Elliptic curves, Elliptic functions, and Complex multiplication

Spencer Martin
Eleanor McSpirit
Badri Vishal Pandey

Spring 2022

Contents

The big picture

The goal of this talk is to prove the First Fundamental Theorem of Complex Multiplication: that is, we will find explicit generators for the maximal unramified abelian extension (Hilbert class field) of an imaginary quadratic field.

To begin, we review the basic properties of elliptic curves and functions over $\mathbb{C}$, giving an explicit parameterization of points on an EC using the Weierstrass $\wp$–function. Then we introduce the notion of complex multiplication, giving a correspondence between the ideal class group of an order in an imaginary quadratic field and elliptic curves with prescribed symmetries.

In the second section of this talk, we will first discuss the j-invariant, which classifies elliptic curves up to isomorphism, or equivalently, lattices up to homothety. We will then promote this construction to a modular function, and along with the modular equation, use these tools to prove that the j-invariant is an algebraic integer of degree bounded by the class number.

The goal of the final section 3 is to prove the first fundamental theorem of CM. In this chapter we start with introducing basic facts from algebraic number theory required to prove the main theorem. Then, using Chebotarev's density theorem, we prove theorem 3.1.5 which tells us when a Galois field extension $L/\mathbb{Q}$ contains another field extension $K/\mathbb{Q}$ in terms of primes in K with relative degree 1 over $\mathbb{Q}$ that split completely in L. This theorem is essential in providing a necessary and sufficient condition when a field extension $\tilde{K}/K$ is maximal unramified abelian extension (Hilbert class field). Finally, using this condition we show that indeed $K(j(\mathcal{O}_K))/K$ is the Hilbert class field for $K = \mathbb{Q}(\sqrt{-d})$.

Chapter 1

Elliptic functions and elliptic curves

In the coming sections, we will see how the geometry of elliptic curves may be used to study abelian extensions of imaginary quadratic number fields. The goal of this section is to develop the necessary background in elliptic curves – particularly from the perspective of complex tori and elliptic functions. We will first define elliptic functions to establish the following correspondence:

$$\text{Lattices} \Leftrightarrow \text{Elliptic curves over } \mathbb{C}.$$

This correspondence will end up being functorial in a suitable manner, so that lattices with prescribed endomorphism rings will correspond to elliptic curves with the same endomorphism ring. Elliptic curves with endomorphism rings larger than $\mathbb{Z}$ are said to have Complex Multiplication (CM). In this case, the endomorphism rings will be orders in imaginary quadratic fields. Remarkably, isomorphism classes of elliptic curves with CM will further correspond to ideal classes in the respective quadratic order:

$$\text{Ideal classes in imaginary quadratic order } \mathcal{O} \Leftrightarrow \text{Lattices with CM } \mathcal{O} \Leftrightarrow E/\mathbb{C} \text{ with CM } \mathcal{O}.$$

We begin by recalling the basic properties of elliptic functions and elliptic curves.

1.1 The $\wp$–function

Definition 1.1.1. *A lattice Λ is a subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$–linearly independent elements ω_1, ω_2.*

We will often denote a lattice generated by two elements ω_1, ω_2 by $[\omega_1, \omega_2]$. More generally, we will let $[\omega_1, \ldots, \omega_n]$ denote the $\mathbb{Z}$–span of $\omega_1, \ldots, \omega_n$ in $\mathbb{C}$.

Definition 1.1.2. *An elliptic curve E is a compact Riemann surface of the form $\mathbb{C}/\Lambda$ where Λ is a lattice, with a distinguished point $O = [0]$ corresponding to the equivalence class of 0.*

Given a complex number $z \in \mathbb{C}$ and a lattice Λ, we may sometimes refer to the coset $z + \Lambda$ as $[z]$.

Definition 1.1.3. *A morphism of lattices $\Lambda_1 \to \Lambda_2$ is a complex number $\alpha \in \mathbb{C}^\times$ so that $\alpha\Lambda_1 \subseteq \Lambda_2$. An isomorphism of lattices is called a homothety.*

Observe that $\mathrm{Hom}(\Lambda_1, \Lambda_2)$ is a subgroup of $\mathbb{C}^\times$, and hence $\mathrm{Hom}(\Lambda_1, \Lambda_1)$ is a subring of $\mathbb{C}^\times$.

Definition 1.1.4. *A morphism of elliptic curves is a holomorphic basepoint preserving map between the underlying Riemann surfaces.*

Similarly to lattices, the hom sets between elliptic curves can be seen as abelian groups: although we view $\mathbb{C}/\Lambda$ as just an abstract Riemann surface (and have hence forgotten any natural group structure one could induce on it), specifying the base point $[0]$ allows us to recover the quotient map $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ which is translation invariant and sending 0 to $[0]$. In particular, this allows us to endow $\mathbb{C}/\Lambda$ with the structure of an abelian group – namely with the quotient group structure. The $\mathrm{Hom}(E_1, E_2)$ ends up being an abelian group under pointwise addition.

From these initial definitions, it is clear to see that a morphism of lattices induces a morphism of elliptic curves: any map $\alpha : \Lambda \to \Lambda'$ induces a map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ by $x + \Lambda \mapsto \alpha x + \Lambda'$, and such a map is well–defined, as $\alpha\Lambda \subseteq \Lambda'$. But we want an equivalence of categories between the category of elliptic curves and the category of lattices. That is, we would like to see that every morphism of elliptic curves arises in this manner. To show this, we must first define elliptic functions.

Definition 1.1.5. *An elliptic function (for Λ) is a meromorphic function f on $\mathbb{C}$ so that $f(x+\omega) = f(x)$ for all $\omega \in \Lambda$ and $x \in \mathbb{C}$ (equivalently $f(x+\omega_1) = f(x+\omega_2) = f(x)$.*

One may also think of an elliptic function (for Λ) as being a meromorphic function factoring through $\mathbb{C}/\Lambda$. With this characterization, it is easy to prove the following theorem:

Theorem 1.1.6. *If f is elliptic and entire, then f is constant.*

Proof. If f is entire, then f is a holomorphic function $f : \mathbb{C} \to \mathbb{C}$ factoring through $\mathbb{C}/\Lambda$ as follows:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "f"] \arrow[d] & \mathbb{C} \\
\mathbb{C}/\Lambda \arrow[ur, dashed, swap, "\bar{f}"] &
\end{tikzcd}$$

We know that $\mathbb{C}/\Lambda$ is compact, and hence its image under $\overline{f}$ is compact and hence bounded. Thus, f is bounded and entire, meaning it is constant. □

The last step in proving the equivalence of categories is to show that every morphism between elliptic curves arises from a morphism of lattices:

Theorem 1.1.7. *Let $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be a morphism of elliptic curves. Then there is $\alpha \in \mathbb{C}$ so that $f(x+\Lambda) = \alpha x + \Lambda'$ for all $x \in \mathbb{C}$.*

Proof. Fix a morphism of elliptic curves $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. Implicitly, when we talk about "$\mathbb{C}/\Lambda$", have endowed the set $\mathbb{C}/\Lambda$ with the quotient topology, and further endowed it with a the structure of a complex manifold in such a way that the projection map $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ is locally a biholomorphic map, an in particular a covering map. By general algebraic topology, a map between spaces induces a map between universal covers, yielding the following commutative diagram:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\tilde{f}"] \arrow[d, swap, "\pi"] & \mathbb{C} \arrow[d, "\pi"] \\
\mathbb{C}/\Lambda \arrow[r, swap, "f"] & \mathbb{C}/\Lambda'
\end{tikzcd}$$

Since holomorphy is a local condition, π is locally biholomorphic, and f is holomorphic, it follows that $\tilde{f}$ is also holomorphic. Furthermore, since $\pi \circ \tilde{f} = f \circ \pi$, it follows that for any $\omega \in \Lambda$, $\tilde{f}(x+\omega) + \Lambda' = \tilde{f}(x) + \Lambda'$, or equivalently, $\tilde{f}(x+\omega) - \tilde{f}(x) \in \Lambda'$. For any $\omega \in \Lambda$, $\tilde{f}(x+\omega) - \tilde{f}(x)$ is a continuous map (in x) from $\mathbb{C}$ to Λ' (with the discrete topology), and is hence constant. Taking derivatives, we see that $\tilde{f}'(x+\omega) = \tilde{f}'(x)$, so $\tilde{f}'$ is elliptic and entire, and is hence a constant $\alpha \in \mathbb{C}$.. Thus, $f(x) = f(0) + \alpha \cdot x$. But by supposition, $f([0]) = [0]$, so we may take $f(0) = 0$, and we are done. □

So far, we have made use of constant elliptic functions to great effect, establishing an equivalence of categories between the category of lattices and the category of elliptic curves over $\mathbb{C}$. However, a number of lingering questions remain. Firstly, are there any non–constant elliptic functions? Furthermore, we have basically rigged the definition of elliptic curves to force this equivalence of categories. What do based complex tori have to do with the cubic curves number theorists may be more familiar with? Both of these questions may be addressed via the Weierstrass $\wp$–function.

Definition 1.1.8. *The Weierstrass $\wp$–function is defined as*

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

We will omit Λ when there is no ambiguity in doing so.

Theorem 1.1.9. *The $\wp$–function is an elliptic function so that*

1. *The only poles lie on Λ and are of order 2*
2. *$\wp$ is meromorphic and satisfies the differential equation*

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

Where $g_2(\Lambda)$ and $g_3(\Lambda)$ are the normalized Eisenstein series, i.e. $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ where

$$G_n(\Lambda) = \sum_{\omega\in\Lambda\backslash\{0\}} \frac{1}{\omega^n}$$

(remark: the G_n's are the modular forms you are probably familiar with)

3. *Let $W(x,y) = y^2 - 4x^3 + g_2(\Lambda)x - g_3(\Lambda)$. Then the map $[\wp : \wp' : 1] : \mathbb{C}/\Lambda \to V_{\mathbb{CP}^2}(W)$ is a bijection (where here, $V_{\mathbb{C}P^2}(W)$ denotes the zero set of the homogenization of W in $\mathbb{C}P^2$).*

Proof. The proof for this theorem comes from [1, Chapter 10].

Part (1) follows directly from the definition.

We will defer the meromorphy in part (2) to [1, Theorem 10.1] The differential equation in (2) is a fairly direct and formal computation. We will not fully justify all interchanges of sums and other analytic arguments, and instead differ to [1, Chapter 10] for more thorough proofs.

Note that $f(z) := \wp'(z)^2 - 4\wp(z)^3 + g_2(\Lambda)\wp(z) + g_3(\Lambda)$ is elliptic (for Λ), so we just need to show that it is entire and vanishes somewhere. Note further that as the only poles of $\wp$ lie on Λ, so too can the only poles of $\wp'$ and f only lie on Λ. Thus, it suffices to show that $f(0) = 0$.

First we compute the Laurent expansion of $\wp$ around 0. Using the geometric series, we get that

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

and hence

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

Taking the derivative with respect to z, we get

$$\wp'(z;\Lambda) = \frac{-2}{z^3} + \sum_{n=0}^{\infty} n(n+2) G_{n+3}(\Lambda) z^n$$

When n is odd, $G_n(\Lambda) = 0$ for all lattices Λ, as for any $\omega \in \Lambda\backslash\{0\}$, we have $-\omega \in \Lambda\backslash\{0\}$ with $\omega \neq -\omega$, and hence we may pair off every term in the sum:

$$G_n(\Lambda) = \sum_{\omega\in\Lambda\{0\}} \frac{1}{\omega^n} = \sum_{\pm\omega\in\Lambda\{0\}} \left(\frac{1}{\omega^n} + \frac{1}{(-\omega)^n}\right) = \sum_{\omega\in\Lambda\{0\}} \frac{1}{\omega^n} - \frac{1}{\omega^n} = 0$$

This means every other term in the series expansions for $\wp$ and $\wp'$ vanish.

If we then compute the first few terms of $\wp^3$, $\wp$, and $\wp'^2$, we get:

$$\begin{aligned}
\wp(z)^3 =& \frac{1}{z^6} + \frac{9G_4(\Lambda)}{z^2} + 15G_6(\Lambda) + \dots \\
\wp(z) =& \frac{1}{z^2} + \dots \\
\wp'(z)^2 =& \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda)
\end{aligned}$$

Substituting these expansions into our expression for f, we get that the terms up to order 0 in the Laurent series for f are:

$$\begin{aligned}
f(z) =& \left(\frac{4}{z^6} - 4\cdot\frac{1}{z^6}\right) + \left(-\frac{24G_4(\Lambda)}{z^2} - \frac{36G_4(\Lambda)}{z^2} + 60\frac{G_4(\Lambda)}{z^2}\right) \\
&+ (-80G_6(\Lambda) - 60G_4(\Lambda) + 140G_6(\Lambda)) + \dots \\
=& 0 + \dots
\end{aligned}$$

Thus, f vanishes at zero, and hence equals 0 everywhere.

For item (3), we have shown that $[\wp : \wp' : 1]$ maps into $V_{\mathbb{C}P^2}(W)$. We now must show that it is bijective. We would like to begin by showing that it is injective. First, we need a few lemmas:

Lemma 1.1.10. *Let $z, w \notin \Lambda$. Then $\wp(z) = \wp(w) \Leftrightarrow z \equiv \pm w \bmod \Lambda$.*

Proof. By inspection, $\wp$ is even, so the reverse implication is trivial.

Conceptually, the forwards direction follows from the following geometric argument:

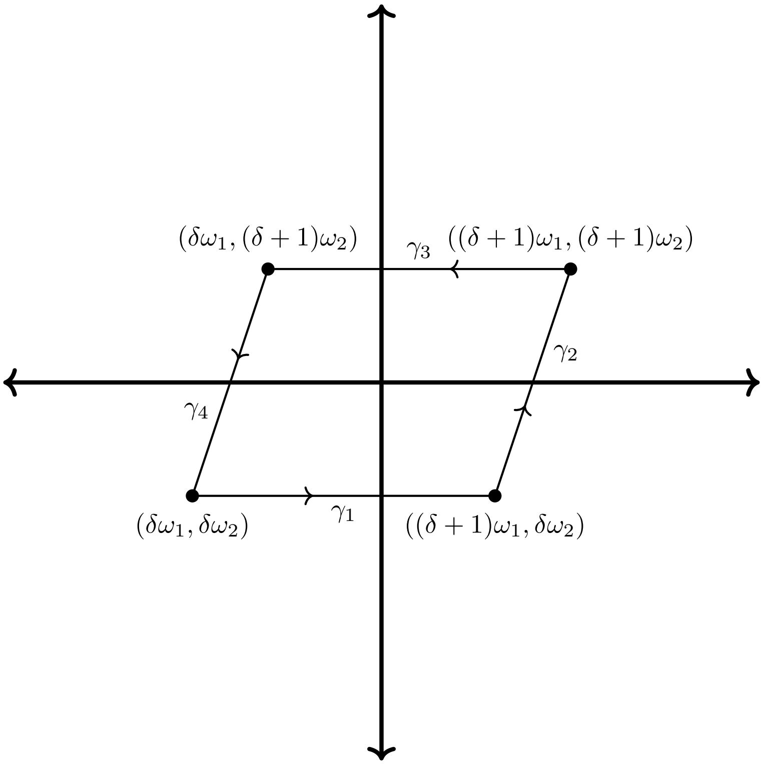
Let $g(z) = \wp(z) - \wp(w)$. Now consider g as a function on $\mathbb{C}/\Lambda$. We have exhibited two zeroes for $g(z)$: $[w]$ and $[-w]$. Furthermore, we know that $\wp(z)$ has a unique pole on $\mathbb{C}/\Lambda$ of order 2. For a rational function of a smooth projective curve, the degree of the associated divisor (that is, the sum of the orders of zeros minus the sum of the orders of poles) is 0, and hence, g has at most two zeros. Thus, $g(z)$ has exactly two zeros: $[w]$ and $[-w]$, meaning $\wp(z) = \wp(w) \Leftrightarrow z = \pm w \bmod \Lambda$. We may also give a more elementary proof using complex analysis.

Suppose $\wp(z) = \wp(w)$. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. For $-1 < \delta < 0$, let $P_\delta = \{s\omega_1 + t\omega_2 \ : \ \delta \leq s, t \leq \delta + 1\}$. Let Γ_δ denote its boundary oriented counterclockwise. Note that $P_\delta/\Lambda = \mathbb{C}/\Lambda$. Furthermore, if $[x] \notin \Gamma$, then x has a unique representative in the interior of P.

Let $g(z) = \wp(z) - \wp(w)$. The zeros and poles of g form a discrete subset of $\mathbb{C}$, and so we may choose δ so that no zeros or poles of g lie on Γ_δ. By the argument principal,

$$\frac{1}{2\pi i} \oint_\Gamma \frac{g'(z)}{g(z)} dz = Z - P$$

where Z and P denote the number of zeros and poles of g in P_δ respectively.


$(\delta\omega_1, (\delta+1)\omega_2)$
γ_3
$((\delta+1)\omega_1, (\delta+1)\omega_2)$
γ_2
γ_4
$(\delta\omega_1, \delta\omega_2)$
γ_1
$((\delta+1)\omega_1, \delta\omega_2)$

As $\wp$ is elliptic for Λ, so is g, and hence $\frac{g'}{g}$. Thus, by the Λ–translation invariance of $\frac{g'}{g}$, we have $\int_{\gamma_1} \frac{g'(z)}{g(z)} dz = -\int_{\gamma_3} \frac{g'(z)}{g(z)} dz$ and $\int_{\gamma_2} \frac{g'(z)}{g(z)} dz = -\int_{\gamma_4} \frac{g'(z)}{g(z)} dz$. Thus, $\oint_\Gamma \frac{g'(z)}{g(z)} dz = 0$, meaning $P = Z$.

We know that the poles of $g(z)$ lie on Λ, and each pole is of order 2. Since $P_\delta \cap \Lambda$ consists of a single point, $P = 2$, meaning $Z = 2$.

If $w \not\equiv -w \bmod \Lambda$, then we may exhibit two zeros of g in P_δ: namely, choose a representatives for $[w]$ and $[-w]$ in P_δ. Thus, again, we conclude that $\wp(z) = \wp(w) \implies z \equiv \pm w \bmod \Lambda$. In particular, this means g has all zeroes of order 1, meaning $\wp'(w) \neq 0$ if $w \not\equiv -w \bmod \Lambda$.

If $w \equiv w' \bmod \Lambda$, then as $g' = \wp'$ is an odd function, we get $\wp'(w) = -\wp'(-w)$, but by Λ–translation invariance, $-\wp'(-w) = -\wp'(w)$, so since $\wp'$ does not have a pole at w, it is forced that $\wp'(w) = 0$. Thus, g has a double zero at w, meaning that the only zero of g in P_δ is the representative for the class $[w] = [-w]$ in P_δ.

Thus, we have shown that $\wp(z) = \wp(w) \implies z \equiv \pm w \bmod \Lambda$, so we are done. □

Note that in the end of the proof, we also showed an important restriction on when $\wp'$ can be zero:

Corollary 1.1.11. *If $w \notin \Lambda$, then $\wp'(w) = 0 \Leftrightarrow 2w \in \Lambda$. In particular, $\wp'$ has three distinct zeros when considered as a function on $\mathbb{C}/\Lambda$.*

With these intermediate results in place, we are now ready to show that $[\wp : \wp' : 1]$ is injective. First note that if $[z] \neq [0]$, then $[\wp([z]) : \wp'([z]) : 1] \neq [0 : 1 : 0] = [\wp([0]), \wp'([0]), 1]$, where this last equality holds since

$\wp'$ has a pole of order 3 at 0, whereas $\wp$ only has a pole of order 2 at 0. Thus, the interesting case is when $[z], [w] \neq [0]$.

Suppose $[z], [w] \neq [0]$ with $\wp([z]) = \wp([w])$ and $\wp'([z]) = \wp'([w])$. By Lemma 1.1.10, $z \equiv \pm w \bmod \Lambda$. If $z \equiv w \bmod \Lambda$, we are done. Suppose that $z \equiv -w \bmod \Lambda$. Then $\wp'(z) = \wp'(-w)$ by Λ–invariance, and $\wp'(-w) = -\wp'(w)$ since $\wp'$ is odd. But by assumption, $\wp'(w) = \wp'(z)$, so $\wp'(z) = -\wp'(z)$, and since $[z] \neq [0]$, it follows that $\wp'(z) = \wp'(w) = 0$. Thus, $2z, 2w \in \Lambda$. In particular, $z \equiv -z \bmod \Lambda$, and hence $z \equiv -w \bmod \Lambda$. Thus, $[\wp : \wp' : 1]$ is injective.

We now wish to show surjectivity. We have already shown that the point at infinity for $V_{\mathbb{C}P^2}(W)$ lies in the image of $[\wp : \wp' : 1]$. Suppose $x, y \in \mathbb{C}$ are such that $W(x, y) = 0$. $\wp$ is meromorphic and nonconstant, it is a surjection from $\mathbb{C}/\Lambda$ to $\mathbb{C}P^1$. Thus, there is $z_0 \in \mathbb{C}/\Lambda$ so that $\wp(z_0) = x$. Now there are two cases: either $y = 0$, in which case, it is forced that $\wp'(z_0) = 0$ and we are done, or $y \neq 0$. In this latter case, it is possible that $\wp'(z_0) \neq y$, but rather $\wp'(z_0) = -y$. In this case, setting $z = -z_0$, we get $[\wp(z) : \wp'(z) : 1] = [x : y : 1]$, meaning $[x : y : 1]$ lies in the image of $[\wp : \wp' : 1]$. Thus, $[\wp : \wp' : 1]$ is bijective, showing (3). □

We have seen now that the Weierstrass $\wp$–function and its derivative are particularly important instances of elliptic functions, making clear that every complex torus is biholomorphic to the solution set of a Weierstrass e quation of the form $y^2 = x^3 - g_2(\Lambda)x - g_3(\Lambda)$. One may wonder if (up to an affine change of variables) every Weierstrass equation is equivalent to one arising from a lattice. In fact, this is the case. It is a general fact that two Weierstrass equations are related by an affine change of coordinates (over an algebraically closed field) if and only if a quantity called the *j–invariant* is the same for both equations. The j–invariant of $y^2 = x^3 - g_2(\Lambda)x - g_3(\Lambda)$ is $1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda^2)}$, which we will see is related to a nonconstant meromorphic function $j(z)$. Any nonconstant meromorphic function is surjective, and hence, we will see that for any Weierstrass equation, one can cook up a corresponding lattice.

One may wonder if there are any other significant elliptic functions. This is essentially not the case.

Proposition 1.1.12. *Every elliptic function is a rational function in $\wp$ and $\wp'$.*

One may prove this using the Riemann–Roch theorem, using crucially the fact that $\wp$ and $\wp'$ have unique poles at [0] of orders 2 and 3 respectively. This may also be done manually using a denominator clearing argument. As this fact is not essential for our exposition, we shall direct the curious reader to [2, Section A.3].

Another important corollary of the differential equation for $\wp$ and its Laurent series expansion is the following:

Lemma 1.1.13. *$G_{2n}(\Lambda)$ is a polynomial (with rational coefficient) in $G_4(\Lambda)$ and $G_6(\Lambda)$ independent of Λ.*

Proof. This proof also comes from [1, Lemma 10.12]. Intuitively speaking, we get such a relationship in the following way: up to scaling, the numbers $G_{2n}(\Lambda)$ are the coefficients in the Laurent series expansion of $\wp(z; \Lambda)$. Moreover, $\wp$ satisfies a nice differential equation. Such differential equations encode recursions in for the Laurent series coefficients, so the values of $G_{2n}(\Lambda)$ for all n should be fully determined by the values for a few small n. Let us now make this precise:

Let $a_n := (2n+1)G_{2n+2}(L)$. As $\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$, we may differentiate with respect to z once more to get $\wp''(z) = 6\wp(z)^2 - (1/2)g_2(\Lambda)$. Substituting in the Laurent series expansion for $\wp$, and comparing the coefficients for each power of z, we get

$$2n(2n-1)a_n = 6\left(2a_n + \sum_{i=1}^{n-2} a_i a_{n-1-i}\right).$$

After rearranging a bit, we get

$$(2n+3)(n-2)a_n = 3\sum_{i=1}^{n-2} a_i a_{n-1-i}$$

and hence an induction argument shows each a_n is a polynomial in a_1 and a_2, thus proving the desired result. □

1.2 Complex multiplication

We have now have a basic appreciation for connection between elliptic curves, complex tori, and lattices. However, the elliptic curves of primary interest to us have a special additional property called complex multiplication. In this section, we will define complex multiplication, and see how it is a fairly restrictive property.

Note that $\mathrm{End}(\Lambda)$ depends only on the homothety class of Λ, so normalizing Λ to be $\mathbb{Z} \oplus \omega_1\mathbb{Z}$, we see that for any $\alpha \in \mathrm{End}(\Lambda)$, $\alpha \cdot 1 \in \Lambda$, so $\mathrm{End}(\Lambda) \subseteq \Lambda$ (for normalized Λ). In particular, as a group, $\mathrm{End}(\Lambda)$ is free abelian of rank at most 2 (and at least 1, as you may always scale by an integer). Unless otherwise stated, every lattice will take this normalization.

Definition 1.2.1. *We say that a lattice Λ has complex multiplication (CM) by a ring $\mathcal{O}$ if $\mathcal{O} \subseteq \operatorname{End}(\Lambda)$ where $\mathcal{O}$ is larger than $\mathbb{Z}$. We will say that Λ has full complex multiplication by $\mathcal{O}$ if $\mathcal{O} = \operatorname{End}(\Lambda)$.*

We ma similarly define CM for elliptic curves, either by appealing to the equivalence of categories, or directly:

Definition 1.2.2. *We say that an elliptic curve E has complex multiplication (CM) by a ring $\mathcal{O}$ if $\mathcal{O} \subseteq \operatorname{End}(E)$ where $\mathcal{O}$ is larger than $\mathbb{Z}$. We will say that E has full complex multiplication by $\mathcal{O}$ if $\mathcal{O} = \operatorname{End}(E)$.*

If Λ has CM, we its endomorphism ring belongs to a fairly restrictive class of rings: it is *imaginary quadratic order.*

Proposition 1.2.3. *If Λ has CM, then $\operatorname{End}(\Lambda)$ is a finite index subring of $\mathcal{O}_{\mathbb{Q}[\sqrt{-d}]}$ for some $d \in \mathbb{N}$.*

Proof. Since $\mathcal{O} := \operatorname{End}(\Lambda) \neq \mathbb{Z}$, we know that $\operatorname{End}(\Lambda)$ is a rank 2 $\mathbb{Z}$–module, so in particular it is a sublattice of Λ. In particular, $\mathcal{O} = [1, \alpha]$. As $\alpha^2 \in \mathcal{O}$, we may represent α^2 as a $\mathbb{Z}$–linear combination of 1 and α. That is, $\alpha^2 - n\alpha - m = 0$ for some integers n, m, meaning α is a quadratic integer. Furthermore, $\mathcal{O} \cap \mathbb{R} \subseteq \Lambda \cap \mathbb{R} = \mathbb{Z}$, so α must be imaginary. Thus, $\mathcal{O}$ is a subring and a sublattice of a ring of integers for some imaginary quadratic field. Every sublattice is of finite index in its ambient lattice, so $[\mathcal{O}_{\mathbb{Q}[\sqrt{-d}]} : \mathcal{O}] < \infty$, and we are done. □

Our main goal in this section will be to establish the following correspondence:

Theorem 1.2.4. *There is an correspondence between*

1. *Ideal classes in $\mathcal{O}$;*
2. *Lattices with full complex multiplication $\mathcal{O}$ (up to homothety);*
3. *Elliptic curves over $\mathbb{C}$ with full complex multiplication $\mathcal{O}$ (up to isomorphism).*

By the equivalence of categories, we already have a correspondence between (2) and (3). If $\mathcal{O}$ is integrally closed, it is fairly quick to show that there is a bijection between (1) and (2) as well:

Proof of Theorem 1.2.4 when $\mathcal{O}$ is integrally closed. Let $L_{\mathcal{O}}$ denote the set of homothety classes of lattices with full CM by $\mathcal{O}$. We wish to define a map $f : L_{\mathcal{O}} \to Cl(\mathcal{O})$ (where $Cl(\mathcal{O})$ denotes the class group of $\mathcal{O}$) which is bijective.

Fix a class $[\Lambda] \in L_{\mathcal{O}}$, and let $\Lambda = [1, \alpha]$. We have shown earlier that $\mathcal{O} \subseteq \Lambda$, and observed that sublattices are always of finite index. Thus, let $n = [\Lambda : \mathcal{O}]$. Then $n\Lambda \subseteq \mathcal{O}$, and $n\Lambda$ is naturally an $\mathcal{O}$–submodule of $\mathcal{O}$ – that is, an ideal of $\mathcal{O}$. We will then let $f([\Lambda])$ be the ideal class of $n\Lambda$.

First we show that f is well defined. Suppose $[\Lambda] = [\Lambda']$ with Λ, Λ' both normalized. Let $\Lambda = [1, \alpha]$, $\Lambda' = [1, \alpha']$. Since Λ, Λ' are homothetic, there is β so that $\beta \cdot 1 \in \Lambda$ and $\beta \cdot \alpha' \in \Lambda$. In particular, $\beta \in \Lambda$, and hence $\beta \in \operatorname{Frac}(\mathcal{O})$. Thus, the ideals corresponding to Λ and Λ' differ by a scaling factor in $\operatorname{Frac}(\mathcal{O})$, so their ideal classes are the same.

If we consider a fixed embedding of $\operatorname{Frac}(\mathcal{O})$ into $\mathbb{C}$, we may see fractional ideals as lattices in $\mathbb{C}$. From this, it is clear that f is injective. For any ideal I in the ideal class $f([\Lambda])$, we have constructed I to be homothetic to Λ, so $f([\Lambda]) = f([\Lambda']) \implies [\Lambda] = [\Lambda']$.

To show that f is surjective, fix an ideal class $[I] \in Cl(\mathcal{O})$, and an ideal I representing that class. Since I is finite index in $\mathcal{O}$, it is a sublattice. Then $\mathcal{O} \subseteq \operatorname{End}(I)$, as ideals are closed under multiplication in the ambient ring. Furthermore, $\operatorname{End}(I)$ is a quadratic order as previously shown. But since $\mathcal{O}$ is integrally closed, it is a maximal order (that is, it is not the proper ring of any quadratic order), meaning that $\operatorname{End}(I) = \mathcal{O}$. That is, $\mathcal{O}$ has full complex multiplication by $\mathcal{O}$. Since $f([I])$ is the ideal class corresponding to I, it follows that f is surjective. □

A general proof, however, requires us to make sense of $Cl(\mathcal{O})$ when $\mathcal{O}$ is not integrally closed. A fuller treatment of quadratic orders may be found in [1, Chapter 7], from which the following proofs and definitions are taken.

Definition 1.2.5. *A fractional $\mathcal{O}$–ideal is a nonzero $\mathcal{O}$–submodule I of Frac($\mathcal{O}$) such that there is $\lambda \in \mathcal{O}^\times$ so $\lambda I \subseteq \mathcal{O}$.*

Just as with traditional fractional ideals, one may multiply fractional ideals in the obvious way:

$$IJ = \{\sum i_n j_n \ : \ i_n \in I, j_n \in J\}$$

Furthremore, we may regard fractional $\mathcal{O}$–ideals as lattices in $\mathbb{C}$ after fixing an embedding of $\operatorname{Frac}(\mathcal{O})$ in $\mathbb{C}$.

Definition 1.2.6. *A fractional $\mathcal{O}$–ideal I is called* proper *if $\operatorname{End}(I) = \mathcal{O}$ where $\operatorname{End}(I)$ are the endomorphisms of I as a lattice.*

Definition 1.2.7. *A fractional $\mathcal{O}$–ideal I is called* invertible *if there is a fractional ideal J so that $IJ = \mathcal{O}$.*

Lemma 1.2.8. *A fractional $\mathcal{O}$–ideal I is proper if and only if it is invertible.*

Proof. Suppose I is invertible. We wish to show it is proper. All $\mathcal{O}$–ideals have CM by $\mathcal{O}$, so we just need to show that it has no more endomorphisms. Let $\alpha \in \mathrm{End}(I)$ and J be a fractional ideal so that $IJ = \mathcal{O}$. Then $\alpha \in \alpha(\mathcal{O}) = \alpha(IJ) = (\alpha I)J \subseteq IJ = \mathcal{O}$, so $\alpha \in \mathcal{O}$, and we are done.

The reverse implication is a bit more involved, and we first require a small lemma.

Lemma 1.2.9. *Let τ be a quadratic algebraic number with minimal polynomial ax^2+bx+c, with $\gcd(a,b,c) = 1$. Note that $a\tau$ is a quadratic integer. Then the lattice $I := [1, \tau]$ is a proper fractional ideal of $\mathcal{O} := [1, a\tau]$.*

Proof. It is clear that $\mathcal{O} \subseteq \mathrm{End}(I)$. Suppose $\beta \in \mathrm{End}(I)$. That means $\beta \in I$ and $\tau\beta \in I$, i.e. $\beta = m + n\tau$ and $\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c)$. As $\frac{-bn}{a}, \frac{-cn}{a} \in \mathbb{Z}$, it follows that $a|bn$ and $a|cn$. But $\gcd(a,b,c) = 1$, so this can only happen if $a|n$. In particular, $m + n\tau \in [1, a\tau] = \mathcal{O}$, so $\mathrm{End}(I) = \mathcal{O}$. □

With this lemma in place, we may now prove the forwards implication. Suppose I is proper. Normalize I to be of the form $I = [1, \tau]$, and let $ax^2 + bx + c$ be the minimal polynomial of τ with $\gcd(a,b,c) = 1$. As I is proper, $\mathcal{O} = [1, a\tau]$ by the above lemma. Let $\beta \to \beta'$ denote the nontrivial automorphism of $\mathrm{Frac}(\mathcal{O})$. Then τ' is the other root of $ax^2 + bx + c$, and the above lemma shows that $J := [1, \tau']$ is also a proper $\mathcal{O}$–fractional ideal. We now compute aIJ:

$$aIJ = [a, a\tau, a\tau', a\tau \cdot \tau'] = [a, a\tau, a\tau', a\tau\tau']$$

Since $\tau\tau' = c/a$ and $\tau + \tau' = b/a$, this is just

$$[a, a\tau, b, c] = [1, a\tau] = \mathcal{O}$$

where this second equality follows from the fact that $\gcd(a,b,c) = 1$. Thus, I is invertible with inverse aJ, concluding the proof.

□

Definition 1.2.10. *The ideal class group $Cl(\mathcal{O})$ of an imaginary quadratic order $\mathcal{O}$ is the group of invertible fractional ideals modulo the subgroup of principal fractional ideals $\{\alpha\mathcal{O} \;:\; \alpha \in Frac(\mathcal{O})\}$.*

The general proof of Theorem 1.2.4 then follows completely analogously to the integrally closed case. To show that f is well–defined, we require the forwards implication of Lemma 1.2.8. To show the surjectivity of f, we also needed that the fractional ideals representing classes in $Cl(\mathcal{O})$ have full CM by $\mathcal{O}$, which is the reverse implication of Lemma 1.2.8. Aside from these appeals to the above lemma, everything follows mutatis mutandis, and so we omit a second proof.

Chapter 2

Modular j-function and the modular equation

In the last section, we introduced the modular parameterization of elliptic curves, which realizes an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the Weierstrass $\wp$ function and its derivative. This gives rise to the Weierstrass equation of an elliptic curve E associated to a lattice Λ:

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{2.1}$$

We can then define the *modular discriminant* as

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

One can check that the RHS of 2.1 has 3 distinct roots (following from Corollary 1.1.11 and Theorem 1.1.9), and hence $\Delta \neq 0$. With this, we can define the j-invariant of Λ (equivalently, of E) as

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

Theorem 2.0.1. *The j-invariant classifies lattices up to homothety (equivalently, elliptic curves up to isomorphism).*

Proof. First, we see that $G_n(\Lambda)$ is a homogeneous function of degree $-2n$ for each n. Comparing degrees, we find that j is homogeneous of degree 0, so it takes the same values on proportional lattices. For the converse, suppose $j(\Lambda) = j(\Lambda')$. We will show the case for $g_2(\Lambda'), g_3(\Lambda') \neq 0$ here, but the others are similar.

Our first goal is to find γ so that $g_n(\Lambda) = g_n(\gamma\Lambda')$ for $n = 2, 3$.

Pick γ such that

$$\gamma^4 = \frac{g_2(\Lambda)}{g_2(\Lambda')}.$$

Using that $j(\Lambda) = j(\Lambda')$, we find

$$\gamma^{12} = \left(\frac{g_3(\Lambda)}{g_3(\Lambda')}\right)^2,$$

so

$$\gamma^6 = \pm\frac{g_3(\Lambda)}{g_3(\Lambda')}.$$

Up to replacing γ with $i\gamma$, we may assume the sign is positive, and we are done with this initial step, since $g_n(\Lambda) = \gamma^{2n}g_n(\Lambda') = g_n(\gamma\Lambda')$.

We may now apply Lemma 1.1.13 to conclude that $G_n(\Lambda) = G_n(\gamma\Lambda')$ for all n. But by the Laurent series expansion for $\wp(z;\Lambda)$, this means $\wp(z;\Lambda) = \wp(z;\gamma\Lambda')$. Since the poles of $\wp(z;\Lambda)$ are precisely located at Λ, we conclude that $\Lambda = \gamma\Lambda'$, so we are done.

□

Remark. *First, note that given $\tau \in \mathbb{H}$, we have a lattice $\Lambda_\tau := [1, \tau]$ so we may define a map $j\colon \mathbb{H} \to \mathbb{C}$ via*

$$j(\tau) := j(\Lambda_\tau).$$

Further, any lattice Λ is homothetic to Λ_τ for some $\tau \in \mathbb{H}$; one first fixes a "positive basis" $[\omega_1, \omega_2]$ such that $Im(\omega_2/\omega_1) > 0$ so then if $\Lambda = [\omega_1, \omega_2]$, then $\omega_1^{-1}\Lambda = \Lambda_\tau$ for $\tau \in \mathbb{H}$.

Moreover, we claim that $[1,\tau] \cong [1,\tau']$ iff $\tau' = \gamma\tau$ for $\gamma \in SL_2(\mathbb{Z})$. First, suppose Λ_τ and $\Lambda_{\tau'}$ are homothetic. Then there is a $\alpha \in \mathbb{C}^\times$ such that $\Lambda_\tau = \gamma\Lambda_{\tau'}$. Thus $\{\alpha, \alpha\tau\}$ and $\{1,\tau'\}$ are bases for the same lattice. Then

$$1 = a\alpha + b\alpha\tau = \alpha(a+b\tau) \quad \textit{and} \quad \tau' = c\alpha + d\alpha\tau = \alpha(c+d\tau),$$

$$\tau' = \frac{\alpha(a+b\tau)}{\alpha(c+d\tau)} = \gamma\tau, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Note that γ is invertible since it is a change-of-basis matrix, and one can show $\det(\gamma) > 0$ as $\tau, \tau' \in \mathbb{H}$, so $\gamma \in SL_2(\mathbb{Z})$ as desired. For the converse, one can find α via the ratios $1/a + b\tau$ and $\tau'/c + d\tau$.

We will not show that j is holomorphic, but the above shows that j is modular of weight 0.

We will additionally use that the Fourier expansion of $j(\tau)$ is

$$j(\tau) = q^{-1} + 744 + O(q),$$

where $q = e^{2\pi i\tau}$. Further, we will use that this Fourier expansion has integer coefficients.

Remark. *As seen in Spencer's section, g_2 and g_3 are the normalized Eisenstein series of weight 4 and 6 respectively. Further, Δ is in the same way a modular form of weight 12.*

Proposition 2.0.2. *Every holomorphic modular function is a polynomial in j.*

Proof. Suppose $f(\tau)$ is a w.h.m.f., in particular f is meromorphic at infinity. Then the prinicipal part of its Fourier expansion is a polynomial in q^{-1}. Let this polynomial be $P(\omega)$. Then $f(\tau) = P(j(\tau))$ is holomorphic at ∞. Analogous to the fact that everywhere holomorphic elliptic functions are constant, a modular function which is holomorphic at infinity must be constant, thus we are done. □

Definition 2.0.3. *For $m \geq 1$, define $\Gamma_0(m) \subset SL_2(\mathbb{Z})$ to be subgroup of matrices which become upper triangular mod m.*

Fact: finite index. In the case where p prime, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$.

Definition 2.0.4. *A weakly holomorphic modular function on level m is a function $f\colon \mathbb{H} \to \mathbb{C}$ such that:*

- *f is holomorphic on $\mathbb{H}$*
- *$f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma_0(m)$*
- *f is meromorphic at the cusps of $\Gamma_0(m)$ (cusps are the points added to compactify the modular curve $Y_0(m) := SL_2(\mathbb{Z})\backslash\mathbb{H}$)*

Example 2.0.5. *$j(m\tau)$ is a weakly holomorphic modular function on level m.*

One can see invariance by considering $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(m)$. Then $\gamma' = \begin{bmatrix} a & mb \\ c/m & d \end{bmatrix} \in SL_2(\mathbb{Z})$, and it is easy to show

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

where the last equality follows from the $SL_2(\mathbb{Z})$-invariance of j. Then holomorphicity and growth conditions follow from the analogous properties of j.

Definition 2.0.6. *For $m \geq 1$, define*

$$\varphi_m(X,\tau) := \prod_{i=1}^{[\Gamma_0(m):SL_2(\mathbb{Z})]} (X - j(\gamma_i m\tau)),$$

where the γ_i are a complete set of coset representatives for $\Gamma_0(m)$.

Claim: this construction is independent of the choice of coset representatives. That is, each function $j(\gamma_i m\tau)$ is $\Gamma_0(m)$-invariant. The argument is equivalent to that which shows $j(m\tau)$ is a w.h.m.f. of level m.

Example 2.0.7. *$\tau = i,\ m = 2$:*

$$\varphi_2(X,i) = (X - j(2i))(X - j(i/2))(X - j((i+1)/2))$$

Proposition 2.0.8. *φ_m is a polynomial in X and $j(\tau)$.*

Proof. First, note that the coefficient of X^k in φ_m is a symmetric polynomial in the $j(\gamma_o m\tau)$. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, note that $\tau \mapsto \gamma\tau$ permutes the cosets represented by $j(\gamma_i m\tau)$. Thus the coefficient of X^k is $\mathrm{SL}_2(\mathbb{Z})$-invariant. Then one analyzes the q-expansions of $j(\gamma_i m\tau)$ to determine that these coefficients are holomorphic on $\mathbb{H}$ and are meromorphic at ∞. Thus, they are polynomials in $j(\tau)$ by Proposition 3.0.2. □

Remark. *We then define $\Phi_m(X, j) := \varphi_m(X, \tau)$. We call Φ_m the mth modular equation.*

Proposition 2.0.9. *If Λ is some lattice and λ is a cyclic sublattice of index m (i.e. $\Lambda/\lambda \cong \mathbb{Z}/m\mathbb{Z}$), then $\Phi_m(j(\lambda), j(\Lambda)) = 0$.*

Proof. Since lattices are just rank 2 free $\mathbb{Z}$-modules, there exists a positive basis $\{\omega_1, \omega_2\}$ of Λ and such that $\{\omega_1, m\omega_2\}$ is a basis for λ. Then if $\tau = \omega_2, \omega_1$, $j(\Lambda) = j(\tau)$ and $j(\lambda) = j(m\tau)$. Then the claim is proven observing that 1 is a coset representative for $\Gamma_0(m)$. □

Example 2.0.10. $\Lambda = [1, i], m = 2$*:*

Theorem 2.0.11. *Let m be a positive integer.*

1. $\Phi_m(X, j) \in \mathbb{Z}[X, j]$.
2. $\Phi_m(X, j)$ *is irreducible as a polynomial in* X.
3. $\Phi_m(X, j) = \Phi_m(j, X)$ *for* $m > 1$.
4. *If m is not a perfect square, then Φ_m has leading coefficient ± 1.*
5. *(Kronecker's Congruence) If p is prime,*

$$\Phi_p(X, j) \equiv (X^p - j)(X - j^p) \bmod p\mathbb{Z}[X, j].$$

Proof. We give a proof of (1) and (2) here:

1. We only give the proof for p prime. Note that $j(\tau) \in \mathbb{Q}((q))$, so $j(p\tau) \in \mathbb{Q}((q))$ as $e^{2\pi i p\tau} = q^m \in \mathbb{Q}((q))$. Now we need to see where $j(p\gamma_k\tau)$ lives. We have

$$e^{2\pi i\gamma_k\tau} = e^{2\pi i\left(\frac{\tau+k}{p}\right)} = e^{2\pi i\tau/p}e^{2\pi ik/p} = q^{1/p}\zeta_p^k,$$

   so $j(p\gamma_k\tau) \in \mathbb{Q}(\zeta_p)((q))$. Now consider the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ on the coefficient of X^k in $\Phi_p(X, j)$ by acting on the fourier coefficients of the $j(p\gamma_k\tau)$. One can see this action permutes the $j(p\gamma_k\tau)$ and fixes $j(p\tau)$ by the above calculation, so the coefficient of X^k as a symmetric polynomial in these arguments must be fixed. Thus, it lies in $\mathbb{Q}$. Further, recall that the coefficients of $j(\tau)$ are in $\mathbb{Z}$, so the coefficients of the $j(p\gamma_k\tau)$ are algebraic integers. Thus, the coefficient of X^k must actually be in $\mathbb{Z}((q))$ as desired.

2. Note that the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(m)]$ gives an upper bound on the degree of the extension $\mathbb{C}(j(\tau), j(m\tau))$ over $\mathbb{C}(j(\tau))$. Equality will imply that $\mu_{j(m\tau),\mathbb{C}(j(\tau)}(X) = \Phi_m(X, j(\tau)$ and hence Φ_m irreducible. Now for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, define

$$\varphi_\gamma \colon \mathbb{C}(j(\tau), j(m\tau)) \to \mathbb{C}((\tau))$$

   via $\varphi_\gamma(f)(\tau) = f(\gamma\tau)$. This is an embedding of the field of modular functions on $\Gamma_0(m)$ into the field of formal Laurent series. Note that this map fixes $\mathbb{C}(j(\tau))$, since $j(\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. The number of distinct embeddings equals the degree of $\mathbb{C}(j(\tau), j(m\tau))$ over $\mathbb{C}(j(\tau))$, and we know that $j(\gamma_i m\tau) = j(\gamma_j m\tau)$ if and only if $i = j$. Thus, we are done.

□

For the main theorem of this section, we need to describe the equivalent notion of a cyclic sublattice in terms of fractional ideals.

Definition 2.0.12. *Given an order $\mathcal{O}$, we say a proper $\mathcal{O}$-ideal is primitive if it is not of the form $d\mathfrak{a}$ where $d > 1$ is an integer and $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal. We say $\alpha \in \mathcal{O}$ is primitive if the principal ideal it generates is.*

Claim: Given $\mathfrak{b}$ a proper fractional $\mathcal{O}$-ideal and $\mathfrak{a}$ a proper $\mathcal{O}-$ideal, then $\mathfrak{a}\mathfrak{b}$ is a cyclic sublattice of $\mathfrak{b}$ of index $N(\mathfrak{a})$ if and only if $\mathfrak{a}$ is primitive.

Theorem 2.0.13. *Let $\mathcal{O}_K$ be the maximal order in an imaginary quadratic field K, $\mathfrak{a}$ a proper fractional $\mathcal{O}_K$–ideal. Then $j(\mathfrak{a})$ is an algebraic integer.*

Proof. Let $\alpha \in \mathcal{O}_K$ be primitive such that $\alpha\mathfrak{a}$ is a cyclic sublattice of index $m := N(\alpha)$. Since $\mathfrak{a}$ has CM by $\mathcal{O}$, we have $j(\alpha\mathfrak{a}) = j((a))$ and

$$\Phi_m(j(\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0,$$

proving $j(\mathfrak{a})$ is algebraic. By Proposition 3.0.6, so long as we can choose α such that $N(\alpha)$ is not a perfect square, $j(\mathfrak{a})$ is an algebraic integer by the same argument. One can show the existence more generally using the tools of the next section, but for our use it suffices to pick $\alpha = 1 + i$ for $\mathbb{Q}(i)$ and $\alpha = \sqrt{-d}$ for $\mathbb{Q}(\sqrt{-d})$ with $d > 1$ squarefree. One finds the norms to be 2 and d respectively. $\square$

Chapter 3

The first fundamental theorem of complex multiplication

3.1 Some basic facts about Algebraic Number Theory

Notation.
For a number fields $K \subset L$, let us take
$\mathcal{O}_K$*:=Ring of integers of K.*
$\mathcal{P}_K$*:=Set of all non-zero prime ideals of $\mathcal{O}_K$.*
P_K*:=Set of all non-zero principal ideals of $\mathcal{O}_K$.*
$\mathrm{Spl(L|K)} := \{$*primes in K splitting completely in L*$\}$
$\mathcal{P}_{K,\mathbb{Q}} := \{\mathfrak{p} \in \mathcal{P}_K : f(\mathfrak{p}|p) = 1\}$
$\mathrm{Spl}_{\mathbb{Q}}\mathrm{(L|K)} = \mathrm{Spl(L|K)} \cap \mathcal{P}_{\mathrm{K},\mathbb{Q}}$
For sets S, T, we write $S \dot{\subset} T$ to denote the fact that $S \backslash T$ is a finite set. We write $S \doteq T$ if $S \dot{\subset} T$ and $T \dot{\subset} S$.

Facts. *(from last time)*

- *Let Λ, Λ' be two lattices such that $\Lambda/\Lambda' \cong \mathbb{Z}/p\mathbb{Z}$, then*
$$\Phi_p(j(\Lambda), j(\Lambda')) = 0.$$
- *Kronecker's congruence:*
$$\Phi_p(X, j) \equiv (X^p - j)(X - j^p) \pmod{p\mathbb{Z}[X, j]}.$$

Let L/K be a Galois extension and $\mathfrak{P}$ be a prime in L lying above $\mathfrak{p}$. Let l and k be the respective residue fields. Let $G(\mathfrak{P})$ be the decomposition group. We have a surjective map
$$G(\mathfrak{P}) \twoheadrightarrow \mathrm{Gal}(l/k).$$
It's kernel is called inertia group, $I(\mathfrak{P})$. If $\mathfrak{p}$ is unramified in L, then inertia group is trivial and we have a unique element in $G(\mathfrak{P})$ that goes to Frobenius automorphism of $\mathrm{Gal}(l/k)$, we call it Frobenius element and denote it by $\mathrm{Fr}(\mathfrak{P}/\mathfrak{p})$ (and by $\mathrm{Fr}(\mathfrak{p})$ if extension is abelian).

Proposition 3.1.1. *Let L/K be a finite Galois extension with Galois group G.*

- *if $\mathfrak{p} \in \mathcal{P}_K$ is unramified in L then the Frobenius automorphisms $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p})$ for all primes $\mathfrak{P} \in \mathcal{P}_L$ lying above $\mathfrak{p}$ form a conjugacy class in G.*
- *$\mathfrak{p} \in \mathcal{P}_K$ splits completely in L if and only if it is unramified and $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p})$ is trivial for some (equivalently, any) prime $\mathfrak{P} \in \mathcal{P}_L$ lying above $\mathfrak{p}$.*

Furthermore, if $K \subset L \subset M$ be a tower of finite extensions such that both L/K and M/K are Galois extensions with $\mathfrak{p} \subset \mathfrak{P}_L \subset \mathfrak{P}_M$, then $\mathrm{Fr_{M/K}(\mathfrak{P}_M|\mathfrak{p})|_L} = \mathrm{Fr_{L/K}(\mathfrak{P}_L|\mathfrak{p})}$.

If $[K : \mathbb{Q}] = m$ then for each prime p, there is atmost m primes $\mathfrak{p} \subset \mathcal{P}_K$ lying above p, and for each of them the norm $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is a power of p. It follows that
$$\sum_{\mathfrak{p}|p} N(\mathfrak{p})^{-s} \leq mp^{-s}.$$
So using generalized harmonic series, it can be shown that $\sum_{\mathfrak{p}\in\mathcal{P}_K} N(\mathfrak{p})^{-s}$ converges for Re(s) > 1, and hence convergence of a similar series for any subset $S \subset \mathcal{P}_K$.

Definition 1 (Dirichlet density)**.** *Given a subset $S \subset \mathcal{P}_K$, its Dirichlet density is defined by*

$$\delta(S) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s}},$$

provided that the limit exists.

Remarks.
1)Since we know that

$$\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s} \to \infty \text{ as } s \to 1^+,$$

for any finite set S, $\delta(S) = 0$. In particular, $\delta(S) > 0$ implies that $\#(S)$ is infinite.
2) If we take $S := \{\mathfrak{p} : f(\mathfrak{p}|p) > 1\}$, then we have that

$$\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s} < m \cdot \sum_{p\, prime} p^{-2} < \infty,$$

and hence S has density 0. So we have that $\delta(T) = \delta(T \cap \mathcal{P}_{K,\mathbb{Q}})$ for any subset $T \subset \mathcal{P}_K$.

Theorem 3.1.2 (Chebotarev's density theorem)**.** *Let L/K be a Galois extension with Galois group G, and let $\mathcal{C}$ be a conjugacy class in G. Then the set $\mathcal{P}_K(\mathcal{C})$ of those primes $\mathfrak{p} \in \mathcal{P}$ which are unramified in L and for which $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p}) \in \mathcal{C}$ for some (equivalently, any) $\mathfrak{P}|\mathfrak{p}$, has Dirichlet density equal to $|\mathcal{C}|/|G|$ (in particular, $\mathcal{P}_K(\mathcal{C})$ is infinite).*

Example 3.1.3 (Cyclotomic extension)**.** *Let $L = \mathbb{Q}(\zeta_n)$, be the nth cyclotomic field extension of $K = \mathbb{Q}$. Then $\mathrm{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, so every conjugacy class $\mathcal{C}$ consists of single element. Take $\mathcal{C}_a = \{\sigma_a\}$, where $(a, n) = 1$ and $\sigma_a(\zeta_n) = \zeta_n^a$. For any prime $p \nmid n$, reduction of the polynomial $X^n - 1$ mod p has no multiple roots, which implies that extension L/K is unramified at p. Furthermore,*

$$\sigma_p(\zeta_n) = \zeta_n^p \equiv \mathrm{Fr}_{\mathrm{p}}(\zeta_{\mathrm{n}}) \pmod{\mathfrak{P}},$$

where $\mathfrak{P}|p$, so $\mathrm{Fr}_{\mathrm{p}} = \sigma_{\mathrm{p}}$. We see that in this case

$$\mathcal{P}_K(\mathcal{C}_a) = \{p \,|\, p \nmid n \text{ and } p \equiv a \,(\bmod n)\}.$$

Thus, Chebotarev's density theorem tells us that there are infinitely many primes $\equiv a \pmod{n}$ which is Dirichlet's prime number theorem.

Example 3.1.4. *Let $L = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic extension over $K = \mathbb{Q}$. Then we have that $\mathrm{Gal}(L/K) = \mathbb{Z}/2\mathbb{Z}$. Then*

$$\text{a prime splits} \iff \left(\frac{-d}{p}\right) = 1 \iff \mathrm{Fr(p)} = \mathrm{id}$$

For our purposes, we need another consequence of Chebotarev's Density Theorem which characterizes inclusions between finite extensions of K in terms of the corresponding sets of completely split primes, at least when one of the extensions is Galois.

Theorem 3.1.5. *Let L and M be finite extensions of K. If M/K is a Galois extension then*

$$L \subset M \iff \mathrm{Spl}_{\mathbb{Q}}(\mathrm{M|K}) \dot{\subset} \mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K}).$$

Proof. ($\Longrightarrow$) is clear by the multiplicativity of the ramification index and the residual degree.
($\Longleftarrow$) Pick a finite subset $S \subset \mathcal{P}_{K,\mathbb{Q}}$ such that

$$\mathrm{Spl}_{\mathbb{Q}}(\mathrm{M|K}) \subset \mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K}) \cup \mathrm{S}. \tag{3.1}$$

Let F be a finite Galois extension over K that contains L and M. Assume that $L \not\subset M$. Then there exists a $\sigma \in G := \mathrm{Gal}(F/K)$ that acts trivially on M and not on L, and we can pick $a \in \mathcal{O}_L$ such that $\sigma(a) \neq a$. Since only finitely many primes divide $(\sigma(a) - a)\mathcal{O}_F$, it follows by Chebotarev's density theorem (and the fact if $\sum \subset \mathcal{P}_K$ has positive density then so is true for $\sum \cap \mathcal{P}_{K,\mathbb{Q}}$) that there exists an ideal $\mathfrak{p} \subset \mathcal{P}_{K,\mathbb{Q}} \setminus S$ and $\mathfrak{P} \subset \mathcal{P}_F$ lying above it and unramified in F such that $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p}) = \sigma$ (in particular, $\sigma \in G(\mathfrak{P})$), and $\sigma(a) \not\equiv a \pmod{\mathfrak{P}}$. Since M/K is Galois extension, for the prime ideal $\mathfrak{P}' \in \mathcal{P}_M$ lying below $\mathfrak{P}$, we have that

$$\mathrm{Fr}(\mathfrak{P}'|\mathfrak{p}) = \mathrm{Fr}(\mathfrak{P}|\mathfrak{p})|_{\mathrm{M}} = \sigma|_{\mathrm{M}} = \mathrm{id}_{\mathrm{M}},$$

which implies that $\mathfrak{p}$ splits completely in M, and therefore belongs to $\mathrm{Spl}_{\mathbb{Q}}(\mathrm{M|K})$. On the other hand, let $\mathfrak{P}'' \in \mathcal{P}_L$ be a prime lying below $\mathfrak{P}$. Since the image of $a \in \mathcal{O}_L$ in $\mathcal{O}_L/\mathfrak{P}'' \subset \mathcal{O}_F/\mathfrak{P}$ is not fixed by the action of σ on $\mathcal{O}_F/\mathfrak{P}$ (recall that $\sigma \in G(\mathfrak{P})$), we see that

$$\mathcal{O}_L/\mathfrak{P}'' \neq \mathcal{O}_K/\mathfrak{p}.$$

Hence, we have that $f(\mathfrak{P}''|\mathfrak{p}) > 1$, and therefore $\mathfrak{p}$ does not split completely in in L. This contradicts the inclusion (3.1) and proves the theorem. □

Fact. ***For any number field K, there exists a Maximal abelian unramified extension, $\tilde{K}$, called Hilbert class field.*** *For example, if we take $K = \mathbb{Q}$ then $\tilde{K} = \mathbb{Q}$, since every extension over $\mathbb{Q}$ is ramified.*

Theorem 3.1.6. *Assume the notations as above. Then we have that $Cl(K) \cong \mathrm{Gal}(\tilde{K}/K)$, given by Frobenius element.*

Fact. *Primes $\mathfrak{p}$ in K that split completely in $\tilde{K}$ are exactly the principal ideals.*

Theorem 3.1.7. *A prime $\mathfrak{p} \subset K$ splits completely in $\tilde{K}$ if and only if $\mathfrak{p}$ is principle. In particular, $L = \tilde{K}$ if $\mathrm{Spl}_{\mathbb{Q}}(L|K) \doteq P_K \cap \mathcal{P}_{K,\mathbb{Q}}$.*

3.2 First fundamental theorem of complex multiplication

Let us take $K = \mathbb{Q}(\sqrt{-d})$ (d positive square-free). Consider K as a subfield of $\mathbb{C}$ then $\mathcal{O}_K$ can be thought of as a lattice in $\mathbb{C}$.

Theorem 3.2.1. *Let $\mathfrak{a}$ be a non-zero ideal in the ring of integers $\mathcal{O}_K$. Then $j(\mathfrak{a})$ is an algebraic integer and the field $K(j(\mathfrak{a}))$ coincides with the Hilbert class field $\tilde{K}$.*

Proof. First part already proved.
We now prove that $K(j(\mathfrak{a})) = \tilde{K}$. We will use the following lemma.

Lemma 3.2.2. *Let p be a rational prime that splits completely in K, and let $\mathfrak{p}$ be one of the primes lying above p. Fix a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, and let F be a finite extension of K that contains $j(\mathfrak{a})$ and $j(\mathfrak{a}\mathfrak{p})$. Then for any prime ideal $\mathfrak{P} \subset \mathcal{O}_F$ lying above $\mathfrak{p}$, one of the following two congruences is true:*

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}\mathfrak{p}) \pmod{\mathfrak{P}} \quad \text{or} \quad j(\mathfrak{a}) \equiv j(\mathfrak{a}\mathfrak{p})^p \pmod{\mathfrak{P}}.$$

Proof. Since p splits in K, we have that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. We also have that There exists $\alpha \in \mathcal{O}_K$ such that $\mathfrak{a} = \alpha\mathcal{O}_K + \mathfrak{a}\mathfrak{p}$, and then multiplication by α induces an isomorphism

$$\mathfrak{a}/\mathfrak{a}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}.$$

So we get that

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a}\mathfrak{p})) = 0.$$

Using Kronecker's congruence, we obtain

$$(j(\mathfrak{a}\mathfrak{p})^p - j(\mathfrak{a}))(j(\mathfrak{a}\mathfrak{p}) - j(\mathfrak{a})^p) \equiv 0 \pmod{\mathfrak{P}}.$$

□

Remark. *This ambiguity in congruence relation can be resolved. We always have $j(\mathfrak{a}) \cong j(\mathfrak{p}\mathfrak{a}) \pmod{\mathfrak{P}}$ or equivalently, $j(\mathfrak{a})^p \cong j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{P}}$. This also explains how $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p})$ acts on these elements. If we consider the representatives of class group of K, $\mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_h$, then $\mathrm{Fr}(\mathfrak{P}|\mathfrak{p})$ permutes them, and adjoining one of them to K adjoins all of them.*

Fix a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and set $L = K(j(\mathfrak{a}))$. By Theorem 3.1.7, $L = \tilde{K}$ if and only if $\mathrm{Spl}_{\mathbb{Q}}(L|K) \doteq P_K \cap \mathcal{P}_{K,\mathbb{Q}}$. Since $\mathcal{O}_K[j(\mathfrak{a})]$ contains a basis of $L/\mathbb{Q}$, the index, $N := [\mathcal{O}_L : \mathcal{O}_K[j(\mathfrak{a})]]$, is finite. Set

$$S := \{\mathfrak{p} \in \mathcal{P}_{K,\mathbb{Q}} \,|\, \mathfrak{p} \text{ divides } N \text{ or } \mathfrak{p} \text{ ramifies in } L\}.$$

We claim that

$$\mathrm{Spl}_{\mathbb{Q}}(\tilde{K}|K) \setminus S = P_K \cap \mathcal{P}_{K,\mathbb{Q}} \setminus S \subset \mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K}). \tag{3.2}$$

Suppose that $\mathfrak{p} \in P_K \cap \mathcal{P}_{K,\mathbb{Q}} \setminus S$, and let p be the corresponding prime in $\mathbb{Q}$. Since $\mathfrak{p}$ is unramified in L, to prove that $\mathfrak{p} \in \mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K})$, we need to show that for any prime $\mathfrak{P}$ lying above p, we have that $\mathcal{O}_L/\mathfrak{P} = \mathcal{O}_{\mathbb{Q}}/p = \mathbb{Z}/p\mathbb{Z}$ which is equivalent to showing that the Frobenius automorphism acts on $\mathcal{O}_L/\mathfrak{P}$ trivially, in other words,

$$a^p \equiv a \pmod{\mathfrak{P}} \text{ for all } a \in \mathcal{O}_L. \tag{3.3}$$

By construction, $\mathfrak{p}$ is principal, say $\mathfrak{p} = (\pi)$. Then $j(\mathfrak{a}\mathfrak{p}) = j(\mathfrak{a}\pi) = j(\mathfrak{a})$, so it follows from Lemma 3.2.2 that

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}.$$

Furthermore, since $\mathfrak{p} \in \mathcal{P}_{K,\mathbb{Q}}$, we have that $f(\mathfrak{p}|p) = 1$, and therefore $a^p \equiv a \pmod{\mathfrak{P}}$ for all $a \in \mathcal{O}_K$. So we have that (3.3) is true for all $a \in \mathcal{O}_K[j(\mathfrak{a})]$. Which in turn proves that (3.3) is true on $\mathcal{O}_L$ since for any $a \in \mathcal{O}_L$, $N \cdot a \in \mathcal{O}_K[j(\mathfrak{a})]$, $N^p \equiv N \pmod{\mathfrak{P}}$, and $\mathfrak{p}$ is coprime to N so we get

$$N \cdot a^p (N \cdot a)^p \equiv N \cdot a \pmod{\mathfrak{P}}.$$

Which proves our claim.

As the class number of K is finite, we can pick a finite set of representatives $\mathfrak{c}_1, \mathfrak{c}_2, .., \mathfrak{c}_h$ of all ideal classes. Then every ideal $\mathfrak{c}$ is proportional to one of the $\mathfrak{c}_i$'s, and then $j(\mathfrak{c}) = j(\mathfrak{c}_i)$. On the other hand, since any of the $\mathfrak{c}_i$ are not proportional to each other so $j(\mathfrak{c}_1), j(\mathfrak{c}_2), .., j(\mathfrak{c}_h)$ are all distinct. The first part of the argument shows that $j(\mathfrak{c}) \to \mathcal{O}_{\tilde{K}}$ for any nonzero ideal $\mathfrak{c}$ of $\mathcal{O}_K$, so

$$\Delta = \prod_{i<j} (j(\mathfrak{c}_i) - j(\mathfrak{c}_j))$$

is a non-zero element of $\mathcal{O}_{\tilde{K}}$. Consider a factorization into a product of prime ideal,

$$\Delta \mathcal{O}_{\tilde{K}} = \tilde{\mathfrak{P}_1}^{\alpha_1} \tilde{\mathfrak{P}_2}^{\alpha_2} ... \tilde{\mathfrak{P}}_r^{\alpha_r},$$

and let $\mathfrak{p}_i \in \mathcal{P}_K$ be the prime lying below $\tilde{\mathfrak{P}}_i$. Set $T := \{\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_r\}$. We will prove that

$$\mathrm{Spl}_{\mathbb{Q}}(L|K) \setminus T \subset P_K \cap \mathcal{P}_{K,\mathbb{Q}}. \tag{3.4}$$

Suppose that $\mathfrak{p} \in \mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K}) \setminus \mathrm{T}$. Let p be the corresponding rational prime, and let $\tilde{\mathfrak{P}}$ be a prime ideal of $\mathcal{O}_{\tilde{K}}$ lying above $\mathfrak{p}$. Then by Lemma 3.2.2, one of the following congruence holds:

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}\mathfrak{p}) \pmod{\mathfrak{P}} \quad \textit{or} \quad j(\mathfrak{a}) \equiv j(\mathfrak{a}\mathfrak{p})^p \pmod{\mathfrak{P}}.$$

But since $\mathfrak{p} \in \mathrm{Spl}_{\mathbb{Q}}(L|K)$, for $\mathfrak{P} = \mathcal{O}_L \cap \tilde{\mathfrak{P}}$, we have $O_L/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$, in particular,

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}.$$

Above two give us

$$j(\mathfrak{a}\mathfrak{p}) \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}.$$

If $j(\mathfrak{a}\mathfrak{p}) \neq j(\mathfrak{a})$, then $j(\mathfrak{a}\mathfrak{p}) - j(\mathfrak{a})$ would divide Δ, which would imply that $\tilde{\mathfrak{P}}$ would coincide with one of the $\tilde{\mathfrak{P}}_i$. This is not the case by our construction. Thus, we get that

$$j(\mathfrak{a}\mathfrak{p}) = j(\mathfrak{a}),$$

which means that the ideals $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{p}$ are proportional, and therefore $\mathfrak{p} \in P_K$. Together (3.2) and (3.4) prove that $\mathrm{Spl}_{\mathbb{Q}}(\mathrm{L|K}) \doteq \mathrm{P_K} \cap \mathcal{P}_{\mathrm{K},\mathbb{Q}}$. Theorem directly follows from Theorem 3.1.7. □

Example 3.2.3. *In his paper* ***Traces of Singular Moduli, Don Zagier*** *gave a way to explicitly calculate Hilbert class polynomials which generates Hilbert class field. Using it, we find the following.*

- $d = 3$, *we know that* $h_3 = 1$ *so* $\tilde{K} = \mathbb{Q}(\sqrt{-3})$ *and it can seen easily by the well known fact that* $j(\frac{1+\sqrt{-3}}{2}) = 0$.
- $d = 15$, *in this case the class number* $h_{15} = 2$ *and the Hilbert class field of* $\mathbb{Q}(\sqrt{-15})$ *is the splitting field of* $H_{15}(X) = X^2 + 191025X - 121287375$ *over* $\mathbb{Q}(\sqrt{-15})$ *which has roots*

$$\left\{\left\{X \to \frac{135}{2}\left(-637\sqrt{5} - 1415\right)\right\}, \left\{X \to \frac{135}{2}\left(637\sqrt{5} - 1415\right)\right\}\right\}$$

  Hence $\widetilde{\mathbb{Q}(\sqrt{-15})} = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$.

- $d = 23$, *In this case the class number* $h_{23} = 3$ *and* $\widetilde{\mathbb{Q}(\sqrt{-23})} = \mathbb{Q}(\sqrt{-23})(\alpha)$ *where alpha is a root of*

$$H_{23}(X) = x^3 + 3491750x^2 - 5151296875x + 12771880859375$$

Bibliography

[1] Cox David A., *Primes of the Form $x^2 + ny^2$, second edition*, Pure and Applied Mathematics, John Wiley & Sons, Ltd, 2013.

[2] Rapinchuk I. *Elliptic Curves with Complex Multiplication and Kronecker's Jugendtraum*

[3] Zagier D.,*Traces of singular moduli*, 2002