^\sigma) \simeq End(E)$.
2. *If E is an elliptic curve with complex multiplication by $\mathcal{O}_k$, where k is a quadratic imaginary field, then the j-invariant of E is algebraic.*
3. $\mathcal{ELL}(R) = \dfrac{\{\text{elliptic curves } E/\overline{\mathsf{Q}} \text{ with } End(E) \simeq R\}}{\text{isomorphism over } \overline{\mathsf{Q}}}$.

Proof. 1. If $\phi : E \to E$ is an endomorphism of E, clearly $\phi^\sigma : E^\sigma \to E^\sigma$ is an endomorphism of E^σ. This gives a homomorphism between the two endomorphism rings. The inverse of this morphism maps $\psi \in End(E^\sigma)$ to $\psi^{\sigma^{-1}} \in End(E)$.

2. Let $\sigma \in Aut(\mathsf{C})$. We consider the action previously described: since $j(E)$ is a rational function of the coefficients of the Weierstrass equation, it is clear that $j(E^\sigma) = (j(E))^\sigma$. On the other hand, the first point implies that $End(E^\sigma) = End(E) = \mathcal{O}_k$. So, $E^\sigma \in \mathcal{ELL}(\mathcal{O}_k)$. Now we recall that $\#\mathcal{ELL}(\mathcal{O}_k) = \#CL(\mathcal{O}_k) < \infty$, then $j(E^\sigma)$ assumes only finitely many values:
$$[\mathsf{Q}(j(E)) : \mathsf{Q}] \leq \#\mathcal{ELL}(\mathcal{O}_k) < \infty.$$
Thus $j(E)$ is algebraic over Q.

3. For any subfield F of C, let us denote by $\mathcal{ELL}_F(\mathcal{O}_k)$ the set
$$\mathcal{ELL}_F(\mathcal{O}_k) \simeq \frac{\{\text{elliptic curves } E/F \text{ with } End(E) \simeq \mathcal{O}_k\}}{\text{isomorphism over } F}.$$

Fix an embedding $\overline{\mathsf{Q}} \subset \mathsf{C}$: it induces a natural map

$$\epsilon : \mathcal{ELL}_{\overline{\mathsf{Q}}}(\mathcal{O}_k) \to \mathcal{ELL}_{\mathsf{C}}(\mathcal{O}_k).$$

We want to prove that ϵ is a bijection:

- **surjectivity** Let $E/\mathsf{C} \in \mathcal{ELL}_{\mathsf{C}}(\mathcal{O}_k)$, then:
  - from the second point we have $j(E) \in \overline{\mathsf{Q}}$;
  - from Proposition 0.4 there exist an elliptic curve $E^0/\mathsf{Q}(j(E))$ with $j(E) = j(E^0)$;
  - from Theorem 0.3 we have that E^0 is isomorphic to E over C. These facts tell us that $\epsilon(E^0) = E$, so that ϵ is surjective.
- **injectivity** Let $E_1, E_2 \in \mathcal{ELL}_{\overline{\mathsf{Q}}}(\mathcal{O}_k)$ be such that $\epsilon(E_1) = \epsilon(E_2)$. From Theorem 0.3 we deduce that $j(E_1) = j(E_2)$, and another application of Theorem 0.3 says that E_1 and E_2 represent the same element of $\mathcal{ELL}_{\overline{\mathsf{Q}}}(\mathcal{O}_k)$.

□

Remark 2.16. Using Proposition 2.15 we can deduce that, if $End(E) \simeq \mathcal{O}_k$, then

$$[\mathsf{Q}(j(E)) : \mathsf{Q}] \leq \#CL(\mathcal{O}_k) = h_k$$

We will prove later that this is an equality.

We recall that isogenies are rational functions, so there is a natural action of $Aut(\mathsf{C})$ on them. Next we study the effect of this action on the maps $[\alpha] : E \to E$ described in Remark 2.4 and find a field of definition for them.

Proposition 2.17.

1. *Let E/C be an elliptic curve with complex multiplication by the ring $R \subset \mathsf{C}$, then*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} \qquad \forall \alpha \in R \text{ and } \forall \sigma \in Aut(\mathsf{C}).$$

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

3. *Let E_1/L and E_2/L be two elliptic curves defined over a field $L \subset \mathsf{C}$. Then there is a finite extension L_0/L such that every isogeny from E_1 to E_2 is defined over L_0.*

Proof.

1. Let $\omega \in \Omega_E$ be an invariant differential on E. Then

$$[\alpha]_E\omega = \alpha\omega \quad \forall\alpha \in R, \qquad [\beta]_{E^\sigma}\omega^\sigma = \beta\omega^\sigma \quad \forall\beta \in R.$$

Then for any $\alpha \in R$ and for any $\sigma \in Aut(\mathsf{C})$ we have

$$([\alpha]_E^\sigma)\ \omega^\sigma = ([\alpha]_E\omega)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma\omega^\sigma = [\alpha^\sigma]_{E^\sigma}(\omega^\sigma)$$

So, the claim follows from Proposition 0.11 that gives us the injectivity of the $*$-operator.

2. Let us consider a Weierstrass equation with coefficients in L for E. Then, for any $\sigma \in Aut(\mathsf{C})$ that fixes L we have $E^\sigma = E$, so it follows that

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} = [\alpha^\sigma]_E, \quad \forall\alpha \in \mathcal{O}_K.$$

If we suppose that σ fixes K too, we have

$$[\alpha]_E^\sigma = [\alpha]_E \quad \forall\alpha \in \mathcal{O}_K \ \ \forall\sigma \in Aut_{LK}(\mathsf{C}),$$

then $[\alpha]$ is defined over LK[5].

3. As in the previous point we can take Weierstrass equations with coefficients in L for E_1 and E_2. Let $\psi \in Hom(E_1, E_2)$ be an isogeny, then for all $\sigma \in Aut_L(\mathsf{C})$ we have that $\psi^\sigma \in Hom(E_1, E_2)$, and that $\deg\psi = \deg\psi^\sigma$. From Theorem 0.16 we know that an isogeny 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 since from Dirichlet's unit theorem we know that $\mathcal{O}_K$ is a finite group, then $Hom(E_1, E_2)$ contains only finitely many isogenies of a given degree. Therefore the orbit of ψ for the action of $Aut_L(\mathsf{C})$ is a finite set, which implies that ψ is defined over a finite extension of L. Finally, it follows from Theorem 0.18 that $Hom(E_1, E_2)$ is a finitely generated group, so it is sufficient to take a field of definition for a finite set of generators.

□

Theorem 2.18. *Let E/C be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$. Let $F = K(j(E))$. Then there exists a Weierstrass equation for E with coe cients in F. This equation de nes an elliptic curve*

[5]Using Lemma 0.17 we know that $[\alpha]$ can be expressed uniquely as a rational map with coefficients in L', an extension of L. Without loss of generality we can assume that L'/L is a Galois extension and that $K \quad L'$. We also know that the map is fixed by $Aut_{LK}(\mathsf{C})$. So if $L' \quad LK$ we already have the claim, otherwise we have that $[\alpha]$ is fixed by $Gal(L'/LK)$, so also the rational maps which were introduced above will be fixed by this group, hence they have coefficients in LK.

E_F, that is not unique up to isomorphism over F. However for each of these curves E_F we have that the field

$$L = F(E_{F,tors}),$$

is an abelian extension of F.

Proof. Let $L_m = F(E_F[m])$. We note that L is the compositum of all the L_m's, so it suffices to show that L_m/F is an abelian extension. In order to do this, we consider the following map

$$\tau : Gal(\overline{K}/F) \to Aut(E_F[m]), \quad \sigma \mapsto \tau(\sigma) : E_F[m] \to E_F[m]$$

where $\tau(\sigma)(P) = P^\sigma$. It is well defined: for all $P \in E_F[m]$ we have that $[m]P = 0$, so $[m](P^\sigma) = ([m]P)^\sigma = 0^\sigma = 0$, i.e. $P^\sigma \in E_F[m]$. So we obtain that for an arbitrary elliptic curve

$$Gal(L_m/F) < Aut(E_{E/F}[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

Using Proposition 2.17 we can assume that every endomorphism of E_F is defined over $\mathbb{Q}(j(E_F))K = F$. So every element $\sigma \in Gal(L_m/F)$ will commute with every endomorphism of E_F in their action on $E_F[m]$, equivalently it will commute with every element $\alpha \in \mathcal{O}_k$ (i.e. $([\alpha]P)^\sigma = [\alpha]P^\sigma$). Thus τ is a morphism from the group $Gal(\overline{K}/F)$ to the group $Aut_{\frac{\mathcal{O}_k}{m\mathcal{O}_k}}(E_F[m])$ of $\frac{\mathcal{O}_k}{m\mathcal{O}_k}$-module automorphisms of $E_F[m]$. This map induces an injection if we restrict to $Gal(L_m/F)$. Then from Proposition 2.13 we get that

$$Aut_{\frac{\mathcal{O}_k}{m\mathcal{O}_k}}(E_F[m]) \simeq \left(\frac{\mathcal{O}_k}{m\mathcal{O}_k}\right)$$

so we conclude that $Gal(L_m/F)$ is abelian. □

CHAPTER 3

Integrality of j

In the previous chapter we proved that the j-invariant of an elliptic curve with complex multiplication is an algebraic number. In this section we will prove the following theorem

Theorem 3.1. *Let R be an order in an imaginary quadratic field and let Λ be a lattice with $R\Lambda \subset \Lambda$, then $j(\Lambda)$ is an algebraic integer. Equivalently, let E be an elliptic curve over $\mathbb{C}$ with complex multiplication, then $j(E)$ is an algebraic integer.*

So $j(E)$ is a root of a monic polynomial with integer coefficients. This is a very important result, leading for example to various simplifications in its computation. The first two sections of this chapter are inspired by the lessons of the course "Forme Modulari" taught by professor A. Maffei at the University of Pisa, 2020/2021, by [2] and by [5].

3.1 Congruence subgroups

We introduce some notions about the so-called congruence subgroups of $\mathbf{SL}_2(\mathbb{Z})$.

Definition 3.2. Let N be a positive integer. The *principal congruence subgroup* $\Gamma(N)$ is defined by

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

A *congruence subgroup* is any subgroup of $\mathbf{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$. A *modular curve* is a quotient of $\mathbb{H}$ or $\mathbb{H}$ by a congruence subgroup.

We note that every congruence subgroup is a finite index subgroup of $\mathbf{SL}_2(\mathsf{Z})$. There are two families of congruence subgroups of particular interest:

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

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

As in section 4 of chapter 1 we define some useful modular curves:

$$X_0(N) := \mathsf{H}\ /\Gamma_0(N), \quad X_1(N) := \mathsf{H}\ /\Gamma_1(N);$$

$$Y_0(N) := \mathsf{H}/\Gamma_0(N), \quad Y_1(N) := \mathsf{H}/\Gamma_1(N).$$

Now we give some important definitions:

Definition 3.3. Let $f : \mathsf{H} \to \mathsf{C}$ be a meromorphic function that is Γ-invariant for some congruence subgroup Γ. The function $f(\tau)$ is said to be meromorphic at the cusps if for every $\gamma \in \mathbf{SL}_2(\mathsf{Z})$ the function $f(\gamma(\tau))$ is meromorphic at ∞.

Definition 3.4. Let Γ be a congruence subgroup. A *modular function for* Γ is a Γ-invariant meromorphic function $f : \mathsf{H} \to \mathsf{C}$ that is meromorphic at the cusps.

It follows immediately from the definition of "meromorphic at the cusps" that for any $\gamma \in \mathbf{SL}_2(\mathsf{Z})$ the function $f(\gamma(\tau))$ is also meromorphic at the cusps. To say that $f(\gamma(\tau))$ is meromorphic at ∞ is to say that $f(\tau)$ is meromorphic at $\gamma(\infty)$. So, in order to check if f is meromorphic at the cusps, it is sufficient to consider a set of Γ-inequivalent cusp representatives $\gamma_1(\infty), \gamma_2(\infty), ..., \gamma_n(\infty)$, one for each Γ-orbit of $\mathsf{P}^1(\mathsf{Q})$; this is a finite set because the congruence subgroup Γ has finite index in $\mathbf{SL}_2(\mathsf{Z})$.
If f is also a modular function for Γ, then for any $\gamma \in \Gamma$ we have

$$\lim_{Im\tau\ !\ 1} f(\gamma(\tau)) = \lim_{Im\tau\ !\ 1} f(\tau)$$

and f must still have the same order at ∞ and $\gamma(\infty)$. So if f is meromorphic at the cusps it determines a meromorphic function $h : X_\Gamma \to \mathsf{C}$, where X_Γ is the modular curve $\mathsf{H}\ /\Gamma$. Sums, products, and quotients of modular functions for Γ are modular functions for Γ, as are constant functions, thus the set of all modular functions for Γ forms a field $\mathsf{C}(\Gamma)$ that we view as a transcendental extension of C. As we will shortly prove for $X_0(N)$, modular curves X_Γ are not only Riemann surfaces, they are also algebraic curves over C; the field $\mathsf{C}(\Gamma)$ of modular functions for Γ is isomorphic to the function field $\mathsf{C}(X_\Gamma)$ of X_Γ/C. We will make this isomorphism completely explicit for $X_0(N)$.

Next we present some important results that will be useful in this section.

Theorem 3.5. *Every modular function for* $\mathbf{SL}_2(\mathsf{Z})$ *is a rational function of* $j(\tau)$.

Proof. It follows immediately from Theorem 1.36. □

Lemma 3.6. *Let* Γ *be a congruence subgroup. The eld of modular functions for* Γ *is a nite extension of* $\mathsf{C}(j)$ *of degree at most* $[\mathbf{SL}_2(\mathsf{Z}) : \Gamma] := n$.

Proof. Let $\{\gamma_1, ..., \gamma_n\} \subseteq \mathbf{SL}_2(\mathsf{Z})$ be a set of right coset representatives for $\Gamma \subset \mathbf{SL}_2(\mathsf{Z})$, where $\gamma_1 = Id_{\mathbf{SL}_2(\mathsf{Z})}$. Let f be a modular function for Γ. We note that for any $\gamma \in \mathbf{SL}_2(\mathsf{Z})$ we have

$$\{\Gamma_0(N)\gamma_i\}_{i=1,...,n} = \{\Gamma_0(N)\gamma_i\gamma\}_{i=1,...,n}.$$

Let us consider the modular functions $f(\gamma_i(\tau))$. Any symmetric function in the functions $\{f(\gamma_i(\tau))\}_{i=1,...,n}$ is $\mathbf{SL}_2(\mathsf{Z})$-invariant and meromorphic at the cusps, since for any i the function $f(\gamma_i(\tau))$ is. In particular the polynomial

$$\prod_{i=1}^{n}(Y - f(\gamma_i(\tau))$$

has f as root and its coefficients are symmetric polynomials in $f(\gamma_i(\tau))$, so using Theorem 3.5 we conclude that they lie in $\mathsf{C}(j)$. Thus $[\mathsf{C}(f) : \mathsf{C}(j)] \leq n$. The result is a consequence of the fact that we are in characteristic zero, so we can use the primitive element theorem. □

3.2 The congruence subgroup $\Gamma_0(N)$

We now consider modular functions for the congruence subgroup $\Gamma_0(N)$.

Proposition 3.7. *The function* $\tau \to j(N\tau) = j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\tau\right)$ *is a modular function for* $\Gamma_0(N)$.

Proof. The function $j(N\tau)$ is holomorphic on H, and is meromorphic at the cusps, since $j(\tau)$ is. Next we will show that $j(N\tau)$ is $\Gamma_0(N)$-invariant. Let $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$, then we have

$$\begin{aligned} j(N\gamma(\tau)) &= j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\begin{pmatrix} N & 1 & 0 \\ 0 & & 1 \end{pmatrix}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\tau\right) \\ &= j\left(\begin{pmatrix} a & Nb \\ c & d \end{pmatrix} N\tau\right) = j(N\tau), \end{aligned}$$

where the last equality follows from the fact that $\begin{pmatrix} a & Nb \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathsf{Z})$ and j is $\mathbf{SL}_2(\mathsf{Z})$-invariant. □

Now we prove a very important Theorem that characterizes the field of modular functions for $\Gamma_0(N)$.

Theorem 3.8. *The field of modular functions, $\mathsf{C}(X_0(N))$, for $\Gamma_0(N)$ is an extension of $\mathsf{C}(j)$ of degree $[\mathbf{SL}_2(\mathsf{Z}) : \Gamma_0(N)] = n$ generated by $j(N\tau)$.*

Proof. From Propositions 1.34 and 3.7 we have that $j(\tau), j(N\tau) \in \mathsf{C}(X_0(N))$. From Theorem 3.6 we know that $[\mathsf{C}(X_0(N)) : \mathsf{C}(j)] \leq n$, so it suffices to show the other inequality.
Let us fix a set of right coset representatives $\{\gamma_1, ..., \gamma_n\}$ for $\Gamma_0(N) \subseteq \mathbf{SL}_2(\mathsf{Z})$, and let $F(j, Y) \in \mathsf{C}(j)[Y]$ be the minimal polynomial of $j(N\tau)$ over $\mathsf{C}(j)$. For any γ_i

$$0 = F(j(\tau), j(N\tau)) = F(j(\gamma_i(\tau)), j(N\gamma_i(\tau))) = F(j(\tau), j(N\gamma_i(\tau))),$$

so the function $j(N\gamma_i(\tau))$ is also a root of $F(j, Y)$. So in order to prove the claim it is sufficient to show that the $j(N\gamma_i(\tau))$ are distinct. Suppose that there exist indices $i \neq k$ such that $j(N\gamma_i(\tau)) = j(N\gamma_k(\tau))$, so $\forall \tau \in \mathsf{H}$ we have that $\exists \gamma \in \mathbf{SL}_2(\mathsf{Z})$ such that

$$N\gamma_i(\tau) = \gamma(\tau) N\gamma_k(\tau).$$

Generically[1], $\gamma(\tau)$ is unique up to sign. Choosing γ such that the first nonzero coefficient is positive, we may observe that γ depends on τ with continuity, but $\mathbf{SL}_2(\mathsf{Z})$ is discrete so it follows that γ is constant in τ.[2] So, there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_i = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_k,$$

and therefore

$$\gamma_i {\gamma_k}^{-1} = \pm \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \pm \begin{pmatrix} a & b/N \\ cN & d \end{pmatrix}.$$

We have that $\gamma_i {\gamma_k}^{-1} \in \mathbf{SL}_2(\mathsf{Z})$, so $b/N \in \mathsf{Z}$, and $N | cN$, so $\gamma_i {\gamma_k}^{-1} \in \Gamma_0(N)$. Then γ_i and γ_k lie in the same right coset, which is a contradiction. □

[1] In this case, this means $N\gamma_i(\tau)$ not in the $\mathbf{SL}_2(\mathsf{Z})$-orbit of i, ζ_3.
[2] The remaining cases are filled by continuity.

3.3 Integrality of j

The theorems of this section and their proof can be found in [6, Chapter 10] and [3, Chapter II]. In this section in order to prove the integrality of j we will study some properties of $P_N(j, Y)$, the minimal polynomial of $j(N\tau)$ over $\mathsf{C}(j)$. We may write P_N as

$$P_N(Y) = \prod_{i=1}^{n}(Y - j(N\gamma_i(\tau))) = \sum a_m X^m,$$

where $\{\gamma_1, ..., \gamma_n\}$ is a set of right coset representative for $\Gamma_0(N) \subset \mathbf{SL}_2(\mathsf{Z})$ and $a_m(\tau) \in \mathsf{C}(j)$ are symmetric polynomials in $j(N\gamma_i(\tau))$. So, as in Theorem 3.6, they are $\mathbf{SL}_2(\mathsf{Z})$-invariant. We also know that $a_m(\tau) \in \mathsf{C}(j)$ are holomorphic functions on H, so they are polynomials in j: suppose that $a_m(\tau) = \frac{p_1(j)}{p_2(j)}$ with $\gcd(p_1, p_2) = 1$, we want to prove that $\deg(p_2(j)) = 0$. If $\deg(p_2(j)) > 0$, there exists $x_0 \in \mathsf{C}$ such that $p_2(x_0) = 0$. However we know that $j(\tau)$ is surjective, so there exists $\tau_0 \in \mathsf{H}$ such that $p_2(\tau_0) = x_0$ and this will be a pole for $a_m(\tau)$, contradiction since $a_m(\tau)$ is holomorphic.

Let $\Lambda = \mathsf{Z}\tau + \mathsf{Z}$ be a lattice with $\tau \in \mathsf{H}$. If $\alpha \in R$, then $\alpha\Lambda \subset \Lambda$ implies that there exist some integers a, b, c, d such that

$$\alpha \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Let $n = ad - bc$. So, it can be useful to consider the set D_n of all 2×2 matrices with determinant n. We also introduce another important set of matrices

$$S_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in D_n : 0 \leq b < d \right\}.$$

Now we prove a proposition that will be useful in the study of the left $\mathbf{SL}_2(\mathsf{Z})$-equivalence classes of D_n, so in particular in the study of the set $\{j(N\gamma_i(\tau))\}_{i=1,...,n}$.

Proposition 3.9. *For all $M \in D_n$ there is a unique matrix $S \in S_n$ such that*

$$MS^{\ 1} \in \mathbf{SL}_2(\mathsf{Z}).$$

Proof. We start by proving the existence of S. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_n$. If we have $\frac{a}{c} = -\frac{x}{y}$ with $\gcd(x, y) = 1$, then there exist $x_1, x_2 \in \mathsf{Z}$ such that $xx_1 - yx_2 = 1$, that is equivalent to $\begin{pmatrix} x_1 & x_2 \\ y & x \end{pmatrix} \in \mathbf{SL}_2(\mathsf{Z})$. Multiplying A with

this matrix we obtain

$$\begin{pmatrix} x_1 & x_2 \\ y & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

so we may assume at the start that $c = 0$. In order to make $d > 0$, if necessary we multiply by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Next we want that $0 \leq b < d$. We note that for all $t \in \mathsf{Z}$

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b + td \\ 0 & d \end{pmatrix}.$$

Hence, if we choose t such that $0 \leq b + td < d$, we conclude the proof of the existence of S.

For the uniqueness, suppose that $A_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \in S_n$ for $i = 1, 2$ are in the same $\mathbf{SL}_2(\mathsf{Z})$-equivalence class. Then

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{1} = \begin{pmatrix} a_1/a_2 & (b_1a_2 - a_1b_2)/n \\ 0 & d_1/d_2 \end{pmatrix} \in \mathbf{SL}_2(\mathsf{Z}).$$

Since a_1/a_2 and d_1/d_2 must be positive integers with product equal to 1, they are both 1. The coefficient in the top-right corner is $(b_1 - b_2)/d_1$, and since it must be an integer and $0 \leq b_1, b_2 < d_1 = d_2$, we have that $b_1 = b_2$. □

Thanks to this proposition and remembering the fact that j is $\mathbf{SL}_2(\mathsf{Z})$-invariant we have

$$\{j(N\gamma_i(\tau))\}_{i=1,\ldots,n} \subset \{j(\alpha(\tau))\}_{\alpha 2 S_N}.$$

Hence $P_N(Y)$ divides the polynomial

$$F_N(Y) = \prod_{\alpha 2 S_N} (Y - j \circ \alpha(\tau)) = \sum a_m X^m.$$

For N squarefree we have that $n = \#S_N$, so the two polynomial are equal. This particular case is sufficient to prove Theorem 3.1 only when $R = \mathcal{O}_K$. In the first part of this section we proved that the coefficients of $P_N(Y)$ are weakly modular functions of weight 0 holomorphic on H and (in particular) in particular $a_m(\tau) \in \mathsf{C}[j]$. This is still true for the the coefficients of $F_N(Y)$. We do not give details for the proof because it is similar to the one already seen. Now we prove several lemmas that will be useful in the study of F_N, and in particular of its coefficients.

Lemma 3.10. *The Fourier q-expansion of s_m has coe cients in Z.*

Proof. Let $\zeta = e^{2\pi i/N}$. For any $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_N$ using the expansion of the j-function we have

$$j \circ \alpha(\tau) = j((a\tau + b)/d) = \sum_{k=\ 1}^{1} c_k(\zeta^b e^{2\pi i a\tau/d})^k,$$

where $c_0, c_1, ...$ are integers. In particular, the Fourier coefficients of $j \circ \alpha$, so also the coefficients of s_m, lie in $\mathsf{Z}[\zeta]$.
Next, for any a, d with $ad = N$, it can be useful to consider the following polynomial in Y

$$P_{a,d}(Y) = \prod_{b=0}^{d\ 1}(Y - j((a\tau + b)/d)) = \sum_{k=0}^{d} b_k(e^{2\pi i a\tau})Y^k.$$

We note that from what we proved in the first part it follows that the coefficients of each b_k lie in $\mathsf{Z}[\zeta]$. The Galois group $Gal(\mathsf{Q}(\zeta)/\mathsf{Q})$ permutes the factors of the product, so it leaves the coefficients of b_k unchanged. Therefore, they lie in $\mathsf{Q} \cap \mathsf{Z}[\zeta] = \mathsf{Z}$.
Finally we prove that s_m has a Fourier expansion in q with integer coefficients. Since $ad = N$ for each matrix in S_N, we have

$$e^{2\pi i a\tau/d} = e^{2\pi i a^2\tau/N}.$$

We note that $F_N(Y)$ is a product of polynomials $P_{a,d}(Y)$ for some a, d, so from what we already proved it follows that the coefficients s_m of $F_n(Y)$ are Laurent series in $e^{2\pi i\tau/N}$ with integer coefficients. We recall that the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acts on H by $\tau \mapsto \tau + 1$ and that s_m is invariant under this transformation. However we also know that $(e^{2\pi i\tau/N})^k$ is invariant under $\tau \mapsto \tau + 1$ only when $N|k$, this completes the proof of the lemma. □

Lemma 3.11. *$s_m(\tau)$ is a polynomial in j with integer coe cients.*

Proof. We already know that $s_m \in \mathsf{C}[j]$ and from Lemma 3.10 that $s_m \in \mathsf{Z}[\![q, q^{\ 1}]\!]$. We will prove that $\mathsf{C}[j] \cap \mathsf{Z}[\![q, q^{\ 1}]\!] = \mathsf{Z}[j]$. Let $f(j) = a_d j^d + a_{d\ 1} j^{d\ 1} + ... + a_0$ be a polynomial in $\mathsf{C}[j]$. Substituting the q-expansion of j we obtain

$$f(q) = \frac{a_d}{q^d} + \frac{a_{d\ 1} + d \cdot 744 \cdot a_d}{q^{d\ 1}} + ...$$

Using the fact that $f(q) \in \mathsf{Z}[\![q, q^{\ 1}]\!]$ we obtain $a_d \in \mathsf{Z}$. If we repeat this argument for $f - a_d j^d \in \mathsf{C}[j] \cap \mathsf{Z}[\![q, q^{\ 1}]\!]$ we obtain $a_{d\ 1} \in \mathsf{Z}$. Continuing in this way, we obtain $f(q) \in \mathsf{Z}[j]$. □

Using these lemmas we are able to prove the following theorem which summarize the most important properties of $F_N(Y)$.

Theorem 3.12.

1. *There is a polynomial $F_N(X,Y) \in \mathsf{Z}[X,Y]$ such that*
$$\prod_{\alpha 2 S_N} (Y - j \circ \alpha) = F_N(j, Y).$$
2. *Let $\beta \in M_2(\mathsf{Z})$ be a matrix with $\det(\beta) > 0$, then the function $j \circ \beta$ is integral over the ring $\mathsf{Z}[j]$.*
3. *If N is not a perfect square, then*
$$H_N = F_N(X,X) \in \mathsf{Z}[X]$$
is nonconstant and the coe cient of its highest power of X is ± 1.

Proof.

1. The previous lemmas say that
$$\prod_{\alpha 2 S_N} (Y - j \circ \alpha) = \sum_m s_m Y^m$$
with $s_m \in \mathsf{Z}[j]$.
2. Let $n = \det \beta$, so $\beta \in D_n$. Using Theorem 3.9 we can find a matrix $\gamma \in \mathbf{SL}_2(\mathsf{Z})$ such that $\gamma\beta \in S_n$. The $\gamma \in \mathbf{SL}_2(\mathsf{Z})$-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 $F_N(j, Y)$. Since F_n is monic by definition and has coefficients in $\mathsf{Z}[j]$ from the first point it follows that $j \circ \beta$ is integral over $\mathsf{Z}[j]$.
3. Let $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_N$ and $\zeta = \zeta_d$. If we consider the Fourier expansion of j and $j \circ \alpha$ in $e^{2\pi i \tau / N}$, the first terms are respectively
$$q^{\ 1} = e^{\ 2\pi i \tau} = (e^{\ 2\pi i \tau / N})^N, \quad \zeta^{\ b} e^{\ 2\pi i a \tau / d} = \zeta^{\ b} (e^{\ 2\pi i a \tau / N})^{a^2}.$$
We call $Q = e^{\ 2\pi i \tau / N} = q^{1/N}$. Since N is not a square, the leading terms cannot cancel, so $j - j \circ \alpha$ has a pole for $Q \to 0$. So the leading term must be a a root of unity. It follows that the coefficient of the first term of the expansion of $H_N(j)$ is the product of these roots of unity, hence it is a root of unity. We know that this leading term has to be an integer, so it must be ± 1. We note that the first term of the expansion of $H_N(j)$ is a negative power of q, so $H_N(X)$ is nonconstant.

□

Now we are able to prove Theorem 3.1.

Proof. We consider first the case $R = \mathcal{O}_k$, the ring of integers of k. Choose an element $\rho \in \mathcal{O}_k$ such that $|N_{k/\mathbb{Q}}\rho| = N$ is not a perfect square[3]. Then Theorem 2.14 says that the isogeny $[\rho] : E \to E$ has degree N. Let $\tau \in \mathsf{H}$ be a number such that $j(\tau) = j(E)$, then multiplication by ρ sends the lattice $\mathsf{Z}\tau \oplus \mathsf{Z}$ to the lattice $\mathsf{Z}\rho\tau \oplus \mathsf{Z}\rho = \mathsf{Z}(a\tau+b) \oplus \mathsf{Z}(c\tau+d)$ for some $a, b, c, d \in \mathsf{Z}$ such that $ad - bc = N$. In other words, there exists a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_N$ such that

$$j \circ \alpha(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) = j(E).$$

We recall that $j \circ \alpha(\tau)$ is a root of the polynomial $F_N(j, Y)$. Substituting $Y = j \circ \alpha$ and evaluating in τ we get

$$0 = F_N(j(\tau), j \circ \alpha(\tau)) = F_N(j(E), j(E)) = H_N(j(E)).$$

The claim follows from Theorem 3.12.
Finally we consider the general case of an arbitrary order R. Let $\Lambda = \mathsf{Z}\omega_1 \oplus \mathsf{Z}\omega_2$ be a lattice for E. From Theorem 1.40 we know that $k = \mathsf{Q}(\omega_1/\omega_2)$. So, replacing Λ with $\lambda\Lambda$ for a suitable $\lambda \in \mathsf{C}$ we may assume that $\Lambda \subset \mathcal{O}_k$. Next we choose $\tau \in \mathsf{H}$ such that $\mathsf{Z}\tau \oplus \mathsf{Z} = \mathcal{O}_k$, then Λ is a sub-lattice of $\mathcal{O}_k$. Hence we can write

$$\begin{cases} \omega_1 = a\tau + b \\ \omega_2 = c\tau + d \end{cases} \quad \text{for some } a, b, c, d \in \mathsf{Z}. \tag{3.2}$$

We call $ad - bc = N$, and we may assume that $N \geq 1$. Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in D_N, then by Theorem 3.12 $j \circ \alpha$ is integral over $\mathsf{Z}[j]$ and the integrality is given by the equation $F_N(j, Y) = 0$. Evaluating this equation in τ we obtain that $j \circ \alpha(\tau)$ is integral over $\mathsf{Z}[j(\tau)]$. We recall that $j \circ \alpha(\tau) = j(E)$ and since $j(\tau)$ is the j-invariant of an elliptic curve with CM by $\mathcal{O}_k$ from the previous point we know that it is integral over Z. Therefore $j(E)$ is integral over Z. □

[3]For example

$$\begin{cases} 1 + i & \text{if } k = \mathsf{Q}(i) \\ p & \text{if } k = \mathsf{Q}(\sqrt{d}). \end{cases} \tag{3.1}$$

CHAPTER 4

Hilbert class field

The results of this chapter can be found in [3, Chapter II]. We will now define a map between $Gal(\overline{K}/K)$ and $CL(\mathcal{O}_K)$, where K is a quadratic imaginary field.

In all this chapter we will use Proposition 2.17 to identify $\mathcal{ELL}(\mathcal{O}_K)$ with $\mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$. There is a natural action of $Gal(\overline{K}/K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ defined as follows:

$$Gal(\overline{K}/K) \times \mathcal{ELL}(\mathcal{O}_K) \to \mathcal{ELL}(\mathcal{O}_K), \quad (\sigma, E) \mapsto E^\sigma.$$

On the other hand, we showed in Theorem 2.10 that $CL(\mathcal{O}_K)$ acts on $\mathcal{ELL}(\mathcal{O}_K)$ with a simply transitive action.
So, for a fix elliptic curve E_0, there is a well defined map

$$F : Gal(\overline{K}/K) \to CL(\mathcal{O}_K), \quad \sigma \mapsto F(\sigma) = \mathfrak{a},$$

where $\mathfrak{a} \in CL(\mathcal{O}_K)$ is such that $\mathfrak{a} * E_0 = E_0^\sigma$.

Proposition 4.1. *The map F has the following properties:*

- *is independent of the choice of the curve $E \in \mathcal{ELL}(\mathcal{O}_K)$;*
- *is a homomorphism.*

Proof.

- Let $E_1, E_2 \in \mathcal{ELL}(\mathcal{O}_K)$ and $\sigma \in Gal(\overline{K}/K)$. There exist $I_1, I_2, J \in CL(\mathcal{O}_K)$ such that

$$E_1^\sigma = I_1 * E_1, \quad E_2^\sigma = I_2 * E_2, \quad E_2 = J * E_1.$$

Using this identity we obtain

$$(J * E_1)^\sigma = E_2^\sigma = I_2 * E_2 = I_2 * (J * E_1) = (I_2 J I_1{}^{-1}) * E_1^\sigma.$$

Thus, using Proposition 4.2 we know that $(J * E_1)^\sigma = J * E_1^\sigma$, then we can cancel J from both sides to conclude that $E_1^\sigma = I_2 I_1{}^{-1} * E_1^\sigma$; and Theorem 2.10 will give $I_1 = I_2$.

- For all $\sigma, \tau \in Gal(\overline{K}/K)$ using the first point we have:

$$F(\sigma\tau)*E = E^{\sigma\tau} = (E^\tau)^\sigma = (F(\tau)*E)^\sigma = F(\sigma)*(F(\tau)*E) = (F(\sigma)F(\tau))*E.$$

□

Now we prove the proposition used to conclude the previous proof.

Proposition 4.2. *Let $E/\overline{\mathsf{Q}}$ be an elliptic curve representing an element of $\mathcal{ELL}(\mathcal{O}_K)$, let $I \in \mathcal{ELL}(\mathcal{O}_K)$ and let $\sigma \in Gal(\overline{\mathsf{Q}}/\mathsf{Q})$. Then*

$$(I * E)^\sigma = I^\sigma * E^\sigma.$$

Proof. We choose a lattice Λ such that $E \simeq E_\Lambda$ and fix an exact sequence

$$\mathcal{O}_K^m \xrightarrow{A} \mathcal{O}_K^n \to I \to 0$$

where A is a $n \times m$ matrix with coefficients in $\mathcal{O}_K$. Now we will use that $\mathsf{C}/I\ {}^1\Lambda \simeq I * E \simeq Hom(I, E)$,[1] where the last isomorphism will be proven below. We apply $Hom(\cdot, \cdot)$ to the product of the previous exact sequence with the sequence $0 \to \Lambda \to \mathsf{C} \to E \to 0$, obtaining the following diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & Hom(I,\Lambda) & \longrightarrow & Hom(I,\mathsf{C}) & \longrightarrow & Hom(I,E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & Hom(\mathcal{O}_K^n,\Lambda) & \longrightarrow & Hom(\mathcal{O}_K^n,\mathsf{C}) & \longrightarrow & Hom(\mathcal{O}_K^n,E) \\
 & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} \\
0 & \longrightarrow & Hom(\mathcal{O}_K^m,\Lambda) & \longrightarrow & Hom(\mathcal{O}_K^m,\mathsf{C}) & \longrightarrow & Hom(\mathcal{O}_K^m,E)
\end{array}$$

For any $\mathcal{O}_K$-module M we have that $Hom(\mathcal{O}_K^n, M) \simeq M^n$; moreover, we have the following lemma that we state without proof:

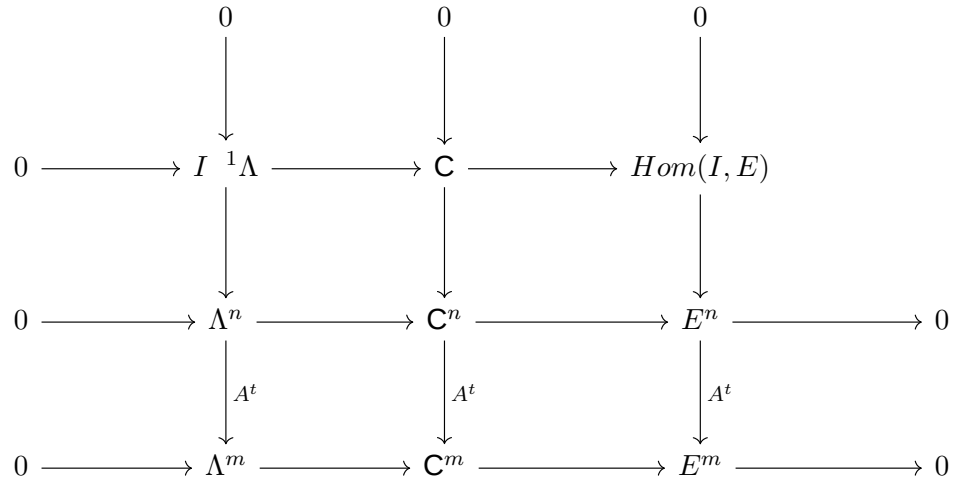
[1] In this proof Hom will always indicate the group of $\mathcal{O}_K$-linear homomorphisms.

Lemma 4.3. *Let R be a Dedekind domain, let I be a fractional ideal of R and let M be a torsion-free R-module. Then the natural map*

$$\Phi : I\ {}^1M \to Hom_R(I, M), \quad x \mapsto (\Phi_x : \alpha \mapsto \alpha x)$$

is an isomorphism.

Applying this lemma first with $M = \Lambda$, then with $M = \mathsf{C}$, the previous diagram can be rewritten as



where the exactness of the last two rows follows from the fact that they are just a number of copies of $0 \to \Lambda \to \mathsf{C} \to E \to 0$. Using the Snake-Lemma on the last two rows we obtain:

$$0 \to I\ {}^1\Lambda \to \mathsf{C} \to \ker(A^t : E^n \to E^m) \simeq Hom(I, E) \to \Lambda^m / A^t(\Lambda^n). \quad (4.1)$$

Note that, since $A^t : E^n \to E^m$ is a matrix with coefficients in $End(E) \simeq \mathcal{O}_K$, it is an algebraic map between algebraic varieties, so $(A^t)\ {}^1(0, ..., 0)$ is an algebraic subvariety of E^n. From Proposition 2.17 it follows that for any $\sigma \in Aut(\mathsf{C})$, the corresponding map

$$(A^t)^\sigma : (E^\sigma)^n \to (E^\sigma)^m,$$

is obtained acting with σ on the coefficients of A^t. From a topological point of view we know that $\Lambda^m / A^t(\Lambda^n)$ is discrete and $\mathsf{C}/I\ {}^1\Lambda$ is connected. Hence from (4.1) we get

$$(I * E)(\mathsf{C}) = \mathsf{C}/I\ {}^1\Lambda \simeq \textit{identity component of } \ker(A^t : E^n \to E^m).$$

So, we have described $I * E$ as an algebraic object. We conclude

$$\begin{aligned}(I * E)^\sigma &\simeq \big(\textit{identity component of } \ker(A^t : E^n \to E^m)\big)^\sigma \\ &= \textit{identity component of } \ker((A^t)^\sigma : (E^\sigma)^n \to (E^\sigma)^m) \\ &\simeq I^\sigma * E^\sigma.\end{aligned}$$

□

Since $CL(\mathcal{O}_K)$ is an abelian group, F factors through $F : Gal(K^{ab}/K) \to CL(\mathcal{O}_K)$ where K^{ab} is the maximal abelian extension of K.

4.1 A brief review of class field theory

We will mostly restrict our attention to totally imaginary fields.
Let K be a totally imaginary number field and let L be a finite abelian extension of K with Galois group G. 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 $\mathfrak{c}$.

Definition 4.4. For each prime ideal $\mathfrak{p}$ of K we define the *Artin symbol for unrami ed 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[2] Frobenius element of $\mathfrak{p}$ in $G = Gal(L/K)$.

Then we observe that, if we factorize $\mathfrak{p}$ as product of prime ideals of L, $\mathfrak{p} = P_1...P_m$, we can define the Artin symbol for each factor 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.

Definition 4.5. The *Artin map* is defined using the Frobenius maps $\sigma_{\mathfrak{p}}$'s and linearity as follows:

$$\left(\frac{L/K}{\cdot}\right) : I(\mathfrak{c}) \to Gal(L/K), \quad \mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}}\right) = \left(\frac{L/K}{\prod_{\mathfrak{p}} \mathfrak{p}^{n_p}}\right) := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_p}.$$

Note that the Artin map is defined by piecing together local information, one prime at a time.
The following proposition is a weak version of the Artin reciprocity law and it provides important global information.

[2]We are using that $Gal(L/K)$ is an abelian group.

Theorem 4.6 (Artin Reciprocity)**.** *Let L/K be a finite abelian extension of number fields. Then there exists an integral ideal $\mathfrak{c} \subset \mathcal{O}_K$, divisible by precisely the primes of K that ramify in L, such that*

$$\left(\frac{L/K}{(\alpha)}\right) = 1 \quad \textit{for all } \alpha \in K \ \textit{ such that } \alpha \equiv 1 \pmod{\mathfrak{c}}$$

Note that Theorem 4.6 ensures only the existence of the ideal $\mathfrak{c}$, and not its uniqueness.

Definition 4.7. Let $\mathfrak{c}_{L/K}$ be the largest ideal for which Artin reciprocity is true. We call it the conductor of the extension L/K.

Theorem 4.6 makes it natural to define the group of principal ideals congruent to 1 modulo $\mathfrak{c}$:

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

Artin reciprocity says that if we take the conductor of the extension:

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

Note that a principal ideal (α) may be in $P(\mathfrak{c})$ even if $\alpha \not\equiv 1 \pmod{\mathfrak{c}}$, it suffices that $\epsilon\alpha \equiv 1 \pmod{\mathfrak{c}}$ for an appropriate unity ϵ. Let $\mathfrak{p}$ a prime of K, unramified in L, then[3] it splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. So, the unramified prime ideals in the kernel of Artin map are the primes of K that split completely in L.

Definition 4.8. 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

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

Intuitively, one can think of the ray class field as the "largest" field with a given conductor. However, it is important to note that the conductor of $K_\mathfrak{c}$ need not[4] be $\mathfrak{c}$.

Theorem 4.9 (Class field theory)**.** *Let L/K be a finite abelian extension of number fields, and let $\mathfrak{c}$ be an integral ideal of K.*

1. *The Artin map is a surjective homomorphism.*
2. *The kernel of the Artin map is $N_{L/K}(I_L)P(\mathfrak{c}_{L/K})$, where I_L is the group of non zero fractional ideals of L coprime to $\mathfrak{c}_{L/K}$.*

[3] $\mathfrak{p}$ is unramified so $e_\mathfrak{p} = 1$, hence it splits if and only if $f_\mathfrak{p} = 1$, $D(\mathfrak{P}/\mathfrak{p}) = \langle \sigma_\mathfrak{p} \rangle = 1$.

[4] For example, the ray class field of $\mathbb{Q}(i)$ modulo the ideal (2) is itself, so its conductor is (1).

3. *There exists a unique ray class field $K_{\mathfrak{c}}$ of K (modulo $\mathfrak{c}$). The conductor of the extension $K_{\mathfrak{c}}/K$ divides $\mathfrak{c}$.*

4. *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:*

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

From points $(1), (2)$ of Theorem 4.9 and by the first homomorphism theorem, we see that the Artin map induces the following isomorphism

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

Definition 4.10. 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_K.

We notice that, by point (3) of Theorem 4.9, the conductor of the extension H_K/K divides the module $\mathfrak{c} = (1)$, so $\mathfrak{c}_{H_K/K}|(1)$, that implies necessarily that $\mathfrak{c}_{H_K/K} = (1)$. We have that:

$$\begin{aligned} I(\mathfrak{c}_{H_K/K}) &= I((1)) = \{\text{all non-zero fractional ideals of } K\} \\ P(\mathfrak{c}_{H_K/K}) &= P((1)) = \{\text{all non-zero principal ideals of } K\}. \end{aligned}$$

Moreover the following theorem can be proved:

Theorem 4.11. *The Artin map induces an isomorphism between the ideal class group of K and the Galois group $Gal(H_K/K)$.*

We will also need the following version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 4.12. *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.*

4.2 Hilbert class field of K

In this section we will prove the following Theorem

Theorem 4.13. *Let $K/\mathbb{Q}$ be a quadratic imaginary field with ring of integers $\mathcal{O}_K$, and let E be an elliptic curve with $End(E) \simeq \mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.*

We prove a useful proposition that will help us to completely determine F.

Proposition 4.14. *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 $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then the Frobenius element associated to $\mathfrak{p}$ is sent by F to the class of $\mathfrak{p}$ in the ideal class group, namely*

$$F(\sigma_{\mathfrak{p}}) = \mathfrak{p} \in CL(\mathcal{O}_K).$$

In order to prove this proposition we state without proof the following lemma. The proof could be found in [3, Chapert II] and it uses some properties of Tate modules and Weil pairing.

Lemma 4.15. *Let L be a number field, let P be a maximal ideal of $\mathcal{O}_L$, let E_1/L and E_2/L be elliptic curves with good reduction at P, with $\tilde{E}_1$ and $\tilde{E}_2$ their reductions modulo P. Then the natural reduction map*

$$Hom(E_1, E_2) \to Hom(\tilde{E}_1, \tilde{E}_2), \quad \Phi \mapsto \tilde{\Phi}$$

is injective. Furthermore, it preserves degree, so $deg(\Phi) = deg(\tilde{\Phi})$.

Proof of Proposition 4.14. From Theorem 2.9 we know that $\mathcal{ELL}(\mathcal{O}_K)$ is finite and from Proposition 2.15 we have that every curve in $\mathcal{ELL}(\mathcal{O}_K)$ can be defined over $\overline{\mathbb{Q}}$, so for a suitable finite extension L/K we can choose a set, $E_1, ..., E_n$, of representatives for $\mathcal{ELL}(\mathcal{O}_K)$ defined over L. Using Proposition 2.17 we may replace L by a finite extension such that any isogeny between E_i and E_j for every $i, j \leq n$ is defined over L. Let $S \subset \mathbb{Z}$ be the finite set of rational primes p satisfying one of the following conditions:

1. p ramifies in L;
2. some E_i has bad reduction at some prime of L over p;
3. p divides either the numerator or the denominator of one of the numbers $N_{L/\mathbb{Q}}(j(E_i) - j(E_k))$ for some $i \neq k$ (this means that, if $p \notin S$ and P is a prime of L dividing p, then $\tilde{E}_i \neq \tilde{E}_k \pmod{P}$, since their invariants are not the same modulo P.).

Let $p \notin S$ be a prime such that $p\mathcal{O}_K = \mathfrak{p}I'$ and let $M|\mathfrak{p}$ be a prime ideal of L. Let Λ be a lattice for E. Next we choose some integral ideal $I \subset \mathcal{O}_K$, relatively prime to p, such that $I\mathfrak{p} = (\alpha)$ is principal.
Using Theorem 1.24 we make the following commutative diagram

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda & \xrightarrow[z \mapsto z]{} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow[z \mapsto z]{} & \mathbb{C}/I^{-1}\mathfrak{p}^{-1}\Lambda = \mathbb{C}/(\alpha^{-1})\Lambda & \xrightarrow[z \mapsto \alpha z]{} & \mathbb{C}/\Lambda \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E & \xrightarrow{\phi} & \mathfrak{p} * E & \xrightarrow{\psi} & I * \mathfrak{p} * E = (\alpha) * E & \xrightarrow{\lambda} & E
\end{array}$$

Next we choose a Weierstrass equation for E/L, minimal at M, and let

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

be the associated invariant differential. As we have already noticed, the pull-back of ω to $\mathbb{C}/\Lambda$ will be a multiple of dz. The composition of maps along the top row is simply $[\alpha]$, so the pull back of dz is αdz. Then from the commutativity of the diagram we obtain:

$$(\lambda \circ \psi \circ \phi)\ \omega = \alpha\omega.$$

We will use a tilde, $\tilde{E}$, to denote reduction of E modulo M. Since we chose a Weierstrass equation for E/L minimal at M, we obtain an equation for $\tilde{E}$ by reducing the coefficients modulo M. From the second point of the definition of S we now that E has good reduction modulo M. Moreover using that $I\mathfrak{p} = (\alpha)$ and $M|\mathfrak{p}$, we find

$$(\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi})\ \tilde{\omega} = (\lambda \circ \hat{\psi} \circ \phi)\ \omega = \tilde{\alpha}\tilde{\omega} = \tilde{0}.$$

So, using Proposition 0.11 we deduce that $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable.
From Lemma 4.15 and Corollary 2.14 we obtain

$$\begin{gathered}\deg(\tilde{\phi}) = \deg(\phi) = N_{K/\mathbb{Q}}(\mathfrak{p}) = p \\ \deg(\tilde{\psi}) = \deg(\psi) = N_{K/\mathbb{Q}}(I) \\ \deg(\tilde{\lambda}) = \deg(\lambda) = 1.\end{gathered}$$

Since, by hypothesis, $N_{K/\mathbb{Q}}(I)$ is coprime to p, then both $\tilde{\psi}$ and $\tilde{\lambda}$ are separable. We deduce that $\tilde{\phi}$ must be inseparable, so it factors as a q^{th}-power Frobenius map and a separable map. Thus, since $\deg(\tilde{\phi}) = p$, it must be the p^{th}-power Frobenius map. In particular, we find that

$$j(\mathfrak{p} * E) = j((\tilde{E})^{(p)}) = j(\tilde{E})^p,$$

from which we obtain the so-called *Kronecker congruence*

$$j(\mathfrak{p} * E) \equiv j(E)^p \pmod{M}.$$

Moreover, by using the definition of F and the other results, it holds that

$$j(\mathfrak{p}*E) \equiv j(E)^p \equiv j(E)^{N_{K/\mathbb{Q}}(\mathfrak{p})} \equiv j(E)^{\sigma_\mathfrak{p}} = j(E^{\sigma_\mathfrak{p}}) = j(F(\sigma_\mathfrak{p})*E) \pmod{M}.$$

But from the original choice of excluded primes S, we have that

$$j(E_i) \equiv j(E_k) \pmod{M} \Leftrightarrow E_i \simeq E_k.$$

Hence it is $\mathfrak{p} * E \equiv F(\sigma_\mathfrak{p}) * E$, then for the simple transitivity of the action of $CL(\mathcal{O}_K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ gives result: $F(\sigma_\mathfrak{p}) = \mathfrak{p}$. □

We are able to prove the Theorem stated at the beginning.

Proof of Theorem 4.13. Let L/K be the finite extension corresponding to the homomorphism

$$F : Gal(\overline{K}/K) \to CL(\mathcal{O}_K)$$

namely, L is the fixed field of the kernel of F. Then

$$\begin{aligned} Gal(\overline{K}/L) &= \ker(F) \\ &= \left\{\sigma \in Gal(\overline{K}/K) : F(\sigma) = 1\right\} \\ &= \left\{\sigma \in Gal(\overline{K}/K) : F(\sigma) * E = E\right\} \\ &= \left\{\sigma \in Gal(\overline{K}/K) : E^{\sigma} = E\right\} \\ &= \left\{\sigma \in Gal(\overline{K}/K) : j(E^{\sigma}) = j(E)\right\} \\ &= \left\{\sigma \in Gal(\overline{K}/K) : j(E)^{\sigma} = j(E)\right\} \\ &= Gal(\overline{K}/K(j(E))). \end{aligned}$$

where the equality $\left\{\sigma \in Gal(\overline{K}/K) : F(\sigma) = 1\right\} = \left\{\sigma \in Gal(\overline{K}/K) : F(\sigma) * E = E\right\}$ follows from the simple transitivity of the action.
Hence $L = K(j(E))$. We also note that since $F : Gal(L/K) \to CL(\mathcal{O}_K)$ is injective, the extension L/K is abelian.
Let us consider $\mathfrak{c}_{L/K}$, the conductor of L/K, and the composition of the Artin map with F:

$$I(\mathfrak{c}_{L/K}) \longrightarrow Gal(L/K) \longrightarrow CL(\mathcal{O}_K)$$

$$\prod P_i^{n_i} \longrightarrow \prod(\sigma_{P_i})^{n_i} \longrightarrow F(\prod(\sigma_{P_i})^{n_i}).$$

We claim that this composition is the natural projection of $I(\mathfrak{c}_{L/K})$ onto $CL(\mathcal{O}_K)$, so we need to prove that

$$F\left(\left(\frac{L/K}{I}\right)\right) = I \in CL(\mathcal{O}_K).$$

Let $I \in I(\mathfrak{c}_{L/K})$ and S be the set defined in Proposition 4.14. From Theorem 4.12 we know that there exists a degree 1 prime ideal $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ that lies in the same $P(\mathfrak{c}_{L/K})$-ideal class as I and not lying over a prime in S (i.e. $\exists \alpha \in K$ such that $\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}} \ \wedge \ I = (\alpha)\mathfrak{p}$). Then

$$F\left(\left(\tfrac{L/K}{I}\right)\right) = F\left(\left(\tfrac{L/K}{(\alpha)\mathfrak{p}}\right)\right) = F\left(\left(\tfrac{L/K}{\mathfrak{p}}\right)\right) = \mathfrak{p} = I$$

where the second equality follows from the fact that $\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}}$, the third equality follows from Proposition 4.14 and since $N_{K/\mathbb{Q}}(\mathfrak{p}) \notin S$. A consequence of what we have seen is that $F\left(\left(\frac{L/K}{(\alpha)}\right)\right) = 1$ for all principal ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$. Furthermore, as we have already seen $F|_{Gal(L/K)}$ is injective, then $\left(\frac{L/K}{(\alpha)}\right) = 1$ for all principal ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$. By the definition of $\mathfrak{c}_{L/K}$ it follows that $\mathfrak{c}_{L/K} = (1)$. Using Artin reciprocity (Theorem 4.6) the conductor is divisible by every prime that ramifies, then 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 $I(\mathfrak{c}_{L/K}) = I(1) \to CL(\mathcal{O}_K)$ is surjective, so by the claim it follows that $F|_{Gal(L/K)}$ is surjective, hence an isomorphism. Therefore

$$[L : K] = |Gal(L/K)| = |CL(\mathcal{O}_K)| = |Gal(H/K)| = [H : K],$$

then $L = H$. □

Finally, we prove some consequences of Proposition 4.14.

Theorem 4.16. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$.*

1. $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$,
2. *Let $E_1, ..., E_h$ be a complete set of representatives for $\mathcal{ELL}(\mathcal{O}_K)$. Then $j(E_1), ..., j(E_h)$ is a complete set of $Gal(\overline{K}/K)$-conjugates for $j(E)$.*
3. *For every prime ideal $\mathfrak{p}$ of K*

$$j(E)^{\sigma_\mathfrak{p}} = j(\mathfrak{p} * E).$$

Proof. 1. The second equality follows from Theorem 4.13. In order to prove the first equality we know from Remark 2.4 that

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K.$$

Furthermore we have that

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \geq [K(j(E)) : K].$$

2. We know that $CL(\mathcal{O}_K)$ acts transitively on $\mathcal{ELL}(\mathcal{O}_K)$, then using Theorem 0.3 $CL(\mathcal{O}_K)$ acts transitively also on $\mathcal{J} = \{j(E_1), ..., j(E_h)\}$. The map $F : Gal(\overline{K}/K) \to CL(\mathcal{O}_K)$ is defined by identifying the action of $Gal(\overline{K}/K)$ on $\mathcal{J}$ with the action of $CL(\mathcal{O}_K)$ on $\mathcal{J}$, so $Gal(\overline{K}/K)$ acts transitively on $\mathcal{J}$.

3. In the proof of Theorem 4.13 we noticed that $F\left(\left(\frac{L/K}{I}\right)\right) = I$ for all $I \in I((\mathfrak{c}_{L/K})) = I((1)) = \{\text{non-zero fractional ideals of } K\}$. This means that
$$j\left(E^{\left(\frac{L/K}{I}\right)}\right) = j\left(F\left(\left(\frac{L/K}{I}\right)\right) * E\right) = j\left(I * E\right).$$

□

Bibliography

[1] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[2] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[3] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[4] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[5] Andrew Sutherland. *MIT Course Number 18.783: Elliptic curves*. https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2019/index.htm, 2019.

[6] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.